БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
НАУЧНО-ИССЛЕДОВАТЕЛЬСКИЙ ИНСТИТУТ
ПРИКЛАДНЫХ ПРОБЛЕМ МАТЕМАТИКИ И ИНФОРМАТИКИ

ТЕОРЕТИЧЕСКАЯ И ПРИКЛАДНАЯ КРИПТОГРАФИЯ

Материалы
II Международной научной конференции

Минск, 19–20 октября 2023 г.

Минск
БГУ
2023

УДК 512.624.95(06)+004.056.55
ББК 22.14я431+32.973-018.2я431
Т33

Т33 **Теоретическая** и прикладная криптография : материалы II Междунар. науч. конф., Минск, 19–20 окт. 2023 г. / Белорус. гос. ун-т ; редкол.: Ю. С. Харин (гл. ред.) [и др.]. – Минск : БГУ, 2023. – 295 с.
ISBN 978-985-881-501-1.

Рассматриваются актуальные проблемы криптографии: математические основы криптографии, булевые функции в криптографии, вероятностно-статистические методы криптологии, криптографические генераторы случайных и псевдослучайных чисел, оценка надежности криптографических алгоритмов и протоколов, постквантовая криптография, криптография на основе sponge-функций, разделение секрета, нейронные сети в криптологии, доказательства с нулевым разглашением, блокчейн-системы, эффективная реализация криптографических примитивов, массовая аутентификация и другие направления криптологии.

УДК 512.624.95(06)+004.056.55
ББК 22.14я431+32.973-018.2я431

ISBN 978-985-881-501-1

Содержание

ПРЕДИСЛОВИЕ

Международная научная конференция “Теоретическая и прикладная криптография”, организованная Белорусским государственным университетом и Научно-исследовательским институтом прикладных проблем математики и информатики (НИИ ППМИ БГУ) 19–20 октября 2023 года, посвящена актуальным проблемам современной криптографии.

Материалы конференции содержат 26 статей. Темы статей отвечают следующим направлениям: математические основы криптографии; булевы функции в криптографии; вероятностно-статистические методы криптологии; криптографические генераторы случайных и псевдослучайных чисел; оценка надежности криптографических алгоритмов и протоколов; постквантовая криптография; криптография на основе sponge-функций; разделение секрета; нейронные сети в криптологии; доказательства с нулевым разглашением; блокчейн-системы; эффективная реализация криптографических примитивов; массовая аутентификация.

Организационный комитет конференции выражает благодарность Белорусскому государственному университету и Научно-исследовательскому институту прикладных проблем математики и информатики за финансовую и организационную поддержку.

Ю.С. Харин

КОМБИНАТОРНЫЙ ПОДХОД К ИССЛЕДОВАНИЮ APN-ПОДСТАНОВОК

А.Р. Белов[1]
[1]*Ярославский государственный университет им. П.Г. Демидова*
Ярославль, РОССИЯ
e-mail: ashmedey@gmail.com

В работе исследуется комбинаторный подход к исследованию биективных APN–функций. Биективная APN–функция рассматривается как элемент симметрической группы, а свойство подстановки быть дифференциально 2–равномерной характеризуется расстоянием Хэмминга между регулярным представлением группы сдвигов поля $\mathbb{F}_{2^n}$ и сопряженной ей группой. В контексте этой характеризации, APN–подстановки – подстановки, которые сопряжением преобразуют группу сдвигов в максимально удаленную от нее изоморфную группу. Исследуется подход к построению APN–подстановки с использованием данной характеризации: задача построения APN–подстановки сводится к поиску подходящей подгруппы симметрической группы и решению уравнения сопряжения.

Ключевые слова: дискретные функции; APN–подстановка; дифференциальная равномерность; симметрическая группа; наибольшее независимое множество

1 Введение

Преобразования, которые используются в симметричных криптосистемах описываются дискретными функциями вида

$$f : A \to B,$$

где A, B – конечные абелевы группы. Обычно это аддитивные группы конечных полей.

Анализ известных методов криптоанализа показывает, что для обеспечения устойчивости к этим методам криптоанализа, соответствующие дискретные функции должны обладать определенными свойствами. Такие свойства описываются различными криптографическими характеристиками. Одна из таких характеристик – *дифференциальная равномерность* [3].

Определение 1. Отображение $f : GF(p^n) \to GF(p^n)$ называется дифференциально δ–равномерным, если для любого $a \in GF(p^n)^*$ и для любого $b \in GF(p^n)$ уравнение

$$f(x + a) - f(x) = b$$

имеет не более δ решений.

Дифференциально 1–равномерные отображения называются *совершенно нелинейными* отображениями или *PN–отображениями*. В случае четной характеристики минимальное возможное значение дифференциальной равномерности равно 2. Дифференциально 2–равномерные отображения называют *почти совершенно нелинейными* или *APN–отображениями*.

Проблема существования биективных APN–отображений (*APN–подстановки*) в случае $p = 2$ и четного n – одна из известных открытых проблем. Для $n = 4$ не существует APN–подстановок [2]. Первый пример APN–подстановки для четного n был построен в работе [1] для $n = 6$. Для $n \geq 8$ вопрос остается открытым.

2 Комбинаторный подход к исследованию APN–подстановок

Введем необходимые определения. Обозначим через $\langle S(\Omega), \cdot, e\rangle$ симметрическую группу на множестве $\Omega = GF(2^n)$ с нейтральным элементом e и операцией *произведения подстановок* [4], определенной для подстановок $f, g \in S(\Omega)$ по правилу $[f \cdot g](x) = g(f(x))$. Множество неподвижных точек подстановки $\pi \in S(\Omega)$ обозначим как $fix(\pi) = \{x \in \Omega \mid \pi(x) = x\}$.

Определение 2. Расстоянием Хэмминга между подстановками $f, g \in S(\Omega)$ называется значение

$$d(f, g) = |\{x \in \Omega \mid f(x) \neq g(x)\}|.$$

Определение 3. Расстоянием Хэмминга между подгруппами $G, G' \leq S(\Omega)$ назовем значение

$$d(G, G') = \min_{\substack{g \in G \setminus \{e\} \\ g' \in G' \setminus \{e\}}} d(g, g').$$

Рассмотрим подгруппу сдвигов симметрической группы

$$T = \{\tau_\alpha \mid \alpha \in \Omega\} \leq S(\Omega),$$

где

$$\begin{aligned} \tau_\alpha \colon GF(2^n) &\to GF(2^n) \\ x &\mapsto x + \alpha. \end{aligned}$$

Отметим простейшие свойства группы T:

– Любая подстановка $\tau \in T$ есть инволюция, т.е. $\tau \cdot \tau = e$;

– Любая $\tau \in T \setminus \{e\}$ не имеет неподвижных точек, т.е. $fix(\tau) = \emptyset$;

– Разложение $\tau \in T \setminus \{e\}$ в произведение независимых циклов имеет вид $\tau = (\alpha_1, \alpha_2)(\alpha_3, \alpha_4)...(\alpha_{|\Omega|-1}, \alpha_{|\Omega|})$, где α_i – различные элементы Ω;

– $T = \langle \tau_{e_1}, ..., \tau_{e_n} \rangle \cong \langle \tau_{e_1} \rangle \times ... \times \langle \tau_{e_n} \rangle$, где $\{e_i\}$ – базис $GF(2^n)$ над $GF(2)$;

– Для любых $x, y \in GF(2^n)$ существует единственный сдвиг $\tau \in T$ такой, что $\tau(x) = y$ (T – регулярная группа).

Дифференциальную равномерность подстановки можно выразить в терминах расстояния Хэмминга между двумя подгруппами симметрической группы:

Теорема 1. *Пусть $f \in S(\Omega)$ и $T' = f^{-1} \cdot T \cdot f$ сопряженная подгруппа. Тогда f это APN–подстановка тогда и только тогда, когда $d(T', T) = |\Omega| - 2$.*

Используя эту характеризацию, можно предложить следующий подход к построению APN–подстановок:

– Найти группу $T' \leq S(\Omega)$ такую, что выполнены условия:

$$1)\ T' \cong T,$$

$$2)\ d(T, T') = |\Omega| - 2;$$

– Решить уравнение $T' = f^{-1} \cdot T \cdot f$.

Основная сложность при таком подходе заключается в поиске подходящей группы T'. Вторая же задача решается

легко. Поскольку T и T' изоморфные регулярные группы, то решение уравнения $T' = f^{-1} \cdot T \cdot f$ основано на

Теорема 2 ([5]). *Две регулярные изоморфные подгруппы симметрической группы сопряжены в ней.*

Из конструктивного доказательства этой теоремы извлекается алгоритм решения этого уравнения:

1. Построить изоморфизм $\phi : T \to T'$;
2. Зафиксировать $o \in \Omega$. Тогда сопрягающей подстановкой будет

$$f = \begin{pmatrix} x_1 & x_2 & \dots & x_{|\Omega|} \\ [\phi(\tau_{x_1})](o) & [\phi(\tau_{x_2})](o) & \dots & [\phi(\tau_{x_{|\Omega|}})](o) \end{pmatrix}.$$

Для небольших показателей n можно предложить следующую стратегию поиска подходящей группы T':

– Найти инволюцию $\tau' \in S(\Omega)$ без неподвижных точек с условием

$$d(T, \langle \tau' \rangle) = |\Omega| - 2;$$

– Достроить $\langle \tau' \rangle \in S(\Omega)$ до группы $\langle \tau', \tau'_2, \tau'_3, ..., \tau'_n \rangle$, изоморфной T и находящейся на расстоянии $|\Omega| - 2$ от нее.

Рассмотрим первую задачу в контексте теории графов. Определим граф $G = (V, E)$ следующим образом:

V – множество всевозможных транспозиций из $S(\Omega)$,

$$(v_1, v_2) \in E \iff \begin{array}{l} v_1 \text{ и } v_2 \text{ зависимы или } v_1 \text{ и } v_2 \\ \text{входят в разложение некоторого} \\ \text{сдвига } \tau \in T. \end{array}$$

Граф G имеет $v = (2^n - 1) \cdot 2^{n-1}$ вершин и является d–регулярным, где $d = (2^{n-1} - 1) + 2 \cdot (2^n - 2)$. Число ребер равно $e = \frac{vd}{2} = 5 \cdot 2^{n-3} \cdot (2^n - 2) \cdot (2^n - 1)$.

Теорема 3. *Пусть* $\tau' = \omega_1 ... \omega_{2^{n-1}} \in S(\Omega)$ – *инволюция без неподвижных точек, а* ω_i – *независимые транспозиции. Тогда условие* $d(\langle \tau' \rangle, T) = |\Omega| - 2$ *выполнено тогда и только тогда, когда множество вершин* $\{\omega_1, ..., \omega_{2^{n-1}}\}$ *образует наибольшее независимое множество в графе* G.

Пусть инволюция τ' уже построена. Достроим ее до группы $\langle \tau', \tau'_2, ..., \tau'_n \rangle \cong T$. Образующие этой группы следует искать среди инволюций без неподвижных точек g, для которых выполнены 2 условия:

– g коммутирует с τ', т.е. $g\tau' g^{-1} = \tau'$;

– разложение g в произведение независимых циклов образует наибольшее независимое множество в графе G.

Обозначим множество g для которых выполнено первое условие через $C(\tau')$. Обозначим множество инволюций из $C(\tau')$ удовлетворяющих второму условию через $MC(\tau')$. Для построения группы T' достаточно выбрать $n-1$ образующих $\tau'_2, ..., \tau'_n \in MC(\tau')$. Такой подход построения группы T' возможен (за обозримое время) для небольших значений $n \leq 5$.

Приведем результаты вычислительных экспериментов. В случае $n = 3$ граф G имеет 56 наибольших независимых множеств. Каждому независимому множеству соответствует инволюция τ', для которой $|C(\tau')| = 12$, $|MC(\tau')| = 6$. По каждому множеству $MC(\tau')$ восстанавливается группа

T'. Таким образом были получены все 8 групп, характеризующих APN–подстановки на $GF(2^3)$:

$$T_1 = \langle (01)(25)(37)(46), (02)(15)(36)(47), (06)(14)(23)(57) \rangle;$$

$$T_2 = \langle (01)(27)(35)(46), (06)(14)(25)(37), (07)(12)(36)(45) \rangle;$$

$$T_3 = \langle (01)(26)(34)(57), (02)(16)(35)(47), (07)(15)(24)(36) \rangle;$$

$$T_4 = \langle (01)(24)(36)(57), (06)(13)(25)(47), (07)(15)(23)(46) \rangle;$$

$$T_5 = \langle (01)(26)(35)(47), (02)(16)(37)(45), (07)(14)(23)(56) \rangle;$$

$$T_6 = \langle (01)(25)(36)(47), (03)(16)(24)(57), (07)(14)(26)(35) \rangle;$$

$$T_7 = \langle (01)(24)(37)(56), (03)(17)(25)(46), (06)(15)(27)(34) \rangle;$$

$$T_8 = \langle (01)(27)(34)(56), (06)(15)(23)(47), (07)(12)(35)(46) \rangle.$$

Среди $8! = 40320$ подстановок имеется 10752 APN–подстановок, которые распадаются на 8 классов эквивалентности: каждая APN–подстановка является решением одного из 8 уравнения сопряжения $T_i = x^{-1} \cdot T \cdot x$.

Для $n = 4$ граф G имеет 167040 наибольших независимых множеств. При этом для каждого независимого множества и соответствующей инволюции τ' выполняется $|C(\tau')| = 1680$, $|MC(\tau')| = 0$. Получилось альтернативное доказательство (к сожалению, тоже вычислительное, а не теоретическое) известного результата о несуществовании APN–подстановок для $n = 4$.

Библиографические ссылки

1. An APN permutations in dimension six / K. Browning [et al.] // Amer. Math. Soc. 2010. No. 518. P. 33–42.

2. *Hou X.D.* Affinity of permutations of F_{2^n} // Disc. Appl. Math. 2006. Vol. 154. P. 313–325.

3. *Nyberg K., Knudsen L.R.* Provable security against differential cryptanalysis // LNCS. 1992. Vol. 740. P. 566–574.

4. *Глухов М.М., Елизаров В.П., Нечаев А.А.* Алгебра: Учебник. Санкт-Петербург: Лань, 2015.

5. *Супруненко Д.А.* Группы подстановок. Минск: Наука и техника, 1996.

ОБ АСИМПТОТИЧЕСКИХ СВОЙСТВАХ СЕМЕЙСТВА χ^2-ТЕСТОВ ЧИСТОЙ СЛУЧАЙНОСТИ ДВОИЧНОЙ ПОСЛЕДОВАТЕЛЬНОСТИ

В.А. Волошко[1]

[1]*НИИ прикладных проблем математики и информатики*

[1]*Белорусский государственный университет*

Минск, БЕЛАРУСЬ

e-mail: valoshka@bsu.by

Установлено взаимно однозначное соответствие между двумя семействами: семейством χ^2-тестов чистой случайности двоичной последовательности на основе частотных статистик пересекающихся s-грамм – с одной стороны, и семейством конечномерных подпространств бесконечномерного касательного пространства равномерного распределения в многообразии Марковских распределений – с другой стороны. На основе установленного взаимно однозначного соответствия в условиях контигуальной асимптотики сближения Марковской альтернативы H_1 с нулевой гипотезой H_0 о чистой случайности наблюдаемой двоичной последовательности получены следующие результаты: выражение для асимптотической мощности χ^2-тестов из исследуемого семейства; достаточное условие асимптотической неразличимости гипотез H_0 и H_1 заданным χ^2-тестом; достаточное условие асимптотической независимости статистик двух χ^2-тестов; алгоритм вычисления статистики χ^2-теста по заданному набору информативных признаков.

Ключевые слова: чистая случайность; двоичная последовательность; статистический тест; хи-квадрат; цепь Маркова; информационная геометрия; асимптотическое распределение

1 Математическая модель наблюдений

Введем обозначения: $\mathbf{V} = \{0,1\}$; $\mathbb{N} = \{1,2,\dots\}$; $\mathbb{N}_0 = \{0,1,\dots\}$; $\mathbf{x}_1^n = (\mathbf{x}_1,\dots,\mathbf{x}_n) \in \mathbf{V}^n$ – наблюдаемая двоичная последовательность длины $n \in \mathbb{N}$, подлежащая статистическому тестированию;

$$\mathbf{x}_a^b = (\mathbf{x}_a, \mathbf{x}_{a+1}, \dots, \mathbf{x}_b), \quad \mathbf{x}_b^a = (\mathbf{x}_b, \mathbf{x}_{b-1}, \dots, \mathbf{x}_a), \quad a \le b;$$

– двоичные подвекторы в прямом и обратном порядке; $\mathbf{x} ::= \mathbf{x}_1^\infty = (\mathbf{x}_i)_{i=1}^\infty$ – бесконечная двоичная последовательность; $\|q\| = s$, $|q| = \sum_{i=1}^s q_i$ – соответственно длина и вес Хэмминга двоичного вектора $q = (q_i)_{i=1}^s \in \mathbf{V}^s$, $s \in \mathbb{N}_0$; $\dagger \in \mathbf{V}^0$ – абстрактный элемент, двоичный вектор нулевой длины ($\|\dagger\| = |\dagger| = 0$); $\mathsf{P}\{\cdot\}$, $\mathbb{1}\{\cdot\}$, $\mathsf{E}\{\cdot\}$, $\mathcal{L}\{\cdot\}$, $\mathcal{O}(\cdot)$, $o(\cdot)$, – соответственно вероятность и индикаторная функция события, математическое ожидание и закон распределения вероятностей случайной величины, символы Ландау “О большое” и “о маленькое”; $\mathbf{I}_L$ – единичная матрица порядка L; $\mathbf{0}_L = (0,\dots,0) \in \mathbb{R}^L$ – нулевой L-вектор; $F_{d,\lambda}(\cdot)$ – функция нецентрального распределения хи-квадрат с $d \in \mathbb{N}$ степенями свободы и параметром нецентральности $\lambda \in \mathbb{R}_+$; $F_d(\cdot) = F_{d,0}(\cdot)$ – функция центрального распределения хи-квадрат с d степенями свободы; $F^{-1}(\cdot)$ – квантильная функция для функции распределения $F(\cdot)$; z^{t} – транспонирование матрицы z; вектор $z \in \mathbb{R}^d$ в матричных выражениях считается вектор-столбцом: $z \in \mathbb{R}^{d\times 1}$;

$$H_0: \ \mathbf{x} - \text{РРСП} \ \Leftrightarrow \ \mathsf{P}\{\mathbf{x}_1^n = q\} = 2^{-n}, \ \forall n \in \mathbb{N}, \ q \in \mathbf{V}^n,$$

– нулевая гипотеза равномерного распределения вероятностей (“чистой случайности”) последовательности $\mathbf{x}$ (РР-

СП – равномерно распределенная случайная последовательность);

$$H_1 : \ \mathcal{L}\{\mathbf{x}\} \in \mathrm{MC}(s), \ s \in \mathbb{N}_0, \tag{1}$$

– сложная Марковская альтернатива некоторого порядка s, состоящая в том, что $\mathbf{x}$ – стационарная цепь Маркова порядка s ($\mathrm{MC}(s)$ – семейство Марковских распределений вероятностей порядка s). Элементы семейства $\mathrm{MC}(s)$ следующим образом параметризованы функцией уклонения $\delta(q) : \mathbf{V}^s \to (-1, 1)$, $q = (q_i)_{i=1}^s \in \mathbf{V}^s$, Марковских переходных вероятностей от значения $1/2$:

$$\mathsf{P}\{\mathbf{x}_i = 0 | \mathbf{x}_j : j < i\} = \frac{1 + \delta(\mathbf{x}_{i-1}^{i-s})}{2}. \tag{2}$$

Отметим, что s предыдущих наблюдений

$$\mathbf{x}_{i-1}^{i-s} = (\mathbf{x}_{i-1}, \ldots, \mathbf{x}_{i-s}) \in \mathbf{V}^s$$

в (2) подаются в функцию уклонения $\delta(\cdot)$ в обратном порядке (от ближних к дальним по отношению к текущему наблюдению $\mathbf{x}_i$). Это сделано для удобства дальнейших обозначений. Нулевому порядку $s = 0$ отвечает случайная последовательность Бернулли независимых одинаково распределенных наблюдений с вероятностью нулевого наблюдения согласно (2):

$$\mathsf{P}\{\mathbf{x}_i = 0\} = \frac{1 + \delta(\dagger)}{2}.$$

Нулевому значению функции уклонения $\delta(q) \equiv 0$, $\forall q \in \mathbf{V}^s$, соответствует РРСП $\mathbf{x}$ (случай совпадения и неразличимости нулевой гипотезы и альтернативы).

Будем также предполагать, что имеет место так называемая контигуальная асимптотика [1] сближения альтернативы H_1 с нулевой гипотезой H_0 при увеличении длины $(n \to \infty)$ наблюдаемой двоичной последовательности:

$$\delta(q) = n^{-1/2} \cdot \boldsymbol{\delta}(q),\ \forall q \in \mathbf{V}^s,\ n \geq n_*, \tag{3}$$

где n_* – некоторое достаточно большое значение, а функция $\boldsymbol{\delta}(\cdot)$ не зависит от n и определяет скорость и направление сближения альтернативы H_1 с нулевой гипотезой H_0. Поэтому далее функцию $\boldsymbol{\delta}(\cdot)$ будем для краткости называть альтернативой. При асимптотике (3) выполняется следующее свойство [2]:

$$\mathsf{KL}_n(H_0||H_1) \underset{n\to\infty}{=} \mathcal{O}(1),$$

где $\mathsf{KL}_n(H_0||H_1)$ – направленная дивергенция Кульбака-Лейблера между распределениями наблюдаемой последовательности длины n в случае истинной нулевой гипотезы и в случае истинной альтернативы:

$$\mathsf{KL}_n(H_0||H_1) = \sum_{q\in\mathbf{V}^n} \pi_q^{(0)} \ln \frac{\pi_q^{(0)}}{\pi_q^{(1)}},$$

$$\pi_q^{(i)} = \mathsf{P}\left\{\mathbf{x}_1^n = q | H_i\right\},\ q \in \mathbf{V}^n,\ i = 0, 1.$$

Другими словами, информационное расхождение нулевой гипотезы и альтернативы остается ограниченным с ростом n.

2 Семейство χ^2-тестов чистой случайности двоичной последовательности

Пусть имеется некоторый вектор из $d \in \mathbb{N}$ информативных признаков двоичных r-грамм:

$$f(q) = (f_i(q))_{i \in I} \in \mathbb{R}^d, \quad q = (q_j)_{j=1}^r \in \mathbf{V}^r,$$

где I – множество индексов информативных признаков, $|I| = d$. Введем оператор усреднения вектора информативных признаков $f(\cdot)$ по пересекающимся r-граммам наблюдаемой последовательности. Данный оператор усреднения встречается в двух формах. Более распространенная форма имеет вид:

$$\tilde{\mathsf{E}}_n \{f\} = \frac{1}{n-s+1} \sum_{i=1}^{n-r+1} f(\mathbf{x}_i^{i+r-1}). \tag{4}$$

Также встречается следующая форма [3] на основе зацикленной последовательности $\mathbf{x}_1^n$:

$$\hat{\mathsf{E}}_n \{f\} = \frac{1}{n} \sum_{i=1}^{n} f(\mathbf{y}_i^{i+r-1}), \tag{5}$$

где $\mathbf{y} = (\mathbf{y}_i)_{i \in \mathbb{N}}$ – бесконечная n-периодическая последовательность, такая что $\mathbf{y}_1^n = \mathbf{x}_1^n$. На уровне интересующего нас порядка малости $\mathcal{O}\left(n^{-1/2}\right)$ формы (4) и (5) асимптотически эквивалентны, и все приведенные ниже результаты верны одновременно для них обеих. Мы будем использовать форму (5), поскольку она обладает некоторыми удобными симметриями. Например, в [3] форма (5) используется в тесте аппроксимации энтропии и гарантирует положительность статистики теста. Также отметим, что если $r_1 < r_2$,

то информативный признак $f_i(q)$ от r_1-граммы $q \in \mathbf{V}^{r_1}$ может быть расширен до эквивалентного признака $\tilde{f}_i(\tilde{q})$ от r_2-граммы $\tilde{q} \in \mathbf{V}^{r_2}$, равного значению признака $f_i(\cdot)$, взятого от r_1-префикса r_2-вектора $\tilde{q}$:

$$\tilde{f}_i(\tilde{q}) ::= f_i(\tilde{q}_1^{r_1}), \quad \tilde{q} \in \mathbf{V}^{r_2}. \tag{6}$$

Очевидно, набор из n r_1-подвекторов зацикленной последовательности $\mathbf{x}_1^n$ есть в точности набор из r_1-префиксов r_2-подвекторов этой последовательности, откуда:

$$\hat{\mathsf{E}}_n \{f_i\} \equiv \hat{\mathsf{E}}_n \left\{ \tilde{f}_i \right\}, \quad \forall \mathbf{x}_1^n \in \mathbf{V}^n, \; n \in \mathbb{N}.$$

Поэтому мы можем объединять в вектора $(f_i(q))_{i \in I}$ любые информативные признаки от двоичных векторов любых различных длин r_i, $i \in I$, и считать без потери общности, что все признаки в векторе берутся от двоичных векторов одинаковой длины $r = \max_{i \in I}\{r_i\}$.

Центрированный оператор усреднения на основе (5) имеет вид:

$$\langle f \rangle_n = \hat{\mathsf{E}}_n \{f\} - \mathsf{E}\{f|H_0\}, \quad \mathsf{E}\{f|H_0\} = 2^{-r} \sum_{q \in \mathbf{V}^r} f(q), \tag{7}$$

где $\mathsf{E}\{f|H_0\}$ – математическое ожидание вектора информативных признаков при истинной нулевой гипотезе.

Лемма 1. *В случае истинной альтернативы H_1 и контигуальной асимптотики (3) случайный d-вектор (7) имеет асимптотическое нормальное распределение:*

$$n^{1/2} \cdot \langle f \rangle_n \xrightarrow[n \to \infty]{D} \mathcal{N}_d(\mu^{(f,\boldsymbol{\delta})}, \Sigma^{(f)}), \tag{8}$$

где вектор $\mu^{(f,\boldsymbol{\delta})} \in \mathbb{R}^d$ билинейно зависит от функции информативных признаков $f(\cdot) : \mathbf{V}^r \to \mathbb{R}^d$ и от альтернативы $\boldsymbol{\delta}(\cdot) : \mathbf{V}^s \to \mathbb{R}$, а ковариационная матрица $\Sigma^{(f)} \in \mathbb{R}^{d \times d}$

квадратично зависит от функции $f(\cdot)$ *и не зависит от альтернативы* $\boldsymbol{\delta}(\cdot)$.

Вектор (набор) информативных признаков $(f_i(\cdot))_{i\in I}$ будем называть невырожденным, если невырождена матрица ковариации, определяемая (8): $|\Sigma^{(f)}| \neq 0$.

Следствие 1. *В случае истинной альтернативы* H_1 *и контигуальной асимптотики* (3) *для невырожденного вектора информативных признаков* $(f_i(\cdot))_{i\in I}$ *статистика:*

$$S_n(f) ::= n \cdot \langle f \rangle_n^{\mathrm{t}} \left(\Sigma^{(f)}\right)^{-1} \langle f \rangle_n \tag{9}$$

при $n \to \infty$ *имеет асимптотическое нецентральное распределение хи-квадрат с* d *степенями свободы и параметром нецентральности* $\lambda = \lambda^{(f)}(\boldsymbol{\delta}) \geq 0$, *квадратично зависящим от альтернативы* $\boldsymbol{\delta}(\cdot)$.

Тест на основе статистики (9) с уровнем значимости $\alpha \in (0,1)$ принимает гипотезу H_0 при условии:

$$S_n(f) \leq F_d^{-1}(1-\alpha), \tag{10}$$

и при контигуальной асимптотике (3) имеет асимптотическую мощность:

$$\omega = 1 - F_{d,\lambda}\left(F_d^{-1}(1-\alpha)\right). \tag{11}$$

Величина (11) позволяет сравнивать мощности различных тестов для заданной альтернативы $\boldsymbol{\delta}$, а ее вычисление сводится к нахождению квадратичной формы $\lambda^{(f)}(\boldsymbol{\delta})$ [4].

Невырожденное линейное преобразование вектора информативных признаков: $\tilde{f} = A \cdot f \in \mathbb{R}^d$, $A \in \mathbb{R}^{d\times d}$, $|A| \neq 0$, сохраняет статистику (9):

$$S_n(\tilde{f}) \equiv S_n(f), \quad \forall \mathbf{x}_1^n \in \mathbf{V}^n,\ n \in \mathbb{N}.$$

Кроме того, сами информативные признаки не единственным образом задают центрированное усреднение (7). А именно, в линейном пространстве этих признаков $U = \{f : \mathbf{V}^r \to \mathbb{R}\}$ размерности $\dim(U) = 2^r$ существует такое подпространство $V \subset U$ размерности $\dim(V) = 2^{r-1}$, что признаки $f_1, f_2 : \mathbf{V}^r \to \mathbb{R}$ эквивалентны:

$$\langle f_1 \rangle_n \equiv \langle f_2 \rangle_n , \quad \forall \mathbf{x}_1^n \in \mathbf{V}^n,\ n \in \mathbb{N}, \tag{12}$$

если $f_1 - f_2 \in V$. Например, при $r = 2$ эквивалентны признаки $f_1(q) = \mathbb{1}\{q = 01\}$ и $f_2(q) = \mathbb{1}\{q = 10\}$. Поэтому векторы информативных признаков избыточно кодируют статистики (9) и не позволяют составить представление о структуре их многообразия. Далее будет показано, как статистики (9) взаимно однозначно кодируются конечномерными подпространствами бесконечномерного касательного пространства равномерного распределения в многообразии Марковских распределений. Из этого взаимно однозначного соответствия будут также выведены некоторые свойства статистик (9) и связанные с ними вычислительные алгоритмы.

3 Касательное пространство равномерного распределения в многообразии Марковских распределений

Введем вспомогательные обозначения: $\mathbf{V}^* = \bigcup_{r=1}^{\infty} \mathbf{V}^r$ – множество двоичных векторов конечной положительной длины; множество $\mathbf{V}_0^* = \mathbf{V}^0 \cup \mathbf{V}^*$ содержит также двоичный вектор нулевой длины $\dagger \in \mathbf{V}^0$;

$$\boldsymbol{\delta}(q_1, \ldots, q_r)$$

$$::= \begin{cases} \boldsymbol{\delta}(q_1,\ldots,q_s), & r \geq s, \\ 2^{r-s}\sum_{q_{r+1},\ldots,q_s\in\mathbf{V}} \boldsymbol{\delta}(q_1,\ldots,q_s), & 0 \leq r < s, \end{cases} \quad (q_i)_{i=1}^r \in \mathbf{V}_0^*, \tag{13}$$

– расширение функции $\boldsymbol{\delta}(\cdot) : \mathbf{V}^s \to \mathbb{R}$ Марковской альтернативы порядка $s \in \mathbb{N}_0$ на множество определения $\mathbf{V}_0^*$;

$$\boldsymbol{\varepsilon}(q_1,\ldots,q_r) ::= \sum_{i=1}^{r}(-1)^{q_i}\boldsymbol{\delta}(q_{i-1},\ldots,q_1),\ (q_i)_{i=1}^r \in \mathbf{V}^*, \tag{14}$$

где $(q_{i-1},\ldots,q_1) = \dagger$ для $i = 1$. Отметим, что расширенная функция $\boldsymbol{\delta}(\cdot) : \mathbf{V}_0^* \to \mathbb{R}$ и функция $\boldsymbol{\varepsilon} : \mathbf{V}^* \to \mathbb{R}$ являются линейными отображениями исходной функции $\boldsymbol{\delta}(\cdot) : \mathbf{V}^s \to \mathbb{R}$. Поэтому мы можем корректно считать квадратичную форму $\lambda^{(f)}(\boldsymbol{\delta})$ из Следствия 1 формой от расширенной версии функции $\boldsymbol{\delta}$. Линейное отображение (14), переводящее расширенную функцию $\boldsymbol{\delta}(\cdot) : \mathbf{V}_0^* \to \mathbb{R}$ в функцию $\boldsymbol{\varepsilon} : \mathbf{V}^* \to \mathbb{R}$, обозначим $\boldsymbol{\Psi}$:

$$\boldsymbol{\varepsilon} = \boldsymbol{\Psi}(\boldsymbol{\delta}). \tag{15}$$

Обратное преобразование имеет вид:

$$\boldsymbol{\delta} = \boldsymbol{\Psi}^{-1}(\boldsymbol{\varepsilon}),$$
$$\boldsymbol{\delta}(q_1,\ldots,q_r) = \frac{\boldsymbol{\varepsilon}(q_r,\ldots,q_1,0) - \boldsymbol{\varepsilon}(q_r,\ldots,q_1,1)}{2}, \quad (q_i)_{i=1}^r \in \mathbf{V}_0^*. \tag{16}$$

Следующий результат описывает содержательный смысл введенных величин.

Лемма 2. *В случае истинной альтернативы H_1 и контигуальной асимптотики* (3) *при $n \to \infty$ для любых i,*

$q = (q_j)_{j=1}^r \in \mathbf{V}_0^*$, $\tilde{q} = (\tilde{q}_j)_{j=1}^r \in \mathbf{V}^*$ *имеют место следующие соотношения:*

$$\mathsf{P}\left\{\mathbf{x}_i = 0 | \mathbf{x}_{i-1}^{i-r} = q\right\} = \frac{1 + n^{-1/2}(\boldsymbol{\delta}(q) + o\,(1))}{2}, \tag{17}$$

$$\mathsf{P}\left\{\mathbf{x}_i^{i+r-1} = \tilde{q}\right\} = \frac{1 + n^{-1/2}(\boldsymbol{\varepsilon}(\tilde{q}) + o\,(1))}{2^r}. \tag{18}$$

В частности,

$$\mathsf{P}\left\{\mathbf{x}_i = 0\right\} = \frac{1 + n^{-1/2}(\boldsymbol{\delta}(\dagger) + o\,(1))}{2}.$$

Множество расширенных функций $\boldsymbol{\delta}$ для Марковских альтернатив порядка $s \in \mathbb{N}_0$ обозначим $\mathbb{T}(s)$ – это касательное пространство равномерного распределения вероятностей (нулевой гипотезы H_0) в многообразии $\mathrm{MC}(s)$ Марковских альтернатив порядка s. На касательном пространстве $\mathbb{T}(s)$ определено скалярное произведение – тензор Фишера-Римана [2]:

$$\left\langle \boldsymbol{\delta}, \boldsymbol{\delta}' \right\rangle_{\mathbb{T}(s)} ::= 2^{-s} \sum_{q \in \mathbf{V}^s} \boldsymbol{\delta}(q)\boldsymbol{\delta}'(q), \quad \boldsymbol{\delta}, \boldsymbol{\delta}' \in \mathbb{T}(s). \tag{19}$$

Для всех $s \in \mathbb{N}_0$ функции $\boldsymbol{\delta} \in \mathbb{T}(s)$ определены на одном и том же общем носителе $\mathbf{V}_0^*$, и касательные пространства $\mathbb{T}(s)$ вложены друг в друга:

$$\mathbb{T}(s) \subset \mathbb{T}(r), \quad \forall r, s \in \mathbb{N}_0,\ r > s,$$

а определение (19) согласовано с этой вложенностью, что следует из (13) (случай $r \geq s$):

$$\left\langle \boldsymbol{\delta}, \boldsymbol{\delta}' \right\rangle_{\mathbb{T}(s)} = \left\langle \boldsymbol{\delta}, \boldsymbol{\delta}' \right\rangle_{\mathbb{T}(r)}, \quad \forall \boldsymbol{\delta}, \boldsymbol{\delta}' \in \mathbb{T}(s),\ s < r.$$

Поэтому мы можем корректно определить касательное пространство нулевой гипотезы H_0 в многообразии

$$\mathrm{MC} = \bigcup_{s=0}^{\infty} \mathrm{MC}(s)$$

Марковских альтернатив всех конечных порядков, и тензор Фишера-Римана на нем:

$$\mathbb{T} ::= \bigcup_{s=0}^{\infty} \mathbb{T}(s), \tag{20}$$

$$\left\langle \boldsymbol{\delta}, \boldsymbol{\delta}' \right\rangle_{\mathbb{T}} ::= \left\langle \boldsymbol{\delta}, \boldsymbol{\delta}' \right\rangle_{\mathbb{T}(s_*)}, \quad \boldsymbol{\delta}, \boldsymbol{\delta}' \in \mathbb{T}, \tag{21}$$

где $s_* \in \mathbb{N}_0$ – такой порядок, для которого $\boldsymbol{\delta}, \boldsymbol{\delta}' \in \mathbb{T}(s_*)$ (такой s_* существует для любых $\boldsymbol{\delta}, \boldsymbol{\delta}' \in \mathbb{T}$ по построению пространства $\mathbb{T}$). Выражение $\left\langle \boldsymbol{\delta}, \boldsymbol{\delta}' \right\rangle_{\mathbb{T}(s)}$ в (19), распространенное на любую пару $\boldsymbol{\delta}, \boldsymbol{\delta}' \in \mathbb{T}$, представляет собой скалярное произведение ортогональных проекций функций $\boldsymbol{\delta}, \boldsymbol{\delta}'$ на подпространство $\mathbb{T}(s) \subset \mathbb{T}$:

$$\left\langle \boldsymbol{\delta}, \boldsymbol{\delta}' \right\rangle_{\mathbb{T}(s)} = 2^{-s} \sum_{q \in \mathbf{V}^s} \boldsymbol{\delta}(q) \boldsymbol{\delta}'(q)$$

$$= \left\langle \mathbf{Pr}_{\mathbb{T}(s)} \boldsymbol{\delta}, \mathbf{Pr}_{\mathbb{T}(s)} \boldsymbol{\delta}' \right\rangle_{\mathbb{T}}, \ \boldsymbol{\delta}, \boldsymbol{\delta}' \in \mathbb{T}, \tag{22}$$

где $s \in \mathbb{N}_0$, $\mathbf{Pr}_U$ – оператор ортогонального проецирования на подпространство U. Порядком элемента $\boldsymbol{\delta} \in \mathbb{T}$ назовем величину:

$$\mathbf{ord}(\boldsymbol{\delta}) ::= \min\{s \in \mathbb{N}_0 : \boldsymbol{\delta} \in \mathbb{T}(s)\}. \tag{23}$$

Порядком конечномерного линейного подпространства $\mathcal{T} \subset \mathbb{T}$ назовем максимальный порядок его элементов:

$$\mathbf{ord}(\mathcal{T}) ::= \max\{\mathbf{ord}(\boldsymbol{\delta}) : \boldsymbol{\delta} \in \mathcal{T}\}$$

$$= \max\{\mathbf{ord}(\boldsymbol{\delta}_i) : i = 1, \ldots, \dim(\mathcal{T})\}, \qquad (24)$$

где $\{\boldsymbol{\delta}_i \in \mathcal{T}\}$ – любой базис $\mathcal{T}$.

Распределение вероятностей случайного двоичного вектора $\mathbf{x}_1^s = (\mathbf{x}_1, \ldots, \mathbf{x}_s) \in \mathbf{V}^s$ длины $s \in \mathbb{N}$ называется инвариантным к сдвигам (shift invariant), если совпадают маргинальные распределения двух его $(s-1)$-подвекторов: $\mathcal{L}\left\{\mathbf{x}_1^{s-1}\right\} = \mathcal{L}\left\{\mathbf{x}_2^s\right\}$ (всегда верно при $s = 1$). Обозначим $\mathrm{SI}(s)$ – многообразие инвариантных к сдвигам распределений на $\mathbf{V}^s$. В $\mathrm{SI}(s)$ очевидно лежит равномерное распределение на $\mathbf{V}^s$ – его касательное пространство в $\mathrm{SI}(s)$ обозначим $\mathbf{T}(s)$. Согласно Лемме 2, ограничение $\boldsymbol{\varepsilon}|_{\mathbf{V}^s}$ функции $\boldsymbol{\varepsilon} : \mathbf{V}^* \to \mathbb{R}$ на $\mathbf{V}^s$ лежит в $\mathbf{T}(s)$ и представляет собой масштабированное асимптотическое "уклонение от равномерности" общего для всех i распределения вероятностей $\mathcal{L}\left\{\mathbf{x}_{i+1}^{i+s}\right\}$ s-подвекторов $\mathbf{x}_{i+1}^{i+s}$ наблюдаемой последовательности $\mathbf{x}_1^n$ в случае истинной альтернативы H_1 и при контигуальной асимптотике (3). Тензор Фишера-Римана на $\mathbf{T}(s)$ имеет такой же вид, как и на включающем $\mathbf{T}(s)$ более широком касательном пространстве расномерного распределения в многообразии всех возможных распределений на $\mathbf{V}^s$:

$$\langle \boldsymbol{\varepsilon}, \boldsymbol{\varepsilon}' \rangle_{\mathbf{T}(s)} = 2^{-s} \sum_{q \in \mathbf{V}^s} \boldsymbol{\varepsilon}(q)\boldsymbol{\varepsilon}'(q), \quad \boldsymbol{\varepsilon}, \boldsymbol{\varepsilon}' \in \boldsymbol{\Psi}(\mathbb{T}), \qquad (25)$$

где линейное отображение $\boldsymbol{\Psi}$ определено (15).

Лемма 3. *Для любого $s \in \mathbb{N}$ тензоры Фишера-Римана* (22) *и* (25) *связаны соотношением:*

$$\langle \boldsymbol{\varepsilon}, \boldsymbol{\varepsilon}' \rangle_{\mathbf{T}(s)} = \sum_{r=0}^{s-1} \left\langle \boldsymbol{\delta}, \boldsymbol{\delta}' \right\rangle_{\mathbb{T}(r)}, \qquad (26)$$

$$\boldsymbol{\varepsilon} = \boldsymbol{\Psi}(\boldsymbol{\delta}),\ \boldsymbol{\varepsilon}' = \boldsymbol{\Psi}(\boldsymbol{\delta}'),\ \boldsymbol{\delta}, \boldsymbol{\delta}' \in \mathbb{T}.$$

Лемма 3 означает, что локальная информационная геометрия стационарных цепей Маркова $\mathbf{x}_1^\infty$ порядка s в окрестности равномерного распределения в некотором смысле есть "соседняя разность" локальных информационных геометрий s-грамм $\mathbf{x}_1^s$ и $(s{+}1)$-грамм $\mathbf{x}_1^{s+1}$ в окрестности равномерных распределений на $\mathbf{V}^s$ и $\mathbf{V}^{s+1}$ соответственно (здесь существенно, что $(s{+}1)$-граммы инвариантны к сдвигам: $\mathcal{L}\left\{\mathbf{x}_1^{s+1}\right\} \in \mathrm{SI}(s+1)$).

4 Статистические оценки функций $\boldsymbol{\delta}(\cdot)$ и $\boldsymbol{\varepsilon}(\cdot)$

Зафиксируем некоторый порядок $s \in \mathbb{N}_0$, не связанный с порядком $\mathbf{ord}(\boldsymbol{\delta})$ Марковской альтернативы H_1, и построим по наблюдаемой последовательности $\mathbf{x}_1^n$ статистические оценки $\hat{\boldsymbol{\delta}}_n^{(s)}(\cdot) \in \mathbb{T}(s)$ и $\hat{\boldsymbol{\varepsilon}}_n^{(s)}(\cdot) = \boldsymbol{\Psi}(\hat{\boldsymbol{\delta}}_n^{(s)}(\cdot))$ функций $\boldsymbol{\delta}(\cdot)$ и $\boldsymbol{\varepsilon}(\cdot)$. Сначала по $(s+1)$-граммам зацикленной последовательности $\mathbf{x}_1^n$ построим ограничение $\hat{\boldsymbol{\varepsilon}}_n^{(s)}|_{\mathbf{V}^{s+1}} \in \mathbf{T}(s+1)$ функции $\hat{\boldsymbol{\varepsilon}}_n^{(s)}$ на множество $\mathbf{V}^{s+1}$. Затем по формулам (16) построим ограничение $\hat{\boldsymbol{\delta}}_n^{(s)}|_{\mathbf{V}^s}$ функции $\hat{\boldsymbol{\delta}}_n^{(s)}$ на множество $\mathbf{V}^s$, по формулам (13) достроим функцию $\hat{\boldsymbol{\delta}}_n^{(s)}$ на всех значениях из $\mathbf{V}_0^*$, и наконец по формулам (14) из функции $\hat{\boldsymbol{\delta}}_n^{(s)}$ достроим функцию $\hat{\boldsymbol{\varepsilon}}_n^{(s)}$ на всех значениях из $\mathbf{V}^*$. Для корректности описанных построений существенно, что функция $\hat{\boldsymbol{\varepsilon}}_n^{(s)}(q)$, $q \in \mathbf{V}^{s+1}$, которая строится на первом шаге, лежит в касательном пространстве $\mathbf{T}(s{+}1)$. Это условие обеспечивается использованием зацикленной последовательности $\mathbf{x}_1^n$.

Для $q, q' \in \mathbf{V}^{s+1}$ обозначим индикаторный информативный признак от двоичных векторов длины $s+1$ и вектор из 2^{s+1} таких признаков:

$$\mathbf{i}_q(q') ::= \mathbb{1}\{q = q'\}, \quad \mathbf{i}^{(s+1)}(q') ::= (\mathbf{i}_q(q'))_{q \in \mathbf{V}^{s+1}}. \tag{27}$$

Функция $\hat{\boldsymbol{\varepsilon}}_n^{(s)}(q)$, $q \in \mathbf{V}^{s+1}$, в описанных выше построениях вычисляется следующим образом на основе центрированного усреднения (7) индикаторных информативных признаков (27):

$$\hat{\boldsymbol{\varepsilon}}_n^{(s)}(q) = 2^{s+1} n^{1/2} \langle \mathbf{i}_q \rangle_n, \quad q \in \mathbf{V}^{s+1},$$
$$\hat{\boldsymbol{\varepsilon}}_n^{(s)}|_{\mathbf{V}^{s+1}} = 2^{s+1} n^{1/2} \left\langle \mathbf{i}^{(s+1)} \right\rangle_n.$$

Статистика $\hat{\boldsymbol{\varepsilon}}_n^{(s)}(q)$ равна масштабированному уклонению от 2^{-s-1} частоты встречаемости $(s+1)$-граммы $q \in \mathbf{V}^{s+1}$ в зацикленной последовательности $\mathbf{x}_1^n$. Построенные функции $\hat{\boldsymbol{\delta}}_n^{(s)} \in \mathbb{T}(s)$ для разных порядков $s \in \mathbb{N}_0$ обладают свойством:

$$\hat{\boldsymbol{\delta}}_n^{(s)} = \mathbf{Pr}_{\mathbb{T}(s)} \hat{\boldsymbol{\delta}}_n^{(r)}, \quad r > s, \tag{28}$$

то есть являются ортогональными проекциями друг друга на подпространства из системы

$$\mathbb{T}(0) \subset \mathbb{T}(1) \subset \mathbb{T}(2) \subset \ldots.$$

Рассмотрим теперь некоторый информативный признак $f(\cdot) : \mathbf{V}^{s+1} \to \mathbb{R}$. Представим его в виде линейной комбинации индикаторных признаков (27):

$$f(q') = \sum_{q \in \mathbf{V}^{s+1}} f(q) \mathbf{i}_q(q'), \quad q' \in \mathbf{V}^{s+1},$$

откуда по линейности оператора центированного усреднения (7) имеем:

$$n^{1/2} \cdot \langle f \rangle_n = n^{1/2} \cdot \sum_{q \in \mathbf{V}^{s+1}} f(q) \langle \mathbf{i}_q \rangle_n = \left\langle f, \hat{\boldsymbol{\varepsilon}}_n^{(s)} \right\rangle_{\mathbf{T}(s+1)}.$$

Последнее выражение определяет линейный функционал на $\mathbf{T}(s+1)$, вычисленный от функции

$$\hat{\boldsymbol{\varepsilon}}_n^{(s)}|_{\mathbf{V}^{s+1}} \in \mathbf{T}(s+1).$$

Поскольку пространства $\mathbf{T}(s+1)$ и $\mathbb{T}(s)$ связаны взаимно однозначным соответствием (16), $n^{1/2} \cdot \langle f \rangle_n$ также является линейным функционалом на $\mathbb{T}(s)$, вычисленным от функции

$$\hat{\boldsymbol{\delta}}_n^{(s)} \in \mathbb{T}(s),$$

и может быть представлен как скалярное произведение:

$$n^{1/2} \cdot \langle f \rangle_n = \left\langle \hat{\boldsymbol{\delta}}_n^{(s)}, \boldsymbol{\tau}^{(f)} \right\rangle_{\mathbb{T}}, \quad \boldsymbol{\tau}^{(f)} \in \mathbb{T}(s). \tag{29}$$

Таким образом, каждому информативному признаку отвечает некоторый элемент касательного пространства $\mathbb{T}$, общий для всех признаков, эквивалентных в смысле (12). Другими словами, между пространством $\mathbb{T}$ и множеством классов эквивалентности информативных признаков установлен естественный изоморфизм. Также получен критерий эквивалентности двух признаков f_1 и f_2:

$$f_1 \sim f_2 \Leftrightarrow \boldsymbol{\tau}^{(f_1)} = \boldsymbol{\tau}^{(f_2)}.$$

Будем называть $\boldsymbol{\tau}^{(f)}$ порождающим элементом признака f. Для вектора информативных признаков $f = (f_i)_{i \in I}$ обозначим:

$$\mathcal{T}^{(f)} ::= \mathcal{T}[\boldsymbol{\tau}^{(f_i)} : i \in I], \quad \mathbf{ord}(f) ::= \mathbf{ord}(\mathcal{T}^{(f)}), \tag{30}$$

где $\mathcal{T}[\cdot]$ – линейная оболочка системы векторов. Пространство $\mathcal{T}^{(f)}$ и величину $\mathbf{ord}(f)$ будем называть соответственно целевым пространством и порядком вектора признаков f и теста (10). Из (29), с учетом (28), для вектора признаков имеем:

$$n^{1/2} \cdot \langle f_i \rangle_n = \left\langle \hat{\boldsymbol{\delta}}_n^{(s_+)}, \boldsymbol{\tau}^{(f_i)} \right\rangle_{\mathbb{T}}, \quad i \in I, \quad s_+ \geq \mathbf{ord}(f). \quad (31)$$

Порядок информативного признака на единицу меньше минимальной длины векторов, от которых этот признак может быть эквивалентно реализован. Уменьшение на единицу сделано для удобства соотнесения порядков признаков с порядками цепей Маркова: для статистической оценки параметров цепи Маркова $\mathrm{MC}(s)$ порядка $s \in \mathbb{N}_0$ используются признаки того же порядка $\mathbf{ord}(f) = s$, то есть признаки от $(s+1)$-грамм. Например, для статистической оценки параметра схемы Бернулли (цепи Маркова нулевого порядка $\mathrm{MC}(0)$) используется статистика нулевого порядка – доля единиц в наблюдаемой последовательности $|\mathbf{x}_1^n|/n = \hat{\mathsf{E}}_n \{f\}$ на основе информативного признака $f(q) = q$ от отдельных знаков $q \in \mathbf{V}^1$ (1-грамм). В этом смысле статистики $\hat{\boldsymbol{\delta}}_n^{(s)}$, $\hat{\boldsymbol{\varepsilon}}_n^{(s)}$ имеют порядок s, записанный в верхнем индексе. Для любого признака $f : \mathbf{V}^r \to \mathbb{R}$, $r \in \mathbb{N}$, очевидно неравенство:

$$\mathbf{ord}(f) \leq r - 1. \quad (32)$$

В (6) построен пример признака, который зависит только от префикса входного вектора, поэтому для него неравенство (32) становится строгим. Менее тривиальный пример строгого неравенства в (32) – признак $f(q) = |q|$, $q \in \mathbf{V}^r$ (вес Хэмминга). Этот признак существенно зависит от всех

компонент входного вектора, однако он эквивалентен признаку $\tilde{f}(q) = r \cdot q$, $q \in \mathbf{V}^1$, поэтому $\mathbf{ord}(f) \equiv 0$ для любого $r \in \mathbb{N}$.

Пусть V – некоторое конечномерное линейное пространство над $\mathbb{R}$ со скалярным произведением $\langle \cdot, \cdot \rangle$. Будем писать $\xi \sim \mathcal{N}_V(\mu)$ и говорить, что случайный вектор $\xi \in V$ имеет стандартное нормальное распределение с центром $\mu \in V$, если в любом ортонормированном базисе $\{v_i \in V\}_{i=1}^k$, $k = \dim(V)$, координаты вектора $\xi - \mu = \sum_{i=1}^k c_i v_i$ имеют центрированное стандартное нормальное распределение: $(c_i)_{i=1}^k \sim \mathcal{N}_k(\mathbf{0}_k, \mathbf{I}_k)$.

Лемма 4. *Для $\xi \sim \mathcal{N}_V(\mu)$ верны следующие утверждения:*

- *квадрат нормы $\|\xi\|^2 = \langle \xi, \xi \rangle$ имеет нецентральное хи-квадрат распределение с k степенями свободы и параметром нецентральности $\lambda = \|\mu\|^2$;*
- *для любого линейного подпространства $U \subset V$:*

$$\xi \sim \mathcal{N}_V(\mu) \Rightarrow \mathbf{Pr}_U \xi \sim \mathcal{N}_U(\mathbf{Pr}_U \mu);$$

- *для любой системы ортогональных подпространств*

$$\{U_i \subset V\}, \quad U_i \perp U_j,\ i \neq j,$$

  проекции $\{\mathbf{Pr}_{U_i} \xi\}$ независимы в совокупности;

- *вектор скалярных произведений ξ с любым конечным набором $\{v_i \in V\}_{i=1}^r$ имеет нормальное распределение с матрицей Грама набора $\{v_i\}$ в качестве матрицы ковариаций:*

$$(\langle \xi, v_i \rangle)_{i=1}^r \sim \mathcal{N}_r \left((\langle \mu, v_i \rangle)_{i=1}^r, (\langle v_i, v_j \rangle)_{i,j=1}^r \right).$$

Лемма 5. *В случае истинной альтернативы H_1 и контигуальной асимптотики* (3) *для любого $s \in \mathbb{N}_0$ имеет место сходимость по распределению:*

$$\hat{\boldsymbol{\delta}}_n^{(s)} \xrightarrow[n\to\infty]{D} \mathcal{N}_{\mathbb{T}(s)}(\mathbf{Pr}_{\mathbb{T}(s)}\boldsymbol{\delta}).$$

5 Основная часть

Перейдем к главным результатам.

Теорема 1. *Матрица ковариаций* (8) *есть матрица Грама системы $\{\boldsymbol{\tau}^{(f_i)}\}_{i\in I}$:*

$$\Sigma_{i,j}^{(f)} = \left\langle \boldsymbol{\tau}^{(f_i)}, \boldsymbol{\tau}^{(f_j)} \right\rangle_{\mathbb{T}}, \quad i,j \in I. \tag{33}$$

Статистика (9) *есть квадрат нормы ортогональной проекции $\hat{\boldsymbol{\delta}}_n^{(s_+)}$ на целевое пространство $\mathcal{T}^{(f)}$ при достаточно больших s_+:*

$$S_n(f) = S_n\left[\mathcal{T}^{(f)}\right] ::= \left\|\mathbf{Pr}_{\mathcal{T}^{(f)}}\hat{\boldsymbol{\delta}}_n^{(s_+)}\right\|_{\mathbb{T}}^2, \ s_+ \geq \mathbf{ord}(f). \tag{34}$$

В случае истинной альтернативы H_1 и контигуальной асимптотики (3) *статистика* (34) *имеет асимптотическое нецентральное распределение хи-квадрат с $d = |I| = \dim(\mathcal{T}^{(f)})$ степенями свободы и параметром нецентральности:*

$$\lambda^{(f)}(\boldsymbol{\delta}) = \lambda\left[\boldsymbol{\delta}|\mathcal{T}^{(f)}\right] ::= \left\|\mathbf{Pr}_{\mathcal{T}^{(f)}}\boldsymbol{\delta}\right\|_{\mathbb{T}}^2. \tag{35}$$

Таким образом, статистика (9) однозначно определяется целевым пространством $\mathcal{T}^{(f)}$ по формуле (34), а вектор информативных признаков $f = (f_i)_{i\in I}$ невырожден, если и

только если система порождающих элементов $\{\boldsymbol{\tau}^{(f_i)}\}_{i\in I}$ линейно независима. На основе установленного взаимно однозначного соответствия (34) между статистиками вида (9) и конечномерными подпространствами $\mathcal{T} = \mathcal{T}^{(f)} \subset \mathbb{T}$ (целевыми пространствами) приведем далее свойства этих статистик в терминах целевых пространств $\mathcal{T}$. Обозначение $S_n[\mathcal{T}]$ с квадратными скобками в (34) введено, чтобы различать два способа задания статистики (34): через вектор информативных признаков f, и через целевое пространство $\mathcal{T}$.

Лемма 6. *При фиксированном уровне значимости α мощность* (11) *монотонно убывает по d и монотонно возрастает по λ.*

Мощность (11) с учетом (35) следующим образом зависит от уровня значимости $\alpha \in (0,1)$, альтернативы $\boldsymbol{\delta} \in \mathbb{T}$, и целевого пространства $\mathcal{T} \subset \mathbb{T}$ теста (10):

$$\omega = \omega[\alpha, \boldsymbol{\delta}, \mathcal{T}] = 1 - F_{d,\lambda}\left(F_d^{-1}(1-\alpha)\right), \qquad (36)$$
$$d = \dim(\mathcal{T}), \quad \lambda = \|\mathbf{Pr}_{\mathcal{T}}\boldsymbol{\delta}\|_{\mathbb{T}}^2 .$$

Теорема 2. *Для любых целевых пространств $\mathcal{T}, \mathcal{T}' \subset \mathbb{T}$, таких что $\boldsymbol{\delta} \in \mathcal{T} \subset \mathcal{T}'$, в случае истинной альтернативы H_1 и контигуальной асимптотики* (3) *тест* (10) *на основе статистики $S_n[\mathcal{T}]$ асимптотически мощнее теста на основе статистики $S_n[\mathcal{T}']$:*

$$\omega[\alpha, \boldsymbol{\delta}, \mathcal{T}] \geq \omega[\alpha, \boldsymbol{\delta}, \mathcal{T}'].$$

Теорема 2 означает, что при наличии априорной информации о принадлежности альтернативы $\boldsymbol{\delta}$ некоторым под-

пространствам в $\mathbb{T}$ наименьшее из этих подпространств следует использовать в качестве целевого пространства для построения наиболее мощного теста (10) для различения данной альтернативы с нулевой гипотезой H_0. Примером такой априорной информации может быть соответствие наблюдаемой последовательности $\mathbf{x}$ некоторой малопараметрической Марковской модели M. Пусть модель M с параметром $\theta = (\theta_i)_{i=1}^d \in \mathbb{R}^d$ задает цепь Маркова $\mathrm{MC}(s)$ порядка $s \in \mathbb{N}_0$ в форме (2):

$$\mathsf{P}\left\{\mathbf{x}_i = 0 | \mathbf{x}_{i-1}^{i-s}\right\} = \frac{1 + \delta(\mathbf{x}_{i-1}^{i-s}; \theta)}{2}. \tag{37}$$

И пусть $\delta(q; \mathbf{0}_d) \equiv 0$, $q \in \mathbf{V}^s$, то есть при нулевом параметре $\theta = \mathbf{0}_d$ модель M задает РРСП. Обозначим касательное пространство равномерного распределения относительно модели M:

$$\mathcal{T}^M ::= \mathcal{T}\left[\left.\frac{\partial}{\partial\theta_i}\delta(\cdot;\theta)\right|_{\theta=\mathbf{0}_d} : i = 1, \ldots, d\right] \subset \mathbb{T}, \tag{38}$$

где $\delta(\cdot;\theta) : \mathbf{V}_0^* \to \mathbb{R}$ – расширенная согласно (13) функция $\delta(\cdot;\theta) : \mathbf{V}^s \to \mathbb{R}$. Например, $\mathcal{T}^{\mathrm{MC}(s)} = \mathbb{T}(s)$, $s \in \mathbb{N}_0$. Если при истинной альтернативе H_1 наблюдаемая последовательность $\mathbf{x}_1^n$ отвечает модели M с параметром

$$\theta^{(n)} = n^{-1/2} \cdot \boldsymbol{\theta} + o\left(n^{-1/2}\right), \quad \boldsymbol{\theta} \in \mathbb{R}^d,\ n \in \mathbb{N},$$

то такая асимптотика с точностью до величины порядка $o\left(n^{-1/2}\right)$ эквивалентна контигуальной асимптотике (3), причем $\boldsymbol{\delta} \in \mathcal{T}^M$.

Для ортогональных подпространств $\mathcal{T}', \mathcal{T}'' \subset \mathbb{T}$, $\mathcal{T}' \perp \mathcal{T}''$, обозначим:

$$\mathcal{T}' \boxplus \mathcal{T}'' ::= \mathcal{T}[\mathcal{T}', \mathcal{T}''] \subset \mathbb{T}$$

– их линейную оболочку (прямую сумму). Для подпространства $\mathcal{T} \subset \mathbb{T}$:

$$\mathcal{T}^{\perp} ::= \{\boldsymbol{\delta} \in \mathbb{T} : \boldsymbol{\delta} \perp \mathcal{T}\}$$

– ортогональное дополнение $\mathcal{T}$ в $\mathbb{T}$. Для вложенных подпространств $\mathcal{T} \subset \mathcal{T}' \subset \mathbb{T}$:

$$\mathcal{T}' \boxminus \mathcal{T} ::= \mathcal{T}' \cap \mathcal{T}^{\perp} \tag{39}$$

– ортогональное дополнение $\mathcal{T}$ в $\mathcal{T}'$.

Теорема 3. *В случае истинной альтернативы H_1 и контигуальной асимптотики* (3) *при условии $\boldsymbol{\delta} \in \mathcal{T}^{\perp}$ гипотезы H_0 и H_1 асимптотически неразличимы для теста* (10) *на основе статистики $S_n[\mathcal{T}]$.*

Подпространство альтернатив $\mathcal{T}^{\perp} \subset \mathbb{T}$ будем по этой причине нахывать слепым пятном теста (10) на основе статистики $S_n[\mathcal{T}]$. Тесты на основе

Теорема 4. *Для ортогональных целевых пространств*

$$\mathcal{T}, \mathcal{T}' \subset \mathbb{T}, \quad \mathcal{T} \perp \mathcal{T}',$$

статистика (34) *обладает свойством:*

$$S_n\left[\mathcal{T} \boxplus \mathcal{T}'\right] = S_n\left[\mathcal{T}\right] + S_n\left[\mathcal{T}'\right]. \tag{40}$$

Для вложенных целевых пространств

$$\mathcal{T} \subset \mathcal{T}' \subset \mathbb{T}$$

статистика (34) *обладает свойством:*

$$S_n\left[\mathcal{T}' \boxminus \mathcal{T}\right] = S_n\left[\mathcal{T}'\right] - S_n\left[\mathcal{T}\right]. \tag{41}$$

Теорема 5. *Для конечной системы ортогональных целевых пространств*

$$\{\mathcal{T}_i \subset \mathbb{T}\}_{i=1}^{k}, \quad \mathcal{T}_i \perp \mathcal{T}_j,\ 1 \leq i < j \leq k,$$

статистики $\{S_n[\mathcal{T}_i]\}_{i=1}^{k}$ *при* $n \to \infty$ *асимптотически независимы в совокупности в случае истинной альтернативы* H_1 *и контигуальной асимптотики* (3).

Введем дополнительные обозначения. Для последовательности вложенных пространств $\{\mathbb{T}(s)\}$, $s \in \mathbb{N}_0$:

$$\Delta\mathbb{T}(s) ::= \mathbb{T}(s) \boxminus \mathbb{T}(s-1),\ \dim(\Delta\mathbb{T}(s)) = 2^{s-1},\ s \in \mathbb{N}, \quad (42)$$

– последовательность "соседних разностей" относительно операции (39). Для $s \in \mathbb{N}_0$:

$$\mathfrak{S}_n(s) ::= n \sum_{q \in \mathbf{V}^{s+1}} \frac{(\hat{\mathsf{E}}_n\{\mathbf{i}_q\} - 2^{-s-1})^2}{2^{-s-1}} = \left\| \hat{\boldsymbol{\varepsilon}}_n^{(s)} \right\|_{\mathbf{T}(s+1)}^2 \quad (43)$$

– стандартная хи-квадрат статистика на основе частот $(s+1)$-грамм. Первые и вторые разности последовательности (43) по аргументу s:

$$\Delta\mathfrak{S}_n(s) = \mathfrak{S}_n(s) - \mathfrak{S}_n(s-1), \quad (44)$$

$$\Delta^2\mathfrak{S}_n(s) = \mathfrak{S}_n(s) - 2\mathfrak{S}_n(s-1) + \mathfrak{S}_n(s-2), \quad (45)$$

где полагаем $\mathfrak{S}_n(-1) = 0$, откуда:

$$\Delta\mathfrak{S}_n(0) = \mathfrak{S}_n(0), \quad \Delta^2\mathfrak{S}_n(1) = \mathfrak{S}_n(1) - 2\mathfrak{S}_n(0).$$

Для $s \in \mathbb{N}$:

$$\mathrm{UMC}(s) \subset \mathrm{MC}(s)$$

– подсемейство Марковских распределений порядка s, имеющих равномерное стационарное распределение s-грамм:

$$\mathcal{L}\{\mathbf{x}\} \in \mathrm{UMC}(s) \Leftrightarrow \mathsf{P}\left\{\mathbf{x}_i^{i+s-1} = q\right\} \equiv 2^{-s},\ q \in \mathbf{V}^s. \quad (46)$$

Пространства (42) являются касательными для равномерного распределения относительно моделей (46):

$$\mathcal{T}^{\mathrm{UMC}(s)} = \Delta\mathbb{T}(s), \quad s \in \mathbb{N}.$$

Из Леммы 3 получаем вид статистики (34) для целевых пространств $\mathbb{T}(s)$:

$$S_n\left[\mathbb{T}(s)\right] = \Delta\mathfrak{S}_n(s), \quad s \in \mathbb{N}_0. \tag{47}$$

Из Теоремы 4 получаем вид статистики (34) для целевых пространств (42):

$$S_n\left[\Delta\mathbb{T}(s)\right] = \Delta^2\mathfrak{S}_n(s), \quad s \in \mathbb{N}. \tag{48}$$

Тесты (10) на основе статистик (47) и (48) в [3] называются "Serial Test". Мы будем называть их тестами равномерности $(s+1)$-грамм, соответственно, I типа (на основе статистики (47)) и II типа (на основе статистики (48)). Тесты равномерности 1-грамм (отдельных знаков) I типа и равномерности 2-грамм (биграмм) II типа на основе статистик:

$$S_n\left[\mathbb{T}(0)\right], \quad S_n\left[\Delta\mathbb{T}(1)\right], \tag{49}$$

эквивалентны, соответственно, тесту Монобит и тесту Знакоперемен ("Monobit Test" и "Runs Test" в [3]).

Из Теорем 2–5 получаем следующие выводы в условиях истинной альтернативы H_1 и контигуальной асимптотики (3) при $n \to \infty$:

– для Марковских альтернатив H_1 порядка $s \in \mathbb{N}_0$ и любого $r > s$ тест (10) на основе статистики $S_n[\mathbb{T}(s)]$ асимптотически мощнее теста на основе $S_n[\mathbb{T}(r)]$;

– для Марковских альтернатив H_1 порядка $s \in \mathbb{N}$ с равномерным стационарным распределением (46) тест (10) на основе статистики $S_n[\Delta\mathbb{T}(s)]$ асимптотически мощнее теста на основе статистики $S_n[\mathbb{T}(s)]$;

– Марковские альтернативы H_1 порядка $s \in \mathbb{N}$ с равномерным стационарным распределением (46) асимптотически неразличимы с нулевой гипотезой H_0 для тестов (10) на основе следующих статистик:

$$S_n\left[\mathbb{T}(r)\right], \quad r < s,$$
$$S_n\left[\Delta\mathbb{T}(r)\right], \quad r \neq s;$$

– для любых целых $0 \leq s_0 < s_1 < \cdots < s_k$, $k > 0$, следующие $k+1$ статистик асимптотически независимы в совокупности:

$$S_n\left[\mathbb{T}(s_0)\right], \quad S_n\left[\Delta\mathbb{T}(s_i)\right], \quad i = 1, \ldots, k,$$

в частности, асимптотически независимы статистики (49) тестов Монобит и Знакоперемен.

На рис. 1 на основе формул (11), (36) изображено подмножество двумерного пространства $\mathbb{T}(1)$ Марковских альтернатив первого порядка, для которых при контигуальной асимптотике (3) тест Монобит асимптотически мощнее теста равномерности биграмм I типа. В согласии с Теоремой 2, это подмножество включает одномерное подпространство $\mathbb{T}(0) \subset \mathbb{T}(1)$ (центральная вертикальная ось на рис. 1). Ввиду асимптотической независимости тестов Монобит и Знакоперемен, батарея из этих двух тестов с одинаковыми уровнями значимости α_* и мощностями ω_1, ω_2 имеет общий

уровень значимости $\alpha = 1 - (1 - \alpha_*)^2$ и общую мощность $\omega = 1 - (1 - \omega_1)(1 - \omega_2)$. На основе этих свойств на рис. 2 по аналогии с рис. 1 изображено подмножество Марковских альтернатив первого порядка, для которых при контигуальной асимптотике (3) батарея "Монобит + Знакоперемен" мощнее теста равномерности биграмм I типа ($\alpha = 0.01$, $\alpha_* = 1 - \sqrt{1 - \alpha} \approx 0.005$).

Отметим также, что часто возникающие на практике статистики (43), в отличие от своих первых и вторых разностей (44), (45), при $s > 0$ не имеют асимптотического распределения хи-квадрат. Их асимптотическое распределение чуть сложнее – это распределение квадрата нормы Гауссовского случайного вектора с не единичной матрицей ковариаций. Согласно Теореме 1, статистики хи-квадрат вида (34) представимы в виде квадратичной формы:

$$S_n[\mathcal{T}] = \left\langle \hat{\boldsymbol{\delta}}_n^{(s_+)}, \boldsymbol{\Sigma} \hat{\boldsymbol{\delta}}_n^{(s_+)} \right\rangle_{\mathbb{T}}, \quad \boldsymbol{\Sigma} = \mathbf{Pr}_{\mathcal{T}}, \tag{50}$$

где самосопряженный линейный оператор $\boldsymbol{\Sigma} : \mathbb{T} \to \mathbb{T}$, определяющий квадратичную форму (50), является проектором на целевое пространство $\mathcal{T}$. Статистики (43) относятся к более общему классу квадратичных форм вида (50), когда оператор $\boldsymbol{\Sigma}$ не является проектором. Лемма 3 позволяет, тем не менее, представить этот оператор в виде суммы проекторов на вложенные подпространства:

$$\mathfrak{S}_n(s) = \left\langle \hat{\boldsymbol{\delta}}_n^{(s_+)}, \boldsymbol{\Sigma} \hat{\boldsymbol{\delta}}_n^{(s_+)} \right\rangle_{\mathbb{T}}, \quad \boldsymbol{\Sigma} = \sum_{r=0}^{s} \mathbf{Pr}_{\mathbb{T}(r)}, \ s_+ \geq s. \tag{51}$$

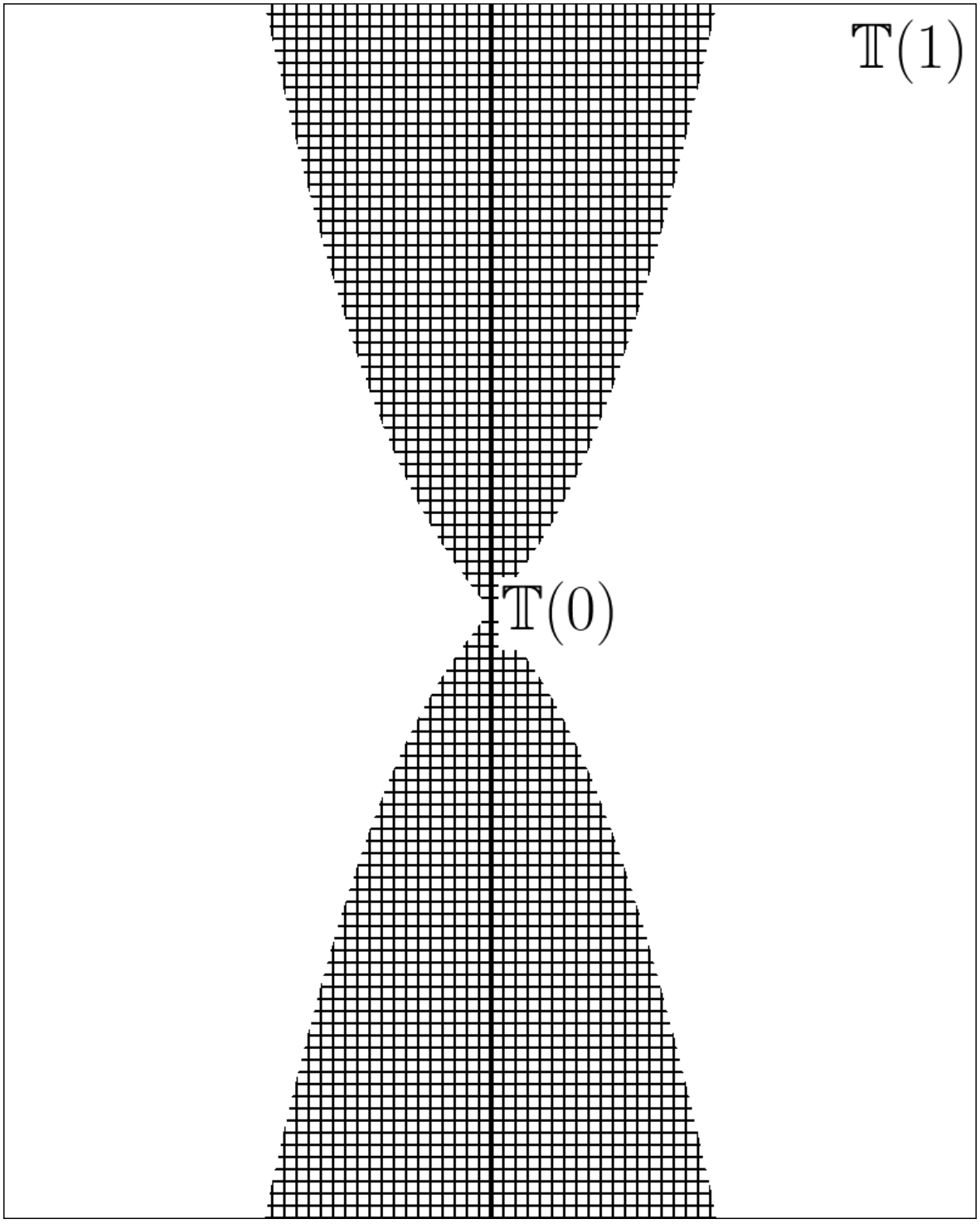

Рис. 1. Подмножество (заштриховано) пространства $\mathbb{T}(1)$ Марковских альтернатив первого порядка, для которых тест Монобит мощнее теста равномерности биграмм I типа

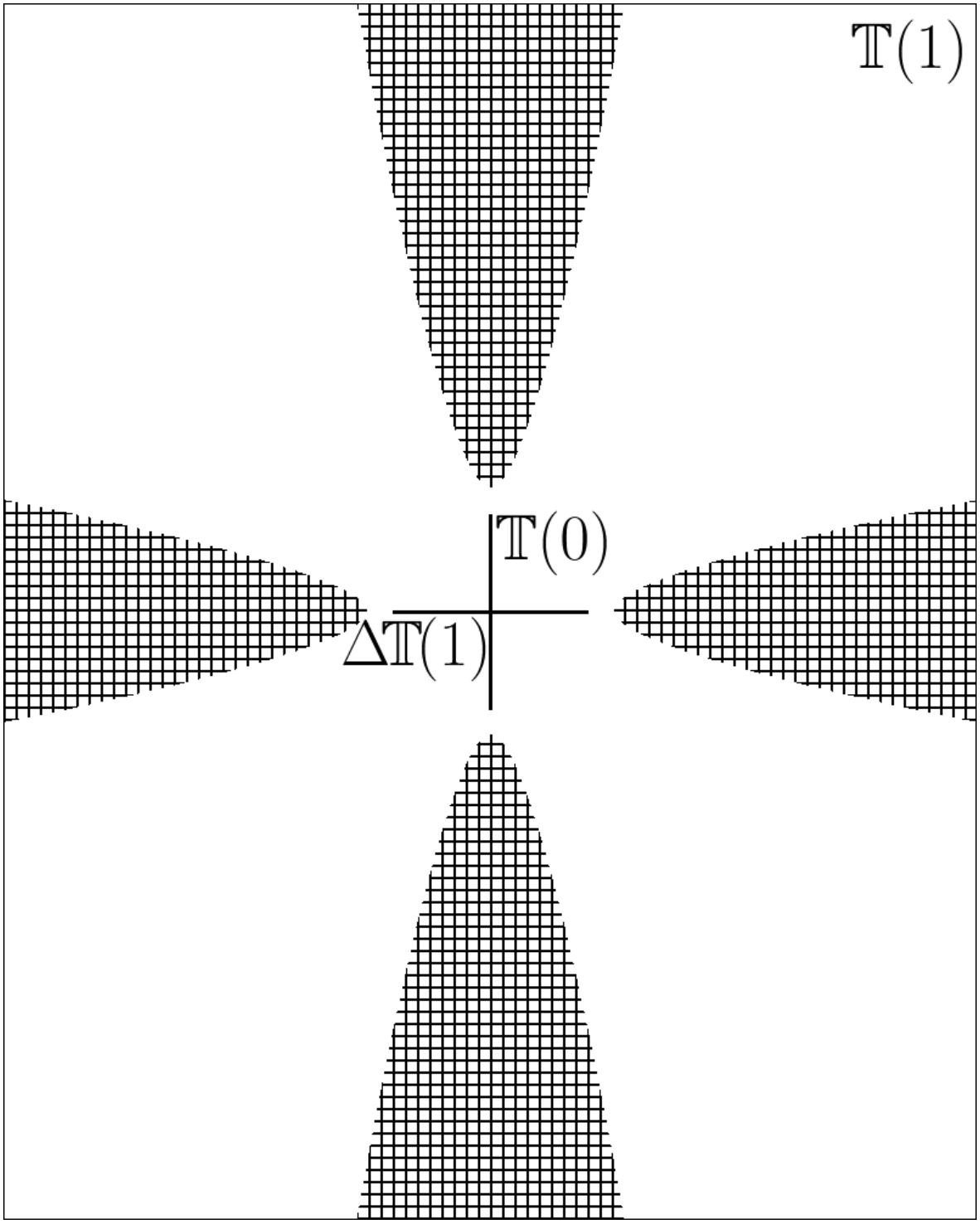

Рис. 2. Подмножество (заштриховано) пространства $\mathbb{T}(1)$ Марковских альтернатив первого порядка, для которых батарея тестов “Монобит + Знакоперемен” мощнее теста равномерности биграмм I типа

Используя разложение:

$$\mathbf{Pr}_{\mathbb{T}(r)} = \mathbf{Pr}_{\mathbb{T}(0)} + \sum_{r'=1}^{r} \mathbf{Pr}_{\Delta\mathbb{T}(r')},$$

получаем представление оператора (51) в виде взвешенной суммы проекторов на ортогональные подпространства:

$$\mathbf{\Sigma} = (s+1)\mathbf{Pr}_{\mathbb{T}(0)} + \sum_{r=1}^{s}(s+1-r)\mathbf{Pr}_{\Delta\mathbb{T}(r)}. \qquad (52)$$

Оператор (51), таким образом, имеет следующий спектр ненулевых собственных чисел: максимальное собственное число $\boldsymbol{\lambda}_0 = s+1$ кратности $\dim(\mathbb{T}(0)) = 1$, и собственные числа $\boldsymbol{\lambda}_r = s+1-r$ кратности $\dim(\Delta\mathbb{T}(r)) = 2^{r-1}$, $r = 1, \ldots, s$. Заметим, что все собственные числа – целые. След оператора (51):

$$\mathrm{Tr}(\mathbf{\Sigma}) = \sum_{r=0}^{s} \mathrm{Tr}(\mathbf{Pr}_{\mathbb{T}(r)})$$

$$= \sum_{r=0}^{s} \dim(\mathbb{T}(r)) = \sum_{r=0}^{s} 2^r = 2^{s+1} - 1.$$

С точностью до множителя 2^{s+1}, такие же спектр ненулевых собственных значений и след имеет асимптотическая матрица ковариаций частот встречаемости $(s+1)$-грамм (в обозначениях Леммы 1 и (27)):

$$\Sigma^{(\mathbf{i}^{(s+1)})} \in \mathbb{R}^{2^{s+1}\times 2^{s+1}}.$$

Эта матрица имеет сложную структуру, и прямое вычисление ее спектральных характеристик весьма затруднитель-

но. Вычисленный след оператора $\boldsymbol{\Sigma}$ позволяет, в частности, найти асимптотическое математическое ожидание статистики (43) при истинной нулевой гипотезе H_0, которая является частным случаем гипотезы H_1 в условиях контигуальной асимптотики (3) с $\boldsymbol{\delta}(q) \equiv 0$, $q \in \mathbf{V}_0^*$:

$$\mathsf{E}\left\{\mathfrak{S}_n(s)|H_0\right\} \underset{n\to\infty}{\longrightarrow} \mathrm{Tr}(\boldsymbol{\Sigma}) = 2^{s+1} - 1, \quad s \in \mathbb{N}_0.$$

Библиографические ссылки

1. *Харин Ю.С., Вечерко Е.В.* Распознавание вкраплений в двоичную цепь Маркова // Дискретная математика. 2015. Т. 27, Вып. 3. С. 123–144.

2. *Amari S., Nagaoka H.* Methods of Information Geometry. Oxford: Oxford University Press, 2000.

3. A statistical test suite for the validation of random number generators and pseudo random number generators for cryptographic applications. NIST Special Publication 800-22 Revision 1a [Electronic resource].
   URL: `https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-22r1a.pdf`
   (date of access: 14.09.2023).

4. *Волошко В.А., Трубей А.И.* О мощности тестов многомерной дискретной равномерности, используемых для статистического анализа генераторов случайных последовательностей // Журнал БГУ. Математика. Информатика. 2022. Ном. 1. С. 26–37.

О КОМПАКТНОМ ЛИНЕАРИЗУЕМОМ АЛГЕБРАИЧЕСКОМ ОПИСАНИИ КРИПТОГРАФИЧЕСКИХ ПРЕОБРАЗОВАНИЙ

Ф.Б. Дасько[1]
[1]*НИИ прикладных проблем математики и информатики*
[1]*Белорусский государственный университет*
Минск, БЕЛАРУСЬ
e-mail: fedd2001@gmail.com

Для описания криптографических преобразований предлагается использовать компактные линеаризуемые системы алгебраических уравнений. Компактность означает простоту уравнений системы и неуменьшаемость их количества. Линеаризуемость означает, что образ преобразования может быть вычислен по прообразу методами линейной алгебры, т.е. эффективно. Линеаризуемость эвристически упрощает алгебраические атаки на криптосистемы, в которые целевое преобразование входит в качестве композиционного элемента. Предложен алгоритм построения компактного линеаризуемого описания заданного преобразования.
Ключевые слова: криптографическое преобразование; система алгебраических уравнений; линейная алгебра; базис Гребнера; алгоритм Бухбергера

1 Введение

Одно из направлений анализа симметричных криптосистем состоит в их описании системами алгебраических уравнений с последующим решением систем. В общем случае нахождение решения является нетривиальной и вычислительно трудной задачей. Алгебраическое описание криптосистемы не единственно, и эффективность анализа зависит от

того, как именно криптосистема описана. Один из подходов к повышению эффективности состоит в представлении криптосистемы в виде композиции отдельных криптографических преобразований и построении для каждого преобразования подходящей системы, его описывающей. Объединение построенных систем уравнений используется для проведения анализа всей криптосистемы.

В связи с объединением нескольких систем уравнений в одну, естественно стремиться к «экономичности» базовых систем. С одной стороны, уравнения системы должны быть достаточно простыми, чтобы облегчить эффективный поиск решения. С другой стороны, общее количество уравнений в системе должно быть небольшим, чтобы избежать чрезмерного объема вычислений.

В разделе 2 мы вводим компактные линеаризуемые описания криптографических преобразований. Компактность формализует идею экономичной системы. Линеаризуемость означает, что образ преобразования может быть вычислен по прообразу методами линейной алгебры. Линеаризуемость позволяет эффективнее проводить анализ, если имеется информация о части входа криптосистемы или эффективнее проверять предположения о значениях таких частей.

В разделе 3 представлен алгоритм построения компактных линеаризуемых описаний, позволяющий повысить эффективность алгебраического анализа за счет соблюдения баланса между простотой и экономичностью описаний криптографических преобразований.

2 Компактное линеаризуемое описание

Пусть $\mathbb{F}_2$ — поле из двух элементов, V_n — n-мерное векторное пространство над $\mathbb{F}_2$,

$$\mathbf{x} = (x_1, \ldots, x_n),\ \mathbf{y} = (y_1, \ldots, y_m),$$

– формальные переменные, $P = \mathbb{F}_2[\mathbf{x}, \mathbf{y}]$ — кольцо многочленов от $\mathbf{x}$ и $\mathbf{y}$ над $\mathbb{F}_2$.

Система алгебраических уравнений — это система вида

$$p_i(\mathbf{x}, \mathbf{y}) = 0, \quad i = 1, \ldots, k, \quad p_i \in P.$$

Так как уравнения $p_i(\mathbf{x}, \mathbf{y}) = 0$ и многочлены $p_i(\mathbf{x}, \mathbf{y})$ однозначно связаны друг с другом, то систему уравнений $\{p_i(\mathbf{x}, \mathbf{y}) = 0\}$ можно отождествить с системой многочленов $\{p_i(\mathbf{x}, \mathbf{y})\}$, что мы далее и будем делать.

Определение 1. Система S называется *описанием* преобразования $f\colon V_n \to V_m$, если решения S из множества V_{n+m} — это всевозможные векторы $(\alpha, f(\alpha))$, $\alpha \in V_n$, и только они.

Множество решений системы S не будет выходить за пределы V_{n+m}, если система содержит так называемые уравнения поля

$$x_1^2 + x_1 = 0, \ldots, x_n^2 + x_n = 0,$$
$$y_1^2 + y_1 = 0, \ldots, y_m^2 + y_m = 0.$$

Далее будем считать, что уравнения поля неявно присутствуют в системе, а все остальные ее многочлены приведены по модулю

$$(x_1^2 + x_1, \ldots, x_n^2 + x_n, y_1^2 + y_1, \ldots, y_m^2 + y_m)$$

и, таким образом, всякая переменная встречается в любом из мономов многочлена не более одного раза.

Пример описания f — система

$$S_0 = \{y_i + f_i(\mathbf{x}) \colon i = 1, \ldots, m\},$$

в которой f_i — координатные многочлены f:

$$f(\mathbf{x}) = (f_1(\mathbf{x}), \ldots, f_m(\mathbf{x})).$$

Систему S_0 будем называть *каноническим* описанием.

Определение 2. Система S называется *компактной относительно свойства* $\mathcal{P}$, если:

– $\mathcal{P}$ выполняется для S;

– $\mathcal{P}$ не выполняется для всякой подсистемы $S' \subsetneq S$;

– если $\mathcal{P}$ выполняется для некоторой системы S', то

$$\max_{p' \in S'} \deg(p') \geq \max_{p \in S} \deg(p).$$

Пусть свойство $\mathcal{D}$ состоит в том, что система является описанием f.

В каноническом описании S_0 степени многочленов f_i могут быть высоки, и описание не обязательно не является компактным относительно $\mathcal{D}$. Компактное описание можно получить, обработав S_0 следующим образом:

1. Выбрать градуированный мономиальный порядок и построить градуированный базис Гребнера G системы S_0. Для реализации этого шага использовать алгоритм Бухбергера или какой-либо из алгоритмов смены порядка в базисе Гребнера [3, 4].

2. Для многочленов $p \in G$, выбираемых в порядке убывания старшего монома, выполнить:

   – если $G \setminus \{p\}$ является описанием f, то $G \leftarrow G \setminus \{p\}$.

3. Возвратить G.

В итоговом описании G максимальная степень многочленов минимальна, число многочленов неуменьшаемо. Однако при переходе от S_0 к G может быть потеряно важное свойство, которое мы называем *линеаризуемостью* и обозначаем через $\mathcal{L}$.

Определение 3. Описание S преобразования f называется *линеаризуемым*, если для любого $\alpha \in V_n$ и всякого $p(\mathbf{x}, \mathbf{y}) \in S$ выполняется: $\deg p(\alpha, \mathbf{y}) \leq 1$.

Линеаризуемость описания S означает, что с его помощью по прообразу α можно эффективно вычислить образ $\beta = f(\alpha)$. Действительно, многочлены

$$\{p(\alpha, \mathbf{y}) \colon p \in S\}$$

будут задавать линейную систему уравнений вида

$$\mathbf{y}A(\alpha) + b(\alpha) = 0,$$

в которой $b(\alpha) \in V_k$, $A(\alpha)$ — матрица $m \times k$ ранга m. Линейная система будет иметь единственное решение $\mathbf{y}$, и это решение легко найти с помощью линейной алгебры.

Линеаризуемость является полезным свойством, эвристически упрощающим решение систем уравнений, в которые S входит в качестве составной части. В связи с этим поставим задачу построения систем, компактных относительно свойств $\mathcal{D}$ и $\mathcal{L}$, другими словами, *компактных линеаризуемых описаний*.

Отметим, что из равенства $\mathrm{rank}(A(\alpha)) = m$ следует, что $k \geq m$. Поэтому число уравнений в компактном линеаризуемом описании S не может быть меньше, чем в каноническом описании S_0. С другой стороны, в силу компактности, максимальная степень многочленов S может быть меньше, чем максимальная степень многочленов S_0.

3 Построение описания

Многочлен, получаемый при подстановке $\mathbf{x} = \alpha$ в многочлен $p(\mathbf{x}, \mathbf{y})$, назовем *проекцией* p и обозначаем через $\mathrm{proj}_\alpha(p)$. Многочлены линеаризуемого описания, т. е. многочлены, степени проекций которых не превосходят 1, будем называть *линеаризуемыми*.

Нетрудно проверить, что линеаризуемый многочлен имеет вид

$$p(\mathbf{x}, \mathbf{y}) = g_0(\mathbf{x}) + \sum_{i=1}^{m} y_i g_i(\mathbf{x}),$$

а все линеаризуемое описание S может быть представлено в следующем виде:

$$\mathbf{y} A_S(\mathbf{x}) + b_S(\mathbf{x}) = 0.$$

Здесь $A_S(\mathbf{x})$ — матрица $m \times k$ над кольцом многочленов от переменных $\mathbf{x}$, $b_S(\mathbf{x})$ — вектор многочленов размерности k.

Отметим, что линеаризуемые многочлены, степени не выше некоторого d, замкнуты по сложению, то есть образуют линейное пространство. Более того,

$$\mathrm{proj}_\alpha(p_1) + \mathrm{proj}_\alpha(p_2) = \mathrm{proj}_\alpha(p_1 + p_2).$$

Вычисление компактного линеаризуемого описания предлагается разбить на следующие этапы:

1. Выбрать градуированный мономиальный порядок и построить градуированный базис Гребнера G системы S_0.
2. Построить линейное пространство L линеаризуемых многочленов степени не выше $\max_{p \in G} \deg(p)$.
3. Определить минимальную степень d такую, что система $\{g \in L \colon \deg(g) \leq d\}$ описывает преобразование f.
4. Задать пустую систему Q. Пополнять Q линеаризуемыми многочленами так, чтобы максимизировать сумму $\sum_\alpha \operatorname{rank}(A_Q(\alpha))$ и до тех пор, пока Q не будет описывать преобразование f, т. е. целевая сумма не достигнет величины $2^n m$.
5. Исключать из Q многочлены до тех пор, пока Q описывает f (см. построение компактного описания f).

Для выполнения шага 2 введем специальный мономиальный порядок $\prec_U$, параметризуемый множеством $U \subseteq \{x_1, \ldots, x_n, y_1, \ldots, y_m\}$. Порядок $\prec_U$ определяется по следующим правилам:

– если моном a содержит больше переменных из множества U, чем моном b, то $b \prec_U a$;

– если моном a содержит меньше переменных из множества U, чем моном b, то $a \prec_U b$;

– если мономы a и b содержат одинаковое количество переменных из множества U, то они сравниваются при по-

мощи некоторого градуированного мономиального порядка.

Обобщенным методом Гаусса с мономиальным порядком $\prec$ назовем алгоритм, который диагонализирует систему алгебраических уравнений. При диагонализации мономы многочленов системы интерпретируются как независимые переменные. Приоритет при диагонализации определяется в соответствии с порядком $\prec$.

На шаге 2 следует градуированный базис Гребнера G пополнить всевозможными многочленами вида

$$p(\mathbf{x}, \mathbf{y})m(\mathbf{x}, \mathbf{y}), \quad p \in G,$$

где $m(\mathbf{x}, \mathbf{y})$ — всевозможные мономы такие, что в результате их умножения на p будет получен многочлен степени не выше $\max_{p \in G} \deg(p)$. К построенной ситеме применить обобщенный метод Гаусса с порядком $\prec_{\{y_1,\ldots,y_m\}}$. После этого исключить все многочлены, старший моном которых кратен более чем одному y_i. Далее, для упрощения следующего шага, следует применить обобщенный метод Гаусса с градуированным порядком и получить в итоге систему B. Искомое пространство L — это линейная оболочка многочленов B.

На шаге 3 следует установить $d = \max_{p \in B} \deg(p)$. Последовательно уменьшая d на единицу проверять, что система $B_d = \{p \in B \colon \deg(p) \leq d\}$ описывает преобразование f. Если для $d = \max_{g \in G} \deg(g)$ система не описывает преобразование f, то вычисления завершаются с ошибкой (на практике такие ситуации не возникали).

На шаге 4 многочлен p, который будет добавляться в систему Q, следует строить так, чтобы проекция $\mathrm{proj}_\alpha(p)$ бы-

ла линейно независима относительно проекций многочленов из Q для как можно большего числа входов α.

Для этого предлагается установить $p = 0$, $D = B_d$ и для каждого входа α действовать следующим образом:

A. Вычислить проекции $\mathrm{proj}_\alpha(d), d \in D$, $\mathrm{proj}_\alpha(q), q \in Q$, $\mathrm{proj}_\alpha(p)$.

B. Каждый из многочленов $\mathrm{proj}_\alpha(d)$ привести по модулю многочленов $\mathrm{proj}_\alpha(q)$ и многочлена $\mathrm{proj}_\alpha(p)$ и получить в результате многочлен d'.

C. Для многочленов d' провести метод Гаусса, совершая соответствующие действия и для прообразов d.

D. Если существует $d' \neq 0$, то $p \leftarrow p + d$ и $D \leftarrow D \setminus \{d\}$.

После обработки всех α многочлен p останется нулевым тогда и только тогда, когда система Q описывает f. Таким образом, равенство $p = 0$ можно использовать как критерий завершения шага 4. При завершении выполняется условие $\min_\alpha \mathrm{rank}(A_Q(\alpha)) = m$. В связи с этим предлагается в первую очередь обрабатывать те входы α, для которых $\mathrm{rank}(A_Q(\alpha))$ меньше.

Пример. Пусть преобразование $f\colon V_8 \to V_8$ описывает умножение неотрицательных целых чисел: прообраз $(x_1, \ldots, x_8)$ разбивается на половинки $(x_1, \ldots, x_4)$ и $(x_5, \ldots, x_8)$; половинки интерпретируются как числа от 0 до 15 и перемножаются; результат умножения кодируется вектором $(y_1, \ldots, y_8)$, который объявляется образом f.

Каноническое описание f состоит из 8 многочленов со степенями

$$2, 2, 4, 5, 6, 6, 7, 7.$$

Компактное линеаризуемое описание f состоит из 10 многочленов, максимальная степень многочленов – 3. Как видим, при переходе от канонического описания к компактному линеаризуемому степени многочленов существенно уменьшаются, при этом число многочленов увеличивается незначительно.

Библиографические ссылки

1. *Аржанцев И.В.* Базисы Гребнера и системы алгебраических уравнений. Москва: МЦНМО, 2003.
2. *Бухбергер Б.* Алгоритмический метод в теории полиномиальных идеалов. Москва: Мир, 1986.
3. *Collart S., Kalkbrener M., Mall D.* Converting Bases with the Grobner Walk // Symbolic Computation. 1997. Vol. 24. P. 465–469.
4. Efficient Computation of Zero-Dimensional Grobner Bases by Change of Ordering / J.C. Faugere [et al.] // Symbolic Computation. 1993. Vol. 16. P. 329–344.

ЛИНЕЙНЫЙ КРИПТОАНАЛИЗ АЛГОРИТМА ШИФРОВАНИЯ ISL_LWC

Д.С. Дюсенбаев[1], С.Е. Нысанбаева[2],
К.С. Сакан[3], А. Хомпыш[4]
[1,2,3,4]*Институт информационных и вычислительных технологий МНВО РК*
Алматы, КАЗАХСТАН
e-mail: [1]dimash_dds@mail.ru, [2]bsultasha1@mail.ru,
[3]kairat_sks@mail.ru, [4]ardabek@mail.ru

В данной исследовательской работе представлены результаты линейного криптоанализа легковесного алгоритма шифрования ISL_LWC. Данный алгоритм шифрования предложен указанными выше авторами и ими же представлены результаты анализа лавинного эффекта и статистической безопасности в других статьях. В ходе исследовательской работы был проведен линейный криптоанализ на полнораундовый алгоритм, в результате которого установлено, что криптостойкость алгоритма шифрования ISL_LWC имеет высокий уровень безопасности к указанному виду криптоанализа.

Ключевые слова: легковесный алгоритм шифрования; криптографическая стойкость; линейный криптоанализ

1 Введение

Линейный криптоанализ – это один из методов криптоанализа, основанный на использовании статистических свойств линейных соотношений между входными и выходными данными. Он применяется для оценки криптостойкости алгоритмов шифрования. Цель линейного криптоанализа состоит в поиске линейных аппроксимаций, которые позволяют

определить биты ключа или другие секретные параметры алгоритма. Используя эти аппроксимации, криптоаналитик может узнать часть информации о ключе или использовать их для других атак. Для защиты от линейного криптоанализа криптографы применяют различные методы и техники, такие как использование нелинейных S-блоков, добавление раундовых ключей и т.д., чтобы создать нелинейности и усложнить построение эффективных линейных аппроксимаций [1, 2, 3].

Структурная схема рассматриваемого легковесного алгоритма шифрования
ISL_LWC приведена в работе [4]. Основные параметры алгоритма следующие: длина блока – 64 бита, длина ключа – 80 бит, количество раундов шифрования – 16. В алгоритме используются преобразования SP, сложения по модулю 2 (операция XOR), циклический сдвиг, нелинейные преобразование S-блока в виде S-box. Процесс шифрования данных осуществляется по конструкции сети Фейстеля.

2 Криптоанализ алгоритма шифрования ISL_LWC

Алгоритм шифрования ISL_LWC оценивается линейным методом криптоанализа. Поскольку метод основан на нелинейных функциях, сначала проводится анализ нелинейных функций по отдельности. Поэтому, можно выделять нелинейные функции из схемы данного алгоритма, классифицировать или комбинировать их так, чтобы это было удобно для анализа, а рассмотрение выбирать так, чтобы оно

не влияло на результаты анализа. Поскольку преобразование S состоит из двух четырехбитных S-блоков, его можно рассматривать как один восьмибитный S-блок или как два четырехбитных S-блока, так как результат анализа одинаков. SP-преобразование расматривается как четыре четырехбитных S-блока.

Таблица 1. Четыре S-блока преобразования SP

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
S_1	4	7	B	5	2	6	E	8	9	C	1	A	0	F	D	3
S_2	F	9	B	2	3	4	1	D	0	A	5	6	8	C	7	E
S_3	2	5	8	0	E	3	A	F	D	4	B	7	6	9	1	C
S_4	F	0	C	1	5	9	2	3	D	6	4	E	8	A	7	B

Поскольку линейные уравнения получены из нелинейных уравнений и в схеме алгоритма нелинейную функцию представляет S-блок, оцениваем только полученные линейные уравнения. В приближенных линейных уравнениях, которые попытаемся составить, стараемся обеспечить минимальное участия S-блоков. Рассмотрим четыре 16-битные части в каждом раунде по отдельности. Для первого раунда вероятность линейного уравнения, полученного с первой частью ввода (или первыми шестнадцатью битами ввода) и с третьей части вывода (или шестнадцатью битами вывода $y_{32}y_{33}\dots y_{47}$), равна $\frac{3}{4}$, а для остальных раундов равна $p_{i+1,3} = \frac{3}{4} \cdot p_{i,1}$. Здесь $p_{i,j}$ – результат j-й части i-го раунда.

Вероятность линейного уравнения, полученного с первой и второй частью входных данных и с четвертой части выходных данных для первого раунда равна $\frac{3}{4}$, а для остальных раундов $p_{i+1,4} = \frac{3}{4} \cdot p_{i,1} \cdot p_{i,2}$. Вероятность линейного уравнения, полученного с первой и четвертой частей входных

данных и со второй части выходных данных для первого раунда равна $\frac{9}{16}$, а для остальных раундов $p_{i+1,2} = \frac{9}{16} \cdot p_{i,1} \cdot p_{i,4}$.

Вероятность линейного уравнения, полученного с первой, второй и третьей частей входных данных и с первой части выходных данных для первого раунда равна $\frac{9}{16}$, для остальных раундов $p_{i+1,1} = \frac{9}{16} \cdot p_{i,1} \cdot p_{i,2} \cdot p_{i,3}$.

Теперь, используя вышеуказанные вероятности, построим наиболее вероятные уравнения, определяющие ключ для пары, состоящей из открытого и закрытого текста. При построении искомого уравнения, вариантов выбора открытых и закрытых составляющих пар очень много, проиллюстрируем это на следующим примере. Пусть $a_0a_1 \ldots a_{63}$ представляет собой открытый текст (биты открытого текста);

$c_0c_1 \ldots c_{63}$ – закрытый текст (биты закрытого текста);

$k_{i0}k_{i1} \ldots k_{i63}$ – ключ i-го раунда (биты ключа i-го раунда);

$x_0x_1 \ldots x_{63}$ и $y_0y_1 \ldots y_{63}$ – раундовые входные (входные биты) и выходые (выходные биты) данные, соответственно.

В результате анализа с вероятностью истинности уравнения 0,75 всего получается 180 уравнений, так как из операций S_1, S_2 и P образуются следующие четыре композиции $P \circ S_1$, $P \circ S_2$, $S_1 \circ P$, $S_2 \circ P$. Поэтому, от каждой из шести следующих нелинейных функций получаем 30 уравнений с наибольшим вероятностным отклонением.

$$P \circ S_1(x \oplus k) : 47b526e89c1a0fd3, \tag{1.1}$$

$$P \circ S_2(x \oplus k) : f9b2341d0a568c7e, \tag{1.2}$$

$$S_1 \circ P(x \oplus k) : 2580e3afd4b7691c, \tag{1.3}$$

$$S_2 \circ P(x \oplus k) : f0c15923d64e8a7b, \tag{1.4}$$

$$S_1(x \oplus k) : 2ed68ab153490f7c, \tag{1.5}$$

$$S_2(x \oplus k) : f5d8c247096a13eb. \tag{1.6}$$

Когда рассматривается уравнение, полученное с участием первых шестнадцати битов открытого текста и первых шестнадцати битов закрытого текста, в нем всего задействовано восемь бит из пары открытого и закрытого текста – четыре бита с каждого, остальные биты – значения раундового ключа, которые задействованы как переменные. В нашем случае, при получении уравнений удобно составлять уравнение не от входа к выходу, а наоборот – от выхода к входу. В программе, предназначенной для получения уравнений из закрытого текста в открытый текст, позиции участвующих переменных в каждом раунде выбираются по следующему соответствию:

15 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
8 0 0 0 0 0 0 1 0 0 2 0 0 0 0 0 0
11 0 0 10 0 0 5 0 0 9 0 0 0 0 0 7
11 3 4 11 6 0 7 0 0 10 9 0 0 0 0 4
11 11 2 11 6 5 7 7 4 10 3 1 0 9 0 12
12 11 4 11 6 9 7 9 3 10 3 5 1 9 5 12
12 11 2 9 6 5 3 9 3 1 3 1 6 9 6 12
12 8 12 9 1 9 3 9 3 1 6 5 1 9 6 3
10 8 9 9 1 3 3 5 9 1 6 1 6 7 6 3
10 8 10 2 1 4 5 5 9 6 6 5 4 7 1 3
10 12 10 10 9 5 5 5 9 6 3 6 12 7 1 4
10 3 2 10 6 5 5 4 7 6 9 6 1 5 1 4
11 11 4 10 6 9 5 7 4 6 9 5 1 9 12 4
12 11 2 11 6 5 7 9 3 10 9 1 6 9 5 4
12 11 4 9 6 9 3 9 3 1 3 5 1 9 6 12
12 8 10 9 1 5 3 9 3 1 6 1 6 9 6 3

Далее, с помощью вышеуказанного соответствия рассмотрим получение необходимых нам уравнений, состоящих шестнадцати шагов. Представленная последовательность, состоящая из 16 строк и 16 столбцов, представляет из себя входную последовательность участвующих переменных, полученных с помощью программы. 16 уравнений получаются за счет наибольшой вероятности линейной аппроксимации S-блока с 16 шагами от 16 раунда до 1 раунда.

Шаг 1. Вероятность истины уравнения равна 0,5625. Подходящее уравнение для шестнадцатого раунда, полученное из выхода первой части и первой, второй и третьей частей входа имеет следующий вид:

$$c_0 \oplus c_1 \oplus c_2 \oplus c_3 \oplus k_{16,0} \oplus k_{16,1} \oplus k_{16,2} \oplus k_{16,3}$$
$$= x_0 \oplus k_{15,0} \oplus x_{27} \oplus k_{15,27} \oplus x_{42} \oplus k_{15,42} \oplus 1.$$

Шаг 2. Вероятность истины уравнения равна 0.100113. Уравнение для пятнадцатого раунда, полученное из входа битов в позициях 0, 27, 42 и из выхода битов в позициях 0, 2, 3, 12, 14, 25, 27, 36, 39, 61, 62, 63:

$$x_0 \oplus x_{27} \oplus x_{42}$$
$$= y_0 \oplus y_2 \oplus y_3 \oplus k_{14,0} \oplus k_{14,2} \oplus k_{14,3}$$
$$\oplus y_{12} \oplus y_{14} \oplus k_{14,12} \oplus k_{14,14} \oplus y_{25}$$
$$\oplus y_{27} \oplus k_{14,25} \oplus k_{14,27} \oplus y_{36} \oplus y_{39}$$
$$\oplus k_{14,36} \oplus k_{14,39} \oplus y_{61} \oplus y_{62} \oplus y_{63}$$
$$\oplus k_{14,61} \oplus k_{14,62} \oplus k_{14,63} \oplus 1.$$

Шаг 3. Вероятность истины уравнения равна 0.013363. Уравнение в четырнадцатом раунде:

$$y_0 \oplus y_2 \oplus y_3 \oplus y_{12} \oplus y_{14} \oplus y_{25}$$

$$\oplus y_{27} \oplus y_{36} \oplus y_{39} \oplus y_{61} \oplus y_{62} \oplus y_{63}$$
$$= x_0 \oplus x_2 \oplus x_3 \oplus k_{13,0} \oplus k_{13,2} \oplus k_{13,3}$$
$$\oplus x_6 \oplus x_7 \oplus k_{13,6} \oplus k_{13,7}$$
$$\oplus x_9 \oplus x_{12} \oplus k_{13,9} \oplus k_{13,12} \oplus x_{14} \oplus x_{15}$$
$$\oplus k_{13,14} \oplus k_{13,15} \oplus x_{17} \oplus x_{18} \oplus k_{13,17}$$
$$\oplus k_{13,18} \oplus x_{25} \oplus x_{26} \oplus x_{27} \oplus k_{13,25}$$
$$\oplus k_{13,26} \oplus k_{13,27} \oplus x_{36} \oplus x_{38} \oplus k_{13,36}$$
$$\oplus k_{13,38} \oplus x_{40} \oplus x_{43} \oplus k_{13,40} \oplus k_{13,43}$$
$$\oplus x_{61} \oplus k_{13,61}.$$

Шаг 4. Для тринадцатого раунда получаем следующее уравнение с вероятностью 0.003171:

$$x_0 \oplus x_2 \oplus x_3 \oplus x_6 \oplus x_7 \oplus x_9$$
$$\oplus x_{12} \oplus x_{14} \oplus x_{15} \oplus x_{17} \oplus x_{18}$$
$$\oplus x_{25} \oplus x_{26} \oplus x_{27} \oplus x_{36} \oplus x_{38}$$
$$\oplus x_40 \oplus x_{43} \oplus x_{61}$$
$$= y_0 \oplus y_2 \oplus y_3 \oplus k_{12,0} \oplus k_{12,2} \oplus k_{12,3}$$
$$\oplus y_4 \oplus y_6 \oplus y_7 \oplus k_{12,4} \oplus k_{12,6}$$
$$\oplus k_{12,7} \oplus y_{10} \oplus k_{12,10} \oplus y_{12} \oplus y_{14}$$
$$\oplus y_{15} \oplus k_{12,12} \oplus k_{12,14} \oplus k_{12,15} \oplus y_{17}$$
$$\oplus y_{18} \oplus k_{12,17} \oplus k_{12,18} \oplus y_{21} \oplus y_{23}$$
$$k_{12,21} \oplus k_{12,23} \oplus y_{25} \oplus y_{26} \oplus y_{27} \oplus k_{12,25}$$
$$\oplus k_{12,26} \oplus k_{12,27} y_{29} \oplus y_{30} \oplus y_{31} \oplus k_{12,29}$$
$$\oplus k_{12,30} \oplus k_{12,31} \oplus y_{33} \oplus k_{12,33} \oplus y_{36}$$
$$\oplus y_{38} \oplus k_{12,36} \oplus k_{12,38} \oplus y_{42} \oplus y_{43}$$
$$\oplus k_{12,42} \oplus k_{12,43} \oplus y_{47} \oplus k_{12,47} \oplus y_{52}$$
$$\oplus y_{55} \oplus k_{12,52} \oplus k_{12,55} \oplus y_{60} \oplus y_{61}$$

$$\oplus k_{12,60} \oplus k_{12,61}.$$

Шаг 5. Для двенадцатого раунда получаем уравнение с вероятностью 0.001003:

$$\begin{gathered}
y_0 \oplus y_2 \oplus y_3 \oplus y_4 \oplus y_6 \oplus y_7 \\
\oplus y_{10} \oplus y_{12} \oplus y_{14} \oplus y_{15} \oplus y_{17} \\
\oplus y_{18} \oplus y_{21} \oplus y_{23} \oplus y_{25} \oplus y_{26} \\
\oplus y_{27} \oplus y_{29} \oplus y_{30} \oplus y_{31} \oplus y_{33} \\
\oplus y_{36} \oplus y_{38} \oplus y_{42} \oplus y_{43} \oplus y_{47} \\
\oplus y_{52} \oplus y_{55} \oplus y_{60} \oplus y_{61} \\
= x_0 \oplus x_1 \oplus k_{11,0} \oplus k_{11,1} \oplus x_4 \oplus x_6 \\
\oplus x_7 \oplus k_{11,4} \oplus k_{11,6} \oplus k_{11,7} \oplus x_9 \\
\oplus k_{11,9} \oplus x_{12} \oplus x_{14} \oplus x_{15} \oplus k_{11,12} \\
\oplus k_{11,14} \oplus k_{11,15} \oplus x_{17} \oplus x_{18} \oplus k_{11,17} \\
\oplus k_{11,18} \oplus x_{20} \oplus x_{23} \oplus k_{11,20} \oplus k_{11,23} \\
\oplus x_{25} \oplus x_{26} \oplus x_{27} \oplus k_{11,25} \oplus k_{11,26} \\
\oplus k_{11,27} \oplus x_{28} \oplus x_{31} \oplus k_{11,28} \oplus k_{11,31} \\
\oplus x_{34} \oplus x_{35} \oplus k_{11,34} \oplus k_{11,35} \oplus x_{36} \\
\oplus x_{38} \oplus k_{11,36} \oplus k_{11,38} \oplus x_{42} \oplus x_{43} \\
\oplus k_{11,42} \oplus k_{11,43} \oplus x_{45} \oplus x_{47} \oplus k_{11,45} \\
\oplus k_{11,47} \oplus x_{51} \oplus k_{11,51} \oplus x_{52} \oplus x_{55} \\
\oplus k_{11,52} \oplus k_{11,55} \oplus x_{57} \oplus x_{59} \oplus k_{11,57} \\
\oplus k_{11,59} \oplus x_{60} \oplus x_{61} \oplus k_{11,60} \oplus k_{11,61}.
\end{gathered}$$

Шаг 6. Для одиннадцатого раунда получаем уравнение с вероятностью 0.001003:

$$x_0 \oplus x_1 \oplus x_4 \oplus x_6 \oplus x_7 \oplus x_9$$

$$\oplus x_{12} \oplus x_{14} \oplus x_{15} \oplus x_{17} \oplus x_{18}$$
$$\oplus x_{20} \oplus x_{23} \oplus x_{25} \oplus x_{26} \oplus x_{27}$$
$$\oplus x_{28} \oplus x_{31} \oplus x_{34} \oplus x_{35} \oplus x_{36}$$
$$\oplus x_{38} \oplus x_{42} \oplus x_{43} \oplus x_{45} \oplus x_{47}$$
$$\oplus x_{51} \oplus x_{52} \oplus x_{55} \oplus x_{57} \oplus x_{59}$$
$$\oplus x_{60} \oplus x_{61}$$
$$= y_0 \oplus y_1 \oplus k_{10,0} \oplus k_{10,1} \oplus y_4 \oplus y_6$$
$$\oplus y_7 \oplus k_{10,4} \oplus k_{10,6} \oplus k_{10,7} \oplus y_{10}$$
$$\oplus k_{10,10} \oplus y_{12} \oplus y_{15} \oplus k_{10,12} \oplus k_{10,15}$$
$$\oplus y_{17} \oplus y_{18} k_{10,17} \oplus k_{10,18} \oplus y_{21} \oplus y_{23}$$
$$\oplus k_{10,21} \oplus k_{10,23} \oplus y_{26} \oplus y_{27} \oplus k_{10,26}$$
$$\oplus k_{10,27} \oplus y_{28} \oplus y_{31} \oplus k_{10,28} \oplus k_{10,31}$$
$$\oplus y_{34} \oplus y_{35} \oplus k_{10,34} \oplus k_{10,35} \oplus y_{39}$$
$$\oplus k_{10,39} \oplus y_{42} \oplus y_{43} \oplus k_{10,42} \oplus k_{10,43}$$
$$\oplus y_{47} \oplus k_{10,47} \oplus y_{49} \oplus y_{50} \oplus k_{10,49}$$
$$\oplus k_{10,50} \oplus y_{52} \oplus y_{55} \oplus k_{10,52} \oplus k_{10,55}$$
$$\oplus y_{57} \oplus y_{58} \oplus k_{10,57} \oplus k_{10,58} \oplus y_{60}$$
$$\oplus y_{61} \oplus k_{10,60} \oplus k_{10,61}.$$

Шаг 7. Для десятого раунда получаем уравнение с вероятностью 0.001003:

$$y_0 \oplus y_1 \oplus y_4 \oplus y_6 \oplus y_7 \oplus y_{10}$$
$$\oplus y_{12} \oplus y_{15} \oplus y_{17} \oplus y_{18} \oplus y_{21}$$
$$\oplus y_{23} \oplus y_{26} \oplus y_{27} \oplus y_{28} \oplus y_{31}$$
$$\oplus y_{34} \oplus y_{35} \oplus y_{39} \oplus y_{42} \oplus y_{43}$$
$$\oplus y_{47} \oplus y_{49} \oplus y_{50} \oplus y_{52} \oplus y_{55}$$
$$\oplus y_{57} \oplus y_{58} \oplus y_{60} \oplus y_{61}$$

$$= x_0 \oplus x_1 \oplus k_{9,0} \oplus k_{9,1} \oplus x_4 \oplus k_{9,4}$$
$$\oplus x_8 \oplus x_9 \oplus k_{9,8} \oplus k_{9,9} \oplus x_{12}$$
$$\oplus x_{15} \oplus k_{9,12} \oplus k_{9,15} \oplus x_{19} \oplus k_{9,19}$$
$$\oplus x_{20} \oplus x_{23} \oplus k_{9,20} \oplus k_{9,23} \oplus x_{26}$$
$$\oplus x_{27} k_{9,26} \oplus k_{9,27} \oplus x_{28} \oplus x_{31} \oplus k_{9,28}$$
$$\oplus k_{9,31} \oplus x_{34} \oplus x_{35} \oplus k_{9,34} \oplus k_{9,35}$$
$$\oplus x_{39} \oplus k_{9,39} \oplus x_{41} \oplus x_{42} \oplus k_{9,41}$$
$$\oplus k_{9,42} \oplus x_{45} \oplus x_{47} \oplus k_{9,45} \oplus k_{9,47}$$
$$\oplus x_{51} \oplus k_{9,51} \oplus x_{52} \oplus x_{55} \oplus k_{9,52}$$
$$\oplus k_{9,55} \oplus x_{57} \oplus x_{58} \oplus k_{9,57} \oplus k_{9,58}$$
$$\oplus x_{62} \oplus x_{63} \oplus k_{9,62} \oplus k_{9,63}.$$

Шаг 8. Для девятого раунда получаем уравнение с вероятностью 0.001003:

$$x_0 \oplus x_1 \oplus x_4 \oplus x_8 \oplus x_9 \oplus x_{12}$$
$$\oplus x_{15} \oplus x_{19} \oplus x_{20} \oplus x_{23} \oplus x_{26}$$
$$\oplus x_{27} \oplus x_{28} \oplus x_{31} \oplus x_{34} \oplus x_{35}$$
$$\oplus x_{39} \oplus x_{41} \oplus x_{42} \oplus x_{45} \oplus x_{47}$$
$$\oplus x_{51} \oplus x_{52} \oplus x_{55} \oplus x_{57} \oplus x_{58}$$
$$\oplus x_{62} \oplus x_{63}$$
$$= y_0 \oplus y_2 \oplus k_{8,0} \oplus k_{8,2} \oplus y_4 \oplus k_{8,4}$$
$$\oplus y_8 \oplus y_{11} \oplus k_{8,8} \oplus k_{8,11} \oplus y_{12}$$
$$\oplus y_{15} \oplus k_{8,12} \oplus k_{8,15} \oplus y_{16} \oplus k_{8,16}$$
$$\oplus y_{22} \oplus y_{23} \oplus k_{8,22} \oplus k_{8,23} \oplus y_{26}$$
$$\oplus y_{27} \oplus k_{8,26} \oplus k_{8,27} \oplus y_{29} \oplus y_{31}$$
$$\oplus k_{8,29} \oplus k_{8,31} \oplus y_{32} \oplus y_{35} \oplus k_{8,32}$$
$$\oplus k_{8,35} \oplus y_{39} \oplus k_{8,39} \oplus y_{41} \oplus y_{42}$$

$$\oplus k_{8,41} \oplus k_{8,42} \oplus y_{47} \oplus k_{8,47} \oplus y_{49}$$
$$\oplus y_{50} \oplus k_{8,49} \oplus k_{8,50} \oplus y_{53} \oplus y_{54}$$
$$\oplus y_{55} \oplus k_{8,53} \oplus k_{8,54} \oplus k_{8,55} \oplus y_{57}$$
$$\oplus y_{58} \oplus k_{8,57} \oplus k_{8,58} \oplus y_{62} \oplus y_{63}$$
$$\oplus k_{8,62} \oplus k_{8,63}.$$

Шаг 9. Для восьмого раунда получаем уравнение с вероятностью 0.001003:

$$y_0 \oplus y_2 \oplus y_4 \oplus y_8 \oplus y_{11} \oplus y_{12}$$
$$\oplus y_{15} \oplus y_{16} \oplus y_{22} \oplus y_{23} \oplus y_{26}$$
$$\oplus y_{27} \oplus y_{29} \oplus y_{31} \oplus y_{32} \oplus y_{35}$$
$$\oplus y_{39} \oplus y_{41} \oplus y_{42} \oplus y_{47} \oplus y_{49}$$
$$\oplus y_{50} \oplus y_{53} \oplus y_{54} \oplus y_{55} \oplus y_{57}$$
$$\oplus y_{58} \oplus y_{62} \oplus y_{63}$$
$$= x_0 \oplus x_2 \oplus k_{7,0} \oplus k_{7,2} \oplus x_4 \oplus k_{7,4}$$
$$\oplus x_8 \oplus x_{10} \oplus k_{7,8} \oplus k_{7,10} \oplus x_{14}$$
$$\oplus k_{7,14} \oplus x_{19} \oplus k_{7,19} \oplus x_{21} \oplus k_{7,21}$$
$$\oplus x_{25} \oplus x_{27} \oplus k_{7,25} \oplus k_{7,27} \oplus x_{29}$$
$$\oplus x_{31} \oplus k_{7,29} \oplus k_{7,31} \oplus x_{32} \oplus x_{35}$$
$$\oplus k_{7,32} \oplus k_{7,35} \oplus x_{37} \oplus x_{38} \oplus k_{7,37}$$
$$\oplus k_{7,38} \oplus x_{41} \oplus x_{42} \oplus k_{7,41} \oplus k_{7,42}$$
$$\oplus x_{45} \oplus x_{47} \oplus k_{7,45} \oplus k_{7,47} \oplus x_{49}$$
$$\oplus k_{7,49} \oplus x_{53} \oplus x_{54} \oplus x_{55} \oplus k_{7,53}$$
$$\oplus k_{7,54} \oplus k_{7,55} \oplus x_{59} \oplus k_{7,59} \oplus x_{62}$$
$$\oplus x_{63} \oplus k_{7,62} \oplus k_{7,63}.$$

Шаг 10. Для седьмого раунда получаем уравнение с ве-

роятностью 0.001003:

$$x_0 \oplus x_2 \oplus x_4 \oplus x_8 \oplus x_{10} \oplus x_{14}$$
$$\oplus x_{19} \oplus x_{21} \oplus x_{25} \oplus x_{27} \oplus x_{29}$$
$$\oplus x_{31} \oplus x_{32} \oplus x_{35} \oplus x_{37} \oplus x_{38}$$
$$\oplus x_{41} \oplus x_{42} \oplus x_{45} \oplus x_{47} \oplus x_{49}$$
$$\oplus x_{53} \oplus x_{54} \oplus x_{55} \oplus x_{59} \oplus x_{62}$$
$$\oplus x_{63}$$
$$= y_0 \oplus y_2 \oplus k_{6,0} \oplus k_{6,2} \oplus y_4$$
$$\oplus y_5 \oplus k_{6,4} \oplus k_{6,5} \oplus y_8 \oplus y_{10}$$
$$\oplus k_{6,8} \oplus k_{6,10} \oplus y_{12}y_{14} \oplus k_{6,12} \oplus k_{6,14}$$
$$\oplus y_{16} \oplus y_{19} \oplus k_{6,16} \oplus k_{6,19} \oplus y_{21}$$
$$\oplus y_{23} \oplus k_{6,21} \oplus k_{6,23} \oplus y_{25} \oplus y_{27}$$
$$\oplus k_{6,25} \oplus k_{6,27} \oplus y_{29} \oplus y_{31} \oplus k_{6,29}$$
$$\oplus k_{6,31} \oplus y_{32} \oplus y_{35} \oplus k_{6,32} \oplus k_{6,35}$$
$$\oplus y_{37} \oplus y_{38} \oplus k_{6,37} \oplus k_{6,38} \oplus y_{42}$$
$$\oplus y_{43} \oplus k_{6,42} \oplus k_{6,43} \oplus y_{45} \oplus y_{46}$$
$$\oplus k_{6,45} \oplus k_{6,46} \oplus y_{48} \oplus y_{49} \oplus k_{6,48}$$
$$\oplus k_{6,49} \oplus y_{53} \oplus y_{54} \oplus y_{55} \oplus k_{6,53}$$
$$\oplus k_{6,54} \oplus k_{6,55} \oplus y_{59}$$
$$\oplus k_{6,59} \oplus y_{61} \oplus k_{6,61}.$$

Шаг 11. Для шестого раунда получаем уравнение с вероятностью 0.001003:

$$y_0 \oplus y_2 \oplus y_4 \oplus y_5 \oplus y_8 \oplus y_{10}$$
$$\oplus y_{12} \oplus y_{14} \oplus y_{16} \oplus y_{19}y_{21} \oplus y_{23}$$
$$\oplus y_{25} \oplus y_{27} \oplus y_{29} \oplus y_{31} \oplus y_{32}$$
$$\oplus y_{35} \oplus y_{37} \oplus y_{38} \oplus y_{42} \oplus y_{43}$$

$$\oplus y_{45} \oplus y_{46} \oplus y_{48} \oplus y_{49} \oplus y_{53}$$
$$\oplus y_{54} \oplus y_{55} \oplus y_{59} \oplus y_{61}$$
$$= x_0 \oplus x_2 \oplus k_{5,0} \oplus k_{5,2} \oplus x_6 \oplus x_7$$
$$\oplus k_{5,6} \oplus k_{5,7} \oplus x_{10} \oplus k_{5,10} \oplus x_{12}$$
$$\oplus x_{14} \oplus k_{5,12} \oplus k_{5,14} \oplus x_{17} \oplus x_{18}$$
$$\oplus k_{5,17} \oplus k_{5,18} \oplus x_{21} \oplus x_{23} \oplus k_{5,21}$$
$$\oplus k_{5,23} \oplus x_{25} \oplus x_{27} \oplus k_{5,25} \oplus k_{5,27}$$
$$\oplus x_{29} \oplus k_{5,29} \oplus x_{33} \oplus x_{34} \oplus x_{35}$$
$$\oplus k_{5,33} \oplus k_{5,34} \oplus k_{5,35} \oplus x_{37} \oplus x_{38}$$
$$\oplus k_{5,37} \oplus k_{5,38} \oplus x_{40} \oplus x_{43} \oplus k_{5,40}$$
$$\oplus k_{5,43} \oplus x_{45} \oplus x_{46} \oplus k_{5,45} \oplus k_{5,46}$$
$$\oplus x_{51} \oplus k_{5,51} \oplus x_{53} \oplus x_{55} \oplus k_{5,53}$$
$$\oplus k_{5,55} \oplus x_{59} \oplus k_{5,59} \oplus x_{61} \oplus k_{5,61}.$$

Шаг 12. Для пятого раунда получаем уравнение с вероятностью 0.001003:

$$x_0 \oplus x_2 \oplus x_6 \oplus x_7 \oplus x_{10} \oplus x_{12}$$
$$\oplus x_{14} \oplus x_{17} \oplus x_{18} \oplus x_{21} \oplus x_{23}$$
$$\oplus x_{25} \oplus x_{27} \oplus x_{29} \oplus x_{33} \oplus x_{34}$$
$$\oplus x_{35} \oplus x_{37} \oplus x_{38} \oplus x_{40} \oplus x_{43}$$
$$\oplus x_{45} \oplus x_{46} \oplus x_{51} \oplus x_{53} \oplus x_{55}$$
$$\oplus x_59 \oplus x_{61}$$
$$= y_0 \oplus y_2 \oplus y_3 \oplus k_{4,0} \oplus k_{4,2} \oplus k_{4,3}$$
$$\oplus y_4 \oplus y_6 \oplus y_7 \oplus k_{4,4} \oplus k_{4,6}$$
$$\oplus k_{4,7} \oplus y_9 \oplus k_{4,9} \oplus y_{12} \oplus y_{14}$$
$$\oplus k_{4,12} \oplus k_{4,14} \oplus y_{17} \oplus y_{18} \oplus k_{4,17}$$
$$\oplus k_{4,18} \oplus y_{20} \oplus y_{23} \oplus k_{4,20} \oplus k_{4,23}$$

$$\oplus y_{25} \oplus y_{27} \oplus k_{4,25} \oplus k_{4,27} \oplus y_{29}$$
$$\oplus y_{30} \oplus y_{31} \oplus k_{4,29} \oplus k_{4,30} \oplus k_{4,31}$$
$$\oplus y_{33} \oplus k_{4,33} \oplus y_{37} \oplus y_{38} \oplus k_{4,37}$$
$$\oplus k_{4,38} \oplus y_{40} \oplus y_{43} \oplus k_{4,40} \oplus k_{4,43}$$
$$\oplus y_{45} \oplus y_{47} \oplus k_{4,45} \oplus k_{4,47} \oplus y_{51}$$
$$\oplus k_{4,51} \oplus y_{52} \oplus y_{55} \oplus k_{4,52} \oplus k_{4,55}$$
$$\oplus y_{56} \oplus y_{57} \oplus k_{4,56}$$
$$\oplus k_{4,57} \oplus y_{61} \oplus k_{4,61}.$$

Шаг 13. Для четвертого раунда получаем уравнение с вероятностью 0.001003:

$$y_0 \oplus y_2 \oplus y_3 \oplus y_4 \oplus y_6 \oplus y_7$$
$$\oplus y_9 \oplus y_{12} \oplus y_{14} \oplus y_{17} \oplus$$
$$y_{18} \oplus y_{20} \oplus y_{23} \oplus y_{25} \oplus y_{27} \oplus y_{29}$$
$$\oplus y_{30} \oplus y_{31} \oplus y_{33} \oplus y_{37} \oplus y_{38}$$
$$\oplus y_{40} \oplus y_{43} \oplus y_{45} \oplus y_{47} \oplus y_{51}$$
$$\oplus y_{52} \oplus y_{55} \oplus y_{56} \oplus y_{57} \oplus y_{61}$$
$$= x_0 \oplus x_1 \oplus k_{3,0} \oplus k_{3,1} \oplus x_4 \oplus x_6$$
$$\oplus x_7 \oplus k_{3,4} \oplus k_{3,6} \oplus k_{3,7} \oplus x_{10}$$
$$\oplus k_{3,10} \oplus x_{12} \oplus x_{14} \oplus x_{15} \oplus k_{3,12}$$
$$\oplus k_{3,14} \oplus k_{3,15} \oplus x_{17} \oplus x_{18} \oplus k_{3,17}$$
$$\oplus k_{3,18} \oplus x_{21} \oplus x_{23} \oplus k_{3,21} \oplus k_{3,23}$$
$$\oplus x_{25} \oplus x_{26} \oplus x_{27} \oplus k_{3,25} \oplus k_{3,26}$$
$$\oplus k_{3,27} \oplus x_{28} \oplus x_{31} \oplus k_{3,28} \oplus k_{3,31}$$
$$\oplus x_{34} \oplus x_{35} \oplus k_{3,34} \oplus k_{3,35} \oplus x_{36}$$
$$\oplus x_{38} \oplus k_{3,36} \oplus k_{3,38} \oplus x_{40} \oplus x_{43}$$
$$\oplus k_{3,40} \oplus k_{3,43} \oplus x_{47} \oplus k_{3,47} \oplus x_{49}$$

$$\oplus x_{50} \oplus k_{3,49} \oplus k_{3,50} \oplus x_{52} \oplus x_{55}$$
$$\oplus k_{3,52} \oplus k_{3,55} \oplus x_{57} \oplus x_{59} \oplus k_{3,57}$$
$$\oplus k_{3,59} \oplus x_{61} \oplus k_{3,61}.$$

Шаг 14. Для третьего раунда получаем уравнение с вероятностью 0.001003:

$$x_0 \oplus x_1 \oplus x_4 \oplus x_6 \oplus x_7 \oplus x_{10}$$
$$\oplus x_{12} \oplus x_{14} \oplus x_{15} \oplus x_{17} \oplus x_{18}$$
$$\oplus x_{21} \oplus x_{23} \oplus x_{25} \oplus x_{26} \oplus x_{27}$$
$$\oplus x_{28} \oplus x_{31} \oplus x_{34} \oplus x_{35} \oplus x_{36}$$
$$\oplus x_{38} \oplus x_{40} \oplus x_{43} \oplus x_{47} \oplus x_{49}$$
$$\oplus x_{50} \oplus x_{52} \oplus x_{55}$$
$$\oplus x_{57} \oplus x_{59} \oplus x_{61}$$
$$= y_0 \oplus y_1 \oplus k_{2,0} \oplus k_{2,1} \oplus y_4 \oplus y_6$$
$$\oplus y_7 \oplus k_{2,4} \oplus k_{2,6} \oplus k_{2,7} \oplus y_9$$
$$\oplus k_{2,9} \oplus y_{12} \oplus y_{15} \oplus k_{2,12} \oplus k_{2,15}$$
$$\oplus y_{17} \oplus y_{18} \oplus k_{2,17} \oplus k_{2,18} \oplus y_{20}$$
$$\oplus y_{23} \oplus k_{2,20} \oplus k_{2,23} \oplus y_{26} \oplus y_{27}$$
$$\oplus k_{2,26} \oplus k_{2,27} \oplus y_{28} \oplus y_{31} \oplus k_{2,28}$$
$$\oplus k_{2,31} \oplus y_{34} \oplus y_{35} \oplus k_{2,34} \oplus k_{2,35}$$
$$\oplus y_{39} \oplus k_{2,39} \oplus y_{42} \oplus y_{43} \oplus k_{2,42}$$
$$\oplus k_{2,43} \oplus y_{45} \oplus y_{47} \oplus k_{2,45} \oplus k_{2,47}$$
$$\oplus y_{51} \oplus k_{2,51} \oplus y_{52} \oplus y_{55} \oplus k_{2,52}$$
$$\oplus k_{2,55} \oplus y_{57} \oplus y_{58} \oplus k_{2,57} \oplus k_{2,58}$$
$$\oplus y_{60} \oplus y_{61} \oplus k_{2,60} \oplus k_{2,61}.$$

Шаг 15. Для второго получаем уравнение с вероятностью

0.001003:

$$
\begin{gathered}
y_0 \oplus y_1 \oplus y_4 \oplus y_6 \oplus y_7 \oplus y_9 \\
\oplus y_{12} \oplus y_{15} \oplus y_{17} \oplus y_{18} \oplus y_{20} \\
\oplus y_{23} \oplus y_{26} \oplus y_{27} \oplus y_{28} \oplus y_{31} \\
\oplus y_{34} \oplus y_{35} \oplus y_3 9 \oplus y_{42} \oplus y_{43} \\
\oplus y_{45} \oplus y_{47} \oplus y_{51} \oplus y_{52} \oplus y_{55} \\
\oplus y_{57} \oplus y_{58} \oplus y_{60} \oplus y_{61} \\
= x_0 \oplus x_1 \oplus k_{1,0} \oplus k_{1,1} \oplus x_4 \oplus x_6 \\
\oplus x_7 \oplus k_{1,4} \oplus k_{1,6} \oplus k_{1,7} \oplus x_9 \\
\oplus k_{1,9} \oplus x_{12} \oplus x_{15} \oplus k_{1,12} \oplus k_{1,15} \\
\oplus x_{17} \oplus x_{18} \oplus k_{1,17} \oplus k_{1,18} \oplus x_{20} \\
\oplus x_{23} \oplus k_{1,20} \oplus k_{1,23} \oplus x_{26} \oplus x_{27} \\
\oplus k_{1,26} \oplus k_{1,27} \oplus x_{28} \oplus x_{31} \oplus k_{1,28} \\
\oplus k_{1,31} \oplus x_{34} \oplus x_{35} \oplus k_{1,34} \oplus k_{1,35} \\
\oplus x_{39} \oplus k_{1,39} \oplus x_{42} \oplus x_{43} \oplus k_{1,42} \\
\oplus k_{1,43} \oplus x_{45} \oplus x_{47} \oplus k_{1,45} \oplus k_{1,47} \\
\oplus x_{51} \oplus k_{1,51} \oplus x_{52} \oplus x_{55} \oplus k_{1,52} \\
\oplus k_{1,55} \oplus x_{57} \oplus x_{58} \oplus k_{1,57} \oplus k_{1,58} \\
\oplus x_{60} \oplus x_{61} \oplus k_{1,60} \oplus k_{1,61}.
\end{gathered}
$$

Шаг 16. Для первого раунда получаем уравнение с вероятностью 0.001003:

$$
\begin{gathered}
x_0 \oplus x_1 \oplus x_4 \oplus x_6 \oplus x_7 \oplus x_9 \\
\oplus x_{12} \oplus x_{15} \oplus x_{17} \oplus x_{18} \oplus x_{20} \\
\oplus x_{23} \oplus x_{26} \oplus x_{27} \oplus x_{28} \oplus x_{31} \\
\oplus x_{34} \oplus x_{35} \oplus x_{39} \oplus x_{42} \oplus x_{43} \\
\oplus x_{45} \oplus x_{47} \oplus x_{51} \oplus x_{52} \oplus x_{55}
\end{gathered}
$$

$$\oplus x_{57} \oplus x_{58} \oplus x_{60} \oplus x_{61}$$
$$= a_0 \oplus a_1 \oplus k_{0,0} \oplus k_{0,1} \oplus a_4 \oplus k_{0,4}$$
$$\oplus a_8 \oplus a_{10} \oplus k_{0,8} \oplus k_{0,10} \oplus a_{12}$$
$$\oplus a_{15} \oplus k_{0,12} \oplus k_{0,15} \oplus a_{19} \oplus k_{0,19}$$
$$\oplus a_{21} \oplus a_{23} \oplus k_{0,21} \oplus k_{0,23} \oplus a_{26}$$
$$\oplus a_{27} \oplus k_{0,26} \oplus k_{0,27} \oplus a_{28} \oplus a_{31}$$
$$\oplus k_{0,28} \oplus k_{0,31} \oplus a_{34} \oplus a_{35} \oplus k_{0,34}$$
$$\oplus k_{0,35} \oplus a_{39} \oplus k_{0,39} \oplus a_{41} \oplus a_{42}$$
$$\oplus k_{0,41} \oplus k_{0,42} \oplus a_{47} \oplus k_{0,47} \oplus a_{49}$$
$$\oplus a_{50} \oplus k_{0,49} \oplus k_{0,50} \oplus a_{52} \oplus a_{55}$$
$$\oplus k_{0,52} \oplus k_{0,55} \oplus a_{57} \oplus a_{58} \oplus k_{0,57}$$
$$\oplus k_{0,58} \oplus a_{62} \oplus a_{63} \oplus k_{0,62} \oplus k_{0,63}.$$

Если рассмотреть общее уравнение для полнораундового алгоритма, то получим вероятностное уравнение, состоящее из значений раундового ключа со значениями некоторых задействованных битов открытого и закрытого текста. В итоге, при объединении уравнений, некоторые уравнения и данные сокращаются. Собирая значения ключа в левую сторону уравнения, а значения открытого и закрытого текста – в правую сторону уравнения, в итоге получаем одно уравнение:

$$k_{16,0} \oplus k_{16,1} \oplus k_{16,2} \oplus k_{16,3} \oplus k_{15,0} \oplus k_{15,27}$$
$$\oplus k_{15,42} \oplus k_{14,0} \oplus k_{14,2} \oplus k_{14,3} \oplus k_{14,12}$$
$$\oplus k_{14,14} \oplus k_{14,25} \oplus k_{14,27} \oplus k_{14,36} \oplus k_{14,39}$$
$$\oplus k_{14,61} \oplus k_{14,62} \oplus k_{14,63} \oplus k_{13,0} \oplus k_{13,2}$$
$$\oplus k_{13,3} \oplus k_{13,6} \oplus k_{13,7} \oplus k_{13,9} \oplus k_{13,12}$$

$$\oplus k_{13,14} \oplus k_{13,15} \oplus k_{13,17} \oplus k_{13,18} \oplus k_{13,25}$$
$$\oplus k_{13,26} \oplus k_{13,27} \oplus k_{13,36} \oplus k_{13,38} \oplus k_{13,40}$$
$$\oplus k_{13,43} \oplus k_{13,61} \oplus k_{12,0} \oplus k_{12,2} \oplus k_{12,3}$$
$$\oplus k_{12,4} \oplus k_{12,6} \oplus k_{12,7} \oplus k_{12,10} \oplus k_{12,12}$$
$$\oplus k_{12,14} \oplus k_{12,15} \oplus k_{12,17} \oplus k_{12,18} \oplus k_{12,21}$$
$$\oplus k_{12,23} \oplus k_{12,25} \oplus k_{12,26} \oplus k_{12,27} \oplus k_{12,29}$$
$$\oplus k_{12,30} \oplus k_{12,31} \oplus k_{12,33} \oplus k_{12,36} \oplus k_{12,38}$$
$$\oplus k_{12,42} \oplus k_{12,43} \oplus k_{12,47} \oplus k_{12,52} \oplus k_{12,55}$$
$$\oplus k_{12,60} \oplus k_{12,61} \oplus k_{11,0} \oplus k_{11,1} \oplus k_{11,4}$$
$$\oplus k_{11,6} \oplus k_{11,7} \oplus k_{11,9} \oplus k_{11,12} \oplus k_{11,14}$$
$$\oplus k_{11,15} \oplus k_{11,17} \oplus k_{11,18} \oplus k_{11,20} \oplus k_{11,23}$$
$$\oplus k_{11,25} \oplus k_{11,26} \oplus k_{11,27} \oplus k_{11,28} \oplus k_{11,31}$$
$$\oplus k_{11,34} \oplus k_{11,35} \oplus k_{11,36} \oplus k_{11,38} \oplus k_{11,42}$$
$$\oplus k_{11,43} \oplus k_{11,45} \oplus k_{11,47} \oplus k_{11,51} \oplus k_{11,52}$$
$$\oplus k_{11,55} \oplus k_{11,57} \oplus k_{11,59} \oplus k_{11,60} \oplus k_{11,61}$$
$$\oplus k_{10,0} \oplus k_{10,1} \oplus k_{10,4} \oplus k_{10,6} \oplus k_{10,7}$$
$$\oplus k_{10,10} \oplus k_{10,12} \oplus k_{10,15} \oplus k_{10,17} \oplus k_{10,18}$$
$$\oplus k_{10,21} \oplus k_{10,23} \oplus k_{10,26} \oplus k_{10,27} \oplus k_{10,28}$$
$$\oplus k_{10,31} \oplus k_{10,34} \oplus k_{10,35} \oplus k_{10,39} \oplus k_{10,42}$$
$$\oplus k_{10,43} \oplus k_{10,47} \oplus k_{10,49} \oplus k_{10,50} \oplus k_{10,52}$$
$$\oplus k_{10,55} \oplus k_{10,57} \oplus k_{10,58} \oplus k_{10,60} \oplus k_{10,61}$$
$$\oplus k_{9,0} \oplus k_{9,1} \oplus k_{9,4} \oplus k_{9,8} \oplus k_{9,9}$$
$$\oplus k_{9,12} \oplus k_{9,15} \oplus k_{9,19} \oplus k_{9,20} \oplus k_{9,23}$$
$$\oplus k_{9,26} \oplus k_{9,27} \oplus k_{9,28} \oplus k_{9,31} \oplus k_{9,34}$$
$$\oplus k_{9,35} \oplus k_{9,39} \oplus k_{9,41} \oplus k_{9,42} \oplus k_{9,45}$$
$$\oplus k_{9,47} \oplus k_{9,51} \oplus k_{9,52} \oplus k_{9,55} \oplus k_{9,57}$$

$$\oplus k_{9,58} \oplus k_{9,62} \oplus k_{9,63} \oplus k_{8,0} \oplus k_{8,2}$$
$$\oplus k_{8,4} \oplus k_{8,8} \oplus k_{8,11} \oplus k_{8,12} \oplus k_{8,15}$$
$$\oplus k_{8,16} \oplus k_{8,22} \oplus k_{8,23} \oplus k_{8,26} \oplus k_{8,27}$$
$$\oplus k_{8,29} \oplus k_{8,31} \oplus k_{8,32} \oplus k_{8,35} \oplus k_{8,39}$$
$$\oplus k_{8,41} \oplus k_{8,42} \oplus k_{8,47} \oplus k_{8,49} \oplus k_{8,50}$$
$$\oplus k_{8,53} \oplus k_{8,54} \oplus k_{8,55} \oplus k_{8,57} \oplus k_{8,58}$$
$$\oplus k_{8,62} \oplus k_{8,63} \oplus k_{7,0} \oplus k_{7,2} \oplus k_{7,4}$$
$$\oplus k_{7,8} \oplus k_{7,10} \oplus k_{7,14} \oplus k_{7,19} \oplus k_{7,21}$$
$$\oplus k_{7,25} \oplus k_{7,27} \oplus k_{7,29} \oplus k_{7,31} \oplus k_{7,32}$$
$$\oplus k_{7,35} \oplus k_{7,37} \oplus k_{7,38} \oplus k_{7,41} \oplus k_{7,42}$$
$$\oplus k_{7,45} \oplus k_{7,47} \oplus k_{7,49} \oplus k_{7,53} \oplus k_{7,54}$$
$$\oplus k_{7,55} \oplus k_{7,59} \oplus k_{7,62} \oplus k_{7,63} \oplus k_{6,0}$$
$$\oplus k_{6,2} \oplus k_{6,4} \oplus k_{6,5} \oplus k_{6,8} \oplus k_{6,10}$$
$$\oplus k_{6,12} \oplus k_{6,14} \oplus k_{6,16} \oplus k_{6,19} \oplus k_{6,21}$$
$$\oplus k_{6,23} k_{6,25} \oplus k_{6,27} \oplus k_{6,29} \oplus k_{6,31} \oplus k_{6,32}$$
$$\oplus k_{6,35} \oplus k_{6,37} \oplus k_{6,38} \oplus k_{6,42} \oplus k_{6,43}$$
$$\oplus k_{6,45} \oplus k_{6,46} \oplus k_{6,48} \oplus k_{6,49} \oplus k_{6,53}$$
$$\oplus k_{6,54} \oplus k_{6,55} \oplus k_{6,59} \oplus k_{6,61} \oplus k_{5,0}$$
$$\oplus k_{5,2} \oplus k_{5,6} \oplus k_{5,7} \oplus k_{5,10} \oplus k_{5,12}$$
$$\oplus k_{5,14} \oplus k_{5,17} \oplus k_{5,18} \oplus k_{5,21} \oplus k_{5,23}$$
$$\oplus k_{5,25} \oplus k_{5,27} \oplus k_{5,29} \oplus k_{5,33} \oplus k_{5,34}$$
$$\oplus k_{5,35} \oplus k_{5,37} \oplus k_{5,38} \oplus k_{5,40} \oplus k_{5,43}$$
$$\oplus k_{5,45} \oplus k_{5,46} \oplus k_{5,51} \oplus k_{5,53} \oplus k_{5,55}$$
$$\oplus k_{5,59} \oplus k_{5,61} \oplus k_{4,0} \oplus k_{4,2} \oplus k_{4,3}$$
$$\oplus k_{4,4} \oplus k_{4,6} \oplus k_{4,7} \oplus k_{4,9} \oplus k_{4,12}$$
$$\oplus k_{4,14} \oplus k_{4,17} \oplus k_{4,18} \oplus k_{4,20} \oplus k_{4,23}$$

$$\oplus k_{4,25} \oplus k_{4,27} \oplus k_{4,29} \oplus k_{4,30} \oplus k_{4,31}$$
$$\oplus k_{4,33} \oplus k_{4,37} \oplus k_{4,38} \oplus k_{4,40} \oplus k_{4,43}$$
$$\oplus k_{4,45} \oplus k_{4,47} \oplus k_{4,51} \oplus k_{4,52} \oplus k_{4,55}$$
$$\oplus k_{4,56} \oplus k_{4,57} \oplus k_{4,61} \oplus k_{3,0} \oplus k_{3,1}$$
$$\oplus k_{3,4} \oplus k_{3,6} \oplus k_{3,7} \oplus k_{3,10} \oplus k_{3,12}$$
$$k_{3,14} \oplus k_{3,15} \oplus k_{3,17} \oplus k_{3,18} \oplus k_{3,21} \oplus k_{3,23}$$
$$\oplus k_{3,25} \oplus k_{3,26} \oplus k_{3,27} \oplus k_{3,28} \oplus k_{3,31}$$
$$\oplus k_{3,34} \oplus k_{3,35} \oplus k_{3,36} \oplus k_{3,38} \oplus k_{3,40}$$
$$\oplus k_{3,43} \oplus k_{3,47} \oplus k_{3,49} \oplus k_{3,50} \oplus k_{3,52}$$
$$\oplus k_{3,55} \oplus k_{3,57} \oplus k_{3,59} \oplus k_{3,61} \oplus k_{2,0}$$
$$\oplus k_{2,1} \oplus k_{2,4} \oplus k_{2,6} \oplus k_{2,7} \oplus k_{2,9}$$
$$\oplus k_{2,12} \oplus k_{2,15} \oplus k_{2,17} \oplus k_{2,18} \oplus k_{2,20}$$
$$\oplus k_{2,23} \oplus k_{2,26} \oplus k_{2,27} \oplus k_{2,28} \oplus k_{2,31}$$
$$\oplus k_{2,34} \oplus k_{2,35} \oplus k_{2,39} \oplus k_{2,42} \oplus k_{2,43}$$
$$\oplus k_{2,45} \oplus k_{2,47} \oplus k_{2,51} \oplus k_{2,52} \oplus k_{2,55}$$
$$\oplus k_{2,57} \oplus k_{2,58} \oplus k_{2,60} \oplus k_{2,61} \oplus k_{1,0}$$
$$\oplus k_{1,1} \oplus k_{1,4} \oplus k_{1,6} \oplus k_{1,7} \oplus k_{1,9}$$
$$\oplus k_{1,12} \oplus k_{1,15} \oplus k_{1,17} \oplus k_{1,18} \oplus k_{1,20}$$
$$\oplus k_{1,23} \oplus k_{1,26} \oplus k_{1,27} \oplus k_{1,28} \oplus k_{1,31}$$
$$\oplus k_{1,34} \oplus k_{1,35} \oplus k_{1,39} \oplus k_{1,42} \oplus k_{1,43}$$
$$\oplus k_{1,45} \oplus k_{1,47} \oplus k_{1,51} \oplus k_{1,52} \oplus k_{1,55}$$
$$\oplus k_{1,57} \oplus k_{1,58} \oplus k_{1,60} \oplus k_{1,61} \oplus k_{0,0}$$
$$\oplus k_{0,1} \oplus k_{0,4} \oplus k_{0,8} \oplus k_{0,10} \oplus k_{0,12}$$
$$\oplus k_{0,15} \oplus k_{0,19} \oplus k_{0,21} \oplus k_{0,23} \oplus k_{0,26}$$
$$\oplus k_{0,27} \oplus k_{0,28} \oplus k_{0,31} \oplus k_{0,34} \oplus k_{0,35}$$
$$\oplus k_{0,39} \oplus k_{0,41} \oplus k_{0,42} \oplus k_{0,47} \oplus k_{0,49}$$

$$\oplus k_{0,50} \oplus k_{0,52} \oplus k_{0,55} \oplus k_{0,57} \oplus k_{0,58}$$
$$\oplus k_{0,62} \oplus k_{0,63}$$
$$= c_0 \oplus c_1 \oplus c_2 \oplus c_3 \oplus a_0 \oplus a_1$$
$$\oplus a_4 \oplus a_8 \oplus a_{10} \oplus a_{12} \oplus a_{15}$$
$$\oplus a_{19} \oplus a_{21} \oplus a_{23} \oplus a_{26} \oplus a_{27}$$
$$\oplus a_{28} \oplus a_{31} \oplus a_{34} \oplus a_{35} \oplus a_{39}$$
$$\oplus a_{41} \oplus a_{42} \oplus a_{47} \oplus a_{49} \oplus a_{50}$$
$$\oplus a_{52} \oplus a_{55} \oplus a_{57}$$
$$\oplus a_{58} \oplus a_{62} \oplus a_{63}.$$

3 Заключение

В последнем уравнении имеются 437 переменных, состоящих из раундовых ключей с вероятностью $3.33 \cdot 10^{-46}$. Как следует из 2-й леммы Мицуру Мацуи, для атаки с вероятностью 0.97 успеха необходимо 2^{276} известных открытых текстов [1]. Это означает, что вероятность намного меньше, чем вероятность угадывания ключа, т.е. атака методом линейного криптоанализа требует больше усилий, чем полный перебор ключей. Исходя, из этого следует, что легковесный алгоритм шифрования ISL_LWC является криптостойким к данному виду криптоанализу.

4 Благодарность

Работа выполнена в рамках проекта грантового финансирования AP14870419 “Разработка средства криптографической защиты информации для защиты переговоров по КВ

связи" Министерства науки и высшего образования Республики Казахстан.

Библиографические ссылки

1. *Matsui M.* Linear Cryptanalysis Method for DES Cipher // LNCS. 1994. Vol. 765. P. 386–397.

2. *Kranz T., Leander G., Wiemer F.* Linear Cryptanalysis: Key Schedules and Tweakable Block Ciphers // IACR Trans. Symmetric Cryptology. 2017. Vol. 1. P. 474–505.

3. *Шнайер Б.* Прикладная криптография. Протоколы, алгоритмы и исходные тексты на языке С. Москва: Триумф, 2003.

4. Development of a New Lightweight Encryption Algorithm / A. Khompysh [et al.] // Int. J. Adv. Comp. Sc. App. 2023. Vol. 14, No. 5. P. 452–459.

ИТЕРАЦИИ СЛУЧАЙНЫХ ОТОБРАЖЕНИЙ КОНЕЧНЫХ МНОЖЕСТВ

А.М. Зубков[1]
[1]*Математический институт им. В.А. Стеклова Российской академии наук*
Москва, РОССИЯ
e-mail: zubkov@mi-ras.ru

Приводится краткий обзор результатов, связанных со структурными свойствами графов случайных отображений конечных множеств и траекторий итераций таких отображений. Рассматриваются свойства как равновероятных, так и некоторых неравновероятных отображений.
Ключевые слова: конечные множества; случайные отображения; итерации отображений

1 Введение

Вопросы, связанные с описанием теоретико-графовой структуры различных модификаций случайных отображений конечных множеств, возникают при решении ряда задач современной криптографии, в частности, при построении теоретико-вероятностных моделей хэш-функций, алгоритмов выработки производных ключей и псевдослучайных последовательностей, при анализе некоторых методов дискретного логарифмирования (ρ-метод Полларда), методов балансировки времени–памяти–данных (метод Хеллмана) и т. п. В работе приводится небольшой обзор результатов, связанных со свойствами итераций случайных отображений.

Пусть $S = \{1, \ldots, N\}$ — конечное множество и $\varphi\colon S \to S$ — отображение этого множества в себя. Отображению φ соответствует ориентированный случайный граф $\Phi = (S, E)$ с множеством вершин S и множеством ребер $(x, \varphi(x))$, $x \in S$. Число различных отображений $S \to S$ равно, очевидно, N^N.

Вершины $x, y \in S$ принадлежат одной связной компоненте графа Φ отображения φ тогда и только тогда, когда существуют такие $s, t \geqslant 0$, что $\varphi^s(x) = \varphi^t(y)$, где $\varphi^t(x)$ обозначает t-кратную итерацию функции φ, $t = 0, 1, \ldots$; $\varphi^0(x) = x$ при любом $x \in S$. Так как в графе Φ отображения φ конечного множества S в себя из каждой вершины выходит ровно одно ориентированное ребро, то каждая связная компонента Φ состоит из одного цикла с подходами, а последовательность $x, \varphi(x), \varphi^2(x), \ldots$ рано или поздно зацикливается. Случайная величина

$$\tau(x) = \min\{t\colon \text{существует такое } u, 0 \leqslant u < t, \text{ что } \varphi^t(x) = \varphi^u(x)\}$$

называется отрезком апериодичности с началом в вершине $x \in S$, а $\lambda(x) = t - u$ — длиной цикла в связной компоненте, содержащей x.

Свойства случайных отображений конечных множеств изучались рядом авторов. Одной из первых обзорных работ по таким задачам была [7], см. также [8]. В большинстве случаев предполагается, что отображение φ случайное и имеет равновероятное распределение на множестве всех отображений множества S в себя, и доказываются предельные теоремы для характеристик таких отображений. В монографии [3] приведен ряд результатов, в том числе отно-

сящихся к структуре и числу компонент графа случайного равновероятного отображения.

2 Некоторые свойства графов случайных отображений и итераций случайных отображений

В [7, 8] приводятся формулы для распределений случайных величин τ и λ как для равновероятных, так и для некоторых неравновероятных отображений. Если отображение φ имеет равновероятное распределение на множестве всех N^N отображений S в себя, а x — любой элемент S, то:

$$\mathbf{P}\{\tau(x) = k\} = \frac{k(N-1)^{k-1}}{N^k},$$

$$\mathbf{P}\{\lambda(x) = j\} = \sum_{k=j}^{N} \frac{k(N-1)^{k-1}}{N^k},$$

$$\mathbf{P}\{\lambda(x) = j \mid \tau(x) = k\} = \frac{1}{k}, \quad j = 1, \ldots, k,$$

$$\lim_{N\to\infty} \mathbf{P}\left\{\tau(x) < z\sqrt{N}\right\} = e^{-z^2/2},$$

$$\lim_{N\to\infty} \mathbf{P}\left\{\lambda(x) < z\sqrt{N}\right\} = 1 - e^{-z^2/2} + z\sqrt{2\pi}(1 - \Phi(z)),$$

где $\Phi(z)$ — функция стандартного нормального распределения.

Точные формулы для распределения числа ρ связных компонент графа Φ случайного равновероятного отображения φ весьма громоздки, но

$$\mathbf{E}\rho = \sum_{m=1}^{N} \frac{1}{m} \sim \ln N, \quad N \to \infty,$$

и распределение ρ при $N \to \infty$ асимптотически нормально с параметрами $(\ln N, \ln N)$ (см. [3]), а максимальная связная компонента содержит $\beta_N N$ вершин и β_N имеет невырожденное предельное распределение на отрезке [0, 1], которое описывается довольно сложной формулой.

С теоретической и прикладной точек зрения представляет интерес вопрос о том, с какой вероятностью заданные элементы множества S принадлежат одной связной компоненте случайного отображения $\varphi\colon S \to S$. В случае равновероятных отображений ответ на этот вопрос содержится в следующий теореме.

Теорема 1. *Если*

$$H_N^k = \{\textit{вершины } 1, \ldots, k \textit{ лежат в одной связной компоненте графа } \Phi\},$$

то

$$\mathbf{P}\{H_N^k\} \to \frac{2^{2k-1}(k!)^2}{k(2k)!} = \frac{(2k-2)!!}{(2k-1)!!}, \quad N \to \infty,$$

где $m!! = \prod_{j=0}^{[m/2]-1}(m-2j)$.

Легко проверить, что

$$\frac{2^{2k-1}(k!)^2}{k(2k)!} = \frac{2}{3}$$

при $k = 2$ и

$$\frac{2^{2k-1}(k!)^2}{k(2k)!} \sim \sqrt{\frac{\pi}{k}}$$

при $k \to \infty$.

Для случая $k = 2$ теорема 1 была доказана в статье Б.Питтеля [10], в общем случае — в статье автора и П.В.Халипова [2].

В нескольких работах решались аналогичные задачи для некоторых классов неравновероятных отображений.

В [9] рассматриваются графы Ф случайных отображений $\varphi\colon S \to S$, $S = \{1, \dots, N\}$, для которых случайные величины $\varphi(x), x \in S$, независимы и $\mathbf{P}\{\varphi(x) = i\} = p_{N,i}, i = 1, \dots, N$ (если $p_{N,i} \equiv \frac{1}{N}$, то φ — равновероятное случайное отображение). Для таких отображений φ изучаются совместные распределения случайных величин $\tau(\alpha)$ — отрезка апериодичности, начинающегося в вершине $\alpha \in S$, $\lambda(\alpha)$ — длины цикла на этом отрезке, и $\kappa(\alpha) = \sum_{x \in \Lambda(\alpha)} p_{N,x}$, где $\Lambda(\alpha)$ — связная компонента графа Ф, содержащая α; при этом α — случайный элемент S, имеющий распределение $\{p_{N,x}, x \in S\}$. В [9] доказано следующее утверждение.

Теорема 2. *Если*

$$c_N = \left(\sum_{x=1}^{N} p_{N,x}^2 \right)^{1/2}$$

и

$$\lim_{N \to \infty} \max_{1 \leqslant x \leqslant N} \frac{p_{N,x}}{c_n} = 0,$$

то совместные распределения

$$(\kappa(\alpha), c_n \tau(\alpha), c_n \lambda(\alpha))$$

при $N \to \infty$ сходятся к предельному распределению, не зависящему от распределений $\{p_{N,x}\}$.

Таким образом, предельные распределения в «слабо неравновероятном» случае такие же, как в равновероятном. Получены также оценки скорости сходимости к предельному распределению.

В [1] изучались свойства случайных неравновероятных отображений $\psi\colon S \to S$, являющихся k-кратными итерациями φ^k равновероятного случайного отображения φ. Пусть $\tau_\psi(x) = \tau_{\varphi^k}(x)$ — длина отрезка апериодичности, начинающегося в вершине x.

Теорема 3. *При любых таких $k \geqslant 1$, $x_0 \in S$ и $z \in \{1, \ldots, n\}$, что $kz \leqslant n$, справедливы равенства*

$$\mathbf{P}\{\tau_{\varphi^k}(x_0) \leqslant z\} = \frac{1}{n} \sum_{m \geqslant 1\colon \frac{m}{(m,k)} \leqslant z} \sum_{t=0}^{\left(z - \frac{m}{(m,k)}\right)k} \prod_{i=1}^{m+t-1} \left(1 - \tfrac{i}{N}\right),$$

где (m, k) — наибольший общий делитель m и k. Кроме того,

$$\lim_{n\to\infty} \mathbf{P}\{\tau_{\varphi^k}(x_0) \leqslant z\sqrt{n}\} = \mathbf{P}\left\{\theta \cdot \left(\frac{\gamma}{(\nu, k)} + \frac{1-\gamma}{k}\right) \leqslant z\right\},$$

где случайные величины θ, γ, ν независимы, $\mathbf{P}\{\theta \leqslant x\} = 1 - e^{-x^2/2}$, $x \geqslant 0$, γ имеет равномерное распределение на отрезке $[0, 1]$, а ν имеет равновероятное распределение на $\{1, 2, \ldots, k\}$.

Предельное распределение случайных величин $\tau_{\varphi^k}(x_0)$ при $k = \text{const}$, $n \to \infty$ существенно зависит от множества делителей числа k.

В [5] доказаны следующие утверждения.

Теорема 4. *Пусть случайное отображение $\psi = \varphi^k$. Тогда при любых $k \geqslant 1$, $x, y \in S$, $x \neq y$, справедливо равенство*

$$\mathbf{P}\left\{y \notin \{x, \psi(x), \psi^2(x), \ldots\}\right\}$$
$$= 1 - \sum_{m=1}^{N} \sum_{t=m}^{N} \frac{\left(\left]\frac{t-m}{k}\right[+ \frac{m}{(m,k)} - 1\right) (N-2)_{t-2}}{N^t},$$

где $(M)_t = \frac{M!}{(M-t)!}$, и

$$\mathbf{P}\left\{y \in \Lambda(x)\right\}$$
$$= \sum_{m=1}^{N} \sum_{v=m}^{N} \sum_{s=0}^{N-v} \frac{\left(\left]\frac{v}{(m,k)}\right[- \omega_{m,v,s}\right) (N-2)_{v+s-2}}{N^{v+s}},$$

где

$$\omega_{m,v,s} = \begin{cases} 1, & \text{если } s = 0, \\ \Delta_{(m,k)}^{s,v} & \text{в противном случае,} \end{cases}$$

$$\Delta_m^{s,t} = \begin{cases} 1, & s_{\bmod m} \geqslant t_{\bmod m} > 0, \\ 0 & \text{в противном случае,} \end{cases}$$

и $s_{\bmod m} = s - m\left[\frac{s}{m}\right]$ — наименьший неотрицательный вычет s по модулю m.

В [4] изучались свойства случайных неравновероятных отображений $\psi_d = \varphi_d(\varphi_{d-1}(\ldots(\varphi_1)\ldots))$, где $\varphi_1, \ldots, \varphi_d$ — независимые случайные равновероятные отображения $S \to S$.

Теорема 5. *Для любых $d \geqslant 1$, $z \in \{1, \ldots, N\}$ и $x_0 \in S$ справедливы равенства*

$$\mathbf{P}\{\tau_{\psi_d} \leqslant z\} = 1 - \left(1 - \tfrac{z}{N}\right) \prod_{i=1}^{z-1} \left(1 - \tfrac{i}{N}\right)^d,$$

$$\mathbf{E}\tau_{\psi_d}(x_0) = \sum_{z=0}^{N} \left(1 - \tfrac{z}{N}\right) \prod_{i=1}^{z-1} \left(1 - \tfrac{i}{N}\right)^d.$$

Кроме того,

$$\lim_{N\to\infty} \mathbf{P}\{\tau_{\psi_d} > u\sqrt{2N}\} = e^{-du^2}.$$

Ряд других результатов, относящихся к свойствам итераций отображений φ^k и ψ_d содержится в диссертации В.О.Миронкина [6]

Библиографические ссылки

1. *Зубков А.М., Миронкин В.О.* Распределение длины отрезка апериодичности в графе k-кратной итерации случайного равновероятного отображения // Матем. вопр. криптографии. 2017. Т. 8, Ном. 4. С. 63–74.

2. *Зубков А.М., Халипов П.В.* Вероятность принадлежности нескольких вершин одной связной компоненте случайного равновероятного отображения // Дискретная математика. 2022. Т. 34, Ном. 4. С. 28–35.

3. *Колчин В.Ф.* Случайные отображения. М.: Наука, 1984.

4. *Миронкин В.О.* Распределение длины отрезка апериодичности в графе композиции независимых равновероятных случайных отображений // Математические вопросы криптографии. 2019. Т. 10, Ном. 3. С. 89–99.

5. *Миронкин В.О.* Коллизии и инцидентность вершин компонентам в графе k-кратной итерации равновероятного случайного отображения // Дискретная математика. 2019. Т. 31, Ном. 4. С. 38–52.

6. *Миронкин В.О.* Явные формулы для распределений характеристик итераций случайных отображений. М.: МГУ, 2021.

7. *Harris B.* Probability distributions related to random mappings // The Annals of Mathematical Statistics. 1960. Vol. 31, Iss. 4. P. 1045–1062.

8. *Harris B.* A survey of the early history of the theory of random mappings // Probabilistic Methods in Discrete Mathematics TVP/TSP. 1993. P. 1–22.

9. *O'Cinneide .A., Pokrovskii A.V.* Nonuniform random transformations // Annals of Applied Probability. 2000. Vol. 10, Iss. 4. P. 1151–1181.

10. *Pittel B.* On distibutions related to transitive closures of random finite mappings // Annals of Probability. 1983. Vol. 11, Iss. 2. P. 428–441.

АНАЛИЗ КРИПТОСИСТЕМЫ НА БУЛЕВЫХ ФУНКЦИЯХ

А.В. Кандинский[1], И.А. Панкратова[2]
[1,2]*Национальный исследовательский*
Томский государственный университет
Томск, РОССИЯ
e-mail: [1]reiligan@mail.ru, [2]pank@mail.tsu.ru

Предложены и исследованы атаки с известным и выбираемым открытым текстом на асимметричную криптосистему с функциональным ключом в случае, когда ключ состоит из двух перестановок, и атаки с известным открытым текстом, когда к этому ключу добавляется одна из инверсий.
Ключевые слова: векторная булева функция; криптосистема на булевых функциях; криптоанализ

1 Введение

Рассматривается шифрсистема ACBF (Asymmetric Cryptosystem on Boolean Functions) [1, 2]. Открытые тексты и шифртексты в ней — это булевы векторы длины n; открытый ключ — функция $f : \mathbb{Z}_2^n \to \mathbb{Z}_2^n$; закрытый ключ — функция f^{-1}; шифрование и расшифрование выполняются по правилам $y = f(x)$ и $x = f^{-1}(y)$ соответственно.

Функция f строится так. Выбирается обратимая функция $g : \mathbb{Z}_2^n \to \mathbb{Z}_2^n$ — *порождающая функция криптосистемы*, которую можно рассматривать как векторную функцию $g = (g_1 \dots g_n)$ с координатами — булевыми функциями g_i, $i = 1, \dots, n$; функция f получается из нее с помощью

перестановки и инверсии переменных x_i и координат g_i: $f(x) = \pi_2(g^{\sigma_2}(\pi_1(x^{\sigma_1})))$, где $\sigma_1, \sigma_2 \in \mathbb{Z}_2^n$; $\pi_1, \pi_2 \in \mathbb{S}_n$; $x^{\sigma_1} = x \oplus \sigma_1$; $g^{\sigma_2}(x) = g(x) \oplus \sigma_2$; $\pi_1(x) = x_{\pi_1(1)} \dots x_{\pi_1(n)}$; $\pi_2(g(x)) = g_{\pi_2(1)}(x) \dots g_{\pi_2(n)}(x)$.

В качестве ключевых параметров шифрсистемы ACBF выступают элементы любого непустого подмножества $J \subseteq \{\pi_1, \pi_2, \sigma_1, \sigma_2\}$ (всего 15 вариантов); операции из множества $\{\pi_1, \pi_2, \sigma_1, \sigma_2\} \backslash J$ считаются тождественными.

Рассмотрим атаки с известным и с выбираемым открытым текстом в следующих предположениях:

1. для любого $x \in \mathbb{Z}_2^n$ криптоаналитик может вычислить $g(x)$ и $g^{-1}(x)$;

2. криптоаналитик знает, какие именно из операций $\pi_1, \pi_2, \sigma_1, \sigma_2$ входят в множество J, но их конкретные значения ему не известны; цель — найти эти значения;

3. при атаке с выбираемым открытым текстом криптоаналитик может вычислить $f(x)$ для любого $x \in \mathbb{Z}_2^n$.

В работе [1] в тех же предположениях описаны атаки с известным открытым текстом для всех 15 вариантов подмножеств ключевых параметров, приведены оценки их сложности. В данной работе более подробно рассмотрены атаки с известным открытым текстом на варианты ключа $J = \{\pi_1, \pi_2\}$, $\{\pi_1, \pi_2, \sigma_1\}$ и $\{\pi_1, \pi_2, \sigma_2\}$ и рассмотрена атака с выбираемым открытым текстом для $J = \{\pi_1, \pi_2\}$.

Для поиска перестановки столбцов матрицы введем операцию T над булевыми матрицами $A = ||a_{ij}||$ и $B = ||b_{ij}||$ размера $m \times n$. Построим матрицу $D = ||d_{jk}||$ размера

$n \times n$ [3]:

$$d_{jk} = \bigwedge_{i=1}^{m} a_{ik}^{b_{ij}}, \quad j,k = 1,\ldots,n,$$

Будем обозначать $D = T(A,B)$.

2 Случай $J = \{\pi_1, \pi_2\}$

2.1 Атака с известным открытым текстом

Пусть известны пары «открытый текст — соответствующий шифртекст» (P_i, C_i), $i = 1,\ldots,m$. По определению получаем

$$C_i = f(P_i) = \pi_2(g(\pi_1(P_i))), \quad i = 1,\ldots,m. \tag{1}$$

Атака с известным открытым текстом может быть проведена следующим образом:

1. строим матрицу C со строками C_i, $i = 1,\ldots,m$;
2. перебираем $n!$ подстановок π_1' («кандидатов» в π_1);
3. для каждой π_1' строим матрицу C' со строками $C_i' = g(\pi_1'(P_i))$, $i = 1,\ldots,m$;
4. находим $D = T(C', C)$;
5. если D не является матрицей подстановок [3], то π_1' не может быть частью ключа; иначе все пары (π_1', π_2), где π_2 содержится в D, удовлетворяют системе (1).

Сложность атаки та же, что и у предложенных в [1, 3, 4], — $O(n!)$. Можно сократить перебор подстановок π_1', воспользовавшись инвариантностью веса булева вектора относительно перестановки его координат, а именно: в качестве

«кандидатов» в π_1 рассматривать только такие подстановки π_1', которые удовлетворяют условиям

$$\mathrm{w}(g(\pi_1'(P_i))) = \mathrm{w}(C_i) \tag{2}$$

для $i = 1, \ldots, m$; через $\mathrm{w}(x)$ обозначен вес булева вектора x. Для этого на шаге 3 атаки надо дополнительно проверять условие (2) и прекращать построение матрицы C', переходя к следующей подстановке π_1' сразу же, как только оно нарушится для некоторого $i \in \{1, \ldots, m\}$.

Оценим, сколько в среднем строк матрицы C' будет построено до первого нарушения условия (2), предполагая, что тексты P_i выбираются из $\mathbb{Z}_2^n$ случайно равновероятно (тогда функция f, являясь подстановкой, сохраняет это распределение и для шифртекстов C_i):

1. вероятность того, что вес случайного булева вектора длины n равен k, равна

$$q_{n,k} = \mathrm{C}_n^k / 2^n;$$

2. вероятность совпадения веса двух случайных булевых векторов длины n составляет

$$p_n = \sum_{k=0}^{n} q_{n,k}^2 = 2^{-2n} \sum_{k=0}^{n} \left(\mathrm{C}_n^k\right)^2 = 2^{-2n} \mathrm{C}_{2n}^n;$$

3. математическое ожидание номера попытки, на которой произойдет нарушение условия (2), равно

$$M_n = (1 - p_n)^{-1}.$$

В табл. 1 приведены значения p_n и M_n для $n = 1, \ldots, 16$.

Результаты расчетов показывают эффективность использования в атаке условия (2); это же подтверждается экспериментами.

Таблица 1. Значения p_n и M_n

n	1	2	3	4	5	6	7	8
p_n	0,5	0,375	0,3125	0,27344	0,24609	0,22559	0,20947	0,19638
M_n	2	1,6	1,45455	1,37634	1,32642	1,2913	1,26498	1,24437
n	9	10	11	12	13	14	15	16
p_n	0,18547	0,1762	0,16819	0,16118	0,15498	0,14945	0,14446	0,13995
M_n	1,2277	1,21388	1,20219	1,19215	1,18341	1,1757	1,16886	1,16272

2.2 Атака с выбираемым открытым текстом

Идея атаки состоит в том, чтобы искать подстановки π_1 и π_2 одновременно, используя инвариантность веса булева вектора относительно перестановки его координат:

$$\mathrm{w}(x) = \mathrm{w}(\pi_1(x)); \quad \mathrm{w}(y) = \mathrm{w}(g(\pi_1(x))).$$

Будем вычислять пары $(x, y = f(x))$ и $(a, z = g(a))$ для всех векторов x и a заданного веса $l \in \{0, 1, n-1, n\}$. Если $\mathrm{w}(y) = \mathrm{w}(z)$, то пары (x, a) (при $l = 1$ или $n-1$) и (z, y) могут быть включены в матрицы для поиска подстановок π_1 и π_2 соответственно. Выбор значений l обусловлен небольшим количеством векторов такого веса по сравнению с остальными весами; пары (x, a) при $l = 0$ или n не имеет смысла использовать для поиска подстановки π_1, так как в этих случаях $a = \pi(x)$ для любой подстановки π.

Условие $\mathrm{w}(y) = \mathrm{w}(z)$ при фиксированном y может выполняться для нескольких значений z. В этом случае матрицы для поиска подстановок надо «размножать» и добавлять в копии по одной из подходящих пар. Эксперименты показали, что «экспоненциального взрыва» количества пар матриц не происходит: в среднем во время работы алгоритма приходится хранить не более двух вариантов (P', C').

Если в результате работы алгоритма одна из подстановок π_1 или π_2 определена однозначно, а вторая — нет, то можно найти верный (единственный) ключ, применив атаку с выбираемым открытым текстом из [3, п. 2.1, 2.2].

Пусть $m = \lceil \log n \rceil$, $t = 2^m \geq n$. Построим матрицу размера $m \times t$ со строками

$$(0)^{t/2}(1)^{t/2},$$
$$(0)^{t/4}(1)^{t/4}(0)^{t/4}(1)^{t/4},$$
$$\dots$$
$$(01)^{t/2}.$$

Здесь для булева вектора a и $k \in \mathbb{N}$ через $(a)^k$ обозначена конкатенация k векторов a. Удалим из матрицы любые $(t-n)$ столбцов и обозначим ее через B, а строки — через B_i, $i = 1, \dots, m$.

Если однозначно определена π_1, то построим матрицу C со строками $f(\pi_1^{-1}(g^{-1}(B_i)))$, $i = 1, \dots, m$, и $D_2 = T(B, C)$. Если однозначно определена π_2, то построим матрицу P' со строками $g^{-1}(\pi_2^{-1}(f(B_i)))$, $i = 1, \dots, m$, и $D_1 = T(B, P')$. Все столбцы матрицы B различны, поэтому, согласно [3, замечание 1], D_1 — матрица подстановки π_1, а D_2 — матрица подстановки π_2.

3 Атаки на шифр с трехэлементным ключом

Рассмотрим атаки с известным открытым текстом для случаев, когда ключом являются обе подстановки и одна из инверсий. Общая схема атаки может быть построена следую-

щим образом: один из ключевых параметров перебирается, а на оставшиеся два осуществляется атака, предложенная в [3]. С учетом сложности последней и мощности перебираемого множества выбраны следующие стратегии: перебор π_2, если в ключ входит σ_1, и перебор π_1, если в ключ входит σ_2.

Случай $J = \{\pi_1, \pi_2, \sigma_1\}$

Пусть имеется $m + 1$ пар открытых текстов и шифртекстов вида (P_i, C_i),

$$C_i = \pi_2(g(\pi_1(P_i \oplus \sigma_1))), \quad i = 1, \ldots, m + 1.$$

Идея состоит в том, чтобы перебрать $n!$ «кандидатов» в π_2, для каждого из которых провести атаку на подмножество $\{\pi_1, \sigma_1\}$ со сложностью $O(nm)$, используя свойство линейности подстановок [3].

Атака с известным открытым текстом на ключ $J = \{\pi_1, \pi_2, \sigma_1\}$

Вход: $g : \mathbb{Z}_2^n \to \mathbb{Z}_2^n$; $\{(P_i, C_i) : i = 1, \ldots, m + 1\}$.

Выход: K — множество вероятных ключей (троек (π_1, π_2, σ_1)).

1. $K := \emptyset$.
2. Построить матрицу S со строками $S_i = P_i \oplus P_{m+1}$ и массив W с элементами $w_i = \mathrm{w}(S_i)$, $i = 1, \ldots, m$.
3. Для всех $\pi_2 \in \mathbb{S}_n$:
4. Для всех $i = 1, \ldots, m$: $S'_i := g^{-1}(\pi_2^{-1}(C_i)) \oplus g^{-1}(\pi_2^{-1}(C_{m+1}))$.
5. Если $\mathrm{w}(S'_i) \neq w_i$, переход к п. 10.

6. $D := T(S, S')$.

7. Если D не является матрицей подстановок, переход к п. 10.

8. Для всех π_1, содержащихся в D:

9. $\sigma_1 := P_{m+1} \oplus \pi_1^{-1}(g^{-1}(\pi_2^{-1}(C_{m+1})))$; $K := K \cup \{(\pi_1, \pi_2, \sigma_1)\}$.

10. конец обработки текущей π_2.

Случай $J = \{\pi_1, \pi_2, \sigma_2\}$

Здесь идея атаки аналогична, только перебирать будем подстановки π_1 и искать решение системы уравнений

$$C_i = \pi_2(g(\pi_1(P_i))) \oplus \sigma_2, \quad i = 1, \ldots, m+1,$$

относительно π_1, π_2, σ_2 при данных (P_i, C_i).

Проведен эксперимент с целью определить необходимое количество пар текстов для однозначного нахождения ключа с вероятностью выше 99,95 %, результаты представлены в табл. 2.

Таблица 2. Значения m, необходимые для успеха атаки

	n					
J	4	5	6	7	8	9
$\{\pi_1, \pi_2, \sigma_1\}$	10	13	16	16	17	17
$\{\pi_1, \pi_2, \sigma_2\}$	10	13	15	16	16	16

Библиографические ссылки

1. *Agibalov G.P., Pankratova I.A.* Asymmetric cryptosystems on Boolean functions // Прикладная дискретная математика. 2018. Ном. 40. С. 23–33.

2. *Агибалов Г.П., Панкратова И.А.* Криптосистемы с открытым ключом на булевых функциях // Прикладная дискретная математика. Приложение. 2018. Ном. 11. С. 54–57.

3. *Боровкова И.В., Кондратьев В.А., Панкратова И.А.* Криптоанализ асимметричного шифра на булевых функциях // Прикладная дискретная математика. 2020. Ном. 50. С. 42–50.

4. *Боровкова И.В., Панкратова И.А.* Криптоанализ шифрсистемы ACBF // Прикладная дискретная математика. Приложение. 2019. Ном. 12. С. 90–93.

ДИФФЕРЕНЦИАЛЬНЫЙ КРИПТОАНАЛИЗ ЛЕГКОВЕСНОГО АЛГОРИТМА LBC

Н.А. Капалова[1], К.Т. Алгазы[2], А. Хаумен[3]
[1,2,3]*Институт информационных и вычислительных технологий МНВО РК*
Алматы, КАЗАХСТАН
e-mail: [1]nkapalova@mail.ru, [2]kunbolat@mail.ru, [3]haumen,armanbek@gmail.com

В статье рассматриваются криптографические свойства алгоритма шифрования LBC. Алгоритм является легковесным блочным симметричным шифром, который обеспечивает оптимальный баланс между безопасностью, производительностью и минимальными затратами в отраслях IoT. Данная работа направлена на исследования надежности алгоритма LBC к некоторым методам криптоанализа. В начале дается краткий обзор по данной тематике и описывается метод дифференциального криптоанализа. На основе результатов проведенных статистических анализов и лавинного эффекта, исследования алгоритма производилась на семи раундах шифрования. Перед проведением дифференциального криптоанализа алгоритма рассмотрены дифференциальные свойства используемых преобразований по отдельности. Данный криптоанализ был осуществлен в четыре этапа. На основании проведенных работ установлено, что данный алгоритм имеет надежную криптостойкость относительно дифференциального анализа. Далее легковесный шифр LBC будет программно реализован на разных платформах для анализа и оценки его надежности.

Ключевые слова: алгоритм шифрования; легковесный алгоритм; криптографические преобразования; криптостойкость; дифференциальный криптоанализ

1 Введение

Прошедшее десятилетие в области технологий ознаменовалось постоянно уменьшающимся размером вычислительных устройств. Это, в сочетании с их все более повсеместным использованием, например, в качестве интеллектуальных устройств, носимых систем, как части Интернета вещей, позволило людям выполнять повседневные действия более эффективно. В то же время эти новые технологии также создали новые проблемы в области безопасности.

Важной проблемой сегодня является разработка криптографических алгоритмов, которые были бы одновременно эффективными и безопасными, занимали бы небольшой объем памяти, были недорогими и простыми в реализации и развертывании на несколько платформ. Поиск оптимального компромисса между этими, часто противоречивыми, требованиями является сложной областью, исследуемой в области облегченной криптографии [1]. Области применения облегченных криптографических алгоритмов варьируются от мобильных устройств, от RFID-меток до электронных замков, и их важность, вероятно, продолжит возрастать в будущем. Чтобы удовлетворить постоянную потребность в безопасных и эффективных облегченных примитивах, за последние несколько лет было выдвинуто множество предложений. В области шифрования с симметричным ключом некоторые из наиболее известными блочными шифрами, которые были предложены, являются: Present [2], Piccolo [3], Klein [4], Twine [5], Katan и Ktantan [6], LED [7], HIGHT [8] и CLEFIA [9].

Важным критерием разработки криптографического ал-

горитма – его криптостойкость, способность алгоритма противостоять различным криптографическим атакам. Самыми распространенными методами криптоанализа являются методы линейного и дифференциального криптоанализа.

Блочный шифр считается достаточно безопасным для практического использования после того, как он подвергся обширному криптоанализу. Одним из основных методов, используемых для криптоанализа блочных шифров, является дифференциальный криптоанализ. Дифференциальный криптоанализ был предложен израильскими криптографами Э. Бихамом и А. Шамиром в 1990 году.

Стойкость к дифференциальному криптоанализу считается обязательным критерием разработки любого блочного шифра. Успешная дифференциальная атака основывается на обнаружении высоковероятной дифференциальной характеристики, которая будет использоваться в качестве статистической характеристики для восстановления ключа [10].

Основная идея дифференциального криптоанализа заключается в изучениях разностей между шифруемыми значениями на различных раундах шифрования. Дифференциальная атака предполагает существование упорядоченных пар (α,β) двоичных строк, таких, что m – блок открытого текста, c и c' являются зашифрованными текстами, которые связаны с m и m+α, побитовая разность $c \oplus c'$ с большой вероятностью будет равна β, чем если бы c и c' были случайно выбранными двоичными строками. Такая упорядоченная пара (α,β) называется дифференциалом. Чем больше вероятность дифференциала, тем эф-

фективнее атака. Связанный критерий для (n,m)-функции F, используемой в качестве S-блока в раундовых функциях шифра, состоит в том, что выход для ее производных $D_a(x) = F(x) + F(x + a);\ x, a \in F_n^2$, должен быть распределен как можно более равномерно [11]. При построении блочных шифров, разработчики пытались создавать алгоритмы, защищенные от дифференциального и линейного криптоанализа. В 1992 году Найберг и Кнудсен впервые предложили концепцию доказуемой защиты от дифференциального криптоанализа и продемонстрировали доказуемую защиту для структуры Фейстеля [12].

2 Дифференциальный криптоанализ алгоритма LBC

Основная трудность дифференциального криптоанализа заключается в трудности нахождения правильных пар текстов, которые, в свою очередь напрямую зависит от значения вероятности рассматриваемого дифференциала. Вот почему поиск дифференциала, который имеет наибольшую вероятность, имеет первостепенное значение. Зная разницу в наиболее вероятном дифференциале, мы можем предсказать, насколько успешным будет анализ самого шифра или его сокращенной версии. Это означает определение количества раундов шифрования, для которых все еще возможен дифференциальный криптоанализ [13].

В алгоритме блочного шифрования LBC размер блока составляет 64 бита, длина ключа – 80 бит, количество раундов шифрования – 20.

При шифровании исходный блок открытого текста делится на 4 подблока по 16 бит. Шифрование начинается с добавления первых 64 битов мастер ключа на исходный текст (рис. 1). Далее выполняются раундовые преобразования.

Каждый раунд включает в себя 4 вида преобразования:

– преобразование S;

– преобразование RL;

– преобразование L;

– преобразование K.

Преобразование S. Это преобразование было сконструировано для замены битов блока на другие биты с помощью таблиц (S-блок). Это нелинейное преобразование алгоритма использует операции с полубайтами (4 бита). К каждому полубайту применяется нелинейная биективная подстановка, задаваемая одномерным массивом, состоящим из 16.

Преобразование RL. Линейным преобразованием алгоритма LBC-3 является циклический сдвиг битов и подблоков на определенную позицию. 64 бита входного блока делятся на 4 подблока по 16 битов. Линейное преобразование на уровне подблока осуществляется с помощью функции RL, которая применяется только к первому подблоку (рис. 1). Результат функции RL суммируется со вторым подблоком по модулю 2 (операция XOR). Функция RL имеет следующий вид:

$$RL(a) = a \oplus (a << 7) \oplus (a << 10), \quad a \in \mathbb{F}_2^{16},$$

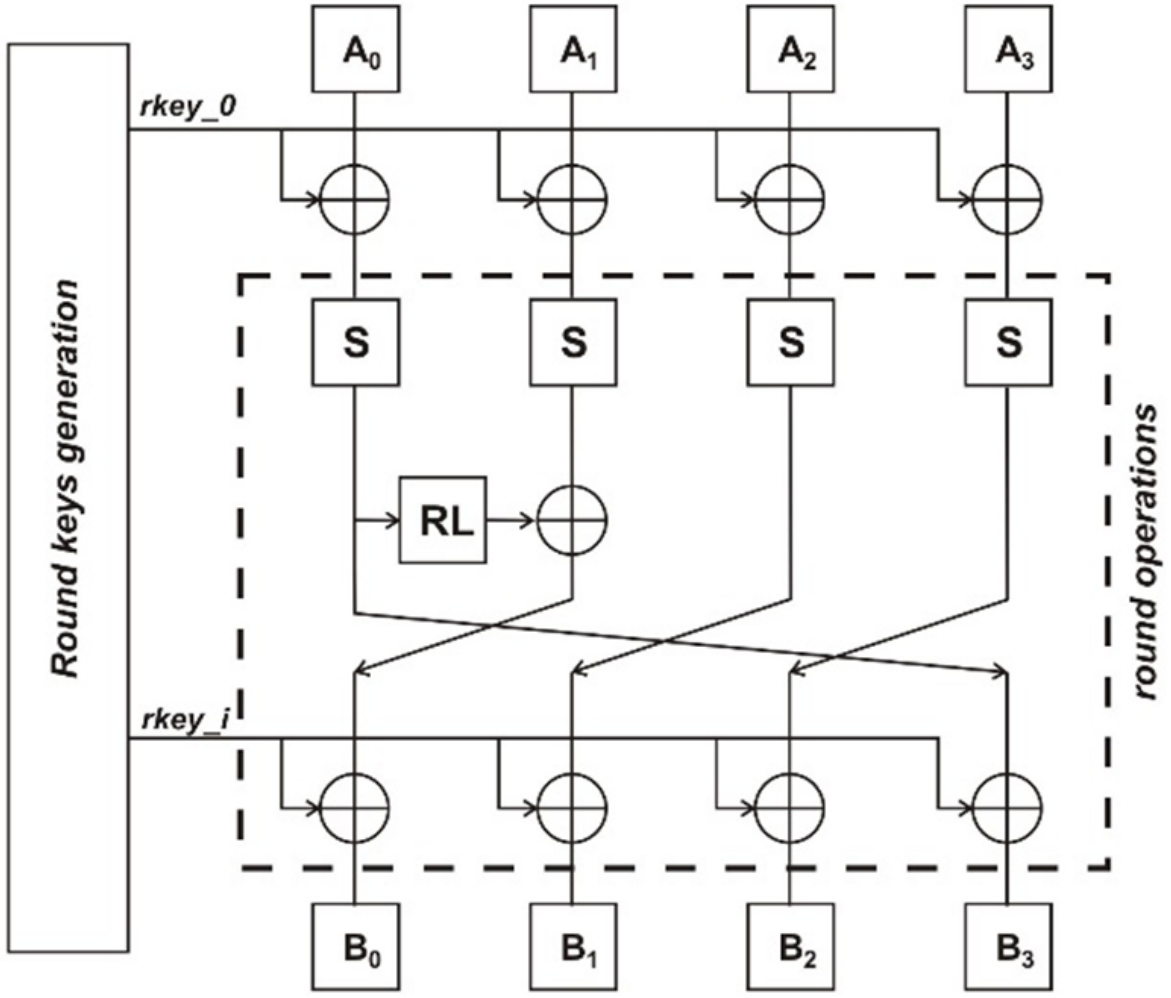

Рис. 1. Общая схема процесса шифрования алгоритма LBC-3

где “<<” – оператор циклического сдвига битов подблока влево.

Преобразование L. Это линейное преобразование осуществляется над целым блоком. При этом подблоки циклически сдвигаются влево на одну позицию, т.е. на первой позиции окажется второй подблок, на месте второго – третий подблок, на месте третьего – четвертый подблок, а первый подблок переместится на четвертую позицию (рис. 1).

Преобразование K. После циклических сдвигов подблоков к блоку данных добавляются раундовые ключи по модулю 2. Раундовый ключ, состоящий из 64 битов, делится на 4 подключа по 16 бит и суммируется с соответствующими подблоками данных.

Полное описание алгоритма LBC и ключевое расписание алгоритма подробно изложены в работах [14], [15]. Каждый раунд шифрования завершается сложением по модулю 2 раундовых ключей с полученными результатами. В работе [14] представлены результаты проведенного анализа алгоритма шифрования на лавинный эффект и показано, что после седьмого раунда все биты выходного блока зависят от всех входных битов. Поэтому в первую очередь целесообразно провести исследование алгоритма шифрования на семи раундах. Перед проведением дифференциального криптоанализа алгоритма шифрования необходимо рассмотреть дифференциальные свойства используемых преобразований по отдельности.

Для проведения дифференциального криптоанализа берутся две пары заранее подобранных шифртекстов A_1 и A_2, где атакующий вычисляет дифференциал: $\triangle A = A_1 \oplus A_2$, и с помощью вычисленного дифференциала пытается определить, каким должен быть дифференциал шифртекстов $\triangle B = B_1 \oplus B_2$.

В большинстве случаев вероятность подбора злоумышленником точного значения $\triangle B$ крайне низкая. Атакующий способен определить частоту возвращения $\triangle B$ для заданного $\triangle A$, что в свою очередь дает ему возможность получить часть ключа или целый ключ.

При проведении дифференциального криптоанализа выделяют четыре этапа:

– анализ дифференциальных свойств используемых преобразований в алгоритме;

– нахождение наиболее вероятного значения разности;

– поиск правильных пар текстов;

– анализ правильных пар текстов для определения битов ключа.

Операция побитового циклического сдвига и xor не оказывают никакого влияния на разность, это легко проверит. Однако для построения многораундовых характеристик важно определить, как именно будут преобразованы значения нужных байтов, которые будут получены после других преобразований. При сложении раундового ключа по модулю 2 его биты будут взаимно уничтожены. Поэтому значение ключа также не влияет на дифференциалы. В связи с этим, изменение разности зависит в основном от дифференциальных свойств S-блоков.

Дифференциальные свойства используемого S-блока

В алгоритме LBC используется 4-битный S-блок. Для S-блока необходимо построить таблицу распределения разности. Методология построения такой таблицы приведена в работах [13], [16]. При проведении дифференциального криптоанализа, необходимо отслеживать все комбинации двоичных векторов, складывать все возможные входные и выходные элементы S-блока, считать его нули и получен-

ные результаты заносить в таблицу распределения разности (табл. 1).

Таблица 1. Распределение разности для S-блока

$\triangle X/\triangle Y$	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
1	2	0	0	2	0	2	2	0	0	2	4	0	0	2	0
2	0	2	4	0	2	2	2	0	0	0	2	0	2	0	0
3	2	2	0	2	0	2	0	2	2	0	0	0	4	0	0
4	0	0	2	2	0	0	0	0	4	0	2	0	2	2	2
5	0	2	2	2	0	0	2	2	0	2	0	0	0	0	4
6	0	2	0	0	0	2	0	0	0	2	0	2	2	4	2
7	0	0	0	4	2	0	2	0	2	2	0	2	2	0	0
8	2	2	2	0	0	0	2	0	2	0	0	4	0	2	0
9	0	0	0	0	0	2	2	4	2	0	2	2	0	0	2
10	4	2	0	0	2	0	0	0	2	2	2	0	0	0	2
11	2	0	2	0	0	0	0	2	0	4	2	2	2	0	0
12	2	0	0	0	2	0	4	2	0	0	0	0	2	2	2
13	2	0	2	2	2	4	0	0	0	0	0	2	0	0	2
14	0	4	0	2	2	0	0	2	0	0	2	2	0	2	0
15	0	0	2	0	4	2	0	2	2	2	0	0	0	2	0

В построенной таблице распределения разностей, максимальным значением вероятности является значение $\frac{4}{16} = \frac{1}{4}$. В табл. 2 приведены входные и соответстующие им выходные разности с максимальными значениями. В таблице $\triangle X$ – вход в блок подстановок, $\triangle Y$ – значение, получаемое на выходе из блока подстановок, соответствующее $\triangle X$.

Таблица 2. Результат преобразование разности для S-блока

$\triangle X$	$\triangle Y$	$\triangle X$	$\triangle Y$	$\triangle X$	$\triangle Y$	$\triangle X$	$\triangle Y$	$\triangle X$	$\triangle Y$
$0x01$	$0x0b$	$0x02$	$0x03$	$0x03$	$0x0d$	$0x04$	$0x09$	$0x05$	$0x0f$
$0x07$	$0x04$	$0x08$	$0x0c$	$0x09$	$0x08$	$0x0a$	$0x01$	$0x0b$	$0x0a$
$0x0d$	$0x06$	$0x0e$	$0x02$	$0x0f$	$0x05$	$0x06$	$0x0a$	$0x0c$	$0x07$

На следующем шаге шифрования (преобразование RL) проводятся линейные преобразования с помощью цикличе-

ского сдвига и операции xor. Они не оказывают никакого влияния на изменение вероятности преобразования разности, так как эти сдвиги выполняется только внутри одного подблока.

Исходя из дифференциальных свойств используемых преобразований в алгоритме шифрования, построим несколько раундовых характеристик и получим их вероятность. Главная задача – найти отрезок зашифрованного текста, где было затронуто наименьшее количество активных S-блоков. От этого зависит вероятность получения правильной пары текстов по заданной характеристике. Затем, нужно определить количество раундов для алгоритма, которые позволят проанализировать шифртекст быстрее, чем метод полного перебора. Сложность полного перебора для блока данных размером 64 бита и длиной ключ 80 битов составляет 2^{80}.

Входной блок размером 64 бита делятся на 4 подблока по 16 битов и обозначается как X_1, X_2, X_3, X_4. При проведении анализа установлено, что наименьшее перемешивание битов происходит во втором подблоке (X_2). Как было отмечено ранее, все выходные биты зависят от всех входных битов после седьмого раунда. Поэтому, описание выходного уравнения для каждого $X_i, i = \overline{1,4}$ после седьмого раунда понадобится для поиска правильных пар. Во втором подблоке (Y_1) используется наименьшее число преобразований. Поэтому, пройдя пошагово по раундам шифрования покажем одну пару с наибольшими вероятностям.

Из таблицы распределения (табл. 1) разности можно выбрать любые пары входных и выходных данных со значе-

ниями в ячейках 4, так как число четыре является самым большим числом в таблице. Выберем пару с входом 1 и выходом 11 и запишем их в шестнадцатеричной системе счисления для одного подблока: $0x1111 \xrightarrow{p=1/4} 0xBBBB$. На следующем этапе шифрования выходная разность преобразуется через функцию R и поскольку она является линейной функцией, сохраняется закономерность и вероятность разностей: $0xBBBB \xrightarrow{p=1/4} 0x888A$. Если то, что нашли до сих пор, относится к первому подблоку ($RS(X_1)$), то можно выбрать эти разности как правильную пару для второго подблока. В общем случае можно выбирать любую пару из табл. 2, так как они являются правильными. Каждая строка таблицы содержит одну ячейку с числом 4, то есть каждому входу найдется соответствующий выходной элемент с одинаковой вероятностью. Итак, $0x888A \rightarrow 0x3331$ являются правильными парами для выражения $S(X_2) \oplus RS(X_1)$ и их вероятность равна $\frac{1}{4} \cdot \frac{1}{4} = \frac{1}{16} = (\frac{1}{2})^4$. Поскольку на следующем шаге шифрования идет S-блок замены, то согласно табл. 2, для $0x3331$ разность с наибольшей вероятностью будет $0xDDDB$.

Согласно схеме алгоритма шифрования, если выберем пары с высокой вероятностью, как указано выше, то в итоге получим следующие входные и выходные последовательности для семи раундов:

$0x1111 \rightarrow 0xBBBB \rightarrow 0x888A \rightarrow 0x3331 \rightarrow 0xDDDB \rightarrow 0x5F40 \rightarrow 0xF5E8 \rightarrow 0x5F2C \rightarrow 0x787F \rightarrow 0x696E \rightarrow 0xE8E2 \rightarrow 0x1235 \rightarrow 0xA98E \rightarrow 0x18C5 \rightarrow 0xBC7F \rightarrow 0xA745$

Следовательно, для входной разности $0x1111$ наиболее

вероятной выходной разностью будет $0xA745$. Нетрудно подсчитать, что S-блок встречается в выходном выражении для второго подблока 13 раз, т.е. вероятность искомой разности равна $(\frac{1}{4})^{13} = (\frac{1}{2})^{26}$ и как следствие, достаточный уровень безопасности не обеспечивается.

При проведении анализа по перемещению каждого элемента и отслеживая на каждом шаге выполнение подстановки, было обнаружено, что после двенадцатого раунда на каждом подблоке S-блок будет задействован 127, 49, 67 и 92 раз. Повторно выбирая дифференциалы с максимальными значениями вероятностей получается, что вероятность нахождения ключа для двенадцати раундов шифра будет равна $\frac{1}{2^{98}}$.

3 Заключение

Дифференциальные криптоанализы алгоритма показали, что полученное значение вероятности по дифференциальному криптоанализу превосходит сложность полного перебора, т.е. после одиннадцатого раунда алгоритм шифрования является стойким к дифференциальному криптоанализу. Из-за чрезвычайно малой вероятности получения правильных пар текстов, алгоритм нахождения таких текстов не может быть реализован теми средствами, которые имеются в настоящее время.

4 Благодарность

Научно-исследовательская работа выполнена в рамках проекта AP09259570 “Разработка и исследование отечествен-

ного легковесного алгоритма шифрования при ограниченности ресурсов" в Институте информационных и вычислительных технологий КН МНВО РК.

Библиографические ссылки

1. *Капалова Н.А., Хаумен А., Сулейменов О.Т.* Легковесные системы криптографической защиты информации // Актуальные проблемы информационной безопасности в Казахстане – 2021: материалы междунар. науч.-практ. конф. / Инст. инф. и выч. техн. МОН РК; редкол.: М.Н. Калимолдаев (гл. ред.) [и др.]. Алматы: Инст. инф. и выч. техн. МОН РК, 2021. С. 48–53.

2. Present: an ultra-lightweight block cipher / A. Bogdanov [et al.] // LNCS. 2007. Vol. 4727. P. 450–466.

3. Piccolo: an ultra-lightweight block cipher / K. Shibutani [et al.] // LNCS. 2011. Vol. 6917. P. 342–357.

4. *Gong Z., Nikova S., Law Y.W.* Klein: a new family of lightweight block ciphers // LNCS. 2011. Vol. 7055. P. 1–18.

5. Twine: a lightweight block cipher for multiple platforms / T. Suzaki [et al.] // LNCS. 2012. Vol. 7707. P. 339–354.

6. *De Cannire C., Dunkelman O., Knezevic M.* Katan and ktantan – a family of small and efficient hardwareoriented block ciphers // LNCS. 2009. Vol. 5747. P. 272–288.

7. The LED block cipher / J. Guo [et al.] // LNCS. 2011. Vol. 6917. P. 326–341.

8. Hight: a new block cipher suitable for low-resource device / D. Hong [et al.] // LNCS. 2006. Vol. 4249. P. 46–59.

9. The 128-bit block cipher clefia (extended abstract) / T. Shirai [et al.] // LNCS. 2007. Vol. 4593. P. 181–195.

10. New differential cryptanalysis results for the lightweight block cipher BORON / J.S. Teh [et al.] // J. Inf. Sec. App. 2022. Vol. 66, Iss. 2. P. 103129.

11. *Crama Y., Hammer P.L.* Boolean Models and Methods in Mathematics, Computer Science, and Engineering: Encyclopedia of Mathematics and its Applications. Cambridge: Cambridge University Press, 2010.

12. *Kim J., Hong S., Lim J.* Impossible differential cryptanalysis using matrix method // Discrete Mathematics. 2010. Vol. 310, Iss. 5. P. 988–1002.

13. Differential Cryptanalysis of New Qamal Encryption Algorithm / K.T. Algazy [et al.] // Int. J. El. Tel. 2020. Vol. 4. P. 647–653.

14. *Kapalova N., Algazy K., Haumen A.* Development of a new lightweight encryption algorithm // Eastern-European J. Ent. Tech. 2023. Vol. 3, No. 9(123). P. 6–19.

15. *Капалова Н.А., Хаумен А., Алгазы К.Т.* Оценка алгоритма генерации раундовых ключей легковесного шифра LBC-3 // Вестник АУЭС. 2023. Ном. 2. С. 66–81.

16. *Бабенко Л.К., Ищукова Е.А.* Современные алгоритмы блочного шифрования и методы их анализа. М.:Гелиос АРВ, 2006.

О РАЗНОСТНОМ АНАЛИЗЕ МОДУЛЯРНОГО СЛОЖЕНИЯ С ПОМОЩЬЮ ЦЛП

Д.В. Коледа[1]
[1]*Институт математики НАН Беларуси*
Минск, БЕЛАРУСЬ
e-mail: koledad@rambler.ru

В статье рассматривается моделирование с помощью задачи целочисленного линейного программирования разностного (по операции $\oplus$) перехода сквозь сложение по модулю 2^n. Линейные ограничения для некоторых из этих моделей были получены другими авторами алгоритмически с помощью систем компьютерной алгебры. Здесь мы предлагаем прямой математический вывод этих линейных ограничений.
Ключевые слова: разностный анализ; модулярное сложение; целочисленное линейное программирование; условия Липмаа—Мориаи

1 Введение

При разностном анализе большинства симметричных криптосистем возникает задача о распространении побитовых разностей сквозь сложение по модулю 2^n (операцию $\boxplus$).

Под *разностным переходом сквозь* $\boxplus$ мы понимаем упорядоченную тройку n-битных чисел, обозначаемую $(\alpha, \beta \xmapsto{\boxplus} \gamma)$, где подразумевается, что α и β — входные $\oplus$-разности, а γ — выходная $\oplus$-разность для операции $\boxplus$. *Вероятность разностного перехода сквозь* $\boxplus$ определим как

$$\mathrm{xdp}(\alpha, \beta \xmapsto{\boxplus} \gamma) := \Pr_{X,Y}\big\{(X \oplus \alpha) \boxplus (Y \oplus \beta) = (X \boxplus Y) \oplus \gamma\big\},$$

где предполагается, что $X, Y \in \{0,1\}^n$ — случайные n-битные числа.

Моделирование таких разностных переходов основано на следующих двух теоремах, установленных в [7].

Теорема 1 (Условия Липмаа—Мориаи [7]). *Разностный переход* $(\alpha, \beta \xmapsto{\boxplus} \gamma)$ *возможен, если и только если выполнены два условия:*

1. $\alpha_0 \oplus \beta_0 \oplus \gamma_0 = 0$;
2. *для тех* i *от* 1 *до* $n-1$, *для которых верно равенство* $\alpha_{i-1} = \beta_{i-1} = \gamma_{i-1}$, *должно быть* $\alpha_{i-1} = \beta_{i-1} = \gamma_{i-1} = \alpha_i \oplus \beta_i \oplus \gamma_i$.

Теорема 2 ([7]). *Если* $X, Y \in \{0,1\}^n$ *распределены независимо и равномерно, тогда вероятность возможного перехода* $(\alpha, \beta \xmapsto{\boxplus} \gamma)$ *удовлетворяет равенству*

$$\log_2 \mathrm{xdp}(\alpha, \beta \xmapsto{\boxplus} \gamma) = -\sum_{i=0}^{n-2} \neg eq(\alpha_i, \beta_i, \gamma_i),$$

где для двоичных x, y, z *функция*

$$\neg eq(x, y, z) := (x \oplus y) \vee (x \oplus z) = \begin{cases} 0 & \text{при } x = y = z, \\ 1 & \text{иначе.} \end{cases}$$

В [6, Sect. 3] предложен метод описания разностной характеристики линейными неравенствами при допущении независимости входов модулярных сложений и независимости тактов алгоритма. Известно, что такие сильные допущения о независимости модулярных сложений могут приводить к значительному расхождению между модельным и

реальным распространением разностей [4], [8]. Тем не менее, существенным достоинством модели [6, Sect. 3] является ее относительная простота, благодаря чему задачи, получаемые на ее основе, досягаемы для практических вычислений.

Данное в [6, Sect. 3] описание строится как ЦЛП-модель — задача целочисленного линейного программирования, где целевой функцией является вероятность разностной характеристики, а линейные ограничения описывают возможные (в такой модели) разностные переходы и соответствующие им вклады в вероятность разностной характеристики. В частности, распространение разностей сквозь модулярные сложения и сопутствующие вероятности смоделированы в [6], [5] линейными соотношениями на основе теорем 1 и 2 с использованием машинных вычислений. В [1] предложено упрощение этой модели в случае, когда одна из входных разностей нулевая.

Цель статьи — показать, что системы линейных ограничений для разностного перехода сквозь $\boxplus$, полученные с помощью машинных вычислений в [6], [5] и [1], можно построить напрямую, применяя прозрачные математические соображения. Также мы обобщим модель, предложенную в [1], на случай произвольного заданного значения одной из входных разностей. А именно, мы покажем, что при любом заданном значении одной из входных разностей соответственную ЦЛП-модель разностного перехода сквозь $\boxplus$ можно единообразно получить из некоторой исходной ЦЛП-модели. При этом модели для разных значений одной из входных разностей оказываются во взаимно однозначном соответствии друг с другом.

2 Построение линейных ограничений

2.1 Общий подход

Пусть $x_1, \ldots, x_n$ — двоичные переменные, а f и g — двоичные функции от этих переменных. Допустим, нужно построить задачу ЦЛП, которая моделирует такое условие:

$$\begin{cases} f(x_1, \ldots, x_n) = 0 & \Rightarrow g(x_1, \ldots, x_n) = 0, \\ f(x_1, \ldots, x_n) = 1 & \Rightarrow \text{ нет иного условия на } (x_i)_{i=1}^n. \end{cases} \tag{1}$$

Моделирование в данном случае означает, что нам нужно построить такую систему линейных неравенств, чтобы двоичные переменные $x_1, \ldots, x_n$ удовлетворяли ей в том и только в том случае, когда для них выполнено условие (1).

Данное условие равнозначно булеву выражению

$$f(x_1, \ldots, x_n) \vee \neg g(x_1, \ldots, x_n),$$

которое для наших целей будет удобно переписать в виде высказывания

$$\{e = f(x_1, \ldots, x_n)\} \wedge \Big(\{e = 1\} \vee \{g(x_1, \ldots, x_n) = 0\}\Big).$$

Введенная здесь промежуточная двоичная переменная e нужна, чтобы с одной стороны упростить линеаризацию выражений, а с другой — учесть вероятность.

Несложно заметить, что если уравнение $g(x_1, \ldots, x_n) = 0$ моделируется набором из N_g линейных неравенств вида

$$\langle \vec{c}_k, (x_1, \ldots, x_n) \rangle \geq d_k, \qquad \vec{c}_k \in \mathbb{R}^n,\ d_k \in \mathbb{R},$$

тогда выражение

$$\{e = 1\} \vee \{g(x_1, \ldots, x_n) = 0\}$$

будет истинно, если и только если двоичные переменные $e, x_1, \ldots, x_n$ удовлетворяют системе неравенств

$$\langle \vec{c}_k, (x_1, \ldots, x_n) \rangle + (d_k - m_k)e \geq d_k, \qquad 1 \leq k \leq N_g,$$

где в качестве постоянных m_k можно взять любые значения $m_k \leq \min_{\vec{x} \in [0,1]^n} \langle \vec{c}_k, \vec{x} \rangle$.

Предположим, что равенство $e = f(x_1, \ldots, x_n)$ точно моделируется набором из N_f линейных неравенств вида

$$\langle \vec{a}_j, (x_1, \ldots, x_n, e) \rangle \geq b_j, \qquad \vec{a}_j \in \mathbb{R}^{n+1},\ b_j \in \mathbb{R}.$$

Таким образом, при этих предположениях справедлива

Лемма 1. *Условие* (1) *можно точно смоделировать системой вида*

$$\begin{cases} \langle \vec{a}_j, (x_1, \ldots, x_n, e) \rangle \geq b_j, & 1 \leq j \leq N_f, \\ \langle \vec{c}_k, (x_1, \ldots, x_n) \rangle + (d_k - m_k)e \geq d_k, & 1 \leq k \leq N_g, \end{cases}$$

где $m_k = \min_{\vec{x} \in [0,1]^n} \langle \vec{c}_k, \vec{x} \rangle$.

Введем обозначения для двоичных величин из теорем 1 и 2:

$$(x, y, z, u, v, w) := (\alpha_{i-1}, \beta_{i-1}, \gamma_{i-1}, \alpha_i, \beta_i, \gamma_i), \tag{2}$$

$$e := e_{i-1} := \neg eq(\alpha_{i-1}, \beta_{i-1}, \gamma_{i-1}). \tag{3}$$

Поскольку наша цель — моделирование второго условия Липмаа—Мориаи, нас будет интересовать случай, когда функции f и g имеют вид

$$f(x, y, z, u, v, w) = \neg eq(x, y, z),$$
$$g(x, y, z, u, v, w) = x \oplus u \oplus v \oplus w.$$

Ввиду леммы 1, достаточно по отдельности смоделировать линейными неравенствами два уравнения:

$$e = \neg eq(x, y, z), \qquad x \oplus u \oplus v \oplus w = 0.$$

Если известен хотя бы один из битов x и u, количество переменных (а вместе с ними и число линейных ограничений) можно уменьшить, определив

$$y' := x \oplus y,\ z' := x \oplus z,\ s := x \oplus u,\ v'' := x \oplus u \oplus v. \quad (4)$$

Соответственные случаи сведены в табл. 1. При этом в линейных ограничениях возврат к старым переменным происходит по правилу

$$x' = x \oplus c \quad \Longleftrightarrow \quad x' = x + c - 2cx, \quad (5)$$

сохраняющему линейность выражений, когда $c \in \{0, 1\}$ — двоичная постоянная.

2.2 ЦЛП-модели

Лемма 2. *Справедливы следующие представления системами линейных неравенств:*

$$e = \neg eq(x, y, z) \Leftrightarrow \begin{cases} e \le x + y + z \le 3 - e, \\ x - y \le e,\ y - z \le e,\ z - x \le e; \end{cases} \quad (6)$$

$$e = y' \vee z' \Leftrightarrow e \le y' + z' \le 2e. \quad (7)$$

Доказательство. Запишем систему (6) в виде двойного (нелинейного) неравенства

$$\max\{x - y, y - z, z - x\} \le e \le \min\{x + y + z, 3 - x - y - z\}.$$

Пусть $x = y = z$. Тогда либо $x = y = z = 0$, либо $x = y = z = 1$. Отсюда $e = 0$.

Пусть равенство $x = y = z$ не выполняется. Значит, $1 \le x+y+z \le 2$ и хотя бы одна из разностей $x-y$, $y-z$, $z-x$ равна 1. Отсюда $e = 1$.

В справедливости (7) несложно убедится прямой проверкой. □

Лемма 3. *Верны следующие представления линейными ограничениями:*

$$\{e=1\} \vee \{x \oplus u \oplus v \oplus w = 0\}$$
$$\Leftrightarrow \begin{cases} -e \le u+v+w-x \le 2+e, \\ -e \le x+v+w-u \le 2+e, \\ -e \le u+x+w-v \le 2+e, \\ -e \le u+v+x-w \le 2+e; \end{cases} \tag{8}$$

$$\{e=1\} \vee \{s \oplus v \oplus w = 0\} \Leftrightarrow \begin{cases} s+v-w \ge -e, \\ w+s-v \ge -e, \\ v+w-s \ge -e, \\ s+v+w \le 2+e; \end{cases} \tag{9}$$

$$\{e=1\} \vee \{s \oplus v \oplus w = 0\}$$
$$\Leftrightarrow 2d \le s+v+w \le 2d+e; \tag{10}$$

$$\{e=1\} \vee \{v'' \oplus w = 0\} \Leftrightarrow -e \le v''-w \le e. \tag{11}$$

В (10) *на вспомогательную двоичную переменную* d *нет иных ограничений.*

Доказательство. При $e = 0$ равносильность системы (8) уравнению $x \oplus u \oplus v \oplus w = 0$ доказана в [9, Sect. 4.1, Table 2, p. 412–413]. Отметим, что данное уравнение нельзя смоделировать меньшим числом неравенств, см. [2, §3.1, Proposition 5, p. 342]. При $e = 1$ система (8) выполняется для всех $(x, u, v, w) \in [0, 1]^4$.

Справедливость (9), (10) и (11) несложно проверить, рассмотрев отдельно случаи $e = 0$ и $e = 1$. При $e = 0$ система (9) приводится в [4, Sect. 4.2], а равенство (10) — в [3, Sect. 2.1]. □

Из лемм 1, 2 и 3 с учетом (5) и обозначений (2), (3), (4) получаем теорему (см. также табл. 1).

Теорема 3. *Второе условие Липмаа—Мориаи в теореме 1 можно точно смоделировать:*

- *в случае неизвестных α_{i-1}, α_i системой из 13 неравенств, которая получается соединением систем* (6) *и* (8)*;*
- *в случае заданного α_{i-1} и неизвестного α_i системой из семи неравенств* (7) *и* (9) *либо системой из четырех неравенств* (7) *и* (10) *с одной вспомогательной переменной;*
- *в случае неизвестного α_{i-1} и заданного α_i системой из девяти неравенств* (6) *и* (9) *либо системой из семи неравенств* (6) *и* (10) *с одной вспомогательной переменной;*
- *при заданных α_{i-1}, α_i системой из четырех неравенств* (7) *и* (11)*.*

Несложно проверить, что соединение систем (6) и (8) совпадает с системой, приведенной в [5, p. 10] и [1, Table 4, p. 597], с точностью до простейших преобразований и очевидных замен переменных друг на друга внутри троек (x, y, z) и (u, v, w). Также легко убедиться в равносильности системы из пяти неравенств в [1, Table 5, p. 597] объединению

систем (7) и (11). В дополнение к рассмотренному в [1] случаю $(x, u) = (0, 0)$ с помощью (5) получаются остальные три случая для заданных (x, u).

Таблица 1. Основные случаи ЦЛП-моделей 2-го условия Липмаа—Мориаи
$(y' := x \oplus y,\ z' := x \oplus z,\ s := x \oplus u,\ v'' := x \oplus u \oplus v)$

Дано (x, u)	f	Модель $\{e = f\}$	g	Модель $\{e = 1\}$ $\vee\{g = 0\}$	Число нерав. для 2-го усл. Л.—М.
$(-, -)$	$\neg eq(x, y, z)$	(6)	$x \oplus u \oplus v \oplus w$	(8)	13
$(x, -)$	$y' \vee z'$	(7)	$s \oplus v \oplus w$	(9) или (10)	7 или 4 (+1 пер.)
$(-, u)$	$\neg eq(x, y, z)$	(6)	$s \oplus v \oplus w$	(9) или (10)	9 или 7 (+1 пер.)
(x, u)	$y' \vee z'$	(7)	$v'' \oplus w$	(11)	4

3 Выводы

Таким образом, моделирующим второе условие Липмаа—Мориаи системам линейных неравенств, приведенным в [5, p. 10] и [1, Tables 4 & 5, p. 597] и полученным машинными методами, можно придать осмысленную математическую структуру. Это позволяет для случаев, когда заданы биты одной из двух разностей на входе сложения по модулю 2^n, напрямую построить линейные модели с меньшим числом неравенств.

Библиографические ссылки

1. *Bagherzadeh E., Ahmadian Z.* MILP-based automatic differential search for LEA and HIGHT block ciphers // IET Inf. Secur. 2020. Vol. 14, No. 5. P. 595–603.

2. *Boura C., Coggia D.* Efficient MILP Modelings for Sboxes and Linear Layers of SPN ciphers // IACR Trans. Symm. Crypt. 2020. Vol. 2020, No. 3. P. 327–361.

3. New automatic search tool for impossible differentials and zero-correlation linear approximations [Electronic resource]. URL: `https://eprint.iacr.org/2016/689.pdf` (date of access: 11.08.2023).

4. *ElSheikh M., Abdelkhalek A., Youssef A.M.* On MILP-Based Automatic Search for Differential Trails Through Modular Additions with Application to Bel-T // LNCS. 2019. Vol. 11627. P. 273–296.

5. MILP-Based Automatic Search Algorithms for Differential and Linear Trails for Speck [Electronic resource]. URL: `https://www.iacr.org/archive/fse2016/97830255/97830255.pdf` (date of access: 11.08.2023).

6. MILP-Based Automatic Search Algorithms for Differential and Linear Trails for Speck / K. Fu [et al.] // LNCS. 2016. Vol. 9783. P. 268–288.

7. *Lipmaa H., Moriai S.* Efficient Algorithms for Computing Differential Properties of Addition // LNCS. 2002. Vol. 2355. P. 336–350.

8. Towards non-independence of modular additions in searching differential trails of ARX ciphers: new automatic methods with application to SPECK and Chaskey [Electronic resource].

URL: https://arxiv.org/abs/2203.09741v1
(date of access: 11.08.2023).

9. Improved Cryptanalysis of an ISO Standard Lightweight Block Cipher with Refined MILP Modelling / J. Yin [et al.] // LNCS. 2018. Vol. 10726. P. 404–426.

РАССЕИВАЮЩИЕ СВОЙСТВА ПРЕОБРАЗОВАНИЙ, ЗАДАННЫХ КОМБИНАЦИЕЙ ЦИКЛИЧЕСКИХ СДВИГОВ, В РАЗЛИЧНЫХ АЛГЕБРАИЧЕСКИХ СТРУКТУРАХ

Д.М. Крапивенцев[1], М.А. Пудовкина[2]
[1,2]*Национальный исследовательский ядерный университет "МИФИ"*
Москва, РОССИЯ
e-mail: [1]zshytciy@gmail.com

В работе рассматриваются преобразования над n-мерным векторным пространством над полем $\mathbb{F}_2$ и над кольцом вычетов $\mathbb{Z}_{2^n}$, заданные композицией "простых" операций, а именно, циклических сдвигов и сложений в соответствующей аддитивной группе. Такие преобразования используются в ARX-криптосистемах. Получены условия их биективности и найдены коэффициенты рассеивания.
Ключевые слова: ARX-криптосистема; свойство рассеивания; циркулянтная матрица; коэффициент рассеивания; циклический сдвиг

1 Введение

При синтезе современных криптосистем, как правило, применяются "простые" операции и преобразования, эффективно реализуемые на процессорах общего назначения. "Простыми" операциями являются сложение $\boxplus$ в кольце вычетов $\mathbb{Z}_{2^n}$, сложение $\oplus$ (XOR) в n-мерном векторном пространстве $V_n(2)$ над полем $\mathbb{F}_2$ и циклический сдвиг $\lll$.

Криптосистемы, использующие преобразования на основе комбинаций только трех таких операций, называются ARX-криптосистемами [5].

При выборе преобразований, составляющих функцию зашифрования, традиционно оценивают их свойства перемешивания и рассеивания, неформально сформулированные К. Шенноном [12]. Преобразования, обеспечивающие свойство рассеивания, часто являются линейными. Так, в ARX-криптосистемах они основаны на комбинации операций XOR и циклического сдвига, например, в криптосистемах SHACAL [7], Keccak [11], SMS4 [2], Alzette [1] и др.

Для $X \in \{V_n(2), \mathbb{Z}_{2^n}\}$ положим

$$* = *_X = \begin{cases} \boxplus, & \text{если } X = \mathbb{Z}_{2^n}, \\ \oplus, & \text{если } X = V_n(2). \end{cases}$$

Аддитивной группе $(X, *)$ и набору $\overline{r} = (r_0, ..., r_{d-1}) \in \mathbb{Z}_n^d$, $0 \le r_0 \le ... \le r_{d-1}$ поставим в соответствие преобразование $f_{\overline{r}}^* : X \to X$, заданное для каждого $\alpha \in X$ условием

$$f_{\overline{r}}^*(\alpha) = (\alpha \lll r_0) * \ldots * (\alpha \lll r_{d-1}). \qquad (1)$$

При $X = V_n(2)$ преобразование $f_{\overline{r}}^{\oplus}$ применяется, например, в функции хеширования SHACAL и блочной шифрсистеме SMS4 . Для ускорения реализации часто полагают $r_0 = 0$. Преобразование $f_{\overline{r}}^{\oplus}$ является линейным оператором, который в стандартном базисе задается циркулянтой матрицей (циркулянтом), определяемой циклическим сдвигом порождающего вектора [10]. Свойства преобразования $f_{\overline{r}}^{\oplus}$ зависят от формы циркулянтной матрицы. Рассматриваются также его обобщения, например, в функции хеширо-

вания Keccak [11] используется преобразование, задаваемое тензорным произведением циркулянтных матриц.

При $X = \mathbb{Z}_{2^n}$ преобразование $f_{\overline{r}}^{\boxplus}$ задается как

$$f_{\overline{r}}^{\boxplus}(\alpha) = (\alpha \lll r_0) \boxplus \ldots \boxplus (\alpha \lll r_{d-1}).$$

Применение его в качестве рассеивающего преобразования может оказаться эффективным, так как биты переноса увеличивают распространение влияния бит входного вектора. Кроме того, преобразование $f_{\overline{r}}^{\boxplus}$, в отличии от преобразования $f_{\overline{r}}^{\oplus}$, является нелинейным. Отметим, что для улучшения рассеивающих свойств похожая идея реализована в белорусском алгоритме шифрования BelT [13].

Для характеризации свойства рассеивания во многих работах (см., например, [4]) используется коэффициент рассеивания b_f (branch number) преобразования $f : V_n(2) \to V_n(2)$, который задается равенством

$$b_f = \min\{||\alpha|| + ||f(\alpha)|| \mid \alpha \in V_n(2), \alpha \neq 0_n\}, \qquad (2)$$

где $||\beta||$ – вес Хемминга вектора $\beta \in V_n(2)$.

В [4] описываются свойства рассеивающих преобразований, основанных на композиции логического сдвига $\ll$ и операции $\oplus$. Получены критерии их биективности, найден наибольший коэффициент рассеивания и условия его достижимости. В [6] рассматриваются различные классы матриц, включая матрицы над $\mathbb{F}_2$, которые являются почти-MDS и исследуются их рассеивающие свойства.

В настоящее время не известен эффективный способ подбора оптимальных значений констант циклического сдвига. В ряде криптосистем они подбираются эмпирическим путем, например, в криптосистеме Skein [3]. Некоторые

криптосистемы используют наиболее оптимальные значения констант относительно времени программной или аппаратной реализации криптосистемы (после проверки отсутствия известных слабостей с данными константами), например, криптосистема Alzette [1].

В данной работе рассматриваются преобразования $f^{\oplus}_{\overline{r}}$, $f^{\boxplus}_{\overline{r}}$ соотвественно над $V_n(2)$ и $\mathbb{Z}_{2^n}$. Получены условия их биективности. Найдены коэффициенты рассеивания.

2 Биективность отображения $f^{*}_{\overline{r}}$

Для $d \in \mathbb{N}$ положим

$$R^{(0)}_d = \{(r_0, ..., r_{d-1}) \in \mathbb{Z}^d_n | 0 \leq r_0 < ... < r_{d-1} \leq n-1\}\},$$

$$R_d = \{(r_0, ..., r_{d-1}) \in \mathbb{Z}^d_n | 0 \leq r_0 \leq ... \leq r_{d-1} \leq n-1\}\}.$$

Приведем условия биективности преобразования $f^{*}_{\overline{r}}$ при $* \in \{\oplus, \boxplus\}$.

Для проверки биективности преобразования $f^{\oplus}_{\overline{r}}$ очевидно, что достаточно рассмотреть только $\overline{r} \in R^{(0)}_d$. Далее представить $f^{\oplus}_{\overline{r}}$ в виде циркулянта, для которого получить многочлен Холла $h_{\overline{r}}$ [10]. Несложно показать, что преобразование $f^{\oplus}_{\overline{r}}$ биективно, если многочлен Холла $h_{\overline{r}}$ принадлежит мультипликативной группе кольца $\mathbb{F}_2[x]/(x^n - 1)$. Отсюда вытекает, что если n четно, то тогда и только тогда преобразование $f^{\oplus}_{\overline{r}}$ биективно, когда d нечетно.

Лемма 1. *Для $\overline{r} = (r_0, ..., r_{d-1}) \in R_d$ необходимым условием биективности преобразования $f^{\boxplus}_{\overline{r}}$ является существование таких различных $i, j \in \{0, ..., d-1\}$, что $r_i = r_j$.*

Отметим, что условие леммы 1 является необходимым, но не достаточным. Так, контрпримером служит набор $\overline{r} = (0, 1, 1)$.

Экспериментально получены следующие наборы $\overline{r}$, соответствующие подстановкам $f_{\overline{r}}^{\boxplus}$.

Лемма 2. *Пусть* $1 < n \leq 16$, $d \in \{3, 5, 7\}$, $\overline{r} = (r_0, ..., r_{d-1}) \in R_d$. *Тогда преобразование* $f_{\overline{r}}^{\boxplus} : \mathbb{Z}_{2^n} \to \mathbb{Z}_{2^n}$ *биективно, если справедливо одно из условий:*

- $d = 3$, $(r_0, r_1, r_2) = (a, a, a)$, $a \in \mathbb{Z}_n$;
- $d = 5$, $(r_i, r_{i+1 \bmod 5}, .., r_{i+4 \bmod 5}) \in \{(a, a, a, a, a), (a, b, b, b, b), (c, c, a, b, b)\}$, *где* $i \in \mathbb{Z}_5, a, b, c \in \mathbb{Z}_n$ *и*

$$b \equiv a + 1 \pmod{n},\ c \equiv a - 1 \pmod{n};$$

- $d = 7$, $(r_i, .., r_{i+6 \bmod 7}) \in \{(0, 0, 0, 1, 1, 1, 1), (0, 0, 0, 0, n - 1, n - 1, n - 1)\}$, *где* $i \in \mathbb{Z}_7$.
- $d = 7$, $(r_i, .., r_{i+6 \bmod 7}) \in \{(a, a, a, a, a, a, a), (c, c, a, a, a, b, b)\}$, *где* $i \in \mathbb{Z}_7, a, b, c \in \mathbb{Z}_n$ *и*

$$b \equiv a + 1 \pmod{n},\ c \equiv a - 2 \pmod{n}.$$

3 Рассеивающие свойства преобразования $f_{\overline{r}}^{*}$

Существуют различные подходы к характеризации свойства рассеивания. Так, рассматриваются наличие инвариантных подпространств [1], коэффициент рассеивания (branch number) и совершенное рассеивание разбиений [9].

Известно (см. [10]), что если характеристический многочлен циркулянтной матрицы не является примитивным, то существуют инвариантные подпространства, а матрица есть тензорное произведение циркулянтных матриц, например, такое линейное преобразование есть в функции хеширования Keccak [11]. В общем случае циркулянты над $V_n(2)$ выбираются таким образом, чтобы их порядок был не меньше чем n. Применение простых или взаимно простых чисел в качестве констант циклического сдвига является обычной практикой [7], [1], [13], [3] для избежания потенциальных слабостей.

Несложно показать, что для всех $n, d \in \mathbb{N},\ n > 1$, и

– для каждого $\overline{r} \in R_d^{(0)}$ коэффициент рассеивания преобразования
$$f_{\overline{r}}^{\oplus} : V_n(2) \to V_n(2)$$
равен d;

– для каждого $\overline{r} \in R_d$ коэффициент рассеивания преобразования
$$f_{\overline{r}}^{\boxplus} : \mathbb{Z}_{2^n} \to \mathbb{Z}_{2^n}$$
равен d.

Среди всех $(n \times n)$-матриц над полем $\mathbb{F}_{2^m}$ при $m \in \mathbb{N}$ наибольший коэффициент рассеивания, равный $n+1$, имеют MDS-матрицы. Хорошо известно (см. [8]), что матрица над полем $\mathbb{F}_2$ не является MDS-матрицей. Следовательно, циркулянтная матрица преобразования $f_{\overline{r}}^{\oplus}$ не есть MDS-матрица.

Замечание 1. Несмотря на небольшой коэффициент рассеивания преобразование $f_{\overline{r}}^{\oplus}$ обеспечивает достаточно хоро-

шее рассеивание на векторах, выбранных случайно и равновероятно из $V_n(2)$. Недостаток проявляется на векторах с небольшим весом Хэмминга – в таких случаях инвертирование бит происходит в ограниченном числе координат.

Библиографические ссылки

1. Alzette: A 64-Bit ARX-box / C. Beierle [et al.] // Adv. Crypt. – CRYPTO 2020. 2020. P. 419–448.

2. SMS4 Encryption Algorithm for Wireless Networks [Electronic resourse].
   URL: `https://eprint.iacr.org/2008/329.pdf`
   (date of access: 29.06.2023).

3. The Skein Hash Function Family [Electronic resourse].
   URL: `https://www.schneier.com/wp-content/uploads/2015/01/skein.pdf`
   (date of access: 29.06.2023).

4. Direct Construction of Optimal Rotational-XOR Diffusion Primitives / Z. Guo [et al.] // IACR Transactions on Symmetric Cryptology. 2017. Vol. 4. P. 169–187.

5. *Khovratovich D., Nikolić I.* Rotational Cryptanalysis of ARX // Fast Software Encr. 2010. Vol. 6147. P. 333–346.

6. *Li C., Wang Q.* Design of Lightweight Linear Diffusion Layers from Near-MDS Matrices // IACR Transactions on Symmetric Cryptology. 2017. Vol. 1. P. 129–155.

7. Related-Key Rectangle Attack on 42-Round SHACAL-2 / J.Lu [et al.] // Inf. Secur. 2006. Vol. 4176. P. 85–100.

8. *Мак-Вильямс Ф.Дж., Слоэн Н.Дж.А.* Теория кодов, исправляющих ошибки. М.: Связь, 1977.

9. *Погорелов Б.А., Пудовкина М.А.* О расстояниях от подстановок до импримитивных групп при фиксированной системе импримитивности // Дискретная математика. 2013. Т. 25, Ном. 3. С. 78–95.

10. *Сачков В.Н., Тараканов В.Е.* Комбинаторика неотрицательных матриц. М.: Научное издательство ТВП, 2000.

11. SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions [Electronic resourse]. URL: `https://www.nist.gov/publications/sha-3-standard-permutation-based-hash-and-extendable-output-functions` (date of access: 28.06.2023).

12. *Погорелов Б.А., Сачков В.Н.* Словарь криптографических терминов. М.: МЦНМО, 2006.

13. СТБ 34.101.31-2011. Криптографические алгоритмы шифрования и контроля целостности [Электронный ресурс]. URL: `https://apmi.bsu.by/assets/files/std/belt-spec27.pdf` (дата обращения: 28.06.2023).

ОЦЕНКИ ДЛЯ РАСПРЕДЕЛЕНИЙ РАНГОВ СЛУЧАЙНЫХ ДВОИЧНЫХ МАТРИЦ, СОСТОЯЩИХ ИЗ СТРОК С ЗАДАННЫМИ ВЕСАМИ

В.И. Круглов[1]

[1]*Математический институт им. В.А. Стеклова Российской академии наук*

Москва, РОССИЯ

e-mail: kruglov@mi-ras.ru

Рассматриваются асимптотические свойства ранга матрицы, состоящей из n независимых случайных строк, каждая из которых равновероятно и независимо от остальных строк выбирается из множества всех m-мерных ($m > n$) двоичных векторов заданного веса s_i, $i = 1, \ldots, n$. Предложена явная оценка сверху для функции распределения ранга такой матрицы.

Ключевые слова: случайная матрица над полем $GF(2)$; распределение ранга матрицы; явная оценка

1 Введение

В 1965 году И.Н. Коваленко в работе [2] доказал, что если двоичная матрица B размера $n \times n$ состоит из независимых в совокупности элементов b_{ij} таких, что

$$0 < \delta \le p_{ij} = \mathbf{P}\{b_{ij} = 1\} \le 1 - \delta,$$

то предел при $n \to \infty$ вероятности того, что матрица B будет иметь полный ранг, не зависит от значения δ и

$$\lim_{n\to\infty} \mathbf{P}\{\text{rank } B = n\} = \prod_{i=1}^{\infty} \left(1 - 2^{-i}\right) \approx 0.29.$$

Как показал М.В. Козлов в статье [3], если матрица B имеет размер $n \times m$, $n < m$, и $1 \leq m/n \leq C < (1 + \log_2(1-\delta))^{-1}$, то равномерно по всем $p_{ij} \in [\delta, 1-\delta]$

$$(1 - \mathbf{P}\{\text{rank } B = n\}) \left(1 - \prod_{i=m-n+1}^{m} \left(1 - 2^{-i}\right)\right)^{-1} \to 1.$$

Естественно, что для случая, когда элементы случайной матрицы зависимы между собой, получить достаточно подробное описание предельного поведения ранга в сколь-либо общей постановке невозможно, поэтому интерес представляет изучение частных постановок задачи, например, матриц из независимых случайных строк или столбцов.

2 Случайные матрицы, состоящие из строк с заданными весами

В статье А.М. Зубкова и В.И. Круглова [1] была рассмотрена задача о ранге двоичной матрицы размера $n \times m$, состоящей из n независимых случайных строк $b_1, \ldots, b_n$, каждая из которых выбирается равновероятно и независимо от остальных строк из множества всех m-мерных ($n < m$) двоичных векторов одинакового фиксированного веса s (под весом вектора понимают число его ненулевых элементов). Для вероятности того, что такая матрица имеет неполный ранг, была получена следующая оценка.

Теорема 1. *Пусть B — двоичная матрица размера $n \times m, n < m$, строки $b_1, \ldots, b_n$ которой независимы (как случайные векторы) и имеют равномерное распределение на*

множестве всех двоичных строк веса s и длины m. Тогда

$$\mathbf{P}\{\text{rank } B < n\}$$
$$\leq \frac{1}{2^m}\sum_{t=0}^{m} C_m^t \left[\left(1+\frac{K_s^m(t)}{C_m^s}\right)^n - n\frac{K_s^m(t)}{C_m^s} - 1\right],$$

где $K_s^m(t)$ – многочлен Кравчука, задаваемый равенством

$$K_s^m(t) = \sum_{\substack{j \geq 0,\\ j \leq s,\, j \leq t}} (-1)^j C_t^j C_{m-t}^{s-j}.$$

В работе [4] В.И. Круглов и В.Г. Михайлов получили более общий результат, рассмотрев двоичные матрицы, у которых строки $b_1, \ldots, b_n$ могут иметь различные заданные веса $s_1, \ldots, s_n$.

Теорема 2. *Пусть B — двоичная матрица размера $n \times m, n < m$, строки $b_1, \ldots, b_n$ которой выбраны независимо и равновероятно из множества всех m-мерных двоичных векторов заданных весов $s_1, \ldots, s_n$ соответственно. Тогда при любом $l \in \{1, \ldots, n-1\}$*

$$l\mathbf{P}\{\text{rank}(B) \leq n-l\}$$
$$\leq \frac{1}{2^m}\sum_{t=0}^{m} C_m^t \left[\prod_{i=1}^{n}\left(1+\frac{K_{s_i}^m(t)}{C_m^{s_i}}\right) - \sum_{i=1}^{n}\frac{K_{s_i}^m(t)}{C_m^{s_i}} - 1\right],$$

в частности,

$$\mathbf{P}\{\text{rank}(B) < n\}$$
$$\leq \frac{1}{2^m}\sum_{t=0}^{m} C_m^t \left[\prod_{i=1}^{n}\left(1+\frac{K_{s_i}^m(t)}{C_m^{s_i}}\right) - \sum_{i=1}^{n}\frac{K_{s_i}^m(t)}{C_m^{s_i}} - 1\right].$$

Известно (см. [5]), что для многочленов Кравчука справедлива оценка

$$\left|\frac{K_s^m(t)}{C_m^s}\right| < \min\left\{1, \sqrt{\frac{2^m}{C_m^s C_m^t}}\right\}.$$

С помощью этого неравенства удается получить довольно грубую, но более удобную оценку для функции распределения ранга. Положим

$$Q(s_1, \ldots, s_n) = \sum_{i=1}^{n} \frac{1}{\sqrt{C_m^{s_i}}}.$$

Теорема 3. *Пусть выполнены условия теоремы 2 и числа* $s_1, \ldots, s_n$ *таковы, что найдется натуральное число* t_0*, для которого*

$$\min\left\{t \in \{1, \ldots, m\} \colon C_m^t \geq 2^m Q^2(s_1, \ldots, s_n)\right\} \leq t_0 \leq \frac{m}{2}.$$

Тогда при любом $l \in \{1, \ldots, n-1\}$

$$l\,\mathbf{P}\{\mathrm{rank}(B) \leq n - l\}$$

$$\leq 2^{n-m+1} \sum_{t=0}^{t_0} C_m^t + e(m - 2t_0 + 1)Q^2(s_1, \ldots, s_n),$$

в частности,

$$\mathbf{P}\{\mathrm{rank}(B) < n\}$$

$$\leq 2^{n-m+1} \sum_{t=0}^{t_0} C_m^t + e(m - 2t_0 + 1)Q^2(s_1, \ldots, s_n).$$

Библиографические ссылки

1. *Зубков А.М., Круглов В.И.* Моментные характеристики весов векторов в случайных двоичных линейных ко-

дах // Математические вопросы криптографии. 2012. Т. 3, Вып. 4. С. 55–70.

2. *Коваленко И.Н.* Об одной предельной теореме для определителей в классе булевых функций // ДАН СССР. 1965. Т. 161, Вып. 3. С. 517–519.

3. *Козлов М.В.* О ранге матриц со случайными булевыми элементами // ДАН СССР. 1966. Т. 169, Вып. 5. С. 1013–1016.

4. *Круглов В.И., Михайлов В.Г.* О ранге случайной двоичной матрицы с заданными весами независимых строк // Математические вопросы криптографии. 2019. Т. 10, Вып. 4. С. 67–76.

5. *Krasikov I.* Nonnegative quadratic forms and bounds on orthogonal polynomials // J. Approx. Theory. 2001. Vol. 111, No. 1. P. 31–49.

ОПТИМИЗАЦИЯ ПРОГРАММНОГО КОДА РАЗРАБОТАННОГО ЛЕГКОВЕСНОГО АЛГОРИТМА ШИФРОВАНИЯ ISL_LWC

О.А. Лизунов[1], А. Хомпыш[2]
[1,2]*Институт информационных и вычислительных технологий МНВО РК*
Алматы, КАЗАХСТАН
e-mail: [1]o.lizunov@bk.ru, [2]ardabek@mail.ru

В данной статье речь пойдет об оптимизации программного кода. Будут представлены несколько примеров оптимизированного исходного кода легковесного алгоритма шифрования ISL_LWC, разработанного сотрудниками Лаборатории информационной безопасности ИИВТ МНВО РК. Алгоритм шифрования реализован на языке программирования C++.
Ключевые слова: легковесный алгоритм шифрования; оптимизация кода; приведение типов

1 Введение

С первых дней появления вычислительной техники остро стояли вопросы увеличения производительности программ и экономии места на устройствах хранения информации. В связи с нехваткой вычислительных ресурсов, от разработчиков требовалось создавать программы, которые могли бы работать с максимальным быстродействием при минимальном размере программного кода. В настоящее время при разработке программного обеспечения предпочтение в основном отдается времени, затраченному на создание программного продукта, а не его оптимизации. Но даже сейчас

существуют сферы деятельности, где необходимость в оптимизации программ сохранилась. Одним из таких направлений является разработка средств криптографической защиты информации. Оптимизация кода – это один из способов преобразования кода, приводящий к улучшению его характеристик и повышению производительности программы. Среди целей оптимизации можно выделить уменьшение размера кода, объема используемой оперативной памяти, повышение скорости выполнения программы, уменьшение количества операций ввода – вывода. Оптимизация кода может проводиться программистом вручную или автоматизировано. В последнем случае оптимизатор может быть реализован как отдельное программное средство или встроен в компилятор. При рассмотрении оптимизации кода выделяют высокоуровневую и низкоуровневую оптимизацию. К высокоуровневой оптимизации относятся сущности, над которыми программисты проводят свою работу по повышению эффективности. Это циклы, ветвления, функции, процедуры, классы и т.д. К низкоуровневой оптимизации относится проводимая пограммистом работа на уровне, близком к машинному коду, с использованием языка ассемблера или машинных команд. Одним из методов, используемым в высокоуровненвой оптимизации является приведение типов. Приведение типа – это способ временно изменить тип данных, хранящихся в переменной, на другой, отличный от ее первоначального объявления. Приведение типа переменной есть указание компилятору обрабатывать ее так, как если бы она имела заданный новый тип, но только на время выполнения текущей операции.

2 Легковесный алгоритм шифрования ISL_LWC

2.1 Схема алгоритма шифрования

Структурная схема легковесного блочного алгоритма шифрования ISL_LWC изображена на рис. 1.
Основные параметры алгоритма:

– длина блока – 64 бита;

– длина ключа – 80 бит;

– количество раундов шифрования – 16.

В алгоритме используются преобразование SP, сложение по модулю 2 (операция XOR), циклический сдвиг, нелинейные преобразования в виде S-блоков.
Процесс шифрования состоит из 4 этапов:

1. 64-битный блок открытого текста суммируется с раундовым ключом по модулю 2 (операция XOR). Далее полученный 64-битный блок разбивается на 4 подблока по 16 бит (*нумерация подблоков идет слева направо*).

2. Первый входной подблок циклически сдвигается на 5, затем полученное значение первого входного подблока суммируется (операция XOR) со вторым подблоком и полученные значения меняются местами в соответствии со схемой, и проходят преобразования SP.

3. Третий и четвертый подблоки проходят преобразование S и потом суммируются (операция XOR) с полученными результатами на втором этапе согласно схеме.

4. Полученные результаты второго и третьего этапов переставляются согласно схеме алгоритма шифрования.

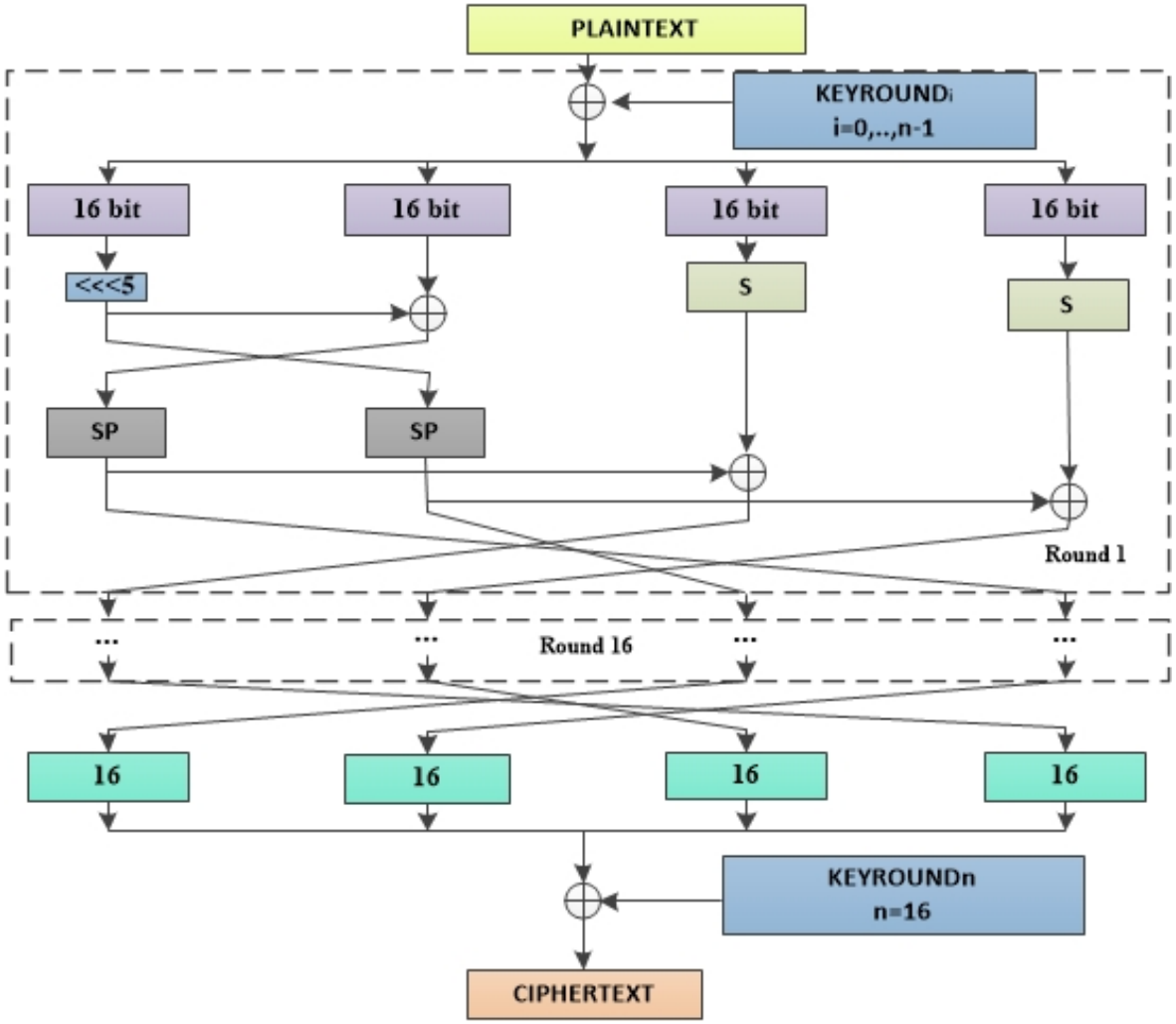

Рис. 1. Схема алгоритма шифрования

2.2 Алгоритм генерации раундовых подключей

Генерация раундовых подключей производится на основе 80 битного базового ключа с разбиением его на 5 подблоков по 16 бит (*нумерация подблоков идет слева направо*). Используемые криптографические преобразования: 4-битный S-блок и сложение второго слова с первым по модулю 2 в степени длины слова [1]. На рис. 2 изображен алгоритм генерации раундовых подключей.

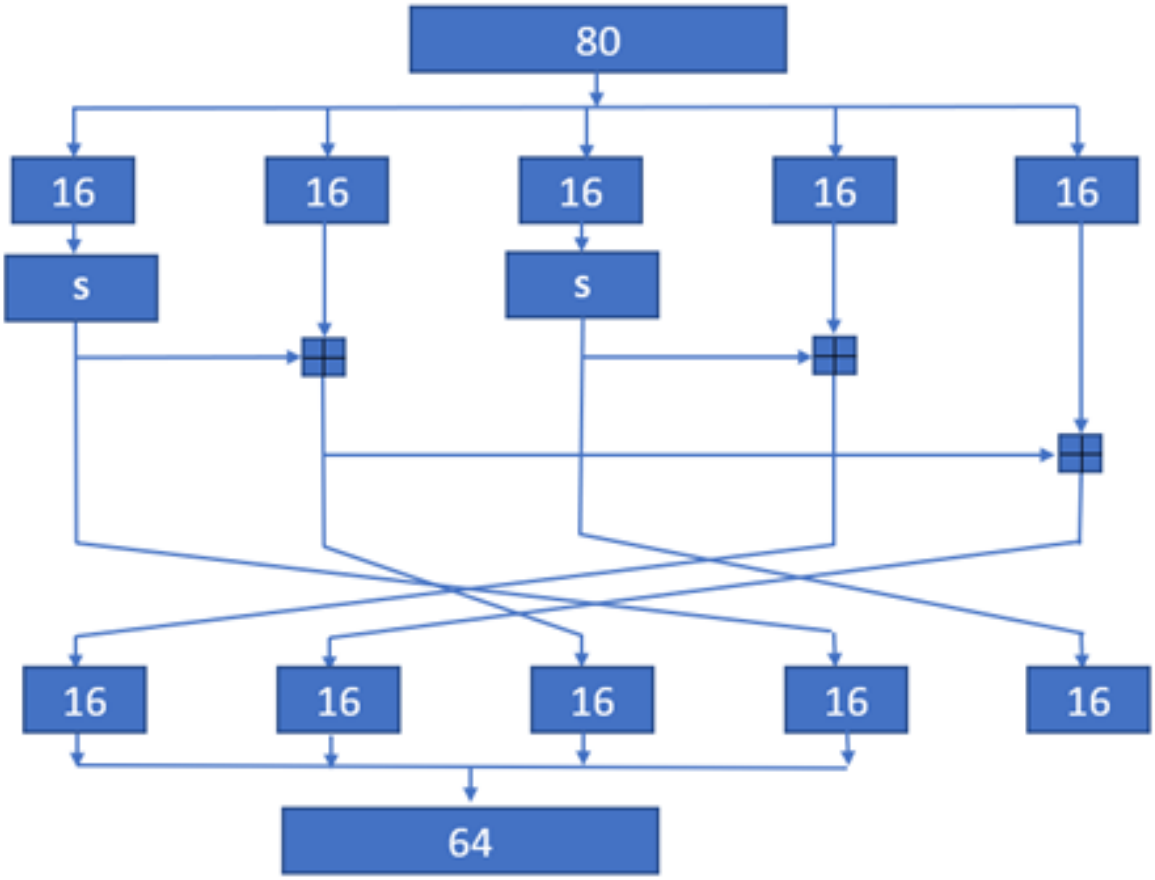

Рис. 2. Алгоритм генерации раундовых подключей

3 Примеры оптимизации программного кода

При разработке первого рабочего варианта алгоритма шифрования ISL_LWC была отмечена медленная работа функций шифрования и генерации раундовых подключей. В связи с этим было принято решение провести оптимизацию кода с целью увеличения скорости функций шифрования и генерации раундовых подключей. Для выполнения операции подстановки (S-блок) в алгоритме генерации раундовых подключей с целью его оптимизации были использованы следующие операции: приведение типов, логический

сдвиг, логические операции “И” и “ИЛИ”. На рис. 3 изображен фрагмент кода S-блока из алгоритма генерации раундовых подключей. Следующий блок кода перестановки битов был оптимизирован с использованием операции приведения типов и встроенной функции в C++. На рис. 4 изображен фрагмент кода перестановки битов из алгоритма генерации раундовых подключей. Хотелось бы отметить, что представленные выше принципы работы с S-блоком и с перестановкой битов используются и в схеме шифрования. Для выполнения операции XOR в схеме алгоритма шифрования с целью оптимизации кода была использована операция приведения типов. На рис. 5 изображен фрагмент кода операции XOR из алгоритма шифрования.

```
((ushort*)key)[i] = (
                      (Sbox_2[(((ushort*)key)[i] & 0xF)] << 4) |
                      (Sbox[(((ushort*)key)[i] & 0xF0) >> 4]) |
                      (Sbox_2[(((ushort*)key)[i] & 0xF00) >> 8] << 12 ) |
                      (Sbox[(((ushort*)key)[i] & 0xF000) >> 12] << 8)
                    );
```

Рис. 3. Фрагмент кода S-блока из алгоритма генерации раундовых подключей

```
//меняем 16 бит местами
qSwap(((ushort*)key)[0], ((ushort*)key)[3]);
qSwap(((ushort*)key)[1], ((ushort*)key)[2]);
qSwap(((ushort*)key)[1], ((ushort*)key)[4]);
```

Рис. 4. Фрагмент кода перестановки битов из алгоритма генерации раундовых подключей

```
// операция xor
((ullong*)fileBlock)[0] ^= ((ullong*)keyTable[i])[0];
```

Рис. 5. Фрагмент кода операции XOR из алгоритма шифрования

Таким образом, приведенные выше фрагменты исходного кода позволили увеличить в несколько раз скорость проведения операций шифрования и генерации раундовых подключей, уменьшить размер исходного кода и объем используемой оперативной памяти.

4 Заключение

В данной статье были рассмотрены вопросы оптимизации программного кода. На примере разработанного легковесного алгоритма шифрования ISL_LWC были приведены фрагменты оптимизированного исходного кода, которые позволили увеличить в несколько раз скорость проведения операций шифрования и генерации раундовых подключей. Уменьшение размера исходного кода и объема используемой оперативной памяти было достигнуто за счет сокращения количества используемых функций и циклов.

5 Благодарность

Статья подготовлена в рамках проекта грантового финансирования AP09259570 “Разработка и исследование отечественного легковесного алгоритма шифрования при ограниченности ресурсов” МНВО РК.

Библиографические ссылки

1. Development of a New Lightweight Encryption Algorithm / A. Khompysh [et al.] // Int. J. Adv. Comp. Sc. App. 2023. Vol. 14, No. 5. P. 452–459.

О СТАТИСТИЧЕСКОМ ОЦЕНИВАНИИ МНОГОМЕРНОЙ ЭНТРОПИИ ДЛЯ ПРОВЕРКИ КАЧЕСТВА КРИПТОГРАФИЧЕСКИХ ГЕНЕРАТОРОВ

М.В. Мальцев[1], Ю.С. Харин[2]
[1,2]*НИИ прикладных проблем математики и информатики*
[1,2]*Белорусский государственный университет*
Минск, БЕЛАРУСЬ
e-mail: [1]maltsew@bsu.by, [2]kharin@bsu.by

Рассматривается задача построения статистических оценок s-мерной энтропии, широко используемой в качестве характеристики качества случайных числовых последовательностей. Рассматривается подход к построению оценок на основе частот состояний, вычисленных по пересекающимся фрагментам последовательности.
Ключевые слова: генераторы случайных числовых последовательностей; статистическое тестирование; энтропия

1 Введение

В системах криптографической защиты информации важнейшими элементами являются генераторы случайных числовых последовательностей (далее — генераторы), используемые для формирования ключей, векторов инициализации, параметров криптографических алгоритмов и протоколов [1]. Использование генераторов с уязвимостями снижает безопасность криптосистем, упрощает задачу злоумышленников по вычислению секретных параметров. В связи с этим актуальной является задача оценки качества

выходных последовательностей генераторов. Для решения данной задачи широко используются методы теории вероятностей и математической статистики, с помощью которых анализируются отклонения последовательностей от модели «чистой случайности» [2]. Широко применяемой на практике характеристикой качества случайных последовательностей является энтропия [3].

2 Равномерно распределенная случайная последовательность

Математической моделью «чистой случайности» является равномерно-распределенная случайная последовательность (РРСП) [1]. Принимающая значения из N-элементного множества A случайная последовательность $\{x_t \in A : t \in \mathbb{N}\}$, называется РРСП, если для нее выполняются следующие два свойства:

- Для любого $n \in \mathbb{N}$ и для любых $1 \leq t_1 < t_2 < \cdots < t_n$ случайные величины $x_{t_1}, \ldots, x_{t_n}$ независимы в совокупности.
- Случайная величина x_t равномерно распределена на множестве $\{0, 1, \ldots, N-1\}$ для любого $t \in \mathbb{N}$:

$$\mathrm{P}\{x_t = j\} = \frac{1}{N},\ j \in \{0, 1, \ldots, N-1\}.$$

3 Статистическое оценивание s-мерной энтропии

Далее рассматриваются двоичные последовательности, т.е. $A = \{0, 1\}$. Из определения РРСП следует, что для любых

$s \in \mathbb{N}$, $t > s$, $J_1^s = (j_1, \ldots, j_s) \in A^s$, $p ::= 2^{-s}$, выполняется:

$$p_{J_1^s} = \mathrm{P}\{X_t^{t+s-1} = J_1^s\} = \mathrm{P}\{x_t = j_1, \ldots, x_{t+s-1} = j_s\} \equiv p,$$

т.е. s-мерное распределение РРСП также является равномерным.

Таким образом, если верна гипотеза $H_0 = \{$последовательность $X_1^T = (x_1, \ldots, x_T) \in A^T$, $T = ms$, согласуется с моделью РРСП, то s-мерная энтропия

$$H(s) = -\sum_{J_1^s \in A^s} p_{J_1^s} \log_2 p_{J_1^s}$$

достигает максимального значения, равного s. Рассмотрим статистическую оценку s-мерной энтропии, построенную по подстановочному принципу:

$$\hat{H}(s) = -\sum_{J_1^s \in A^s} \hat{p}_{J_1^s} \log_2 \hat{p}_{J_1^s},$$

где $\hat{p}_{J_1^s}$ — статистические оценки вероятностей $p_{J_1^s}$, построенные по последовательности X_1^n. Существует два подхода к вычислению $\hat{p}_{J_1^s}$: по пересекающимся и по непересекающимся фрагментам X_1^n. В первом случае оценки имеют следующий вид:

$$\hat{p}_{J_1^s} = \frac{1}{m} \sum_{t=1}^{m} \mathbb{1}\{x_{(t-1)s+1} = j_1, \ldots, x_{ts} = j_s\}. \qquad (1)$$

При таком подходе частоты состояний $J_1^s \in A^s$, входящие в формулу (1), в случае верной H_0 представляют собой независимые в совокупности случайные величины с биномиальным распределением вероятностей. Во втором случае при

использовании пересекающихся фрагментов X_1^n оценки вероятностей $p_{J_1^s}$ имеют следующий вид:

$$\hat{p}_{J_1^s} = \frac{1}{T'} \sum_{t=1}^{T'} \mathbb{1}\{x_t = j_1, \ldots, x_{t+s-1} = j_s\}$$

$$= \frac{1}{T'} \sum_{t=1}^{T'} \mathbb{1}\{X_t^{t+s-1} = J_1^s\},\ T' = T - s + 1.$$

При таком подходе используется больше информации о тестируемой последовательности X_1^n, однако частоты $\nu(J_1^s) = \sum_{t=1}^{T'} \mathbb{1}\{X_t^{t+s-1} = J_1^s\}$ уже не являются суммами независимых величин Бернулли и их применение для статистического анализа генераторов требует дополнительных вычислений. Математическое ожидание $\hat{p}_{J_1^s}$, как и для случая непересекающихся фрагментов, равно $p_{J_1^s}$. Вычислим далее дисперсии $\hat{p}_{J_1^s}$ при верной H_0, используя соотношение: $\mathbf{D}\{\hat{p}_{J_1^s}\} = \mathbf{E}\{\hat{p}_{J_1^s}^2\} - \mathbf{E}\{\hat{p}_{J_1^s}\}^2$. Найдем $\mathbf{E}\{\hat{p}_{J_1^s}^2\}$:

$$\mathbf{E}\{\hat{p}_{J_1^s}^2\} = \mathbf{E}\left\{ \frac{1}{(T')^2} \sum_{t=1}^{T'} \sum_{u=1}^{T'} \mathbb{1}\{X_t^{t+s-1} = J_1^s, X_u^{u+s-1} = J_1^s\} \right\}$$

$$= \frac{1}{(T')^2} \sum_{t=1}^{T'} \sum_{u=1}^{T'} \mathbf{P}\{X_t^{t+s-1} = J_1^s, X_u^{u+s-1} = J_1^s\}$$

$$= \frac{1}{(T')^2} \sum_{t=1}^{T'} \mathbf{P}\{X_t^{t+s-1} = J_1^s\}$$

$$+ \frac{2}{(T')^2} \sum_{t=1}^{T'-1} \sum_{\Delta=1}^{T'-t} \mathbf{P}\{X_t^{t+s-1} = J_1^s, X_{t+\Delta}^{t+\Delta+s-1} = J_1^s\}$$

$$= \frac{p}{T'} + \frac{2}{(T')^2} \sum_{t=1}^{T'-1} \left(\sum_{\Delta=1}^{s-1} \mathbf{P}\{X_t^{t+s-1} = J_1^s, X_{t+\Delta}^{t+\Delta+s-1} = J_1^s\} \right.$$

$$\left. + \sum_{\Delta=s}^{T'-t} \mathbf{P}\{X_t^{t+s-1} = J_1^s, X_{t+\Delta}^{t+\Delta+s-1} = J_1^s\} \right)$$

$$= \frac{p}{T'} + \frac{p^2(T'-s)(T'-s+1)}{(T')^2}$$

$$+ \frac{2p(T'-1)}{(T')^2} \sum_{\Delta=1}^{s-1} \mathbb{1}\{J_{1+\Delta}^s = J_1^{s-\Delta}\} 2^{-\Delta} = p^2 + \mathcal{O}(T^{-2})$$

$$+ T^{-1} \left(p - p^2(2s-1) + 2p \sum_{\Delta=1}^{s-1} \mathbb{1}\{J_{1+\Delta}^s = J_1^{s-\Delta}\} 2^{-\Delta} \right). \quad (2)$$

Найдем далее разложение $\hat{H}(s)$, обозначив $\xi_{J_1^s} = \hat{p}_{J_1^s} - p_{J_1^s}$:

$$\hat{H}(s) = - \sum_{J_1^s \in A^s} (p_{J_1^s} + \xi_{J_1^s}) \log_2 (p_{J_1^s} + \xi_{J_1^s}) =$$

$$= - \sum_{J_1^s \in A^s} (p_{J_1^s} + \xi_{J_1^s}) \left(\log_2 p_{J_1^s} + \frac{\xi_{J_1^s}}{p_{J_1^s} \ln 2} \right.$$

$$\left. - \frac{\xi_{J_1^s}^2}{2p_{J_1^s}^2 \ln 2} + \mathcal{O}(|\xi_{J_1^s}|^3) \right).$$

При истинной гипотезе H_0: $p_{J_1^s} = p = 2^{-s}$ для любых $J_1^s \in A^s$, поэтому с учетом того, что $\sum\limits_{J_1^s \in A^s} \xi_{J_1^s} = 0$, имеем:

$$\hat{H}(s) = H(s) - \frac{1}{2p \ln 2} \sum_{J_1^s \in A^s} \xi_{J_1^s}^2 + \mathcal{O}(\max_{J_1^s \in A^s} |\xi_{J_1^s}^3|)$$

$$= s - \frac{1}{2p \ln 2} \sum_{J_1^s \in A^s} \xi_{J_1^s}^2 + \mathcal{O}(\max_{J_1^s \in A^s} |\xi_{J_1^s}^3|).$$

Математическое ожидание $\hat{H}(s)$ при истинной H_0 имеет вид:

$$\mathbf{E}\{\hat{H}(s)\} = s - \frac{2^{s-1}}{\ln 2} \sum_{J_1^s \in A^s} \mathbf{E}\{\xi_{J_1^s}^2\} + \mathcal{O}(\max_{J_1^s \in A^s} |\xi_{J_1^s}^3|). \qquad (3)$$

Найдем сумму величин $\mathbf{E}\{\xi_{J_1^s}^2\} = \mathbf{E}\{\hat{p}_{J_1^s}^2\} - p^2$ в (3) с помощью формулы (2):

$$\sum_{J_1^s \in A^s} \mathbf{E}\{\xi_{J_1^s}^2\} = \mathcal{O}(T^{-2})$$

$$+T^{-1} \left(1 - p(2s-1) + 2p \sum_{\Delta=1}^{s-1} 2^{-\Delta} \sum_{J_1^s \in A^s} \mathbb{1}\{J_{1+\Delta}^s = J_1^{s-\Delta}\} \right)$$

$$= \mathcal{O}(T^{-2}) + T^{-1} \left(1 - p(2s-1) + 2p \sum_{\Delta=1}^{s-1} 2^{-\Delta+\Delta} \right)$$

$$= T^{-1}(1-p) + O(T^{-2}) = T^{-1}(1-2^{-s}) + O(T^{-2}). \qquad (4)$$

Здесь использовано тождество:

$$\sum_{J_1^s \in A^s} \mathbb{1}\{J_{1+\Delta}^s = J_1^{s-\Delta}\} = 2^{\Delta},$$

которое следует из того свойства, что условие $J_{1+\Delta}^s = J_1^{s-\Delta}$ эквивалентно наличию в векторе J_1^s периода длины Δ, потому число таких векторов равно 2^{Δ} – числу возможных заполнений периода. Из (4) и (3) получаем:

$$\mathbf{E}\{\hat{H}(s)\} = s - \frac{2^s - 1}{2T \ln 2} + \mathcal{O}(T^{-2}). \qquad (5)$$

Поведение величин (5) при $s = 3$ и $T \to \infty$ проиллюстрировано на рис. 1: по горизонтальной оси откладывалась

длина последовательности T, по вертикальной оси — значение $\mathbf{E}\{\hat{H}(s)\}$, вычисленное по двум первым слагаемым формулы (5) (без остаточного члена).

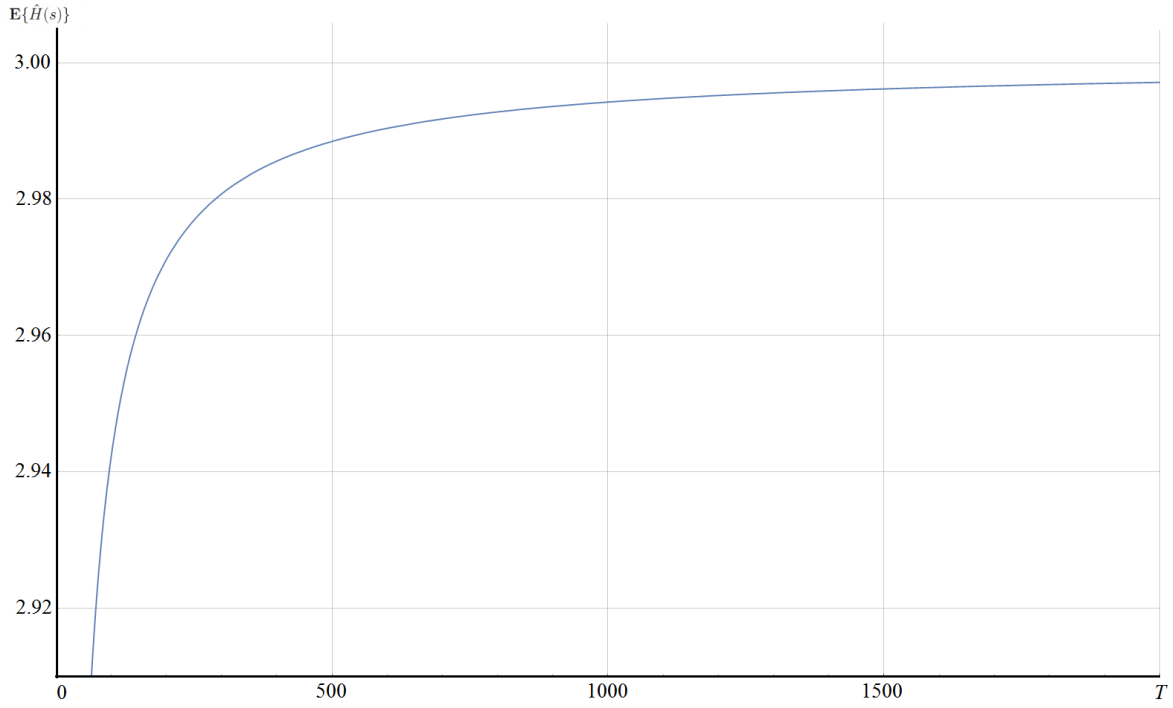

Рис. 1. Зависимость $\mathbf{E}\{\hat{H}(s)\}$ от T

Библиографические ссылки

1. *Харин Ю.С. [и др.].* Криптология. Минск: БГУ, 2013.

2. A statistical test suite for the validation of random number generators and pseudo random number generators for cryptographic applications. NIST Special Publication 800-22 Revision 1a [Electronic resource].
URL: `https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-22r1a.pdf` (date of access: 14.09.2023).

3. *Зубков А.М.* Энтропия как характеристика качества случайных последовательностей // Математические вопросы криптографии. 2021. Т. 12, Вып. 3. С. 31–48.

ОБЕСПЕЧЕНИЕ КОНФИДЕНЦИАЛЬНОСТИ В ПРИВАТНЫХ БЛОКЧЕЙН-СИСТЕМАХ

М.Н. Мицкевич[1]
[1]*НИИ прикладных проблем математики и информатики*
[1]*Белорусский государственный университет*
Минск, БЕЛАРУСЬ
e-mail: mitskevichmn@gmail.com

Построена модель обеспечения конфиденциальности данных в приватных блокчейн-системах, основанная на решениях Hyperledger Fabric.
Ключевые слова: распределенный реестр; блокчейн-система; смарт-контракт

1 Введение

Распределенный реестр – это система консенсуса реплицированных, разделенных и синхронизируемых цифровых данных, которые географически размещены (распределены) в различных городах, странах и организациях. В отличие от централизованных баз данных распределенный реестр не требует центрального администрирования и, следовательно, не имеет центральной точки отказа.

Под блокчейн-системами обычно понимают системы хранения данных в распределенном реестре, построенные на основе связанных цепочек блоков данных (англ. block chain). Иногда в это понятие также включают и системы распределенного реестра, построенные на основе направленных ациклических графов и более сложных структур данных.

Блокчейн-система имеет следующие особенности, которые отличают ее от других систем:

– криптографическое связывание данных, хранящихся в распределенном реестре;

– синхронизация хранимых данных;

– наличие механизмов построения бизнес-логики для хранимых данных, известных как смарт-контракты.

Для реализации перечисленных механизмов данные распределенных реестров должны должны быть открыты и доступны для проверки всеми валидаторами (участниками) системы. При этом стандарты экономической безопасности требуют, чтобы информационные системы, хранящие и обрабатывающие данные, обеспечивали конфиденциальность информации. В таком случае используются приватные блокчейн-системы, в которых права чтения и записи данных реестра выдаются единственным администратором. Это централизованные персонифицированные системы, в которых существует иерархия полномочий. Сбои можно быстро исправить вручную. Нет смысла применять сложные механизмы консенсуса — информация без задержки попадает в блоки, формируемые по мере необходимости, и не требует дополнительного подтверждения, что максимизирует скорость работы сети и минимизирует стоимость транзакций. Однако сохраняется распределенный характер хранения данных, при котором узлы содержат полные копии данных в формате взаимосвязанных цепочек блоков. Чаще всего речь идет о системе передачи информации внутри одной компании, что не требует общего доступа ко всей ин-

формации, но может предусматривать возможность аудита со стороны руководства или регуляторов.

В общем случае конфиденциальность может быть обеспечена внешними сервисами передачи защищенной информации. В настоящей работе мы рассмотрим другой подход – конфиденциальность обеспечивается собственными средствами приватной блокчейн-системы. Более конкретно мы рассмотрим систему Hyperledger Fabric [1], в которой реализованы следующие инструменты:

1. Приватные смарт-контракты – смарт-контракты, внутренние состояния которых скрыты от неавторизованных пользователей. Используются для реализации сложной бизнес-логики и защиты от несанкционированного доступа.

2. Закрытые подсети (каналы) – выделение части пользователей реестра в доверенную группу, которые проводят между собой открытые транзакции в отдельном реестре.

Следует отметить, что модели обеспечения конфиденциальности данных в приватных блокчейн-системах слабо представлены в научно-технической литературе. Настоящая работа частично устраняет данный пробел.

2 Модель обработки данных в смарт-контрактах

В блокчейн-системах используются следующие криптографические примитивы: хэш-функция H, алгоритмы выработки `Sign` и проверки `Vfy` электронной цифровой подписи (ЭЦП).

Данные D, отправляемые от A к B, оформляются в виде транзакции, которая обозначается $Tr(D, A, B)$. Данные D – это набор $D = (d_0, \ldots, d_{n-1}), \quad d_k \in \{0,1\}^*$ произвольной длины.

Данные D обрабатываются хэш-деревом или деревом Меркла (англ. Merkle tree). Дерево Меркла – это полное двоичное дерево, в листовые вершины которого помещены хэш-значения от блоков данных, а внутренние вершины a_j^h содержат хэш-хначения от конкатенации значений в дочерних вершинах $a_{2j}^{h-1}, a_{2j+1}^{h-1}$:

$$a_k^0 = \begin{cases} H(d_k), & k = 0, \ldots, n-1, \\ H(\perp), & k = n, \ldots, 2^N - 1, \quad N = \lceil \log_2(n) \rceil, \end{cases}$$

$$a_j^h = H(a_{2j}^{h-1} \parallel a_{2j+1}^{h-1}), \quad h = 1, \ldots, N, \quad j = 0, \ldots, 2^{N-h} - 1.$$

Здесь $\perp$ – пустое слово.

Корневой узел дерева содержит хэш-значение от всего набора данных. Хэш-значением блока данных D назовем корневое значение дерева Меркла, построенного по этому набору данных: $H(D) = a_0^N$. Хэш-значение транзакции $Tr(D, A, B)$ определяется как хэш-значение ее блока данных $H(Tr) = H(D)$.

Транзакция Tr подписывается на личном ключе sk_A отправителя A, $s_A(Tr) = \mathtt{Sign}(H(Tr), sk_A)$ – полученная подпись, а $Tr_A^s = Tr \parallel s_A(Tr)$ – подписанная транзакция. Транзакция может подписываться несколькими сторонами, например, $Tr_{A,B}^s = Tr \parallel s_A(Tr) \parallel s_B(Tr)$ – транзакция, подписанная сторонами A и B.

Подписанные транзакции помещаются в блок транзакций B.

Перед помещением транзакции Tr_A^s в блок каждый участник системы проверяет подпись транзакции с помощью открытого ключа pk_A отправителя A через вызов алгоритма $\texttt{Vfy}$. Транзакция принимается, если $\texttt{Vfy}(H(Tr), s_A(Tr), pk_A) = 1$ (подпись корректна), и отвергается, если $\texttt{Vfy}(H(Tr), s_A(Tr), pk_A) = 0$.

В Hyperledger Fabric блок B состоит из трех частей – заголовок BH, данные BD и метаданные BM:

$$B = (BH, BD, BM).$$

Данные блока состоят из подписанных транзакций:

$$BD = (Tr_0^s, Tr_1^s, \ldots).$$

Заголовок блока B_k содержит номер блока, хэш-значение заголовка предыдущего блока и хэш-значение данных текущего блока:

$$BH_k = (k, H(BH_{k-1}), H(BD_k)).$$

Метаданные блока содержат время создания блока, сертификат открытого ключа и подпись создателя блока V:

$$BM = (t, Cert_V, s_V(BH)).$$

Блокчейн – это последовательность блоков:

$$BC = (B_1, B_2, \ldots).$$

Реестр состоит из двух частей – блокчейна и глобального состояния:

$$R = (BC, S).$$

В общем случае состояние можно представить как словарь пар имен и значений объектов, в котором имена уникальны:

$$S = \{(Name, Value)\}, \quad Name \in \{0,1\}^*, \quad Value \in \{0,1\}^*.$$

Смарт-контракт получает доступ к реестру и содержит три основные типа команд:

– чтение текущего значения объекта

$$Get(Name)\colon \text{return } S[Name];$$

– создание нового объекта или изменение значения существующего

$$Put(Name, Value)\colon S[Name] \leftarrow Value;$$

– удаление объекта

$$Del(Name)\colon S[Name] \leftarrow \varnothing.$$

Команды собираются в последовательность и помещаются в блок данных транзакции:

$$Cmd = (Cmd_1, Cmd_2, \ldots), \quad Cmd_i = (Op, Arg),$$
$$Op \in \{Get, Put, Del\}, \quad Arg = (Name[, Value]).$$

Кроме изменения глобального состояния, смарт-контракт может записывать произвольные данные в транзакцию с целью хранения их в блокчейне.

Отвечает за помещение транзакций в блок выделенная группа узлов OS, которая называется службой упорядочения (англ. ordering service).

Канал в Hyperledger Fabric имеет свой отдельный реестр R, набор участников F вместе с выделенной службой упорядочения OS и чейнкод CC (набор смарт-контрактов):

$$K = (R, F, OS, CC), \quad CC = \{C_1, C_2, \ldots\}.$$

Каждый смарт-контракт C имеет связанную с ним политику одобрения, определяющую участников $V \subset F$, которые должны одобрить сгенерированную транзакцию, прежде чем транзакция будет считаться подтвержденной. Все транзакции, подтвержденные или неподтвержденные, записываются в блокчейн, но только подтвержденные транзакции изменяют глобальное состояние.

Порядок выполнения транзакции в смарт-контракте:

1. $A \to V$: $Tr^s_A(D, A, S)$.
2. V: выполняет $Cmd \subset D$ на копии S и получает измененное состояние S'.
3. $V \to A$: $(S', s_V(Tr))$.
4. $A \to OS$: $Tr^s_{A,V}(D, A, S)$.
5. $OS \to F$: $Tr^s_{A,V}(D, A, S) \in B_i, \quad B_i \in BC$.
6. F: выполняет $Cmd \subset D$ на S.

Здесь $\to$ означает пересылку между узлами с помощью API Hyperledger Fabric.

3 Модель обработки конфиденциальных данных

Конфиденциальные данные хранятся в приватном состоянии и изменяются приватными транзакциями. Блокчейн-

система обеспечивает конфиденциальный доступ к приватному состоянию PS для выделенного подмножества участников канала $G \subset F$.

$$Get_A(Name) = \text{return} \begin{cases} PS[Name], & A \in G, \\ \varnothing, & A \notin G. \end{cases}$$

Данные PS хранятся в отдельной конфиденциальной базе данных участников G и недоступны остальным участникам канала. При изменении значения в приватной коллекции данных в блокчейн записывается хэш-значение ее нового состояния с помощью транзакции $Tr(H(PS'), A, PS)$.

Порядок выполнения приватной транзакции в смарт-контракте:

1. $A \Rightarrow V$: $Tr^s_A(D, A, PS)$.
2. V: выполняет $Cmd \subset D$ на копии PS и получает измененное состояние PS'.
3. $V \Rightarrow G$: PS'.
4. $V \to A$: $Tr^s_V(H(PS'), A, PS)$.
5. $A \to OS$: $Tr^s_{A,V}(H(PS'), A, PS)$.
6. $OS \to F$: $Tr^s_{A,V}(H(PS'), A, PS) \in B_i, \quad B_i \in BC$.
7. G: $PS \leftarrow PS'$.

Здесь $\Rightarrow$ означает пересылку между узлами по защищенному каналу с проверкой доступа к конфиденциальным данным.

В Hyperledger Fabric приватные состояния называются приватными коллекциями данных и имеют дополнительные возможности:

– не нужно быть участником коллекции, чтобы записать что-либо в нее, при условии, что соблюдена политика подтверждения;

– у узлов без доступа к коллекции имеется возможность получения хэш-значения конфиденциальных данных по ключу, позволяя сверять их с теми, что лежат в блокчейне.

Следует отметить, что в блокчейне сохраняются только открытые для всего канала транзакции и хэш-значение приватного состояния. Приватные транзакции не сохраняются, а сохранность приватной коллекции данных обеспечивается участниками доверенной группы самостоятельно сторонними средствами.

Библиографические ссылки

1. A Blockchain Platform for the Enterprise: Hyperledger Fabric [Electronic resource].
URL: `https://hyperledger-fabric.readthedocs.io`
(date of access: 14.09.2023).

ИСПОЛЬЗОВАНИЕ ПОРОГОВОЙ КРИПТОСХЕМЫ РАЗДЕЛЕНИЯ СЕКРЕТА ДЛЯ БИОМЕТРИЧЕСКОЙ АУТЕНТИФИКАЦИИ

С.Е. Нысанбаева[1], Н.А. Капалова[2],
С.Б. Бейсенова[3]
[1,2]*Институт информационных и вычислительных технологий МНВО РК*
[3]*НАО Казахский национальный университет им. Аль-Фараби*
Алматы, КАЗАХСТАН
e-mail: [1]sultasha1@mail.ru, [2]nkapalova@mail.ru,
[3]saltanat.erkebulan@gmail.com

Использование современных биометрических технологий обеспечивают удобство и скорость, но также существуют и определенные риски, связанные с угрозой безопасности. Одним из самых уязвимых процессов в этой технологии считается снятия биометрических характеристик. Здесь возникает большое количество возможностей для атак, и методы защиты не всегда эффективны. Данной работе рассматривается один из существующих угроз, как кража информации. Биометрический образец, создаваемый сканером, может быть украден и использован в дальнейшем для подмены. Также существуют некоторые проблемы связанный с размером базы данных хранения биометрического образца. Для решения этих вопросов предлагается биометрическая аутентификация с использованием схемы разделения секрета. Разбиение и хранение биометрического образца с использованием схемы разделения секрета поможет уменьшить размер базы данных и устранить угрозы. Кроме того, конфиденциальность пользователей будет сохранена за счет децентрализации базы данных. Среди биометрических признаков выбран

отпечаток пальца, так как стойкость, различительные способности и эффективность отпечатка пальца считается более высокой. Также приведен небольшой обзор существующих криптосхемы разделения секрета для биометрической аутентификации.
Ключевые слова: разделение секрета; схема Шамира; аутентификация

1 Введение

В современных информационных системах хранится и обрабатывается большой объем данных, для обеспечения их сохранность и конфиденциальность нужно ограничить к ним доступ, предоставив его только доверенным пользователям и системам. Поэтому вопросы, связанные с методами аутентификация заслуживают особого внимания.

Самыми распространенными методами аутентификации являются:

– проверка подлинности на основе пароля;

– беспарольная аутентификация;

– двухфакторная/многофакторная аутентификация;

– социальная и биометрия аутентификация и т.д.

Остановимся на биометрии, так как данный метод предотвращает утечку или кражу персональной информации. Проверка проходит по физиологическим характеристикам пользователя, например, по отпечатку пальца, сетчатке глаза, тембру голоса, ДНК или даже характерные особенности набора текста на клавиатуре. Биометрические параметры не только уникальны, но и неотделимы часть от

человека, что позволяет с гораздо большей уверенностью говорить о подлинности пользователя.

Однако, использование современных биометрических технологий – это не только удобство и скорость, но и определенные риски, связанные с угрозой мошенничества.

Одним из самых уязвимых процессов в этой технологии считается снятия биометрических характеристик. Здесь возникает большое количество возможностей для атак, и методы защиты не всегда эффективны. Мы рассмотрим одну из существующих угроз, как кража информации. Биометрический образец, создаваемый сканером, может быть украден и использован в дальнейшем для подмены. Также существуют некоторые трудности связанный с размером базы данных хранения биометрического образца (шаблона). Для решения этих вопросов предлагается биометрическая аутентификация с использованием схемы разделения секрета (СРС). Совместное использование СРС и разделения баз данных по разным местам, поможет уменьшить размер базы данных и устранить угрозы в централизованной базе данных. Кроме того, конфиденциальность пользователей будет сохранена за счет децентрализации базы данных. Приведем небольшой обзор по результатам разных исследовании биометрических признаков. Среди биометрических признаков отпечаток пальца имеет большое значение в таких факторах, как стойкость, различительной способности и эффективности [1].

В работе [2] авторы показывают, что наиболее эффективным способом обеспечения доступности и конфиденциальности информации в случае утраты ключевой инфрмации

является методы разделения секрета, которые применяются для распределенного хранения данных. Недостаток данной схемы заключается в ее невысокой надежности. Если доля одного из пользователей утеряна, то секрет невозможно восстановить. По этой причине были разработаны (k, t)-*пороговые схемы разделения секрета.*

Пороговые СРС позволяют распределить секрет между абонентами (участниками) групп таким образом, чтобы легитимные абоненты могли однозначно восстановить секрет, а нелегитимные – не получали никакой дополнительной (по отношению к уже имеющейся) априорной информации о возможном содержании секрета.

В данной работе СРС будет применен для обеспечения безопасности шаблонов отпечатка пальцев при биометрической аутентификации.

2 Криптосхемы разделения секрета для биометрической аутентификации

Обмен секретами – это метод безопасного обмена информацией между несколькими сторонами. Секрет делится на части, распределяется между сторонами и восстанавливается уполномоченным набором сторон. Для защиты данных были разработаны различные методы обмена секретами. В статье [3] авторы исследуют улучшенную схему совместного использования секретов для биометрической аутентификации с использованием конечного поля. Мастер-копия биометрического шаблона преобразуется в конечное поле для маскировки подробной информации. Концепция совместного использования секретов используется для раз-

деления шаблона на несколько копий и поддерживается смарт-картой и общественным консорциумом. Такой подход обеспечивает идеальную биометрическую аутентификацию для работы со смарт-картами с высоким уровнем безопасности.

В работе [4] предлагается онлайн-схема (t, n) порогового обмена секретами, в которой система будет рассредоточивать первичный секретный ключ совместного использования K для n пользователей, и, по крайней мере, t пользователей вместе могут реконструировать секрет K. Безопасность схемы основана на биометрической проверке и аутентификации по пороговому паролю. Таким образом, предложенная схема не только защищена от нескольких распространенных атак, но также подходит для применения к другим приложениям, таких как системы охраны входа и системы управления казначейством.

Методы аутентификации, основанные на измерении биометрических параметров человека, обеспечивают почти стопроцентную идентификацию, решая проблемы утраты паролей и личных данных. Секретный обмен был применен для защиты этого биометрического образца, когда в анализируемой системе шаблон отпечатка пальца разделен на две частичные секреты с помощью основных методов визуальной криптографии, сохраняя одну часть у участника в виде ID-карты, а другую сохраняя в базе данных. Этот частичный секрет, хранящаяся в базе данных, будет одинаковый для всех участников. Такой подход решает две основные проблемы, связанные с системой на основе отпечатков пальцев, такие как фальсификация и дорогостоящее обслу-

живание большой базы данных отпечатков пальцев [5].

Увеличение количества пользователей расширяет размер базы данных, это привело к пространственной и временной сложности. Эти проблемы решились путем применения разработанной схемы в 2014 году [6]. заключалась в том, что секретный образ будет разделен на несколько частичные секреты с помощью визуальной криптографии, позже полученные частичные секреты будут сжатые с помощью IDCT и передается через Интернет, для восстановление всю информацию будут необходимы все части. Экспериментальные результаты показывают значительное снижение пространственной и временной сложности. Предоставление разных методов защиты для биометрических шаблонов и в то же время обеспечение высокой точности идентификации является актуальной исследовательской задачей как в настоящее время, так и в будущем. Следовательно, применение СРС в различных областях возрастает.

3 Схема разделения секрета

Основные понятия разделения секрета.

Разделение секрета (англ. secret sharing) – термин в криптографии, под которым понимают любой из способов распределения секрета среди группы участников, каждому из которых достается своя некая доля. Схема разделения данных (secret sharing scheme) – довольно редкий и специфический способ защиты информации. Разделение секрета является одной из наиболее широко изучаемых тем в теоретико-информационной криптографии. В схеме разделения сек-

рета, значение секрета распределяется на частичные секреты между набором участников таким образом, что только некоторые квалифицированные коалиции участников могут восстановить секрет стоимость своих акций.

Существующие схемы имеют две составляющие: разделение и восстановление секрета.

1. Разделение секрета – фаза раздачи, в рамках которой дилер, знающий секрет C, генерирует n долей $c_1, \ldots, c_n$ секрета и отправляет каждому участнику его долю по защищенному каналу связи. Раздача организовывается таким образом, чтобы легитимные абоненты только при совместных действиях могли восстановить секрет, а нелегетимные – не могли.

2. Восстановление секрета – фаза, при которой легитимные абоненты могут объединить свои частичные секреты и получить секрет. В большинстве рассматриваемых далее алгоритмов требуется обязательное участие в востановлении всех легитимных абонентов, между которыми была распределена “секретная” информация.

Существующие пороговые СРС:

– СРС Шамира [7];

– СРС Блэкли [8];

– СРС, основанная на эллиптической кривой [9];

– СРС Карнина – Грина – Хеллмана [10];

– СРС Асмута – Блума [11].

4 Применение (k,t) пороговую схему на базе непозиционной полиномиальной системы счисления (НПСС)

Основная цель алгоритма – разделить секрет, который необходимо зашифровать, на различные уникальные части (в нашем случае это шаблон отпечатка пальца). Исходное изображение (шаблон отпечатка пальца), получаемое от сенсора, проходит специализированную процедуру бинаризации с помощью известных алгоритмов. Далее, этот шаблон принимается в качестве секрета для распределения между участниками по схеме Шамира. В рассматриваемой схеме "участниками" являются децентрализованная база данных хранение шаблонов и пользователь. Предлагаемая схема аутентификации строится на модифицированном алгоритме разделения секрета, т.е. на базе непозиционной полиномиальной системы счисления.

Разделение секрета, так же называемой пороговой схемой основывается на модульной арифметике и китайской теореме об остатках.

В начале дадим формальное определение пороговой схемы: Будем говорить, что t участников A_i, где $i \in \{1, \ldots, t\}$, разделяют секрет C, где $1 < k \leq t$, если и только если выполняются следующие 3 условия:

1. Каждый участник A_i знает некоторую информацию $z_i(x)$, неизвестную остальным участником A_j , где $i \neq j$.
2. Секрет C легко может быть вычислен любым k значениями $z_i(x)$.

3. Знания любых $k-1$ значений $z_i(x)$, не важно каких, не позволяет определить секрет C.

Многочлены $z_1(x), \ldots, z_t(x)$, удовлетворяющие условиям 2 и 3, будем называть (k,t)-*пороговой схемой* для секрета C.

Схема аутентификации с применением модифицированного алгоритма разделения секрета на базе НПСС, осуществляется следующим образом.

Для этого:

1. Формируется НПСС: ее основаниями (рабочими) выбираются неприводимые многочлены $p_1(x), \ldots, p_t(x)$ над полем $GF(2)$ степени $m_1, \ldots, m_t$. Эти полиномы с учетом порядка их расположения образуют одну систему оснований. В соответствии с китайской теоремой об остатках все основания должны быть различными, в том числе и тогда, когда они имеют одну степень [12]. Рабочий диапазон НПСС определяется многочленом (модулем) $P_t(x) = \prod_{i=1}^{t} p_i(x)$ степени $m = \sum_{i=1}^{t} m_i$.

2. Для построение схемы разделения секрета: в качестве секрета рассматривается бинарный образ отпечатка пальца в виде многочлена $C(x)$ степени меньшей m, где $C(x) \equiv z_i(x) \pmod{p_i(x)}$. Значения $z_i(x)$ являются частичными секретами каждого участника A_i, $i \in \{1, \ldots, t\}$.

Восстановление секрета C выполняется следующим образом:

$$C = \sum_{i=1}^{t} z_i(x) B_i(x) \pmod{P_t(x)}. \qquad (1)$$

Далее определяются базисы НПСС по формуле (1) для восстановления результата по остаткам. Для этого вычисляются $\partial_i(x) \equiv \frac{P_t(x)}{p_i(x)} \pmod{p_i(x)}$ и инверсные к ним $\partial_i^{-1}(x)$: $\partial_i^{-1}(x) * \partial_i(x) \equiv 1 \pmod{p_i(x)}$, где $i \in \{1, \ldots, t\}$. Тогда базисы находятся по формуле:

$$B_i(x) = \partial_i^{-1}(x) * \frac{P_t(x)}{p_i(x)}.$$

Далее, если известны k значения $z_i(x)$, то легко вычислить секрет $C(x)$. В нашем случай $C(x)$ информация, которая преобразована из шаблона отпечатков пальцев пользователей при регистрации.

Преимущество такой системы, построенной на базе НПСС заключается в отсутствии избыточности, которая присутствует при использовании положительных целых чисел.

5 Заключение

Биометрическая техника включает в себя уникальную идентификацию человека на основе его физических или поведенческих характеристик. В основном он используется для аутентификации. В качестве биометрического параметра была выбрана дактилоскопия, поскольку отпечатки пальцев удобны в использовании и обладают высокой надежностью по сравнению с другими биометрическими данными. Такие схемы были бы полезны для областей, внедряющих биометрию, таких как правоохранительные органы, контроль доступа, банковских операции, управление персоналом и т.д.

В этой статье проведен обзор схемы разделения секрета и рассмотрен варианты применения его для биометрической аутентификации. Нами предложена схема на базе НПСС, одно из преимуществ является в том, что в ней нет избыточности, которая присутствует при использовании положительных целых чисел и возможность распараллеливания вычисления по основаниям.

6 Благодарность

Данная работа написана в рамках проекта AP14870719 “Разработка и исследование алгоритмов пост-квантовой криптографии, основанных на хеш-функциях”.

Библиографические ссылки

1. *Patil R.S., Patil S.D., Thepade S.D.* Secret Sharing based Secure Authentication System // Int. J. Comp. App. 2015. Vol. 118, Iss. 22. P. 8–11.

2. Актуальные киберугрозы: II квартал 2018 года [Электронный ресурс].
URL: `https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2018-q2`
(дата обращения: 14.09.2023).

3. *Kumar N.R., Krisnan R.B., Raajan N.R.* An Improved Secret Sharing Scheme for Biometric Authentication using Finite Field // Int. J. Rec. Tech. Eng. 2019. Vol. 8. P. 1–4.

4. *Li C.T., Hwang M.* An online biometrics-based secret sharing scheme for multiparty cryptosystem using smart cards // Int. J. Inn. Comp. Inf. Con. 2010. Vol. 6. P. 1–8.

5. *Patil S., Tajane K., Sirdeshpande J.* Secret sharing schemes for secure biometric authentication // Int. J. Sc. Eng. Res. 2013. Vol. 6. P. 1–6.

6. Design and Implementation of Secure Biometric Based Authentication System Using RFID and Secret Sharing / Patil S.D. [et al.] // 2nd Int. Conf. Conv. Tech. 2017. P. 480–482.

7. *Stadler M.* Publicly verifiable secret sharing // Int. Conf. Th. App. Crypt. Tech. 1996. Vol. 1070. P. 190–199.

8. *Bozkurt I.N.* Threshold cryptography is based on blakely secret sharing // Information Sciences. 2008. P. 1–4.

9. *Медведев Н.В., Титов С.С.* Почти пороговые схемы разделения секрета на эллиптических кривых // Доклады ТУСУР. 2011. Ном. 1. С. 91–95.

10. *Karnin E., Greene J., Hellman M.* On secret sharing systems // IEEE Trans. Inf. Th. 1983. Vol. 29. P. 35–41.

11. *Ito M., Saito A., Nishizeki T.* Secret sharing scheme realizing general access structure // El. Com. Japan. 1989. Vol. 72, No. 9. P. 56–64.

12. *Виноградов И.М.* Основы теории чисел. М. : Наука, 1965.

ОБ ОРГАНИЗАЦИИ НАУЧНОЙ РАБОТЫ НА ФАКУЛЬТЕТЕ ПРИКЛАДНОЙ МАТЕМАТИКИ И ИНФОРМАТИКИ БЕЛОРУССКОГО ГОСУДАРСТВЕННОГО УНИВЕРСИТЕТА

Ю.Л. Орлович[1], И.Н. Сафонова[2]
[1,2]*Белорусский государственный университет*
Минск, БЕЛАРУСЬ
e-mail: [1]orlovich@bsu.by, [2]safonova@bsu.by

Научно-исследовательская работа на ФПМИ, проводится в соответствии с приоритетными направлениями научной, научно-технической и инновационной деятельности Республики Беларусь на 2021–2025 годы, утвержденные Указом Президента Республики Беларусь от 7 мая 2020 г. ном. 156.

Научные исследования и разработки выполняют 11 кафедр, 2 научно-исследовательские лаборатории (НИЛ) в составе кафедр ИСУ и ТВиМС, работают 4 студенческие научно-исследовательские лаборатории (СНИЛ) и 6 студенческих научных кружков (СНК). На факультете функционируют известные в Республике Беларусь и за рубежом Научные школы, Совет молодых ученых ФПМИ и Совет по НИРСА.

Ключевые слова: научная работа; прикладная математика; информатика; инновации

1 Выполнение НИР

ФПМИ принимает участие в выполнении трех Государственных программ научных исследований на 2021–2025 годы: “Энергетические и ядерные процессы и технологии”, “Цифровые и космические технологии, безопасность человека, общества и государства”, “Конвергенция-2025”, по

двум из них осуществляет научно-организационное сопровождение в части заданий и НИР, выполняемых учреждениями Министерства образования Республики Беларусь.

Совместно с Институтом тепло- и массообмена им. А.В. Лыкова НАН Беларуси факультет участвует в выполнении мероприятия Государственной программы "Наукоемкие технологии и техника" на 2021–2025 годы (Подпрограмма 3 "Научное обеспечение эффективной и безопасной работы Белорусской атомной электростанции и перспективных направлений развития атомной энергетики"). ФПМИ принимает участие в выполнении Государственной программы "Обеспечение национальной безопасности".

Сотрудники факультета выполняют НИР по госбюджетным и хозяйственным договорам с организациями и предприятиями Республики Беларусь, договорам с БРФФИ, в том числе в рамках международного научного и научно-технического сотрудничества, осуществляют выполнение международных контрактов, НИР в пределах основного рабочего времени. Выполнение НИР осуществляется научными сотрудниками, профессорско-преподавательским составом, к их выполнению привлекаются докторанты, аспиранты, магистранты и студенты.

Результаты выполнения НИР на ФПМИ активно используются в учебном процессе при составлении учебных планов и программ, разработке лекционных курсов, при проведении лабораторных и практических занятий, чтении спецкурсов, при выполнении курсовых и дипломных работ, а также обучающимися при работе над магистерскими, кандидатскими и докторскими диссертациями.

Кафедры ФПМИ активно осуществляют инновационную деятельность в образовательном процессе и производстве, используя информационные ресурсы, интерактивные формы обучения, новые формы контроля знаний (в том числе связанные с информационными технологиями). В учебный процесс внедряются современные методы дистанционного обучения. На лекциях, практических и семинарских занятиях используются презентационные материалы и другие возможности, связанные с информационными технологиями.

Многие сотрудники ФПМИ являются членами государственных экспертных и научно-технических советов.

2 Аспирантура и докторантура

Планирование подготовки научных работников высшей квалификации на факультете осуществляется в соответствии с кадровыми потребностями кафедр и НИЛ. Цель планирования – формирование контингента интеллектуально-творческих работников для обеспечения успешного функционирования ФПМИ и в целом БГУ. Планирование и подготовка кадров высшей квалификации проводится в соответствии с требованиями нормативных документов.

Факультет ведет подготовку научных работников высшей квалификации в аспирантуре и докторантуре по следующим восьми специальностям (в том числе и на английском языке):

01.01.02 “Дифференциальные уравнения, динамические

системы и оптимальное управление”;

01.01.05 “Теория вероятностей и математическая статистика”;

01.01.07 “Вычислительная математика”;

01.01.09 “Дискретная математика и математическая кибернетика”;

05.13.11 “Математическое и программное обеспечение вычислительных машин, комплексов и компьютерных сетей”;

05.13.17 “Теоретические основы информатики”;

05.13.18 “Математическое моделирование, численные методы и комплексы программ"; 05.13.19 "Методы и системы защиты информации, информационная безопасность”.

Вся образовательная и научная деятельность кафедр и НИЛ факультета, научных руководителей курсовых, дипломных и магистерских работ, организаторов НИРС, Совета молодых ученых направлена на решение следующих задач:

– создание дополнительных условий для овладения обучающимися научными методами познания, углубленного освоения учебного материала;

– формирование профессиональных компетенций, потребности в знаниях и продолжении научной работы, создание научного “задела” для проведения диссертационного исследования, начиная с младших курсов;

– системная работа с обучающимися с целью выявления потенциальных кандидатов для поступления в аспирантуру;

– повышение качества отбора выпускников для дальнейшего обучения в аспирантуре;

– укрепление преемственности поколений исследователей в рамках деятельности научных школ ФПМИ;

– обеспечение положительной динамики защит диссертаций в срок окончания обучения в аспирантуре.

К руководству аспирантами и докторантами привлекаются наиболее опытные, высококвалифицированные ученые, известные своими достижениями как в Республике Беларусь, так и далеко за пределами. Среди них академики НАН Беларуси Абламейко С.В., Харин Ю.С., члены-корреспонденты Ковалев М.Я., Матус П.П., Тузиков А.В., доктора наук Астровский А.И., Васьковский М.М., Калинин А.И., Котов В.М., Краснопрошин В.В., Недзьведь А.М., Харин А.Ю. и др.

Для отбора выпускников с целью их дальнейшего обучения в аспирантуре, на ФПМИ применяются разнообразные формы НИРС, которые нацелены на раннее выявление способных студентов. Важнейшей целью НИРС является активное вовлечение студентов в научно-исследовательскую деятельность, включая работу по НИР кафедр, участие в работе СНИЛ и СНК, что способствует наращиванию кадрового потенциала научных школ ФПМИ.

На факультете осуществляется комплекс мероприятий, а также используются существующие в БГУ методы стимулирования сотрудников, аспирантов, докторантов и их научных руководителей/консультантов при осуществлении подготовки научных работников высшей квалификации. С

этой целью применяются утвержденные в БГУ Положение “О премировании за эффективную подготовку научных работников высшей квалификации” и Положение “О назначении надбавок аспирантам”.

Все это обеспечивает непрерывность процесса роста и совершенствования будущего ученого по схеме: “СНК – СНИЛ – Магистратура – Аспирантура – Докторантура”.

Ежегодно на ФПМИ успешно проходят защиты кандидатских и докторских диссертаций. Так в феврале 2023 года уже защищена 1 кандидатская диссертация, прошли предварительную экспертизу и подают документы в Советы еще три кандидатские диссертации.

По решению ВАК диссертации, защищаемые сотрудниками ФПМИ, неоднократно становились лучшими диссертациями года. Так, в 2019 году победителем ежегодного конкурса на лучшую докторскую диссертацию с вручением диплома лауреата конкурса в номинации “естественные науки” признана диссертация заведующего кафедрой ТВиМС Харина А.Ю. “Робастность байесовских и последовательных статистических решений”.

Многие сотрудники ФПМИ являются членами Советов по защите диссертаций, членами экспертных советов ВАК, выступают в качестве экспертов и официальных оппонентов при защите диссертаций, являются председателями и членами государственных аттестационных комиссий.

3 Международные и республиканские конференции, конгрессы, симпозиумы

Ежегодно, в соответствии с Планом проведения научных и научно-практических мероприятий БГУ, факультетом проводятся международные и республиканские конференции, конгрессы, симпозиумы и др. Студенты и аспиранты ФПМИ принимают активное участие в ежегодной научной конференции студентов и аспирантов БГУ. Традиционно факультет организует работу секций данной конференции (“Актуарная математика”, “Информатика”, “Компьютерная безопасность”, “Прикладная математика”, “Экономическая кибернетика”, “Педагогика”).

В 2023 году на базе факультета запланировано проведение трех международных конференций:

– Международная научная конференция “Теоретическая и прикладная криптография”;

– Международная научная конференция “Распознавание образов и обработка информации” (International Scientific Conference “Pattern Recognition and Information Processing” – PRIP 2023);

– 4-я Международная научно-практическая конференция “Непрерывное ориентированное образование в области математики и естественных наук: состояние, развитие, перспективы”.

В работе конференций традиционно принимает участие большое число ученых и специалистов из разных стран как ближнего, так и дальнего зарубежья. На этих мероприя-

тиях ученые и специалисты обмениваются опытом, рассказывают о своих достижениях, обсуждают актуальные проблемы фундаментальных и прикладных исследований, используют возможность наладить связи и дальнейшее взаимовыгодное сотрудничество с коллегами из разных стран по всем направлениям.

Ежегодно ученые ФПМИ принимают также активное участие в работе международных, республиканских конференций, проводимых на базе различных учреждений и организаций как в Республике Беларусь, так и в странах ближнего и дальнего зарубежья, выступают с докладами на конференциях международного и республиканского уровня. Участие в международных конференциях сотрудников факультета не ограничивается выступлениями с докладами (в том числе в качестве приглашенных докладчиков), а включает в себя также непосредственную работу в программных и организационных комитетах конференций в качестве председателей и секретарей секций.

4 Публикации в научных изданиях

Результаты исследований и разработок ученых ФПМИ находят отражение в издаваемых монографиях, учебных пособиях, материалах и тезисах докладов научных конференций и других научных и учебных изданиях. Сотрудники ФПМИ успешно публикуются в рецензируемых научных журналах Республики Беларусь, входящих в перечень ВАК, а также в зарубежных журналах, входящих в БД Scopus и Web of Science. Многие сотрудники факультета

являются членами редакционных коллегий отечественных и зарубежных журналов.

В 2022 году ФПМИ опубликовано 23 научных и учебных книжных изданий, в том числе 3 монографии, 2 сборника научных трудов, входящих в перечень ВАК, 3 сборника материалов и тезисов докладов на научных конференциях, 15 других научных и учебных изданий. Сотрудниками факультета опубликовано 248 научных статей в научных журналах и др. научных изданиях, из них: 148 в Республике Беларусь (26 входит в перечень ВАК) и 100 за рубежом (75 входит в базы Scopus и Web of Science).

5 Работа Совета по НИРС и Совета молодых ученых ФПМИ

Научно-исследовательская работа студентов на ФПМИ организуется в соответствии с Методическими рекомендациями по организации научно-исследовательской работы студентов учреждений высшего образования, Положением о системе организации научно-исследовательской работы студентов БГУ, Положением о Совете молодых ученых БГУ и Стратегией развития системы научно-исследовательской работы студентов и аспирантов БГУ на 2021–2025 годы.

Система научных мероприятий организации молодежной науки на ФПМИ является эффективным механизмом выявления, поощрения и стимулирования студентов, способных к научно-исследовательской деятельности.

На факультете функционируют 4 СНИЛ, 6 СНК, Совет по НИРСА и СМУ.

Ежегодно сотрудники и обучающиеся ФПМИ выступают в качестве организаторов и принимают участие в ряде проводимых в БГУ мероприятиях для студентов, аспирантов и молодых ученых:

– республиканском конкурсе научных работ студентов;

– конкурсе на лучшего руководителя и организатора научно-исследовательской работы студентов и аспирантов БГУ;

– конкурсе на лучшую СНИЛ БГУ;

– конкурсе грантов в области интеллектуальных информационных систем для студентов и аспирантов БГУ;

– конкурсе на соискание премий имени В.И. Пичеты и А.Н. Севченко для молодых ученых;

– конкурсе ФПМИ на лучшую научную студенческую работу;

– научной конференции студентов и аспирантов БГУ;

– открытом республиканском конкурсе для назначения стипендий Президента Республики Беларусь талантливым молодым ученым;

– республиканском конкурсе по назначению стипендий Президента Республики Беларусь для аспирантов;

– конкурсе научных проектов для участия в совместном тематическом конкурсе Министерства образования Республики Беларусь и БРФФИ для молодых ученых “БРФФИ – Минобразование М”;

– выставке достижений молодежной науки БГУ;

– заседаниях Совета по НИРСА и Совета молодых ученых БГУ.

С инициативой о проведении Конкурса грантов в области интеллектуальных информационных систем для студентов и аспирантов БГУ выступила СНИЛ “Интеллектуальные информационные системы” кафедры ИСУ (научные руководители – заведующий кафедрой ИСУ Краснопрошин В.В. и доцент Вальвачев А.Н.).

Молодые ученые ФПМИ принимают участие в ежегодном Республиканском конкурсе по назначению стипендий Президента Республики Беларусь талантливым молодым ученым. Так, в соответствии с распоряжениями Президента Республики Беларусь “О поощрении талантливых молодых ученых” президентской стипендии на 2021 год был удостоен заведующий кафедрой ТВиМС доктор физ.-мат. наук Харин А.Ю., в 2022 году заведующий кафедрой ВМ доктор физ.-мат. наук Васьковский М.М.

В конкурсе по назначению стипендии Президента аспирантам в 2023 году, стипендии удостоен аспирант 2 года обучения Мацкевич В.В. “за разработку и программную реализацию алгоритма обучения нейронных сетей на основе метода отжига, включающего оригинальную процедуру распараллеливания данных, что существенно повышает качество и скорость обучения и способствует эффективному решению широкого спектра прикладных задач в области технических наук, медицины, дистанционного зондирования Земли” (научный руководитель – заведующий кафедрой ИСУ, доктор тех. наук Краснопрошин В.В.).

В соответствии с Положением о конкурсе на лучшую студенческую научно-исследовательскую лабораторию БГУ руководители СНИЛ ФПМИ ежегодно становятся победителями в различных номинациях с вручением дипломов БГУ. Так, в 2023 году следует отметить победу СНИЛ ФПМИ в номинациях “Вклад СНИЛ в подготовку кадров высшей квалификации” (научный руководитель – заведующий кафедрой ММАД, доктор экономических наук, Малюгин В.И.), “СНИЛ с наилучшей положительной динамикой за последние три года” (научные руководители – заведующий кафедрой ИСУ Краснопрошин В.В. и доцент Вальвачев А.Н.).

По результатам конкурса на лучшего руководителя и организатора НИРСА БГУ в номинации “Популяризация науки среди студенческой молодежи и школьников” в 2023 году победили Задворный Б.В. (1 премия), Буславский А.А. (2 премия).

Лучшие студенты, выпускники и научные руководители ФПМИ за успехи в НИРС неоднократно отмечались дипломами и награждались денежными поощрениями из средств специального фонда Президента Республики Беларусь по социальной поддержке одаренных учащихся и студентов. Более 20 лет активно работают с одаренной молодежью заведующий кафедрой ММАД, доктор экономических наук, доцент Малюгин В.И., заместитель декана по профориентации и дополнительному образованию, канд. физ.-мат. наук, доцент Задворный Б.В. и др.

Ежегодно обучающиеся ФПМИ принимают активное участие и становятся лауреатами и победителями Респуб-

ликанского конкурса научных работ студентов.

Студенты и аспиранты под руководством сотрудников кафедр принимают активное участие в научных конференциях и конкурсах различного уровня, участвуют в выполнении НИР, в том числе и на платной основе.

В 2022 году были опубликованы более 100 работ в числе авторов (соавторов) которых были студенты и аспиранты.

6 Международное научное и научно-техническое сотрудничество

ФПМИ имеет тесные творческие связи и долгосрочные программы сотрудничества со многими зарубежными партнерами.

Важнейшими направлениями международного научного и научно-технического сотрудничества на ФПМИ являются: выполнение договоров о сотрудничестве с зарубежными организациями, участие в выполнении совместных программ и проектов.

В рамках подписанных международных соглашений с зарубежными организациями, факультет осуществляет взаимовыгодное международное научное и научно-техническое сотрудничество в области математики и информационных технологий, включающее в себя обмен научными сотрудниками и преподавателями для чтения лекций и консультаций, проведение научных стажировок, выполнение совместных научно-исследовательских работ над проектами, обмен информацией, учебными материалами и результатами научных исследований.

Так в 2022 году выполнялось 4 проекта БРФФИ в рамках совместных конкурсов с аналогичными фондами и организациями 2 стран: Российская Федерация, Республика Армения.

Совместно с зарубежными организациями ФПМИ осуществляет проведение научных конференций и семинаров. Результатом проведения совместных научных исследований являются публикации научных статей с зарубежными коллегами в международных высокорейтинговых журналах. Сотрудники факультета выполняют международные научные контракты по заказам зарубежных партнеров. Факультет осуществляет подготовку иностранных граждан в аспирантуре, в том числе и на английском языке.

7 Сотрудничество с НАН Беларуси

ФПМИ имеет тесные творческие связи и долгосрочные программы сотрудничества с организациями и предприятиями реального сектора экономики Республики Беларусь, а также с организациями Национальной академии наук Беларуси.

К основным формам сотрудничества относятся:

– выполнение научных исследований и разработок в рамках совместных программ и проектов, главным образом, в рамках ГПНИ, ГП, хозяйственных и бюджетных договоров;

– участие ученых и специалистов ФПМИ и НАН Беларуси в работе научных советов по ГПНИ “Конвергенция-2025” и “Цифровые и космические технологии, без-

опасность человека, общества и государства", а также советов по защитам диссертаций, научных и научно-технических советов, комитетов, комиссий, членство в редакционных коллегиях академических и университетских изданий;

– проведение совместных научных мероприятий: конференций, симпозиумов и др.;

– предоставление ученым и специалистам ФПМИ возможности использования материально-технической базы и научного оборудования НАН Беларуси для учебных и исследовательских целей;

– участие сотрудников НАН Беларуси в учебном процессе и подготовке кадров высшей квалификации на ФПМИ;

– консультации, согласование тем научных исследований, совместные публикации, консультирование студентов по тематике дипломных работ, прохождение преддипломной практики.

ФПМИ имеет тесные научные контакты с ведущими специалистами ГНУ "Институт физики им. Б.И. Степанова НАН Беларуси", ГНУ "Институт математики НАН Беларуси", ГНУ "Институт тепло- и массообмена им. А.В. Лыкова НАН Беларуси", ГНУ "Объединенный институт проблем информатики НАН Беларуси".

8 Учебно-научно-производственный кластер “Математика и информационные технологии (МИТ)”

В 2019 году ФПМИ совместно с ММФ, НИИ ППМИ и ЦИТ подписал Соглашение о создании и функционировании “Учебно-научно-производственного кластера по подготовке специалистов в области математики и информационных технологий БГУ”.

Основные направления научно-технической и инновационной деятельности кластера:

– развитие сотрудничества и проведение совместных научных исследований;

– выполнение международных научных договоров и контрактов;

– совместное проведение международных и республиканских научных конференций, научной конференции студентов и аспирантов БГУ;

– участие в научных конкурсах БГУ;

– совместные научные публикации с зарубежными авторами в международных журналах;

– выполнение работ в рамках международных договоров о научном сотрудничестве с зарубежными организациями.

СТАТИСТИЧЕСКОЕ ТЕСТИРОВАНИЕ КРИПТОГРАФИЧЕСКИХ ГЕНЕРАТОРОВ НА ОСНОВЕ СЛОЖНОЙ НУЛЕВОЙ ГИПОТЕЗЫ

В.Ю. Палуха[1], Ю.С. Харин[2]
[1,2]*НИИ прикладных проблем математики и информатики*
[1,2]*Белорусский государственный университет*
Минск, БЕЛАРУСЬ
e-mail: [1]palukha@bsu.by, [2]kharin@bsu.by

В докладе рассматривается построение решающего правила для статистического тестирования криптографических генераторов на основе сложной нулевой гипотезы с использованием оценки энтропии Тсаллиса.

Ключевые слова: статистическое тестирование; криптографические генераторы; сложная нулевая гипотеза; энтропия Тсаллиса

1 Введение

Одним из важнейших элементов систем криптографической защиты информации (СКЗИ) являются генераторы случайных и псевдослучайных последовательностей. Стойкость СКЗИ зависит от того, насколько близка генерируемая последовательность по своим свойствам к равномерно распределенной случайной последовательности (РРСП), которая на практике называется “чисто случайной” последовательностью. Для проверки качества криптографических генераторов используются статистические тесты, в которых проверяется нулевая гипотеза о том, что наблюдаемая последовательность является РРСП. Известные наборы (батареи) статистических тестов проверяют простую

нулевую гипотезу. Однако на практике возможны незначительные отклонения тестируемой последовательности от модели. Например, вероятности фрагментов длины s (s-грамм) могут отличаться от 2^{-s} на близкую к нулю величину ε. В данном докладе рассмотрено построение статистического теста на основе сложной нулевой гипотезы с использованием оценки энтропии Тсаллиса.

2 Оценки энтропии

Пусть имеется случайная выборка $X_n = \{x_t : t = 1, \ldots, n\}$ объема n из распределения вероятностей $\{p_k\}$. Построим частотные оценки распределения вероятностей $\{p_k : k = 1, \ldots, N\}$:

$$\hat{p}_k = \frac{v_k}{n}, \quad v_k = \sum_{t=1}^{n} I\{x_t = \omega_k\} \in \mathbb{N}_0 = \mathbb{N} \cup \{0\}, \qquad (1)$$

$$I\{x_t = \omega_k\} = \begin{cases} 1, \ x_t = \omega_k; \\ 0, \ x_t \neq \omega_k. \end{cases} \qquad (2)$$

Введем в рассмотрение нулевую гипотезу $H_0 = \{\{x_t\}$является РРСП$\} = \{\{x_t\}$ – н.о.р.с.в., $p_k = p_k^0 = 1/N, \ k = 1, \ldots, N\}$ и альтернативу общего вида $\overline{H_*}$. Будем полагать, что имеет место схема серий. В таком случае вектор $(v_1, \ldots, v_N)^T$, составленный из частот v_k из (1), (2) имеет полиномиальное распределение вероятностей $Pol(n, N, p_1, \ldots, p_N)$, а каждая из компонент распределена по биномиальному закону $Bi(n, p_k)$. Рассмотрим специальную асимптотику:

$$n, \ N \to \infty, \ n/N \to \lambda, \ 0 < \lambda < \infty, \qquad (3)$$

которая отличается от классической ($n \to \infty, N < \infty$) тем, что длительность наблюдения n и число значений (сложность модели) N растут синхронно. В асимптотике (3) для распределения вероятностей статистик (v_k справедлива аппроксимация законом Пуассона $\Pi(\lambda_k)$ с параметром $\lambda_k = np_k$. При истинной гипотезе H_0 все элементарные вероятности равны: $p_k = 1/N, k = 1, \ldots, N$, поэтому все частоты v_k имеют одинаковый параметр распределения Пуассона $\lambda = n/N$.

В [1] доказана теорема об асимптотически нормальном распределении статистик, являющихся функциями от частот v_k, которую кратко можно переформулировать следующим образом. Пусть $f(\cdot) : \mathbb{N}_0 \to \mathbb{R}$ – некоторая функция; $Z = \sum_{k=1}^{N} f(v_k)$, где $v_k, k = 1, \ldots, N$, – частоты с совместным полиномиальным распределением, аппроксимированным законом Пуассона в асимптотике (3). Тогда при выполнении ряда условий регулярности статистика Z имеет асимптотически нормальное распределение:

$$\mathcal{L}\left\{\frac{Z-\mu}{\sigma}\right\} \to \mathcal{N}_1(0,1),$$

$$\mu = \sum_{k=1}^{N} E\{f(v_k)\}, \tag{4}$$

$$\sigma^2 = \sum_{k=1}^{N} D\{f(v_k)\} - \left(\sum_{k=1}^{N} cov\{v_k,\ f(v_k)\}\right)^2 \Big/ n, \tag{5}$$

где $\mathcal{N}_1(0,1)$ – стандартный одномерный нормальный закон распределения вероятностей с нулевым математическим ожиданием и единичной дисперсией, $E\{\xi\}$ и $D\{\xi\}$ –

соответственно математическое ожидание и дисперсия случайной величины ξ, $cov\{\xi,\eta\}$ – ковариация случайных величин ξ и η.

Перейдем теперь к статистическому оцениванию функционала энтропии Тсаллиса при $r=2$:

$$S_r(p)=\frac{1}{r-1}\left(1-\sum_{k=1}^{N}p_k^r\right),\quad S_2(p)=1-\sum_{k=1}^{N}p_k^2. \tag{6}$$

Видно, что энтропия Тсаллиса является функцией от величины

$$P_2(p)=\sum_{k=1}^{N}p_k^2. \tag{7}$$

Следовательно, возникает задача статистического оценивания величины $P_r(p)$.

Известно [2], что статистическая оценка для (7) $\hat{P}_2(P)=\sum_{k=1}^{N}\hat{p}_k^2=\sum_{k=1}^{N}\left(\frac{v_k}{n}\right)^2$, построенная по подстановочному принципу, является смещенной. Для построения асимптотически несмещенной оценки определим 2-ю нисходящую факториальную степень x:

$$x^{\underline{2}}=x(x-1). \tag{8}$$

В [2] предложена статистическая оценка для (7), которая основана на (8):

$$\tilde{P}_2(p)=\sum_{k=1}^{N}\frac{v_k^{\underline{2}}}{n^2}. \tag{9}$$

Согласно [2], оценка (9) в асимптотике (3) является асимптотически несмещенной и состоятельной.

Положим

$$f(v)=v^{\underline{2}}=v(v-1),$$

$$Z_{n,2} = \sum_{k=1}^{N} f(v_k) = \sum_{k=1}^{N} v_k^2 = n^2 \tilde{P}_2(p). \tag{10}$$

Теорема 1. *[3]. При истинной гипотезе H_0 в асимптотике* (3) *статистика* (10) *имеет асимптотически нормальное распределение:*

$$\mathcal{L}\left\{\frac{Z_{n,2} - \mu_{n,2}}{\sigma_{n,2}}\right\} \to \mathcal{N}_1(0,1),$$

$$\mu_{n,2} = N\lambda^2 = n\lambda, \tag{11}$$

$$\sigma_{n,2}^2 = 2n\lambda. \tag{12}$$

Согласно (6) и (10) статистическая оценка энтропии Тсаллиса выражается через $Z_{n,2}$, о чем свидетельствует следующая лемма.

Лемма 1. *[3]. Статистическая оценка энтропии Тсаллиса, построенная с использованием оценки* (9)*, выражается через статистику* (10)*:*

$$\hat{S}_2(n,\ N) = 1 - \sum_{k=1}^{N} \frac{v_k^2}{n^2} = 1 - \frac{Z_{n,2}}{n^2}. \tag{13}$$

Используя полученные результаты, построим статистическую оценку энтропии Тсаллиса.

Теорема 2. *[3]. В асимптотике* (3) *статистика* (13) *является состоятельной асимптотически несмещенной оценкой энтропии Тсаллиса и при истинной гипотезе H_0 имеет асимптотически нормальное распределение:*

$$\mathcal{L}\left\{\frac{\hat{S}_r - \mu_{S,r}}{\sigma_{S,r}}\right\} \to \mathcal{N}_1(0,1),$$

$$\mu_{S,2} = 1 - \frac{1}{N}, \tag{14}$$

$$\sigma^2_{S,2} = \frac{2}{Nn^2}. \tag{15}$$

Введем в рассмотрение сложную нулевую гипотезу $H_0^{(\varepsilon)}$, согласно которой для распределения вероятностей $\{p_k\}$ справедливо

$$p_k = \frac{1}{N} + \varepsilon_k,\ k = 1,\ \ldots,\ N, \tag{16}$$

$$\sum_{k=1}^{N} \varepsilon_k = 0, \quad \sum_{k=1}^{N} \varepsilon_k^2 = \varepsilon^2,\ 0 < \varepsilon \leq \varepsilon_+.$$

Заметим, что при $\varepsilon = 0$ получаем гипотезу H_0, поскольку $\varepsilon_k = 0,\ k = 1,\ \ldots,\ N$.

В асимптотике (3) для распределения вероятностей статистик $\{v_k\}$ справедлива аппроксимация законом Пуассона $\Pi(\lambda_k)$ с параметром

$$\lambda_k = np_k = \frac{n}{N} + n\varepsilon_k = \lambda + n\varepsilon_k. \tag{17}$$

Теорема 3. *При истинной гипотезе* $H_0^{(\varepsilon)}$ *в асимптотике* (3) *статистика* (10) *имеет асимптотически нормальное распределение:*

$$\mathcal{L}\left\{\frac{Z_{n,2} - \mu_{n,2}^{(\varepsilon)}}{\sigma_{n,2}^{(\varepsilon)}}\right\} \to \mathcal{N}_1(0,1),$$

$$\mu_{n,2}^{(\varepsilon)} = \frac{n^2}{N} + n^2 \sum_{k=1}^{N} \varepsilon_k^2 = n\lambda + n^2\varepsilon^2, \tag{18}$$

$$\sigma_{n,2}^{2(\varepsilon)} = \frac{2n^2}{N} + \left(\frac{4n^3}{N} + 2n^2\right)\varepsilon^2 + 4n^3\left(\sum_{k=1}^{N} \varepsilon_k^3 - \varepsilon^4\right). \tag{19}$$

Теорема 4. *В асимптотике* (3) *статистика* (13) *является состоятельной асимптотически несмещенной оценкой энтропии Тсаллиса и при истинной гипотезе* $H_0^{(\varepsilon)}$ *имеет асимптотически нормальное распределение:*

$$\mathcal{L}\left\{\frac{\hat{S}_r - \mu_{S,2}^{(\varepsilon)}}{\sigma_{S,2}^{(\varepsilon)}}\right\} \to \mathcal{N}_1(0,1),$$

$$\mu_{S,2}^{(\varepsilon)} = 1 - \frac{1}{N} - \sum_{k=1}^{N} \varepsilon_k^2 = \mu_{S,2} - \varepsilon^2, \tag{20}$$

$$\sigma_{S,2}^{2(\varepsilon)} = \sigma_{S,2}^2 + \frac{2}{n^2}(2\lambda+1)\,\varepsilon^2 + \frac{4}{n}\left(\sum_{k=1}^{N}\varepsilon_k^3 - \varepsilon^4\right). \tag{21}$$

Лемма 2. *В условиях гипотезы* $H_0^{(\varepsilon)}$ *справедливо:*

$$\sum_{k=1}^{N} \varepsilon_k^3 \le \frac{\varepsilon^3(N-2)}{\sqrt{N(N-1)}} < \varepsilon^3. \tag{22}$$

Следствие. *Для* (20) *и* (21) *с учетом* $\varepsilon \le \varepsilon_+$ *справедливы оценки снизу и сверху соответственно:*

$$\mu_{S,2}^{(\varepsilon)} = \mu_{S,2} - \varepsilon^2 \ge \mu_{S,2}^{(\varepsilon_+)} = \mu_{S,2} - \varepsilon_+^2, \tag{23}$$

$$\sigma_{S,2}^{2(\varepsilon)} < \sigma_{S,2}^2 + \frac{2}{n^2}(2\lambda+1)\,\varepsilon^2 + \frac{4\varepsilon^3}{n}(1-\varepsilon). \tag{24}$$

Легко показать, что при $0 < \varepsilon \le \varepsilon_+ \le \dfrac{3}{4}$ функция $f(\varepsilon) = \varepsilon^3 - \varepsilon^4$ монотонно возрастает. Тогда на основе (24) при выполнении указанного условия получим

$$\sigma_{S,2}^{2(\varepsilon)} < \sigma_{S,2}^{2(\varepsilon_+)} = \sigma_{S,2}^2 + \frac{2}{n^2}(2\lambda+1)\,\varepsilon_+^2 + \frac{4\varepsilon_+^3}{n}(1-\varepsilon_+). \tag{25}$$

3 Решающее правило

Теорема 5. *Пусть* $\alpha \in (0,\ 1)$ *– заданный уровень значимости. Тогда в асимптотике* (3) *при истинной гипотезе* $H_0^{(\varepsilon)}$ *и* $0 < \varepsilon_+ \leq \dfrac{3}{4}$ *для статистики* (13) *справедливо*

$$P\left\{\Delta_- < \hat{S}_2 < \Delta_+\right\} \geq 1 - \alpha, \tag{26}$$

$$\Delta_- = \mu_{S,2}^{(\varepsilon_+)} - \sigma_{S,2}^{2(\varepsilon_+)}\Phi^{-1}\left(1 - \frac{\alpha}{2}\right),$$

$$\Delta_+ = \mu_{S,2} + \sigma_{S,2}^{2(\varepsilon_+)}\Phi^{-1}\left(1 - \frac{\alpha}{2}\right),$$

где Φ *– функция распределения стандартного нормального закона [4].*

На основе (26) построим решающее правило. Пусть вычислена статистика (13) и задан уровень значимости $\alpha \in (0,\ 1)$, тогда

$$\text{принимается} \quad \begin{cases} H_0^{(\varepsilon)}, \text{ если } \Delta_- < \hat{S}_2 < \Delta_+, \\ \overline{H_0^{(\varepsilon)}}, \text{ в противном случае,} \end{cases} \tag{27}$$

$$\Delta_- = \mu_{S,2}^{(\varepsilon_+)} - \sigma_{S,2}^{2(\varepsilon_+)}\Phi^{-1}\left(1 - \frac{\alpha}{2}\right),$$

$$\Delta_+ = \mu_{S,2} + \sigma_{S,2}^{2(\varepsilon_+)}\Phi^{-1}\left(1 - \frac{\alpha}{2}\right),$$

$$\varepsilon_+ \leq \frac{3}{4}.$$

Библиографические ссылки

1. *Holst L.* Asymptotic normality and efficiency for certain goodness-of-fit tests // Biometrika. 1972. Vol. 59. P. 137–145.

2. *Acharya J.* Estimating Renyi Entropy of Discrete Distributions // IEEE Trans. Inf. Th. 2017. Vol. 63, Iss. 1. P. 38–56.

3. *Харин Ю.С., Палуха В.Ю.* Статистические оценки энтропии Реньи и Тсаллиса и их использование для проверки гипотез о “чистой случайности” // Весці НАН Беларусі. Серыя фізіка-матэматычных навук. 2016. Ном. 2. С. 37–47.

4. *Харин Ю.С., Зуев Н.М., Жук Е.Е.* Теория вероятностей, математическая и прикладная статистика. Минск: БГУ, 2011.

ВАРИАНТ РЕАЛИЗАЦИИ НИЗКОРЕСУРСНОГО БЛОКЧЕЙНА ДЛЯ ИНДУСТРИАЛЬНОГО ИНТЕРНЕТА ВЕЩЕЙ

С.П. Панасенко[1]
[1]*АО "Актив-софт"*
Москва, РОССИЯ
e-mail: panasenko@guardant.ru

В данной работе предложен подход к реализации низкоресурсного блокчейна для применения в системах интернета вещей (включая индустриальные), имеющих в своем составе низкоресурсные сенсоры. Предложенный подход обеспечивает уменьшение ресурсоемкости блокчейна за счет применения кодов аутентификации сообщения на основе хеш-функций и простейшего метода достижения консенсуса.
Ключевые слова: низкоресурсный блокчейн; интернет вещей; HMAC; консенсус

1 Введение

В настоящий момент блокчейн-технологии активно адаптируются для использования в системах интернета вещей (Internet of Things, IoT) по той причине, что основные свойства блокчейн-систем (децентрализация, неизменяемость и отслеживаемость данных) являются весьма востребованными в IoT [9] и особенно актуальны для ряда применений IoT с ярко выраженной спецификой, включая индустриальный интернет вещей (Industrial Internet of Things, IIoT). При этом блокчейн-технологии основаны на применении требовательных к ресурсам алгоритмов, тогда как IoT

обычно имеют в своем составе устройства с незначительными вычислительными ресурсами. Это объясняет появление и развитие различных методов создания низкоресурсных блокчейнов для их использования в IoT и схожих системах.

Подобные методы основаны на различных подходах, включая следующие:

– применение низкоресурсных криптографических алгоритмов [6], [5], [2];

– перенос ресурсоемких операций на верхние уровни IoT-систем [7], [8];

– минимальная реализация криптоалгоритмов с их тонкой настройкой под платформу используемого устройства [1].

2 Предлагаемый подход

Предлагаемый подход направлен на уменьшение общей ресурсоемкости поддержки блокчейна, хранящего данные, получаемые от низкоресурсных IoT-устройств. Уменьшение ресурсоемкости предлагается за счет ее минимизации в следующих составляющих блокчейна:

– процедурах обеспечения целостности данных;

– протоколах выработки консенсуса.

Данный подход предполагает следующий сценарий применения IoT:

– IoT-устройства представляют собой сенсоры (например, IIoT-сенсоры для получения параметров промышленного оборудования или неких сборочных единиц), не оснащенные функциями по выполнению каких-либо действий; данный подход не предназначен для применения в IoT с устройствами, имеющими дополнительный функционал;

– IoT-система имеет достаточно широко распространенную трехуровневую структуру, в которой сенсоры находятся на нижнем уровне, средний уровень состоит из промежуточных компьютеров (составляющих узлы блокчейн-сети), каждый из которых имеет некоторый закрепленный за ним набор сенсоров, а на верхнем уровне располагается информационная система (система управления), которая использует собираемые сенсорами данные;

– промежуточные компьютеры являются доверенными;

– предъявляются только требования по обеспечению целостности и аутентичности передаваемых сенсорами данных, отсутствует требование по обеспечению их конфиденциальности.

Данный сценарий соответствует существующей практике применения IIoT и не накладывает, таким образом, значительных дополнительных ограничений. Отметим, что в данной структуре ресурсоемкость вычислений не так важна для всех уровней системы, за исключением только нижнего из них, на котором располагаются сенсоры,

обладающие низкими вычислительными ресурсами.

Классические блокчейн-системы (работающие в недоверенном окружении – см., например, [3]) обычно используют электронную подпись для обеспечения целостности и аутентичности данных как на уровне транзакций, так и на уровне блоков. Для уменьшения ресурсоемкости предлагается использовать ключевое хеширование с помощью кодов аутентификации сообщений на основе хеш-функций (Hash-based Message Authentication Codes, HMAC) вместо электронной подписи на уровне транзакций.

Это предполагает изменение классической процедуры добавления данных в блокчейн следующим образом:

1. На первом предварительном этапе выполняется генерация ключей электронной подписи и их распределение между промежуточными компьютерами (узлами блокчейн-сети): каждый узел i снабжается собственным приватным ключом D_i, при этом набор соответствующих им публичных ключей (E_i и другие) становится доступным остальным узлам сети, например, с помощью инфраструктуры открытых ключей.
2. На втором предварительном этапе генерируются и распределяются секретные ключи для вычисления HMAC:
   - каждый промежуточный компьютер рассматривается как центр ключевой системы типа “звезда” и снабжается набором секретных ключей для связи с

каждым сенсором, закрепленным за данным промежуточным компьютером;

– каждый сенсор снабжается собственным секретным ключом для связи с промежуточным компьютером, к которому он относится.

Таким образом, промежуточный компьютер i имеет набор ключей $K_{i,1}K_{i,N}$ для защиты обмена данными с его N сенсорами, тогда как каждый сенсор j, относящийся к этому компьютеру, обладает собственным секретным ключом $K_{i,j}$ с целью вычисления значений HMAC для передаваемых данных.

Распределение ключей между участниками системы после выполнения предварительных этапов показано на рис. 1.

3. Процедура добавления данных в блокчейн инициируется сенсором. После получения данных, которые необходимо передать вышележащей системе, сенсор j (относящийся к компьютеру i) формирует пакет P для отправки. Пакет состоит из сообщения M (включающего в себя отправляемые данные) и кода, обеспечивающего целостность и аутентичность сообщения, который является результатом вычисления HMAC на основе данных сообщения и секретного ключа сенсора $K_{i,j}$:

$$P = <M, \text{HMAC}(M,\ K_{i,j})>$$

Сформированный пакет отправляется на промежуточный компьютер.

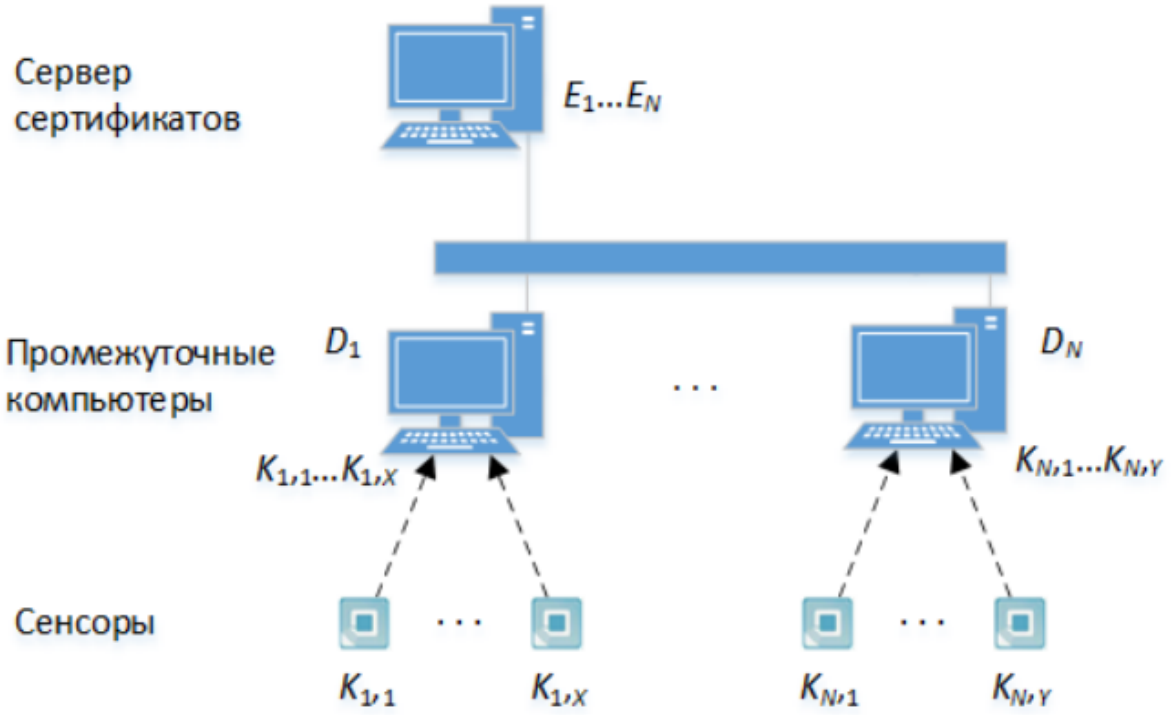

Рис. 1. Распределение криптографических ключей

4. После получения пакета P промежуточный компьютер i проверяет его целостность с помощью своей копии ключа $K_{i,j}$, снабжает его меткой времени T и сохраняет пакет с меткой времени в собственном пуле пакетов, ожидающих добавления в блокчейн.

5. Когда промежуточный компьютер i получает возможность добавления данных в блокчейн в результате работы алгоритма консенсуса (который будет описан далее), он формирует блок B, содержащий в своем составе все пакеты, ожидающие в пуле данного узла, $\{P, T\}$ и метку времени создания блока T_b, где:

   – пакеты (каждый из которых является аналогом транзакции в классическом блокчейне) сортируют-

ся по их меткам времени;

– сформированный блок подписывается электронной подписью S, которая вычисляется промежуточным компьютером на основе его приватного ключа D_i.

Созданный в результате блок имеет следующую структуру:

$$B = <\{P,\ T\},\ T_b,\ \text{Sign}(<\{P,\ T\},\ T_b>,\ D_i)>.$$

Блок публикуется в блокчейне и становится видимым всем узлам блокчейн-сети, а также информационной системе, расположенной на верхнем уровне.

6. При необходимости проверки целостности сформированного блока любой узел, находящийся на верхних уровнях системы, может выполнить такую проверку с помощью открытого ключа E_i того узла, который опубликовал данный блок.

В описанной выше последовательности добавления данных в блокчейн основная вычислительная нагрузка ложится на промежуточные компьютеры, снабженные достаточными ресурсами, тогда как низкоресурсные IoT-сенсоры всего лишь формируют пакеты данных и вычисляют HMAC сообщений, что является относительно простыми и нересурсоемкими операциями.

В части достижения консенсуса необходимо отметить, что процедура достижения консенсуса является одной из наиболее ресурсоемких в традиционных блокчейн-системах. Прежде всего, это касается методов консенсуса,

основывающихся на доказательстве выполненной работы (Proof-of-Work, PoW). Несмотря на это, PoW-консенсус используется и в некоторых вариантах низкоресурсного блокчейна в случаях, когда блокчейн-сеть имеет в своем составе недоверенные узлы. В качестве примера низкоресурсного блокчейна, использующего PoW-консенсус, можно привести описанный в работе [6].

В рассматриваемой здесь структуре IoT-системы все узлы блокчейн-сети (промежуточные компьютеры) являются доверенными (например, принадлежат одной организации или сообществу взаимно доверенных организаций), что является реалистичным для IIoT. Это означает, что нет необходимости в использовании ресурсоемких методов достижения консенсуса, изначально предназначенных для использования в недоверенном окружении.

Следовательно, в данной системе могут быть использованы простейшие методы достижения консенсуса; в качестве такового мы считаем возможным и оптимальным использование метода “Round robin”, предоставляющего узлам право создания блока поочередно или псевдослучайным образом (см. [4]). Данный метод консенсуса позволяет избавиться от избыточной ресурсоемкости, свойственной сложным методам консенсуса наподобие PoW.

3 Преимущества и недостатки подхода

Использование HMAC вместо электронной подписи на уровне транзакций дает возможность, во первых, уменьшить ресурсоемкость обеспечения целостности и аутентичности данных. HMAC фактически представляет собой двойное хеширование данных, тогда как формирование электронной подписи включает в себя две операции: хеширование подписанных данных и вычисление подписи полученного хеш-кода. Вычисление хеш-кода блока данных по сравнению с вычислением электронной подписи на несколько порядков менее ресурсоемко (см., например, замеры производительности в [10]). Во-вторых, при использовании HMAC не требуется реализовывать алгоритм электронной подписи в устройстве с ограниченными ресурсами, тогда как реализация алгоритма хеширования требуется в обоих случаях.

Использование простейшего метода достижения консенсуса приводит к дальнейшему уменьшению ресурсоемкости блокчейна.

Помимо описанного выше ограничения на использование на нижнем уровне системы только IoT-сенсоров, не способных выполнять дополнительные функции, предложенный подход имеет следующие недостатки:

– каждый кластер IoT-системы (характеризующийся привязкой к конкретному промежуточному компьютеру) должен состоять из ограниченного и предопреде-

ленного набора сенсоров, в каждый из которых должен быть загружен секретный ключ (с другой стороны, в IIoT, теоретически, не должно быть возможности подключения произвольных сенсоров без их предварительной регистрации в системе);

– каждый кластер является статичным - предложенный подход не подразумевает перевода сенсора из одного кластера в другой, тогда как в ряде применений IIoT такой перевод является необходимым (например, при конвейерном производстве).

Для устранения второго из перечисленных недостатков необходима разработка протокола передачи сенсоров из одного кластера системы в другой, не требующей перепрошивки ключевой информации в сенсор. Разработка такого протокола ведется.

Библиографические ссылки

1. *Guruprakash J., Koppu S.* EC-ElGamal and Genetic Algorithm-Based Enhancement for Lightweight Scalable Blockchain in IoT Domain // IEEE Access. 2020. Vol. 8. P. 141269–141281.

2. *Kwan S., Lee W.K., Hwang S.O.* AEchain: A Lightweight Blockchain for IoT Applications // IEEE Consumer Electronics Magazine. 2022. Vol. 11, Iss. 2. P. 64–76.

3. Bitcoin: A Peer-to-Peer Electronic Cash System [Electronic resourse].

URL: https://bitcoin.org/bitcoin.pdf
(date of access: 01.06.2023).

4. National Institute of Standards and Technology Internal Report 8202. Blockchain Technology Overview. 2018. [Electronic resourse].
URL: https://csrc.nist.gov/pubs/ir/8202/final
(date of access: 01.06.2023).

5. *Pohrmen F.H., Saha G.* LightBC: A Lightweight Hash-Based Blockchain for the Secured Internet of Things // Advances in Intelligent Systems and Computing. 2021. Vol. 1165. P. 811–819.

6. *Seok B., Park J., Park J.H.* A Lightweight Hash-Based Blockchain Architecture for Industrial IoT // Applied Sciences. 2019. Vol. 9, Iss. 18. P. 3740.

7. Secure Data Provenance in Internet of Things based Networks by Outsourcing Attribute based Signatures and Using Bloom Filters / M.S. Siddiqui [et al.] // International Journal of Advanced Computer Science and Applications. 2019. Vol. 10, Iss. 5. P. 221–226.

8. Block-Track-L: A Lightweight Blockchain-based Provenance Message Tracking in IoT / M.S. Siddiqui [et al.] // International Journal of Advanced Computer Science and Applications. 2020. Vol. 11, Iss. 4. P. 463–470.

9. A Systematic Literature Review of Lightweight Blockchain for IoT / D.Stefanescu [et al.] // IEEE Access. 2022. Vol. 10. P. 123138–123159.

10. Virtual Applications and Implementations Research Lab eBACS Project: ECRYPT Benchmarking of Cryptographic Systems [Electronic resourse].
URL: `https://bench.cr.yp.to`
(date of access: 01.06.2023).

МЕТОДЫ ВЫЯВЛЕНИЯ И АНАЛИЗА УЯЗВИМОСТЕЙ В РАСПРЕДЕЛЕННЫХ КОМПЬЮТЕРНЫХ СИСТЕМАХ

И.К. Пирштук[1], Н.А. Возовиков[2]
[1,2]*НИИ прикладных проблем математики и информатики*
[1,2]*Белорусский государственный университет*
Минск, БЕЛАРУСЬ
e-mail: [1]pirshtuk@bsu.by, [2]dylordcrp@gmail.com

Проведен анализ уязвимостей в компьютерных системах, рассмотрены современные подходы к классификации и агрегации уязвимостей, описаны методы обнаружения уязвимостей, приведены сканеры уязвимостей.
Ключевые слова: атака; уязвимость; классификация уязвимостей; статистический анализ кода; распределенные компьютерные системы

1 Введение

В современном мире безопасность компьютерных систем, вне зависимости от их внутреннего или внешнего устройства, является наиболее значимым и важным аспектом в мировом информационном пространстве. На сегодняшний день все сферы человеческой деятельности в той или иной степени информатизированы и компьютезированы, а также подключены к локальным и глобальным сетям. Очевидно, что революционные преобразования такого рода способствовали бурному развитию последующих технологий и увеличению эффективности во всех промышленных и

непромышленных процессах. Однако, чем глубже информационные технологии и автоматизация процессов проникают в человеческую деятельность, тем больше возрастают риски, связанные с компьютерной и информационной безопасностью.

Недостаточное внимание обеспечению безопасности каких-либо компьютерных систем может привести к очень большим проблемам, начиная от утечки конфиденциальной информации, заканчивая остановкой или несанкционированным управлением промышленными процессами [1].

В основе любого взлома компьютерной системы лежит уязвимость — недостаток в программном обеспечении, случайно или неслучайно допущенный разработчиками. К сожалению, невозможно изначально разработать программное обеспечение, в котором полностью отсутствуют уязвимости и недостатки. Поэтому одной из главных задач в сфере информационной безопасности являются методы распознавания и обнаружения уязвимостей в компьютерных системах.

Чаще всего компьютерные системы подвергаются тестированию различного характера. Тестирование системы может проводиться специалистом по обеспечению информационной безопасности полностью вручную (например, анализируя исходный код программного обеспечения), полуавтоматически с использованием вспомогательных тестирующих инструментов или полностью автоматически, используя комплексные решения по поиску уязвимостей.

В идеальной ситуации, по крайней мере, часть тести-

рований должна проводится автоматически, что даст тестировщику больше времени на тестирование тех областей компьютерных систем, которые невозможно на данный момент проверить автоматически. Например, в такую область входят проблемы, связанные с контролем доступа, так как проблематично предусмотреть, каким именно пользователям надо разрешить выполнять те или иные действия при непосредственном использовании программного обеспечения. Другой причиной востребованности автоматизации тестирований являются короткие циклы разработки программного обеспечения, которые нуждаются в быстрых и многократно воспроизводимых проверках на безопасность.

Существуют различные средства проведения автоматизированных тестов безопасности. Наиболее популярными подходами являются статический и динамический анализ кода, а также сканирование уязвимостей. Сканеры уязвимостей тестируют работающую в реальном времени компьютерную систему “извне”, имитируя таким образом изначальные условия, в которых находится атакующее систему третье лицо, посылая в нее специально подготовленные данные и анализируя полученные ответы.

В статье речь пойдет об анализе и улучшениях сканеров уязвимостей. Основными целями настоящей работы являлись следующие задачи:

– исследовать современные концепции уязвимостей в сфере информационной безопасности и рассмотреть передовые подходы к классификации и агрегации уязвимостей;

– деконструировать процесс сканирования и проанализировать эффективность применения сканеров уязвимостей в симулируемых и реальных условиях;

– выявить типичные для сканеров уязвимостей проблемы, снижающие эффективность процесса поиска;

– предложить технические решения выявленных проблем на низком и высоких уровнях взаимодействия со сканерами;

– по возможности реализовать описанные технические решения и привести оценки прироста эффективности после их интеграции в сканеры уязвимости.

2 Классификация уязвимостей и атак

Определение уязвимости. Существует множество определений уязвимости в зависимости от рассматриваемого источника. Ниже приведены несколько определений от различных органов по компьютерной безопасности.

– Существование недостатка, ошибки проектирования или реализации, которая может привести к неожиданному, нежелательному событию, ставящему под угрозу безопасность компьютерной системы, сети, приложения или протокола (ENISA) [1].

– Недостаток (слабость) программного (программно-технического) средства или информационной системы в целом, который может быть использован для реализации угроз безопасности информации (ГОСТ Р 50922) [3].

– Недостаток или слабое место в разработке, реализации, использовании и управлении системой, которое может быть использовано для нарушения политики безопасности системы (IETF RFC 4949).

– Слабость в информационной системе, процедурах безопасности системы, внутреннем контроле или реализации, которая может быть использована или спровоцирована источником угрозы (Национальный институт стандартов и технологий (NIST)) [4].

– Вероятность того, что возможности угрозы превышают способность противостоять угрозе (The Open Group).

– Недостаток в разработке, внедрении, эксплуатации или внутреннем контроле (ISACA).

Рассмотрев также другие различные источники, описывающие определение уязвимости, нельзя прийти к консенсусу относительно этого понятия. Однако, так или иначе — это некоторое слабое место в какой-либо компьютерной системе, которое может быть использовано третьими лицами для несанкционированного доступа к данной системе, в каких-либо личных целях.

Уязвимость нулевого дня. Уязвимость нулевого дня (0-day) — это уязвимость, которая неизвестна или не устранена разработчиками по какой-либо причине. Также уязвимостью нулевого дня можно считать известную уязвимость, против которой еще не разработаны защитные механизмы.

Пока уязвимость не устранена, злоумышленники могут использовать ее для негативного воздействия на программ-

ное обеспечение, хранилище данных, компьютерные системы или сети.

“Нулевой день” (0-day) – это день, когда заинтересованная сторона узнает об уязвимости, что дает им преимущество при атаке на компьютерную систему. Как правило, об уязвимостях нулевого дня становится известно только после проведения атаки на систему с использованием этой уязвимости.

Однако разработчики также могут обнаружить эту уязвимость через какое-то время, поэтому чем меньше дней прошло с “нулевого дня”, тем выше вероятность того, что уязвимость не была устранена или не были предприняты какие-либо действия по уменьшению последствий от использования этой уязвимости.

Причины возникновения уязвимостей. Причин возникновения уязвимостей существует множество. Однако можно выделить ключевые из них: сложность компьютерных систем, ошибки в программном обеспечении, открытая информация о конфигурации системы, недостатки используемой ОС, разветвленность компьютерной сети, доступ компьютерной сети к интернету, плохая политика аутентификации, высокое доверие к корректности вводимых в систему данных и человеческий фактор. Они образуются исходя из следующих факторов:

1. Сложные системы увеличивают вероятность появления изъяна, неправильной конфигурации или непреднамеренного доступа.

2. Программисты могут случайно или намеренно оставить в программном обеспечении ошибку, которую можно

использовать. Иногда конечные пользователи не обновляют свое программное обеспечение, оставляя его необновленным и уязвимым для эксплуатации.

3. Открытый исходный код, информация об используемом программном обеспечении, ОС и аппаратном обеспечении — увеличивают вероятность того, что злоумышленник сможет найти или имеет информацию об известных уязвимостях в соответствующих компонентах системы.

4. Как и любое программное обеспечение, операционные системы могут иметь недостатки. Операционные системы по своей сути небезопасны и предоставляют возможность получить доступ к системе, что позволяет потенциально внедрить вирусы или другое вредоносное ПО.

5. Чем больше к сети подключено устройств, тем выше вероятность наличия уязвимости.

6. Интернет полон шпионских и рекламных программ, которые могут автоматически устанавливаться на компьютеры.

7. Слабые пароли могут быть взломаны крипто атакой грубой силы (brute-force), а повторное использование паролей предоставляет злоумышленнику более глубокий доступ в систему.

8. Веб приложение или программное обеспечение полагает, что все вводимые данные безопасны в своем контексте, но не учитывает синтаксически небезопасные конструкции вводимые в систему пользователем, что позволяет злоумышленнику выполнять несанкционирован-

ные команды внутри системы (например SQL-injection, OS command injection).

9. Самая большая уязвимость в любой организации — это человек использующий систему. Социальная инженерия является самой большой угрозой для большинства организаций.

Базы данных уязвимостей. Базы данных уязвимостей — это постоянно поддерживающиеся и обновляемые базы данных, в которых собраны данные о всех обнаруженных уязвимостях на сегодняшний день. Среди множества различных баз данных можно выделить одну из крупнейших баз под названием CVE (Common Vulnerabilities and Exposures), в которой каждой уязвимости присваивается балл CVSS (Common Vulnerability Scoring System), отражающий потенциальный риск, который уязвимость может представлять для организации. Очень часто данная база данных используется в качестве базы знаний сканерами в процессе тестирования компьютерных систем.

Преимущество открытых баз данных уязвимостей заключается в том, что они позволяют организациям разрабатывать, определять приоритеты и вводить исправления и другие меры по устранению уязвимостей разных уровней риска.

Тем не менее, они также могут привести к созданию дополнительных уязвимостей из-за поспешно выпущенных исправлений, которые устраняют одну уязвимость и моментально создают другую.

База данных уязвимостей и атак: $MITREATT\&CK$**.** Структура данных $ATT\&CK$ пред-

ставляет собой структурированный список известных типов поведения злоумышленников при компрометации сетей [5]. Модуль разделяется на несколько различных матриц:

1. Enterprise (корпоративные системы на базе $Windows, LinuxMacOS$).
2. $Mobile$ (мобильные устройства).
3. $PRE - ATT\&CK$ (подготовительные стадии атак).

Вышеперечисленные матрицы содержат различные тактики и техники, обусловленные спецификой их назначения.

Если рассматривать $ATT\&CK$ как матрицу, заголовки столбцов в верхней части соответствуют тактикам и являются категориями техник. Тактика — это то, чего пытаются достичь злоумышленники, в то время как отдельные техники — это то, как они достигают своих целей.

Например, в [5] 6-я колонка является тактикой повышения привилегий (Privilege Escalation). Чтобы получить доступ к привилегированным правам в системе злоумышленник должен использовать одну или несколько техник, перечисленных в данном столбце.

Техника — это конкретное поведение для достижения цели, которое часто является одним из шагов в последовательности действий, используемых для выполнения намерения злоумышленника. $ATT\&CK$ предоставляет множество подробных сведений о каждой технике, включая описание, примеры, ссылки и предложения по снижению рисков и обнаружению.

В качестве примера того, как тактики и техники работают в $ATT\&CK$, предположим, что злоумышленник хочет получить доступ к сети и установить программное обеспечение для добычи криптовалюты на максимально возможном количестве систем внутри этой сети. Для достижения этой главной цели злоумышленнику необходимо успешно выполнить несколько промежуточных шагов. Во-первых, получить доступ к сети, возможно, через "ссылку направленного фишинга" (Spearphishing Link). Затем может потребоваться повышение привилегий путем "встраивания в процесс" (Process Injection). Теперь он может получить другие учетные данные из системы с помощью "дампинга учетных данных" (OS Credential Dumping), а затем обеспечить закрепление, настроив скрипт добычи криптовалюты в качестве "запланированной задачи" (Scheduled Task/Job). Благодаря этому злоумышленник может перемещаться в горизонтальном направлении по сети с помощью техники Pass the Hash и распространять программное обеспечение для добычи криптовалюты на максимально возможное количество систем.

В этом примере злоумышленник успешно выполнил пять шагов, каждый из которых представляет собой определенную тактику или этап общей атаки: первоначальный доступ, повышение привилегий, получение учетных данных, закрепление и горизонтальное перемещение. Он использовал специальные техники в рамках этой тактики для выполнения каждого этапа атаки (ссылка направленного фишинга, встраивание в процесс, дампинг учетных данных и т.д.).

Практическое использование баз данных уязвимостей. $ATT\&CK$ можно успешно применять для анализа кибер угроз, так как это позволит описать поведение злоумышленников в унифицированной форме. Злоумышленников можно отслеживать путем сопоставления с техниками и тактиками в $ATT\&CK$, характерными именно для них. Так специалисты по информационной безопасности получают план мероприятий, которые нужно провести в отношении средств оперативного контроля для выявления сильных и слабых сторон защиты от определенных источников угроз.

Также на основе описанных баз данных работают различные инструменты по анализу и обнаружению уязвимостей. Одним из примеров подобного взаимодействия являются сканеры уязвимостей. В зависимости от специфики и назначения сканера, а также учитывая особенности выбранной базы данных, функциональная составляющая практического использования может отличаться от случая к случаю. Однако, в большинстве случаев сканер уязвимостей сопоставляет найденные уязвимости с записями в базах данных для получения дополнительной информации о возможных направлениях атаки либо для получения актуального уровня риска и других оценок.

3 Анализ сканеров уязвимостей

Сканеры уязвимостей. Сканер уязвимостей — это программное обеспечение, предназначенное для проверки компьютеров, сетей или приложений на наличие известных уяз-

вимостей. Они могут определять и обнаруживать уязвимости, возникающие из-за неправильной конфигурации в компьютерных сетях и системах, выполнять аутентифицированное и неаутентифицированное сканирование.

Аутентифицированное сканирование позволяет сканеру уязвимостей получить прямой доступ к сетевым ресурсам, используя протоколы удаленного администрирования, такие как SSH (протокол удаленного управления) или протокол удаленного рабочего стола (RDP), используя предоставленные учетные данные для входа в систему. Такой подход дает доступ к низкоуровневым данным, сведениям о конкретных службах и деталях конфигурации, подробной и точной информации об операционных системах, установленном программном обеспечении, проблемах конфигурации и о последнем обновлении безопасности.

Неаутентифицированное сканирование подразумевает под собой сканирование системы без наличия какой-либо информации об объекте исследования при первом запуске сканера уязвимостей. Данный метод более подвержен к выявлению ложных уязвимостей, получению недостоверной информации об операционных системах и установленном программном обеспечении. Такой подход обычно используется злоумышленниками и аналитиками безопасности для определения уровня безопасности внешних модулей и поиска возможных утечек данных.

Анализ сканеров уязвимостей. С целью выяснить практическую эффективность сканирования было проведено исследование на основе трех сканеров уязвимостей и эмулирующего реальное аппаратное и программное обеспече-

ние системы.

Для проведения анализа были выбраны три наиболее популярных сканеров уязвимостей Nessus [6], Nexpose [7] и OpenVAS [8].Сканирование проводилось против виртуальной системы $Metasploitable2$ — специально созданной операционной системы на базе Ubuntu, которая была разработана для тестирования и демонстрации распространенных атак на уязвимости [9].

При сравнении выбранных сканеров уязвимостей было принято решение исключить анализ на основе распространенных метрик баз данных уязвимостей, поскольку получение точного результата является сложной задачей из-за больших различий в классификации найденных уязвимостей различными сканерами.

Важно отметить, что исследование было сфокусировано на том, насколько эффективно сканеры способны выявлять уязвимости при ненастроенных конфигурациях сканирования. В худшем случае, сканер уязвимостей должен быть способен выявлять плохо настроенные службы и службы по умолчанию, которые каким-либо образом могут привести к взлому системы, а также выявлять известные на текущий момент уязвимости в установленном программном обеспечении.

В конфигурации сканеров не передавались какие-либо вспомогательные данные о системе, в том числе никакие учетные данные для аутентифицированного сканирования.

Сканер уязвимостей $Nessus$ был запущен с использованием профиля сканирования внешней сети. Он также был протестирован с профилем сканирования внутренней се-

ти, однако результаты оказались аналогичными. $OpenVAS$ был протестирован с полным профилем сканирования. Сканер Nexpose был запущен с профилем полного аудита.

В результате сканирования системы каждый из сканеров уязвимостей нашел в целевой системе некоторое количество уязвимостей. В табл. 1 представлены данные о количестве найденных уязвимостей каждым сканером. Уязвимости были распределены по риску угрозы на критические, среднего уровня риска и низкого уровня риска.

Таблица 1. Результаты сканирований

	Nessus	OpenVas	Nexpose
High	9	38	49
Medium	22	24	103
Low	8	36	18

Очевидно, что $Nessus$ выявил меньшее количество уязвимостей, в отличие от $OpenVas$ и $Nexpose$. Однако, надо учитывать, что некоторые выявленные уязвимости являются ложными и в действительности, как показал более подробный анализ, $Nessus$ оказался более точным, несмотря на меньшее количество обнаруженных уязвимостей.

Полученные результаты без дополнительной категоризации и обработки дают мало ценной информации об эффективности сканирования, за исключением того, что подчеркивают большой количественный разброс найденных уязвимостей между различными сканерами.

Чтобы получить некоторые более значимые результаты, была взята выборка из 15 наиболее критических уязвимостей, существующих в целевой системе. Несмотря на то, что

это только малая часть наиболее критических эксплуатируемых сервисов и в системе присутствует гораздо больше уязвимостей, такой подход позволил проанализировать поведения сканеров в частных случаях и сделать соответствующие выводы относительно проблемных областей процесса сканирования как такового.

В результате анализа и сопоставления данных, выяснилось, что далеко не все критические уязвимости были обнаружены. В табл. 2 знаком "+" отмечены уязвимости, которые были обнаружены соответствующим сканером.

В результате проведенных сканирований из 15 критических уязвимостей в системе было выявлено только 10. Все перечисленные в табл. 2 уязвимости и проблемы, связанные с неправильными конфигурациями программного обеспечения, за исключением анонимного доступа к FTP, могут быть использованы для получения доступа к системе (в большинстве случаев с привилегиями администратора) с помощью фреймворка Metasploit или других инструментов.

Стоит обратить внимание на ряд случаев, когда сканеры не обнаружили уязвимости связанные с аунтификационными данными по умолчанию или учетными данными, не соответствующими политике безопасности. Согласно собранным данным, все сканеры обнаружили уязвимости такого типа для базы данных MySQL, однако аналогичные уязвимости не были выявлены в других аналогичных службах (VNC 5900, POSTGRESQL).

Такие малоизвестные уязвимости, как бэкдор INGRESLOCK и Unreal IRCd, а также уязвимость в распределенном компиляторе DISTCCd 3632, не были вы-

Таблица 2. Обзор выборки обнаруженных уязвимостей

Уязвимость	Nessus	OpenVas	Nexpose
FTP 21 Анонимный доступ к FTP	+	+	+
FTP 21 VsFTPd Smiley Face Backdoor	+	+	
FTP 2121 ProFTPD Уязвимости		+	
SSH 22 Слабые ключи хоста	+		+
PHP-CGI, Инъекция параметров строки запроса	+	+	+
CIFS Нулевые сессии	+	+	+
INGRESLOCK 1524			
NFS 2049		+	
MYSQL 3306 слабая аутентификация (root-права без пароля)	+	+	+
РЕЕСТР RMI 1099 Небезопасная конфигурация по умолчанию			
DISTCCd 3632 распределенный компилятор			
POSTGRESQL 5432 слабая аутентификация			
VNC 5900 слабая аутентификация (пароль)			+
IRC 6667 Unreal IRCd Backdoor			
Tomcat 8180	+		+

явлены ни одним сканером уязвимостей. Учитывая то, что сигнатуры этих уязвимостей хорошо задокументированы и присутствуют в большинстве баз данных, существует некоторая проблема в процессе сканирования, связанная с обнаружением существующих и запущенных сервисов на целевой системе.

В документации тестируемой системы Metasploitable2 есть хорошие примеры, демонстрирующие то, каким именно образом существующие в этой системе уязвимости могут использоваться при атаке на систему и какой ущерб могут нанести. В большинстве случаев даже плохо настроенная служба, в которой отсутствуют уязвимости, может привести к несанкционированному доступу в системе.

Все сканирования проводились в режиме “черного ящика” без каких-либо дополнительных настроек конфигураций сканеров. Однако, при проведении внутренних аудитов компьютерных систем рекомендуется выполнять сканирование с предоставлением учетных данных. Как показали дополнительные сканирования системы с настройкой сканеров на аутентифицированное тестирование, результаты оказались намного лучше. Но, как показала практика, большинство сканеров некорректно сопровождают аутентифицированную сессию во время всего процесса сканирования. Например, сессия может время от времени обнуляться ввиду политики безопасности веб приложения. В таком случае сканеры не имеют функционала, позволяющего восстановить сессию, и дальнейшее сканирование системы проводится некорректно. Также было обнаружено, что сканеры во время исследования адресного пространства могут при-

нудительно обнулять сессию, например, при исследовании страницы выхода из пользовательского аккаунта.

Полученные результаты показывают, что сканеры при любой конфигурации эффективно могут обнаруживать распространенные, известные и задокументированные уязвимости, однако, не задокументированные или неизвестные уязвимости сканеры не способны выявить, так как в основе процесса сканирования лежат базы данных уязвимостей. Также были выявлены проблемы при неаутентифицированном сканировании, касающиеся плохого распознавания запущенных служб в тестируемой системе, что приводит к снижению эффективности обнаружения уязвимостей, которые, в отличие от предыдущей проблемы, хорошо задокументированы и описаны в базах данных.

Несмотря на присутствующие недостатки, в общем случае сканеры уязвимостей показали хороший результат. Однако, полученные данные все еще необходимо проверять и проводить дополнительные аудиты под руководством специалиста по безопасности. Очевидно, что проведение внутреннего целенаправленного тестирования в сочетании с внешним сканированием уязвимостей повысит эффективность работы по обеспечению безопасности сетей или серверов, подключенных к интернету.

4 Заключение

Безопасность любой компьютерной или программной системы строится на одних и тех же концепциях и основах. Однако, предприняв все меры предосторожности по без-

опасности при реализации проекта, невозможно сделать систему полностью неуязвимой. Именно поэтому необходимо постоянно тестировать компьютерные системы, занимающие важные места в человеческой деятельности, на наличие атак и уязвимостей.

В данной статье рассмотрен один из важнейших методов по выявлению атак и уязвимостей в компьютерных системах — сканеры уязвимостей. На примере множества различных сканеров уязвимостей были изучены процесс и объект сканирования, выявлены присущие большинству сканеров проблемы, дана оценка эффективности сканирования при различных конфигурациях сканеров. На основе исследований предложены и продемонстрированы технические решения по повышению эффективности сканирования на низком и высоком уровнях взаимодействия со сканерами. В качестве демонстрации был разработан модуль по улучшению области сканирования, который на примере четырех различных сканеров показал средний прирост эффективности в 44% относительно общего количества уязвимостей и более 50% прироста относительно доли критических уязвимостей.

Библиографические ссылки

1. *Лукацкий А.В.* Обнаружение атак. Санкт-Петербург: BHV, 2003.

2. Агентство Европейского Союза по кибербезопасности [Электронный ресурс]. URL:

https://www.enisa.europa.eu (дата обращения: 30.08.2023).

3. ГОСТ Р 50922 [Электронный ресурс]. URL: https://docs.cntd.ru/document/1200058320 (дата обращения: 30.08.2023).

4. Национальная база данных уязвимостей США [Электронный ресурс]. URL: https://nvd.nist.gov/vuln (дата обращения: 30.08.2023).

5. База данных уязвимостей и атак: $MITREATT\&CK$ [Электронный ресурс]. URL: https://attack.mitre.org (дата обращения: 30.08.2023).

6. Сканер уязвимостей $Nessus$ [Электронный ресурс]. URL: https://www.tenable.com/products/nessus (дата обращения: 30.08.2023).

7. 11. Сканер уязвимостей $Nexpose$ [Электронный ресурс]. URL: https://www.rapid7.com/products/nexpose (дата обращения: 30.08.2023).

8. Сканер уязвимостей $OpenVas$ [Электронный ресурс]. URL: https://www.openvas.org (дата обращения: 30.08.2023).

9. Виртуальная система Metasploitable2 [Электронный ресурс]. URL: https://docs.rapid7.com/metasploit (дата обращения: 30.08.2023).

ПРЕДЕЛЬНЫЕ СОВМЕСТНЫЕ РАСПРЕДЕЛЕНИЯ СТАТИСТИК КРИТЕРИЕВ ПАКЕТА NIST

М.П. Савелов[1]
[1]*Московский государственный университет им. М.В. Ломоносова*
Москва, РОССИЯ
e-mail: savelovmp@gmail.com

В докладе будет представлено предельное совместное распределение статистик $T_{mon}, T_{fr}, T_{serial}$ следующих критериев пакета NIST: "Monobit Test", "Frequency Test within a Block" и "Serial Test" в ситуации, когда исследуемая последовательность состоит из независимых случайных величин, имеющих распределение Бернулли с параметром $p = \frac{1}{2}$. Доказано, что T_{mon} и (T_{fr}, T_{serial}) асимптотически некоррелированы, а T_{fr} и T_{serial} асимптотически положительно коррелированы, причем $T_{mon}, T_{fr}, T_{serial}$ попарно асимптотически зависимы. Аналогичные результаты установлены для тройки статистик T_{mon}, T_{fr} и статистики критерия "Approximate Entropy Test".
Ключевые слова: совместное распределение статистических критериев; пакет критериев NIST; критерий частот; критерий частот в блоках; критерий подпоследовательностей фиксированной длины; энтропийный критерий; критерий аппроксимированной энтропии; асимптотически некоррелированные статистики; асимптотически независимые статистики

Введение

Пусть $\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_n$ — последовательность независимых случайных величин, имеющих распределение Бернулли

$Bern(p)$, $p \in (0,1)$. Через H_{p_0} обозначим гипотезу, в соответствии с которой $p = p_0$. Для проверки гипотезы $H_{\frac{1}{2}}$ в пакете NIST [3] предлагается использовать 15 статистических критериев. Мы рассмотрим статистики критерия частот ("Monobit Test"), критерия частот в блоках ("Frequency Test within a Block"), критерия подпоследовательностей фиксированной длины ("Serial Test") и энтропийного критерия ("Approximate Entropy Test"). Мы будем предполагать, что в критерии "Frequency Test within a Block" используется N блоков, в критерии "Serial Test" рассматриваются подпоследовательности длин m и $m-1$, в критерии "Approximate Entropy Test" рассматриваются подпоследовательности длин $m+1$ и m. Нас будет интересовать случай, когда $N, m \geq 2$ фиксированы и n стремится к бесконечности. Отметим, что критерий подпоследовательностей рассматривался, в частности, в [1]–[2], [7].

Положим $M = \left[\frac{n}{N}\right]$. Если из исходной последовательности случайных величин $\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_n$ отбросить последние $n - NM$ элементов, то оставшиеся элементы разбиваются на N непересекающихся блоков длины M: первый блок состоит из случайных величин $\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_M$, второй — из случайных величин $\varepsilon_{M+1}, \varepsilon_{M+2}, \ldots, \varepsilon_{2M}$, и т.д. Положим

$$\pi_j = \frac{1}{M} \sum_{i=(j-1)M+1}^{jM} \varepsilon_i \quad (1 \leq j \leq N), \quad S_n = \sum_{i=1}^{n} \varepsilon_i.$$

Индикатор события A будем обозначать символом I_A.

Пусть $(i_1 \ldots i_m) \in \{0,1\}^m$. Количество появлений цепочки $(i_1 \ldots i_m)$ в последовательности $\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_{n-1}, \varepsilon_n, \varepsilon_1, \varepsilon_2, \ldots, \varepsilon_{m-1}$ обозначим через $\nu_{i_1 \ldots i_m}$.

Другими словами,

$$\nu_{i_1\ldots i_m} = \sum_{i=1}^{n} I_{(\tilde{\varepsilon}_i\ldots\tilde{\varepsilon}_{i+m-1})=(i_1\ldots i_m)},$$

где $\tilde{\varepsilon}_i = \varepsilon_i I_{i\le n} + \varepsilon_{i-n} I_{i>n}$. Величина $\nu_{i_1\ldots i_{m-1}}$ определяется аналогично. Положим

$$\Psi_m^2 = \frac{2^m}{n}\sum_{i_1\ldots i_m}\left(\nu_{i_1\ldots i_m} - \frac{n}{2^m}\right)^2 = \frac{2^m}{n}\sum_{i_1\ldots i_m}\nu_{i_1\ldots i_m}^2 - n,$$

$$T_{mon} = \frac{2S_n - n}{\sqrt{n}}, \quad T_{fr} = 4M\sum_{j=1}^{N}\left(\pi_j - \frac{1}{2}\right)^2,$$

$$T_{serial} = \Psi_m^2 - \Psi_{m-1}^2.$$

Пусть $f : [0,1] \to \mathbb{R}$ — непрерывная функция. Положим

$$\Phi_m^{[f(x)]} = \sum_{(i_1\ldots i_m)\in\{0,1\}^m} f\left(\frac{\nu_{i_1\ldots i_m}}{n}\right).$$

Будем считать, что $x\ln x = 0$ при $x = 0$. Положим

$$T_{entr} = 2n\left(\Phi_{m+1}^{[x\ln x]} - \Phi_m^{[x\ln x]} + \ln 2\right).$$

Статистики T_{mon}, T_{fr}, T_{serial}, T_{entr} используются в критериях согласия “Monobit Test”, “Frequency Test within a Block”, “Serial Test” и “Approximate Entropy Test” пакета [3] для проверки гипотезы $H_{\frac{1}{2}}$. Предельные распределения отдельных статистик $T_{mon}, T_{fr}, T_{serial}, T_{entr}$ известны (см. [3]). Предельное совместное распределение статистик $T_{mon}, T_{fr}, T_{serial}$ было найдено в [6]. Предельное совместное распределение статистик $T_{mon}, T_{fr}, T_{entr}$ было найдено в [5]. В докладе будут изложены основные результаты работ [5]–[6].

Основные результаты

Под асимптотической независимостью, асимптотической некоррелированностью и асимптотической положительной коррелированностью статистик будем понимать то же, что понимается под этими терминами в [5]–[6].

Следующая теорема доказана в [6].

Теорема 1. *Пусть* $\varepsilon_1, \varepsilon_2, \ldots$ *— последовательность испытаний Бернулли с параметром* $p = \frac{1}{2}$. *Пусть случайные величины* $Z_j^{(i)}, 1 \le i \le N, 1 \le j \le 2^{m-1}$, *независимы, имеют распределение* $\mathcal{N}(0,1)$ *и* $Z^{(i)}_{2^{m-1}+1} = 2^{-\frac{m-1}{2}} \sum_{j=1}^{2^{m-1}} Z_j^{(i)}$. *Если* $m \ge 2$ *и* N *фиксированы, то*

$$\left(\sqrt{N}T_{mon}, T_{fr}, N \cdot T_{serial}\right)$$
$$\xrightarrow{d} \left(\sum_{i=1}^{N} Z^{(i)}_{2^{m-1}+1}, \sum_{i=1}^{N} \left(Z^{(i)}_{2^{m-1}+1}\right)^2, \sum_{j=1}^{2^{m-1}} \left(\sum_{i=1}^{N} Z_j^{(i)}\right)^2\right)$$

при $n \to \infty$. *Ковариационная матрица предельного распределения вектора* $\left(T_{mon}, T_{fr}, T_{serial}\right)$ *имеет вид*

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 2N & 2 \\ 0 & 2 & 2^m \end{pmatrix}.$$

Статистики $T_{mon}, T_{fr}, T_{serial}$ *попарно асимптотически зависимы. Статистики* T_{mon} *и* (T_{fr}, T_{serial}) *асимптотически некоррелированы, статистики* T_{fr} *и* T_{serial} *асимптотически положительно коррелированы.*

Следующая теорема доказана в [5].

Теорема 2. *Пусть* $\varepsilon_1, \varepsilon_2, \ldots$ — *последовательность испытаний Бернулли с параметром* $p = \frac{1}{2}$. *Пусть случайные величины* $Z_j^{(i)}, 1 \le i \le N, 1 \le j \le 2^m$, *независимы, имеют распределение* $\mathcal{N}(0,1)$ *и* $Z_{2^m+1}^{(i)} = 2^{-\frac{m}{2}} \sum_{j=1}^{2^m} Z_j^{(i)}$. *Если* m *и* N *фиксированы, то*

$$\left(\sqrt{N}T_{mon}, T_{fr}, N \cdot T_{entr}\right)$$
$$\xrightarrow{d} \left(\sum_{i=1}^{N} Z_{2^m+1}^{(i)}, \sum_{i=1}^{N} \left(Z_{2^m+1}^{(i)}\right)^2, \sum_{j=1}^{2^m} \left(\sum_{i=1}^{N} Z_j^{(i)}\right)^2\right)$$

при $n \to \infty$. *Ковариационная матрица предельного распределения вектора* $\left(T_{mon}, T_{fr}, T_{entr}\right)$ *имеет вид*

$$F = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2N & 2 \\ 0 & 2 & 2^{m+1} \end{pmatrix}.$$

и является пределом ковариационных матриц $\mathbf{D}\left(T_{mon}, T_{fr}, T_{entr}\right)$ *при* $n \to \infty$. *Статистики* $T_{mon}, T_{fr}, T_{entr}$ *попарно асимптотически зависимы. Статистики* T_{mon} *и* (T_{fr}, T_{entr}) *асимптотически некоррелированы, статистики* T_{fr} *и* T_{entr} *асимптотически положительно коррелированы.*

Доказательство теоремы 2 основано на идеях работ [4] и [6]. Идея доказательства теоремы 2 будет обсуждаться в докладе.

Библиографические ссылки

1. *Good I.J.* The serial test for sampling numbers and other tests for randomness // Proc. Camb. Phil. Soc. 1953.

Vol. 49, Iss. 2. P. 276–284.

2. *Good I.J., Gover T. N.* The generalized serial test and the binary expansion of $\sqrt{2}$ // J. Roy. Statist. Soc. Ser. A. 1967. Vol. 130, Iss. 1. P. 102–107.

3. A statistical test suite for the validation of random number generators and pseudo random number generators for cryptographic applications. NIST Special Publication 800-22 Revision 1a [Electronic resource].
URL: `https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-22r1a.pdf` (date of access: 14.09.2023).

4. *Киевец Н.Г., Корзун А.И.* Сравнение статистик тестов серий и аппроксимированной энтропии // Доклады БГУИР. 2014. Т. 3. С. 12–17.

5. *Савелов М.П.* Предельное совместное распределение статистик критериев пакета NIST “Monobit Test”, “Frequency Test within a Block” и обобщения критерия “Approximate Entropy Test” // Дискрет. матем. 2023. Т. 35, Вып. 2. С. 98–108.

6. *Савелов М.П.* Предельное совместное распределение статистик критериев “Monobit test”, “Frequency Test within a Block” и обобщения критерия “Serial Test” // Дискрет. матем. 2023. Т. 35, Вып. 1. С. 88–106.

7. *Степанов В.Е.* Некоторые статистические критерии для цепей Маркова // Теория вероятн. и ее примен. 1957. Т. 2, Вып. 1. С. 143–144.

СТЕГАНОГРАФИЧЕСКАЯ СТОЙКОСТЬ РАСТРИРОВАННЫХ ИЗОБРАЖЕНИЙ С ОСАЖДЕНИЕМ ТАЙНОЙ ИНФОРМАЦИИ В ПОЛУТОНОВЫХ ОТТЕНКАХ

М.Г. Савельева[1], П.П. Урбанович[2]
[1,2]*Белорусский государственный технологический университет*
Минск, БЕЛАРУСЬ
[2]*Люблинский Католический университет Яна Павла II*
Люблин, ПОЛЬША
e-mail: [1]saveleva@belstu.by, [2]p.urbanovich@belstu.by

Проанализирована стеганографическая стойкость метода, основанного на модификации пространственно-геометрических и цветовых параметров символов текста при его растрировании, к модификации (конвертация в иной формат и сжатие) документа-контейнера.
Ключевые слова: стеганография; авторское право; осаждение; изображение; растрирование; пространственная область; модель RGB; стеганографическая стойкость

1 Введение

В стеганографии основным принципом является сохранение в тайне факта применения стеганографического преобразования. Однако, помимо этого, стеганография также должна обеспечивать высокую пропускную способность создаваемого стеганографического канала при необходимом уровне стойкости к атакам, а также различным преднамеренным или случайным модификациям стеганоконтейнера. Пропускная способность (или емкость реализуемого

метода) определяет объем передачи информации через стеганоканал. Стеганостойкость основана во многом на том, что скрываемая информация должна быть внедрена в носитель (контейнер) с минимальными изменениями самого носителя, т.е. стеганосистема (или стеганоканал) скрывает от третьих лиц наличие в контейнере тайной информации. Оценка стеганографической стойкости включает в себя анализ возможности обнаружения скрытой информации при помощи различных статистических, алгоритмических и машинно-обучающихся методов [1][2].

Одним из основных факторов, влияющих на стеганографическую стойкость, является естественность изменений, внесенных в документ-контейнер при внедрении в него тайной информации, предназначенной для передачи или для решения задач по защите авторского права на электронный контент. Чем меньше изменений и чем более естественно они выглядят, тем сложнее обнаружить наличие скрытой информации. Система должна быть способна сохранить скрытую информацию при обработке носителя, например, при конвертации или редактировании изображения.

В данном исследовании анализируется стеганографическая стойкость при конвертации и изменении размера контейнера, представляемого в виде растрированного изображения.

В [3] были описаны общая концепция и основные особенности нового метода тестовой стеганографии, развивающего и дополняющего теорию и практику стеганографических преобразований текстовых документов-контейнеров на основе растровой графики. В предлагаемой статье представ-

лены новые результаты, характеризующие стеганографическую стойкость метода из [3].

2 Основная часть

В качестве документа-контейнера с внедренным сообщением выступает изображение формата PNG, целиком заполненное текстом. Исходный размер документа-контейнера – 2481×3509 пикселей. Размер внедряемого сообщения составляет 1272 битов.

Особенностью анализируемого метода является то, что процессы внедрения (извлечения) информации осуществляются при сравнительном анализе значений одной или двух цветовых координат (в модели RGB) некоторого пикселя для выбора документа-контейнера и пикселя – для внедрения битов сообщения. Таким образом, в качестве базового элемента контейнера в рассматриваемом методе, цветовые параметры которого модифицируются при размещении тайной информации, выступает пиксель изображения.

Максимальное значение пропускной способности можно получить при использовании контейнера с большим количеством полутонов, в частности растрированные текстовые документы. Однако, при конвертации или преобразовании текстовых документов-контейнеров одной из важных проблем является растрирование текста: контуры букв начинают расплываться, цвет по контуру переходит в градиент. Получаемый таким образом массив равнораспределенных полутоновых от черного (0, 0, 0) до белого (255, 255, 255; цвет фона) пикселей хорошо подходит для внедрения тай-

ного сообщения.

Для внедрения необходимо выбрать массив пикселей, для которых совпадает значение координат одного или двух цветовых каналов. В изображениях с большим количеством полутонов, монохроматических или черно-белых изображений выбор пикселей, в которых будет происходить внедрение, целесообразно осуществлять по двум цветовым каналам. При этом непосредственно для внедрения битов сообщения в выбранные пиксели целесообразно использовать один канал. На рис. 1 изображен фрагмент контейнера, поясняющий сущность метода. Цифры соответствуют цветовым кодам каналов в модели RGB. Из массива выбирается базовый пиксель. Для примера на рисунке он выделен красным цветом. Все остальные пиксели массива (на рис. 1 выделены желтым цветом) будут использованы для внедрения сообщения. Далее собственно внедрение будет происходить при сравнении значений цветовых координат канала базового (первого) и второго, базового и третьего и т.д.; в конечном итоге – базового и n-ного пикселей массива.

Для оценки стеганографической стойкости при изменении размера стеганоконтейнера нами рассмотрены варианты незначительного изменения контейнера (до 5%). В табл. 1 приведены результаты преобразования контейнера с использованием программы Adobe Photoshop с указанием сохранившейся части исходного сообщения после его извлечения.

Исходя из полученных результатов, можно отметить, что выполненное преобразование стеганоконтейнера путем изменения его размера приводит к потере примерно 24% оса-

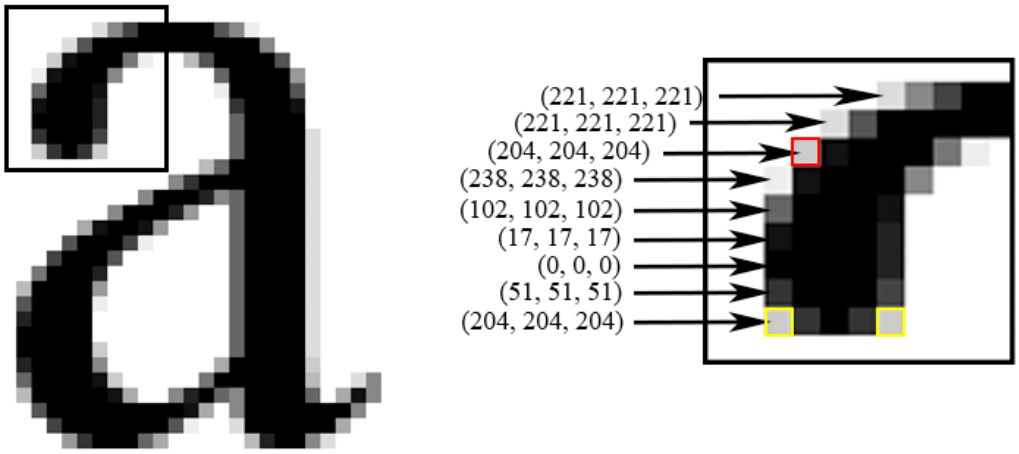

Рис. 1. Фрагмент изображения-контейнера с указанием цветовых кодов пикселей

Таблица 1. Результат изменения размера документа-контейнера

Процент изменения	Размер контейнера, пикселей	Размер контейнера, битов	Количество сохранившейся информации, %
0,25	2475 × 3501	1786306	75,70
0,50	2469 × 3492	1782112	76,66
1,00	2456 × 3474	1751522	75,82
1,50	2444 × 3457	1743567	76,41
5,00	2357 × 3334	1643845	75,86

жденной информации. Количество сохранившейся информации в данном конкретном случае обусловлено наличием большого количества нулей в исходном сообщении (около 75% от всего сообщения), то есть единицы практически полностью не сохраняются, поэтому восстановить сообщение невозможно. Таким образом, можно сделать вывод, что метод не является стойким к изменениям размера документа-контейнера.

Нами применялась также конвертация документа-контейнера в другие форматы. Преобразованное изображение конвертировалось в исходный формат PNG, после чего проводилось извлечение сообщения (по схеме PNG-BMP-PNG). В табл. 2 приведены результаты конвертации контейнера с указанием сохранившейся части исходного сообщения.

Таблица 2. Результат конвертации документа-контейнера

Формат	Размер контейнера, битов	Количество сохранившейся информации, %
GIF	449202	100,00
BMP	854991	100,00
JPG	1603713	27,27
TIFF (без сжатия)	854991	100,00
TIFF (JZW сжатие)	854991	100,00

Таким образом, установлено, что текстовый документ-контейнер формата PNG с тайной информацией, внедренной в полутоновые оттенки, сохраняет целостность этой информации после конвертации в форматы GIF, BMP, TIFF (с JZW сжатием и без сжатия), однако при конвертации в JPG примерно 70-75% битов исходного сообщения являются ошибочными.

Во всех случаях, когда при извлечении получена битовая строка, состоящая практически только из нулей, это можно объяснить тем, что изменились цветовые параметры пикселей при повторном растрировании (из-за изменения размера контейнера или формата). В этом случае восстановить исходное сообщение невозможно.

После проведенных исследований можно сделать вывод, что анализируемый метод является стойким к конвертации стеганоконтейнера в некоторые форматы, однако не устойчив к изменению размера документа-контейнера.

Библиографические ссылки

1. *Шутько Н.П., Листопад Н.И., Урбанович П.П.* Моделирование стеганографической системы в задачах по охране авторских прав // Восьмая Междунар. научно-техн. конф. “Информационные технологии в промышленности” (ITI’2015): тезисы докладов / ОИПИ НАН РБ; редкол.: М.Я. Ковалев (гл. ред.) [и др.]. Минск: ОИПИ НАН РБ, 2015. С. 30–31.
2. *Curran K., Bailey K.* An evaluation of image based steganography methods // Multimedia Tools and Applications. 2006. Vol. 30, Iss. 1. P. 55–88.
3. *Савельева М.Г., Урбанович П.П.* Метод стеганографического преобразования web-документов на основе растровой графики и модели RGB // Труды БГТУ. Сер. 3, Физико-математические науки и информатика. 2022. Т. 2. С. 99–107.

К ВОПРОСУ ИСПОЛЬЗОВАНИЯ ОПЕНСОРСНЫХ СРЕДСТВ ШИФРОВАНИЯ ПРИ ЗАЩИТЕ КАНАЛОВ СВЯЗИ

А.М. Сапрыкин[1]
[1]*ООО "С-Терра Бел"*
Минск, БЕЛАРУСЬ
e-mail: info@s-terra.by

Рассматриваются проблемы использования опенсорсного ПО при разработке СКЗИ.
Ключевые слова: средства шифрования; опенсорсное ПО; уязвимости; импортозамещение

Ситуация на **прикладном** рынке белорусских средств канального шифрования в последние годы складывается в пользу повсеместного использования свободно доступного криптографического западного ПО, поскольку значительно удешевляется разработка продуктов, предназначенных для сертификации в Национальной системе соответствия Республики Беларусь.

Такие средства шифрования можно свободно скачать с европейских и американских интернет-сайтов – они предлагаются в исходных кодах со стандартной общественной лицензией GNU GPL (GPL), надо лишь встроить белорусскую криптобиблиотеку и сертифицировать. Библиотека по объему составляет примерно 2% от ПО, остальные 98% скачиваются. По такой схеме на базе ПО "StrongSwan" (Швейцария) создан "белорусский" БАС (ЗАО "НТЦ Контакт"), на базе ОрепVPN (США) – itVPN (ООО "ИТТАС").

Опенсорсные СКЗИ – это не обычное ПО с открытыми кодами, под которое они маскируются. Средства шифрования во всем мире относят к товарам двойного (военного) назначения. Их создание, ввоз и вывоз – это исключительная компетенция спецслужб. Без их участия никакое СКЗИ не может быть создано, и тем, более куда-то вывезено. При этом проверить скачиваемое ПО (около миллиона строк исходных кодов), созданное неизвестными разработчиками, невозможно. Не секрет, что в наше время техническими спецслужбами осуществляется тотальный контроль за информационными потоками – прослушивание, мониторинг, взломы и проникновения стали повседневностью. Поэтому я разделяю мнение экспертов международной конференции "Инфофорум-Евразия" (страны ШОС, БРИКС, ОДКБ), в оргкомитет которой вхожу, о том, что в опенсорсных СКЗИ (ПО), вне всякого сомнения, имеются закладки, позволяющие получить доступ к защищаемой информации и/или блокировать работу шифраторов.

Есть у опенсорсных СКЗИ и другие проблемы: поскольку код ПО общедоступен, то все могут искать и находить в нем уязвимости, которые иногда публикуются, понятно, что далеко не все. Опасно работать с теми уязвимостями, которые длительное время (месяцами) не закрываются патчами по безопасности. И лицензии наши опенсорсные производители выбирают вовсе не "апач", а жесткие "GPL", которые требуют свободного распространения всех продуктов, созданных на их основе. И тут не о правах западных вендоров беспокойство, а речь о мошенничестве – контрафактных коммерческих продажах на внутреннем рынке заведо-

мо бесплатных продуктов.

Трудно согласиться с тем фактом, что СКЗИ на основе иностранного ПО и собственной разработки имеют одинаковые уровни защиты.

АНАЛИЗ ПОЛНОРАУНДОВОГО АЛГОРИТМА ШИФРОВАНИЯ LILLIPUT-TBC-II-256

А.М. Смирнов[1], М.А. Пудовкина[2]
[1,2]*Национальный исследовательский ядерный университет "МИФИ"*
Москва, РОССИЯ
e-mail: [1]smirnovanton.m@mail.ru

Алгоритм аутентифицированного шифрования LILLIPUT-AE — участник конкурса американского института стандартов и технологий на стандарт низкоресурсного алгоритма шифрования США. В работе предложена атака на полнораундовый алгоритм шифрования LILLIPUT-TBC-II-256 с ключом длины 256 бит методом бумеранга, комбинированным с подходом на основе «йо-йо» игры. Для атаки требуется $2^{128} + 2^{16}$ текстов, $30 \cdot 2^{16}$ бит памяти. Ее трудоемкость равна $31 \cdot (2^{128} + 2^{144})$ зашифрований. Вероятность успеха равна 1.

Ключевые слова: низкоресурсный алгоритм шифрования; подход йо-йо; аутентифицированное шифрование; линейное преобразование; S-блок; режим OFB; метод бумеранга; разностный метод

1 Введение

Алгоритм блочного шифрования LILLIPUT [1] разработан в 2015 г. Он основан на расширенном обобщенном преобразовании Фейстеля (Generalized Feistel Networks (EGFN)) [2]. Длина ключа шифрования алгоритма LILLIPUT равна 80 бит, длина блока — 64 бит, число раундов — 30. Подстановки S-блока являются 4-битными. Редуцированный алгоритм LILLIPUT анализировался интегральным методом

[3], методом невозможных разностей [4] и разностным методом [5]. Обнаруженные в ходе анализа слабости привели к синтезу семейства алгоритмов аутентифицированного шифрования LILLIPUT-AE [6] для участия в конкурсе американского института стандартизации (NIST) на стандарт низкоресурсного алгоритма шифрования США.

Основой семейства LILLIPUT-AE являются блочная шифрсистема LILLIPUT-TBC в режиме OCB [7] (Offset Codebook) с длиной блока 128 бит и длинами ключей шифрования 128, 192, 256 бит, где буквы TBC означают модифицированные алгоритм шифрования LILLIPUT с 8-битной подстановкой S-блока и алгоритм развертывания ключа (tweakable block cipher). В [8] на поданную на конкурс первую версию семейства LILLIPUT-AE приведена практическая атака, позволяющая подделывать сообщения из-за выявленных слабостей модифицированного алгоритма развертывания ключа. В результате авторами семейства LILLIPUT-AE предложена вторая версия блочной шифрсистемы LILLIPUT-TBC, которая рассматривается далее.

Настоящая работа посвящена анализу полнораундового алгоритма шифрования LILLIPUT-TBC-II с ключом длины 256 бит (LILLIPUT-TBC-II-256) с помощью модификации метода бумеранга и подхода на основе «йо-йо» игры, используемого для построения различителя. Отметим, что подход на основе «йо-йо» игры [9] применялся для атаки на алгоритм блочного шифрования AES.

2 Основные обозначения

Пусть $V_n(2^m)$ — n-мерное векторное пространство над полем $\mathbb{F}_{2^m}$, где $n, m \in \mathbb{N}$; $\oplus$ — операция сложения в $V_n(2^m)$; 0_n — n-мерный вектор, у которого все координаты равны нулю; $I(A)$ — индикатор выполнения условия A; $M^{(4)}_{\mathbb{F}_{2^8}}$ — множество всех 4×4-матриц над полем $\mathbb{F}_{2^8}$; $g\colon V_{16}(2^8) \times V_{16}(2^8) \to V_{16}(2^8)$ — раундовая функция алгоритма LILLIPUT-TBC-II-256.

Для произвольного $\alpha = (\alpha_{0,0}, \alpha_{0,1}, ..., \alpha_{3,3}) \in V_{16}(2^8)$ рассмотрим отображение $\phi\colon V_{16}(2^8) \to M^{(4)}_{\mathbb{F}_{2^8}}$, заданное условием

$$\hat{\alpha} = \phi(\alpha) = \begin{pmatrix} \alpha_{0,0} & \alpha_{0,1} & \alpha_{0,2} & \alpha_{0,3} \\ \alpha_{1,0} & \alpha_{1,1} & \alpha_{1,2} & \alpha_{1,3} \\ \alpha_{2,0} & \alpha_{2,1} & \alpha_{2,2} & \alpha_{2,3} \\ \alpha_{3,0} & \alpha_{3,2} & \alpha_{3,2} & \alpha_{3,3} \end{pmatrix}.$$

Пусть h — $(0,1)$-матрица порядка 16 над полем $\mathbb{F}_{2^8}$ линейного слоя раундовой функции g, а π — 8-битная подстановка S-блока

$$s = (s_{0,0}, ..., s_{0,3}, ..., s_{3,0}, ..., s_{3,3}) \in S(V_{16}(2^8)),$$

где

$$s_{i,j}(\alpha_{i,j}) = \pi(\alpha_{i,j}) \oplus \gamma_{i,j},$$

$\gamma_{i,j}$ — фиксированная константа, $\gamma_{i,j} \in \mathbb{F}_{2^8}$, $i, j \in \{0, ..., 3\}$. Тогда раундовая функция g задается равенством

$$g(\alpha, k) = g_k(\alpha) = h(s(\alpha \oplus k))^T$$

для каждых $(\alpha, k) \in V_{16}(2^8) \times V_{16}(2^8)$, где T – знак транспонирования.

Для произвольного вектора

$$\alpha = (\alpha_0, ..., \alpha_{15}) \in V_{16}(2^8)$$

и каждого $i \in \{0, ..., 15\}$ определим отображение $w^{(i)} \colon V_{16}(2^8) \to \mathbb{F}_2$ условием

$$w^{(i)}(\alpha) = I(\alpha_i \neq 0).$$

Положим

$$w(\alpha) = (w^{(0)}(\alpha), w^{(1)}(\alpha), ..., w^{(15)}(\alpha)).$$

3 Атака на алгоритм LILLIPUT-TBC-II-256

Главный этап атаки на алгоритм LILLIPUT-TBC-II-256 методом бумеранга, комбинированным с модификацией «йо-йо» игры, для нахождения ключа шифрованием алгоритма LILLIPUT-TBC-II-256 состоит в нахождении различителя. Его построение основано на Теоремах 1, 2.

Теорема 1. *Пусть* $\alpha_0, \alpha_1, k_0, k_1, k_2, ..., k_{31}$ – *произвольные элементы векторного пространства* $V_{16}(2^8)$,

$$\beta_i = k_{31} \oplus g_{k_{30}} ... g_{k_1} g_{k_0}(\alpha_i),\ i = 0, 1.$$

Тогда справедливо равенство

$$w((sh)^{-1}(\beta_0) \oplus (sh)^{-1}(\beta_1))$$
$$= w(g_{k_{29}} ... g_{k_1} g_{k_0}(\alpha_0) \oplus g_{k_{29}} ... g_{k_1} g_{k_0}(\alpha_1)).$$

Теорема 2. *Пусть* $\alpha_0, \alpha_1, k_0, k_1, k_2, ..., k_{30}$ – *произвольные элементы векторного пространства* $V_{16}(2^8)$,

$$\beta_i = g_{k_{30}} ... g_{k_1} g_{k_0}(\alpha_i),\ i = 0, 1.$$

Тогда справедливо равенство

$$w((sh)^{-2}(\beta_0) \oplus (sh)^{-2}(\beta_1))$$
$$= w(g_{k_{28}}...g_{k_1}g_{k_0}(\alpha_0) \oplus g_{k_{28}}...g_{k_1}g_{k_0}(\alpha_1)).$$

Матрице h поставим в соответствие блочную (4×4)-матрицу $\hat{h}$ с блоками $h_{i,j}$, $i, j \in \{0, 1, 2, 3\}$, где

$$\hat{h} = \begin{pmatrix} h_{0,0} & h_{0,1} & h_{0,2} & h_{0,3} \\ h_{1,0} & h_{1,1} & h_{1,2} & h_{1,3} \\ h_{2,0} & h_{2,1} & h_{2,2} & h_{2,3} \\ h_{3,0} & h_{3,2} & h_{3,2} & h_{3,3} \end{pmatrix}.$$

Раундовый ключ $k \in V_{16}(2^8)$ также представим в табличном виде

$$\hat{k} = \phi(k) = \begin{pmatrix} k_{0,0} & k_{0,1} & k_{0,2} & k_{0,3} \\ k_{1,0} & k_{1,1} & k_{1,2} & k_{1,3} \\ k_{2,0} & k_{2,1} & k_{2,2} & k_{2,3} \\ k_{3,0} & k_{3,1} & k_{3,2} & k_{3,3} \end{pmatrix}.$$

Теорема 3. *Пусть существуют такие* $i, j_1, j_2, r, t \in \{0, ..., 3\}$, $\gamma_{j_1,j_2,r} \in \mathbb{F}_{2^8}$, *что элементы подматриц* h^{-1}_{i,j_1}, h^{-1}_{i,j_2} *матрицы* $\hat{h}^{-1}$ *и подстановки* $s_{j_1,r}, s_{j_2,r}$ *алгоритма LILLIPUT-TBC-II-256 удовлетворяют условиям*

$$(h^{-1}_{i,j_1})_{t,r} = (h^{-1}_{i,j_2})_{t,r}, (c_{i,j_1})_{t,r} \neq 0,$$

$$s_{j_1,r}(\beta) = s_{j_2,r}(\beta \oplus \gamma_{j_1,j_2,r}) \text{ для всех } \beta \in \mathbb{F}_{2^8}.$$

Тогда для каждого $\delta \in \mathbb{F}_{2^8}$ *и* $k \in V_{16}(2^8)$ *существует вектор*

$$\omega \in \langle \alpha_{j_1,r} \oplus \alpha_{j_2,r} \oplus k_{j_1,r} \oplus k_{j_2,r} \rangle \oplus \delta,$$

удовлетворяющий равенству

$$s_{j_1,r}(\alpha_{j_1,r} \oplus k_{j_1,r} \oplus \delta) \oplus s_{j_1,r}(\alpha_{j_1,r} \oplus k_{j_1,r}) \oplus$$

$$\oplus s_{j_2,r}(\alpha_{j_2,r} \oplus k_{j_2,r} \oplus \omega \oplus \delta) \oplus s_{j_2,r}(\alpha_{j_2,r} \oplus k_{j_2,r} \oplus \omega) = 0.$$

Для $\epsilon_{i,j} \in V_{16}(2^8)$ при $i, j, t, r \in \{0, ..., 3\}$ положим

$$(\epsilon_{i,j})_{t,r} = I((i,j) = (t,r)).$$

Теорема 4. *Пусть существуют такие* $i, j_1, j_2, r, t \in \{0, ..., 3\}$, $\gamma_{j_1,j_2,r} \in \mathbb{F}_{2^8}$, *что элементы подматриц* h^{-1}_{i,j_1}, h^{-1}_{i,j_2} *матрицы* $\hat{h}^{-1}$ *и подстановки* $s_{j_1,r}, s_{j_2,r}$ *алгоритма LILLIPUT-TBC-II-256 удовлетворяют условиям*

$$(h^{-1}_{i,j_1})_{t,r} = (h^{-1}_{i,j_2})_{t,r}, (c_{i,j_1})_{t,r} \neq 0,$$

$$s_{j_1,r}(\beta) = s_{j_2,r}(\beta \oplus \gamma_{j_1,j_2,r}) \text{ для всех } \beta \in \mathbb{F}_{2^8}.$$

Тогда для каждых $\delta \in \mathbb{F}_{2^8}$, $\alpha \in V_{16}(2^8)$ *равенство* $\vartheta^{(\omega)}_{i,t} = 0$ *выполняется для всех* $\omega \in \mathbb{F}_{2^8}$, *где разность* $\vartheta^{(\omega)}_{i,t}$ *при расшифровании раундовой функцией пары шифртекстов* $\alpha \oplus \omega \cdot \epsilon_{j_2,r}$ *и* $\alpha \oplus \delta \cdot \epsilon_{j_1,r} \oplus (\delta \oplus \omega) \cdot \epsilon_{j_2,r}$ *задается условием*

$$\vartheta^{(\omega)} = ((sh)^{-1}(\alpha \oplus \omega \cdot \epsilon_{j_2,r}) \oplus k)^T$$
$$\oplus((sh)^{-1}(\alpha \oplus \delta \cdot \epsilon_{j_1,r} \oplus (\omega \oplus \delta) \cdot \epsilon_{j_2,r}) \oplus k)^T.$$

На основании теорем 1 — 4 предложена атака методом бумеранга, комбинированным с модификацией «йо-йо» игры, на полнораундовый алгоритм LILLIPUT-TBC-II-256. Для определения истинного раундового ключа k_r, $r \in \{0, 1, ..., 31\}$ на первом шаге предлагаемой атаки выбирается произвольным образом некоторый открытый текст α_0, формируется множество $\mathcal{P}_r$ в соответствии с Теоремой 1. Далее, можно построить различитель последнего раундового ключа k_r, согласно Теореме 2, следующим образом. Раундовые ключи k_r и $\tilde{k}_r$ равны в том случае, если более,

чем для 2^9-2 шифртекстов β'_1, соответствующих открытым текстам из множества $\mathcal{P}_r$, верно равенство:

$$((sh)^{-2}(\beta_0 \oplus \tilde{k}_r) \oplus sh^{-2}(\beta'_1 \oplus \tilde{k}_r))_{i,t} = 0,$$

где индексы i, t выбираются согласно Теореме 4.

Доказано, что для атаки требуется $2^{128} + 2^{16}$ текстов, $30 \cdot 2^{16}$ бит памяти. Трудоемкость нахождения 256-битного ключа равна $31 \cdot (2^{128} + 2^{144})$ операций зашифрования. Вероятность успеха атаки равна 1.

Библиографические ссылки

1. Extended generalized Feistel networks using matrix representation to propose a new lightweight block cipher: Lilliput / T.P. Berger [et al.] // IEEE Trans. Computers. 2016. Vol. 65, No. 7. P. 2074–2089.

2. *Berger T.P., Minier M., Thomas G.* Extended generalized feistel networks using matrix representation // LNCS. 2014. Vol. 8282. P. 289–305.

3. *Sasaki Y., Todo Y.* New Differential Bounds and Division Property of LILLIPUT: Block Cipher with Extended Generalized Feistel Network // LNCS. 2016. Vol. 10532. P. 264–283.

4. *Sasaki Y., Todo Y.* New Impossible Differential Search Tool from Design and Cryptanalysis Aspects Revealing Structural Properties of Several Ciphers // LNCS. 2017. Vol. 10212, No. 3. P. 185–215.

5. *Marriere N., Nachef V., Volte E.* Differential Attacks on Reduced Round LILLIPUT // LNCS. 2018. Vol. 10946. P. 188–206.

6. Lilliput-AE: a New Lightweight Tweakable Block Cipher for Authenticated Encryption with Associated Data [Electronic resource].
URL: `https://csrc.nist.gov/CSRC/media/Projects/Lightweight-Cryptography/documents/round-1/spec-doc/LILLIPUT-AE-spec.pdf`
(date of access: 10.08.2023).

7. OCB: a block-cipher mode of operation for efficient authenticated encryption / P. Rogaway [et al.] // Proc. 8th ACM Conf. Comp. Comm. Security. 2001. P. 196–205.

8. A Practical Forgery Attack on Lilliput-AE [Electronic resource]. URL: `https://eprint.iacr.org/2019/867`
(date of access: 10.08.2023).

9. *Ronjom S., Bardeh N.G., Helleseth T.* Yoyo tricks with AES // LNCS. 2017. Vol. 10624, No. 1. P. 217–243.

ОБЛАЧНАЯ ЭЛЕКТРОННАЯ ЦИФРОВАЯ ПОДПИСЬ: ПРОТОКОЛ АКТИВАЦИИ ПОДПИСИ

О.В. Соловей[1]
[1]*НИИ прикладных проблем математики и информатики*
[1]*Белорусский государственный университет*
Минск, БЕЛАРУСЬ
e-mail: solovey@bsu.by

Предложен протокол активации подписи, предназначенный для использования в системах облачной подписи.
Ключевые слова: облачный сервис; электронная цифровая подпись; облачная подпись; протокол активации подписи

1 Введение

В последние годы активно развиваются облачные сервисы. Они обеспечивают удаленный доступ к набору конфигурируемых вычислительных ресурсов, предоставляемых серверами Интернет по запросу пользователя.

Одним из востребованных облачных сервисов является сервис облачной подписи, под которым понимают удаленную выработку электронной цифровой подписи (ЭЦП) под контролем владельца личного ключа (подписанта). Личный ключ хранится и управляется удаленной службой подписи (СП). Выработка ЭЦП на личном ключе подписанта выполняется СП после аутентификации подписанта и передачи подписантом права подписи документа.

Чтобы обеспечить безопасность процесса создания облачной ЭЦП и гарантировать использование ключей подписи

только под контролем владельца, поставщик услуг по удаленной выработке подписи должен применять надежные механизмы и протоколы безопасности. В частности, при выработке ЭЦП должен применяться надежный протокол активации подписи (ПАП), предназначенный для передачи СП права выработки ЭЦП на личном ключе подписанта.

В Европейском союзе действует ряд стандартов и спецификаций, определяющих требования к системам облачной подписи (СОП) — информационным системам, использующим личные ключи подписантов под их контролем для дистанционного создания подписанного документа. Основные стандарты: EN 419241-1 [2], EN 419241-2 [3], ETSI TS 119 431-1 V1.1.1 [4], ETSI TS 119 431-2 V1.1.1 [5], ETSI TS 119 432 V1.1.1 [6].

В разделе 2 мы опишем структуру СОП и правила выработки облачной подписи. Наше описание соответствует упомянутым стандартам Европейского союза. В разделе 3 мы предложим протокол активации подписи.

2 Системы облачной подписи

В СОП выделяют следующие компоненты:

– служба подписи (СП), предназначенная для генерации и хранения личных ключей подписантов, выработки ЭЦП на личных ключах подписантов под их контролем;

– служба документов (СД), предназначенная для создания и проверки подписанных документов;

– клиентская программа (КП), предназначенная для взаимодействия подписанта с СД, СП и, возможно, внешними по отношению к СОП компонентами.

Компоненты СОП взаимодействуют с такими внешними компонентами, как служба регистрации подписантов, удостоверяющий центр (УЦ), OCSP-сервер, служба штампов времени (СШВ). Компоненты СОП могут дополнительно взаимодействовать с другими внешними компонентами, например, со службой идентификации (СИ), выполняющей идентификацию и аутентификацию подписантов вместо компонентов СОП, и прикладной системой (ПС), предоставляющей документ для подписи.

Компоненты СОП взаимодействуют между собой и с внешними компонентами по защищенным соединениям, обеспечивающим конфиденциальность и целостность передаваемых данных. При установлении защищенных соединений выполняется взаимная аутентификация сторон. Аутентификация КП, как правило, выполняется неявно, через аутентификацию подписанта.

В СОП предусмотрено два типа аутентификации подписанта:

1) аутентификация подписанта в системе — проводится при создании сеанса взаимодействия подписанта с СОП;

2) аутентификация подписанта для управления личным ключом — проводится после аутентификации подписанта в системе перед генерацией личного ключа и при активации операции подписи.

Подписантом использует для аутентификации токен аутентификации — объект (устройство или данные), которым подписант владеет или который подписант знает. Например, в качестве токена аутентификации может выступать статический пароль. Владение токеном подтверждает подлинность владельца. В свою очередь, владение токеном аутентификации подтверждается аутентификатором — данными, полученными с помощью токена.

Проверку аутентификаторов выполняет СП и (или) СИ. Если проверка аутентификатора выполняется СИ, то СП проверяет подтверждение аутентификации, сформированное СИ.

Для подписи документов применяется личный ключ подписанта, который генерируется, хранится и используется только в СП. Перед генерацией ключа выполняется аутентификация подписанта для управления личным ключом. После генерации личного ключа для соответствующего открытого ключа с помощью УЦ выпускается сертификат открытого ключа (СОК), который устанавливается в СП и который проверяется на действительность перед каждым использованием личного ключа. Для одного подписанта СП может поддерживать несколько личных ключей. При этом подписант может использовать одни и те же токены аутентификации для управления всеми своими личными ключами.

В СОП подписываемый документ может формироваться подписантом средствами СД, передаваться в СД подписантом или ПС. Вместо документа в СД может передаваться хэш-значение документа, вычисленное с помощью КП.

При этом СОП должна обеспечивать защиту от подмены подписываемого документа и его хэш-значения. Применяемые механизмы защиты должны соответствовать принципу «Что вы видите, то и подписываете».

В подписи документа участвуют КП (представляет подписанта), СД (формирует данные для подписи и подписанный документ) и СП (вычисляет ЭЦП). Дополнительно участвуют внешние службы: УЦ или OCSP-сервер (для проверки статуса СОК), СШВ (для получения штампа времени, включаемого в подписанный документ). Также в процессе подписи может участвовать ПС, если подписываемый документ предоставляется ею.

Подпись документа требует аутентификации подписанта с целью активации операции подписи. Подписант может быть аутентифицирован один раз для подписи группы документов, если такая возможность поддерживается СП. В этом случае, каждый документ из группы подписывается по отдельности.

При подписи документа значение ЭЦП вырабатывается СП на личном ключе подписанта от представления данных для подписи (ПДП) — хэш-значения, которое вычисляется СД от хэш-значения подписываемого документа и других данных, определяемых форматом подписанного документа. Как правило, для подписанных документов используются форматы AdES (от англ. Advanced Electronic Signature), которые в Республике Беларусь представлены в СТБ 34.101.80. Сформированный подписанный документ передается подписанту или ПС.

3 Протокол активации подписи

При выполнении ПАП производится (проверяется) аутентификация подписанта и формируются данные активации подписи (ДАП). ДАП связывают, как минимум, аутентификацию подписанта, ПДП и идентификатор личного ключа подписанта. ДАП используются для непосредственной активации операции подписи.

Если СП поддерживает подпись группы документов, то одно значение ДАП может формироваться для набора ПДП. Идентификатор личного ключа может не определяться ДАП, если ключ выбирается неявно, например, если у подписанта только один личный ключ. Если аутентификация подписанта для управления личным ключом выполняется СИ, то в ДАП включается подтверждение аутентификации подписанта, сформированное данной СИ. Это подтверждение используется СП для проверки аутентификации подписанта.

В Европейских стандартах и спецификациях не определяется дизайн ПАП, но устанавливаются требования безопасности для ПАП и ДАП. В частности требуется, чтобы ПАП противостоял определенным атакам, таким как «злоумышленник посередине», «кража сеанса», перехват, повтор, подделка и др.

Отметим, что в спецификации [1], разработанной консорциумом облачной подписи (группой компаний и научных организаций), описывается несколько вариантов процесса выработки подписи. При этом ни один из описанных вариантов не поддерживает передачу подписываемого документа (ПД) непосредственно подписантом.

Предложим ПАП, который может использоваться для случая, когда ПД передается подписантом, а аутентификация подписанта с целью активации подписи выполняется СП на основании статического пароля (PIN-кода) и одноразового пароля (ОП). Предполагается, что подписант предварительно был успешно аутентифицирован в системе и для каждого подписанта в СП хранится только один личный ключ.

ПАП являются частью процесса подписи документа. Алгоритм выполнения данного процесса включает следующие шаги (см. рис. 1):

1. Подписант с помощью КП вводит PIN-код доступа к личному ключу и передает PIN-код в СД.
2. СД передает полученный от подписанта PIN-код в СП.
3. СП проверяет PIN-код и передает СОК подписанта в СД.
4. СД проверяет действительность СОК подписанта (с использованием УЦ или OCSP-сервера).
5. СД передает в КП запрос на предоставление ПД.
6. Подписант с помощью КП выбирает ПД и вычисляет его хэш-значение.
7. КП передает ПД в СД.
8. СД формирует подписываемые атрибуты (ПА), определяемые форматом подписанного документа, и вычисляет по ПД и ПА значение ПДП.
9. СД передает ПДП в СП.

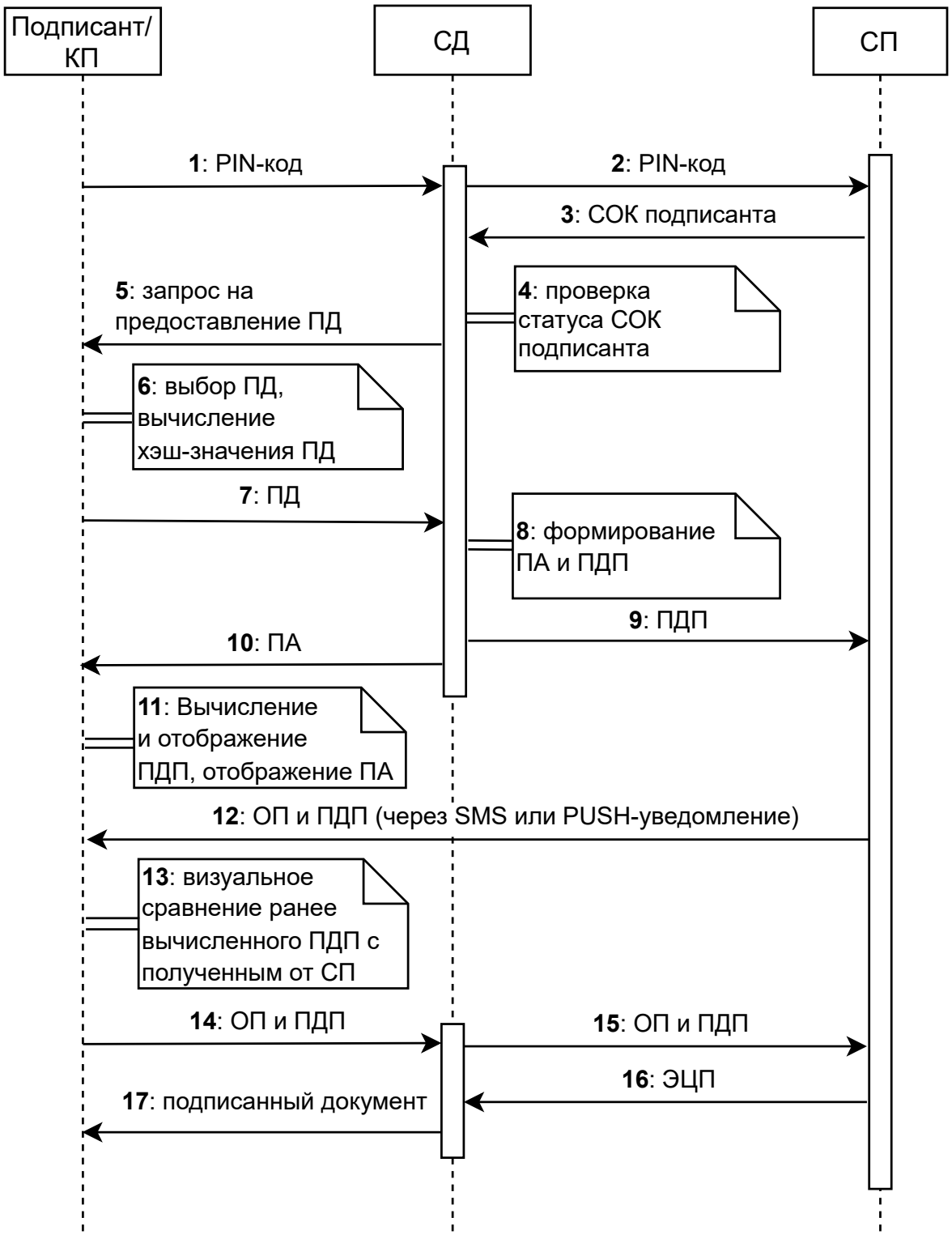

Рис. 1. Активация операции подписи и подпись документа

10. СД передает ПА в КП.

11. КП на основании ПА, полученных от СД, и хэш-значения ПД, вычисленного на шаге 6, вычисляет ПДП и отображает подписанту ПДП и ПА.

12. СП формирует ОП и отправляет на мобильное устройство подписанта ОП и ПДП (как SMS-сообщение или PUSH-уведомление).

13. Подписант визуально сравнивает значение ПДП, отображаемое КП, со значением ПДП, полученным на мобильное устройство.

14. Подписант с помощью КП вводит полученное на шаге 12 значение ОП и передает ОП и ПДП в СД.

15. СД сравнивает ПДП, вычисленное на шаге 8, со значением, полученным от КП, и передает ОП и ПДП в СП.

16. СП проверяет ОП, сравнивает ПДП, полученные на шагах 9 и 15, и, в случае корректности ОП и ПДП, вычисляет ЭЦП и передает его в СД.

17. СД формирует подписанный документ и передает его в КП.

В описании алгоритма для простоты опущена обработка ошибок, например, ошибок аутентификации подписанта или ошибок при обработке СОК.

Предложенный алгоритм реализует ПАП и механизм защиты от подмены подписываемого документа. В качестве

ДАП выступают ОП и ПДП. Формирование ДАП выполняется с участием подписанта под его контролем. Согласие на подпись документа дается подписантом путем ввода ОП после визуального сравнения ПДП, вычисленного КП, со значением, полученным от СП по каналам мобильной связи (минуя СД). Защита от атак на ПАП обеспечивается использованием защищенных соединений и взаимной аутентификацией сторон. Для этих целей может использоваться протокол TLS.

Библиографические ссылки

1. Cloud Signature Consortium Standard. Architectures and protocols for remote signature applications. Version 2.0.0.2 [Electronic resource].
   URL: `https://cloudsignatureconsortium.org/resources/download-api-specifications`
   (date of access: 28.07.2023).

2. EN 419241-1 «Security Requirements for Trustworthy Systems Supporting Server Signing — Part 1: General System Security Requirements» [Electronic resource].
   URL: `https://www.en-standard.eu/csn-en-419241-1-trustworthy-systems-supporting-server-signing-part-1-general-system-security-requirements`
   (date of access: 28.07.2023).

3. EN 419241-2 «Security Requirements for Trustworthy Systems Supporting Server Signing — Part 2: Protection profile for QSCD for Server Signing» [Electronic resource].

URL: https://www.en-standard.eu
/csn-en-419211-2-protection-
profiles-for-secure-signature-creation-
device-part-2-device-with-key-generation
(date of access: 28.07.2023).

4. ETSI TS 119 431-1 V1.1.1 «Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service providers; Part 1: TSP service components operating a remote QSCD / SCDev» [Electronic resource]. URL: https://www.etsi.org/deliver/etsi_ts
/119400_119499/11943101/01.01.01_60
/ts_11943101v010101p.pdf
(date of access: 28.07.2023).

5. ETSI TS 119 431-2 V1.1.1 «Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service providers; Part 2: TSP service components supporting AdES digital signature creation» [Electronic resource]. URL: https://www.etsi.org/deliver
/etsi_ts/119400_119499/11943102/01.01.01_60
/ts_11943102v010101p.pdf
(date of access: 28.07.2023).

6. ETSI TS 119 432 V1.1.1 «Electronic Signatures and Infrastructures (ESI); Protocols for remote digital signature creation» [Electronic resource].
URL: https://www.etsi.org/deliver/etsi_ts
/119400_119499/119432/01.01.01_60
/ts_119432v010101p.pdf
(date of access: 28.07.2023).

СТАТИСТИЧЕСКАЯ ПРОВЕРКА СЛОЖНЫХ ГИПОТЕЗ ОБ s-МЕРНОМ РАВНОМЕРНОМ РАСПРЕДЕЛЕНИИ ВЕРОЯТНОСТЕЙ ДВОИЧНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ

Ю.С. Харин[1]

[1]*НИИ прикладных проблем математики и информатики*

[1]*Белорусский государственный университет*

Минск, БЕЛАРУСЬ

e-mail: kharin@bsu.by

В докладе рассматривается подход к статистической проверке сложных гипотез об s-мерном равномерном распределении вероятностей двоичных случайных последовательностей.

Ключевые слова: статистическое тестирование; сложные гипотезы; решающее правило

Пусть $V = \{0,1\}$ и на вероятностном пространстве $(\Omega, \mathcal{F}, \mathbf{P})$ наблюдается двоичная случайная последовательность $X = X_1^T = (x_1, \ldots, x_T)$ длины $T = n \cdot s$, разбитая на n последовательных s-грамм:

$$X \equiv \left(X_1^s, X_{s+1}^{2s}, \ldots, X_{(n-1)s+1}^{T} \right) \in V^T. \qquad (1)$$

Предполагается, что эти s-граммы независимы в совокупности и одинаково распределены с некоторым распределением $p = \left(p_{J_1^s}\right) \in \mathcal{P}$:

$$\mathbf{P}\left\{ X_{(i-1)s+1}^{is} = J_1^s \right\}$$
$$::= \mathbf{P}\left\{ x_{(i-1)s+1} = j_1, \ldots, x_{is} = j_s \right\} = p_{J_1^s}, \qquad (2)$$

$J_1^s = (j_k) \in V^s$, $i = 1, \ldots, n$, где

$$\mathcal{P} = \left\{ p = \left(p_{J_1^s}\right) : p_{J_1^s} \geq 0, \quad J_1^s \in V^s, \quad \sum_{J_1^s \in V^s} p_{J_1^s} = 1 \right\} \quad (3)$$

– семейство (симплекс) всевозможных s-мерных вероятностных распределений в V^s.

В дальнейшем для упрощения обозначений перейдем от мультииндекса $J_1^s = (j_1, ..., j_s) \in V^s$ к одномерному индексу $k \in \{0, 1, \ldots, 2^s - 1\}$:

$$k =< J_1^s >::= \sum_{i=1}^{s} j_i \cdot 2^{i-1} \in \{0, 1, \ldots, K-1\},\ K = 2^s;$$

обратное преобразование:

$$J_1^s = (j_1, \ldots, j_s) => k <,$$

$$j_{s-i+1} = \left[\left(k - \sum_{l=s-i+2}^{s} j_l \cdot 2^{l-1} \right) / 2^{s-i} \right],\ i = 1, \ldots, s.$$

В существующих «батареях тестов» [1,2], подвергнутых многочисленным модификациям и критике [3–5], используются тесты статистической проверки **простой гипотезы**

$$H_* = \{p = p_*\}, \quad p_* = (p_{*k}), \quad p_{*k} \equiv \frac{1}{K}, \quad (4)$$

против сложной альтернативы $\overline{H}_*$. В связи с тем, что на практике «идеальные генераторы», порождающие «чисто случайную» последовательность, не существуют, то любой состоятельный тест для проверки $\left\{H_*, \overline{H}_*\right\}$ при $T \to +\infty$ отвергает гипотезу H_*. Для преодоления этого парадокса

введем в рассмотрение сложную нулевую гипотезу об s-мерной равномерности:

$$H_0^{\varepsilon+} = \{p = (p_k) \in \mathcal{P}_0^{\varepsilon+}\}, \tag{5}$$

где

$$\mathcal{P}_0^{\varepsilon+} = \left\{ p \in \mathcal{P} : \|p - p_*\| = \sqrt{\sum_{k=0}^{K-1} \left(p_k - \frac{1}{K}\right)^2} \leq \varepsilon_+ \right\}$$

– гипершар в $\mathbb{R}^K$ (точнее в симплексе $\mathcal{P}$) заданного радиуса ε_+ с центром в точке p_* s-мерного равномерного распределения; $\varepsilon_+ \in \left(0, K^{-1}\right)$ – достаточно малый параметр сложной нулевой гипотезы, определяющий допустимые отклонения от простой (точечной) нулевой гипотезы H_*. Гипотеза H_* является предельной по отношению к $H_0^{\varepsilon+}$:

$$H_0^{\varepsilon+} \underset{\varepsilon_+ \to 0}{\longrightarrow} H_*.$$

Построим критерий отношения правдоподобия по наблюдаемой последовательности X_1^T для проверки сложной нулевой гипотезы $H_0^{\varepsilon+}$ против сложной альтернативы

$$H_1^{\varepsilon+} = \overline{H_0^{\varepsilon+}} = \{p = (p_k) \in \mathcal{P}_1^{\varepsilon+}\}, \quad \mathcal{P}_0^{\varepsilon+} \sqcup \mathcal{P}_1^{\varepsilon+} = \mathcal{P}.$$

Примем следующие обозначения: $\mathbf{1}\{C\}$ – индикатор события C, $\mathbf{1}_N$ – вектор-столбец, все N компонент которого равны единице; $\mathbf{0}_N$ – вектор-столбец, все N компонент которого равны нулю;

$$S_\varepsilon = \{p \in \mathcal{P} : \|p - p_*\| = \varepsilon\} \subset \mathcal{P}_0^\varepsilon \tag{6}$$

– гиперсфера радиуса $\varepsilon \in [0, \varepsilon_+]$ с центром в точке $p_* = \frac{1}{K}\mathbf{1}_K$;

$$\nu_k(n) = \sum_{i=1}^{n} \mathbf{1}\left\{ < X^{is}_{(i-1)s+1} >= k \right\} \geq 0, \ \sum_{k=0}^{K-1} \nu_k(n) \equiv 1, \quad (7)$$

где $\nu_k(n)$ – частота встречаемости s-граммы $> k <$ в последовательности n фрагментов $X_1^s, X_{s+1}^{2s}, \ldots, X_{(n-1)s}^T$,

$$\hat{p}_k = \frac{\nu_k}{n}, \quad k = 0, 1, \ldots, K-1, \quad (8)$$

– несмещенная, строго состоятельная, эффективная оценка максимального правдоподобия для p_k;

$$l(X; p) = \sum_{k=0}^{K-1} \nu_k \ln p_k = n \sum_{k=0}^{K-1} \hat{p}_k \ln p_k \quad (9)$$

– логарифмическая функция правдоподобия (ЛФП);

$$l^*_{S_\varepsilon}(X) = \max_{p \in S_\varepsilon} l(X; p) \quad (10)$$

– максимальное на гиперсфере S_ε значение ЛФП.

Лемма 1. *Логарифмическая статистика отношения правдоподобия для проверки сложных гипотез $H_0^{\varepsilon_+}$, $H_1^{\varepsilon_+}$ об s-мерной равномерности по наблюдаемой двоичной последовательности $X \in V^T$ имеет вид:*

$$\lambda(X) = \max_{0 \leq \varepsilon \leq \varepsilon_+} l^*_{S_\varepsilon}(X) - n \sum_{k=0}^{K-1} \hat{p}_k \ln \hat{p}_k, \quad (11)$$

где

$$\lambda(X) = \ln \Lambda(X), \quad \Lambda(X) = \frac{\sup\limits_{p \in \mathcal{P}_0^{\varepsilon_+}} L(X; p)}{\sup\limits_{p \in \mathcal{P}} L(X; p)} \in [0, 1].$$

Лемма 2. *Для максимального на гиперсфере S_ε значения ЛФП (10) справедливо выражение*

$$l^*_{S_\varepsilon}(X) = n \sum_{k=0}^{K-1} \hat{p}_k \ln p^*_k, \tag{12}$$

$$p^* = (p^*_k)\,,\ p^*_k = q^* + \sqrt{(q^*)^2 + \rho^* \hat{p}_k},\ k = 0, \ldots, K-1, \tag{13}$$

где $q^* \in \mathbb{R}^1$ – корень уравнения

$$q = F(q), \tag{14}$$

$$F(q) ::= \frac{1}{K}\left(1 - \sum_{k=0}^{K-1} \sqrt{q^2 + \left(\frac{1}{K} + \varepsilon^2 - 2q\right)\hat{p}_k}\right),$$

а

$$\rho^* = \frac{1}{K} + \varepsilon^2 - 2q^*.$$

Для доказательства решается экстремальная задача (10) с ограничениями (6):

$$l(X; p) = \sum_{k=0}^{K-1} \nu_k \ln p_k \to \max_p, \tag{15}$$

$$\sum_{k=0}^{K-1} p_k = 1,\ \sum_{k=0}^{K-1} \left(p_k - \frac{1}{K}\right)^2 = \varepsilon^2,\ p_k > 0,\ k = 0, \ldots, K-1.$$

Лемма 3. *Если $\|\hat{p} - p_*\| > \varepsilon$, то есть точка $\hat{p}$ лежит вне $\mathcal{P}_0^\varepsilon$, то ближайшей к точке $\hat{p} \in \mathcal{P}$ точкой $p^{**} \in \mathcal{P}_0^\varepsilon$ является точка*

$$p^{**} = p_* + \frac{\varepsilon}{\|\hat{p} - p_*\|}\,(\hat{p} - p_*)\,; \tag{16}$$

при этом квадрат минимального расстояния между этими точками $\hat{p}$ и p^{**} равен

$$\|\hat{p} - p^{**}\|^2 = \left(\|\hat{p} - p_*\| - \varepsilon\right)^2. \tag{17}$$

Следствие 1. *Если в условиях Леммы 3 радиус ε гиперсферы S_ε изменяется: $0 \le \varepsilon \le \varepsilon_+$, то ближайшей точкой к гипершару (5) является точка p^{**}, определяемая (16), (17) при $\varepsilon = \varepsilon_+$.*

Исследуем соотношение между точками p^* и p^{**}, определяемыми Леммами 2 и 3 соответственно.

Лемма 4. *В условиях Леммы 3 при $\varepsilon \to 0$ справедливо асимптотическое соотношение между точками $p^*, p^{**} \in S_\varepsilon$ при $\varepsilon \to 0$:*

$$p^* = p^{**} + O\left(\varepsilon^2\right) \cdot \mathbf{1}_K. \tag{18}$$

Графическая схема, иллюстрирующая соотношение между точками p^* и p^{**}, представлена на рис. 1.

Следствие 2. *В условиях Леммы 3 логарифмитческая статистика отношения правдоподобия (11) удовлетворяет стохастическому разложению:*

$$\lambda(X) = n\left(H(\hat{p}) - \ln K + \varepsilon_+ K \|\hat{p} - p_*\|\right) + O_{\mathcal{P}}\left(\varepsilon_+^2\right), \tag{19}$$

где

$$H(\hat{p}) = -\sum_{i=0}^{K-1} \hat{p}_i \ln \hat{p}_i \ge 0 \tag{20}$$

– подстановочная оценка энтропии Шеннона s-граммы, а $\hat{p} = (\hat{p}_k)$ определяется (8).

Лемма 5. *Пусть $p = (p_i) \in \mathcal{P}$, $\mu = (\mu_i) \in \mathbb{R}^K$, $\Sigma = (\sigma_{ij}) \in \mathbb{R}^{K\times K}$ – ковариационная матрица полиномиального распределения:*

$$\sigma_{ij} = \begin{cases} p_i(1-p_i), & j = i, \\ -p_i p_j, & j \ne i. \end{cases} \tag{21}$$

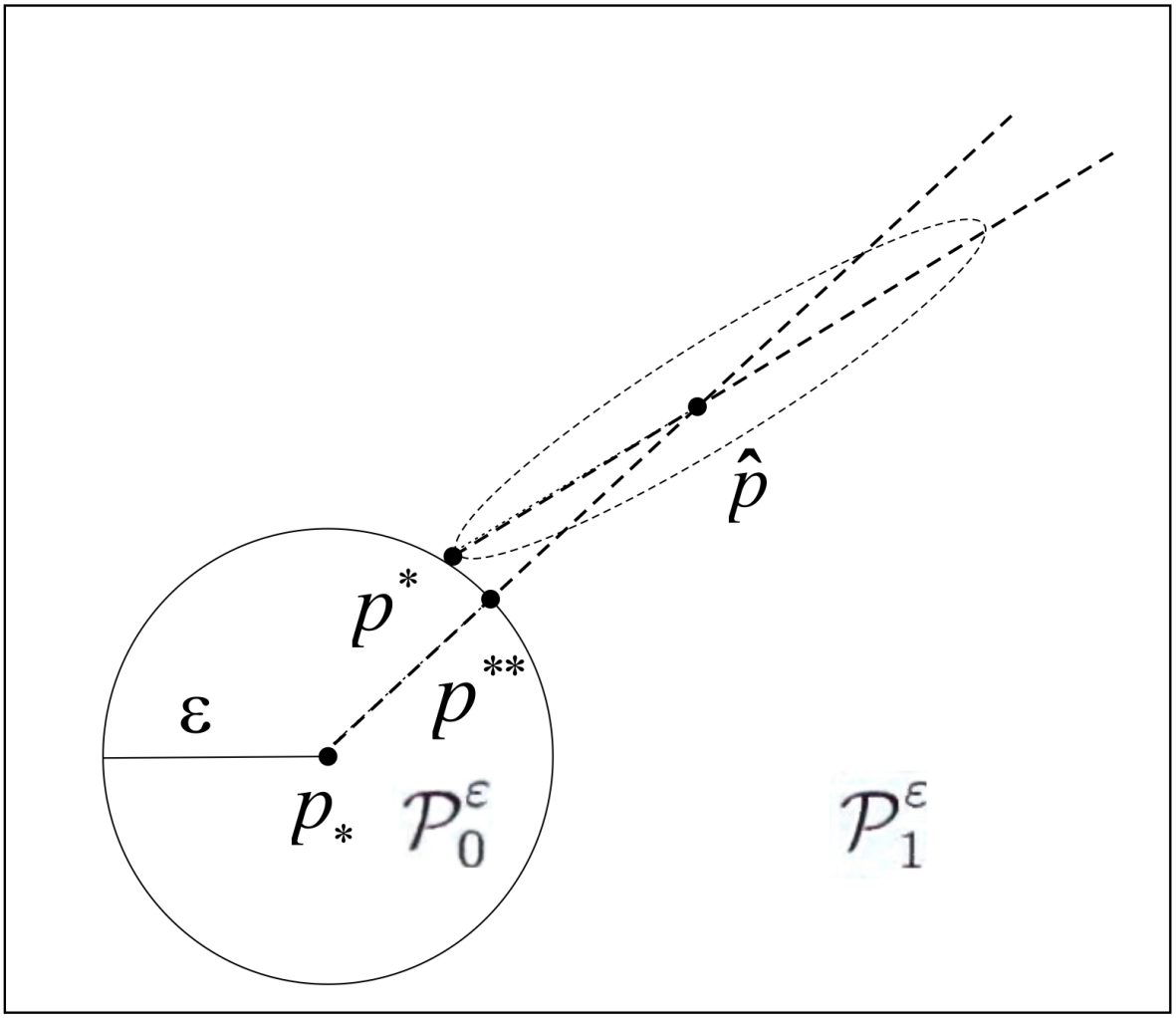

Рис. 1. Схема соотношений между p^* и p^{**}

Тогда $\mathrm{D} ::= \mu'\Sigma\mu = \mathrm{D}\{\mu_\xi\}$, *где* $\xi \in \{0, \ldots, K-1\}$ – *дискретная случайная величина с распределением* $p \in \mathcal{P}$.

С учетом Леммы 1, используя главный член стохастического разложения (19), (20), для проверки сложных гипотез $H_0^{\varepsilon+}$, $H_1^{\varepsilon+}$, будем использовать решающее правило (статистический тест):

$$d = d(X) = \begin{cases} 0, & \tilde{\lambda}(\hat{p}) \geq \Delta_n, \\ 1, & \tilde{\lambda}(\hat{p}) < \Delta_n, \end{cases} \tag{22}$$

где $\triangle_n < 0$ – некоторый пока не определенный порог,

$$\begin{aligned} \tilde{\lambda}(p) &= H(p) - \ln K + \varepsilon_+ K \|p - p_*\|, \\ \lambda(X) &= n\tilde{\lambda}(\hat{p}) + O\left(\varepsilon_+^2\right), \end{aligned} \tag{23}$$

Обозначим:

$$B = H_{(2)}(p) - H^2(p) - \frac{2\varepsilon_+ K}{\|p - p_*\|} \sum_{i=0}^{K-1} p_i^2 (H(p) + \ln p_i)$$
$$+ \frac{\varepsilon_+^2 K^2}{\|p - p_*\|^2} \left(\sum_{i=0}^{K-1} p_i^3 - \left(\sum_{i=0}^{K-1} p_i^2 \right)^2 \right), \tag{24}$$

где

$$H_{(2)}(p) = \sum_{i=0}^{K-1} p_i \ln^2 p_i \geq 0.$$

Теорема 1. *Если имеет место математическая модель двоичной последовательности с s-мерным распределением $p \in \mathcal{P}$, то при $n \to +\infty$ справедлива сходимость:*

$$\tilde{\lambda}(\hat{p}) \xrightarrow{\mathbf{P}} a = \tilde{\lambda}(p) = H(p) - \ln K + \varepsilon_+ K \|p - p_*\| \tag{25}$$

и тестовая статистика в (22) распределена асимптотически нормально:

$$\mathcal{L}\left\{ \sqrt{n} \left(\tilde{\lambda}(\hat{p}) - a \right) \right\} \to \mathcal{N}_1(0, B) \tag{26}$$

с асимптотической дисперсией B.

Следствие 3. *В условиях Теоремы 1, если $p \in S_\varepsilon$, причем $\varepsilon \leq \varepsilon_+$, асимптотическая дисперсия (24) удовлетворяет асимптотическому разложению:*

$$B = K\varepsilon_+^2 \left(1 - \frac{\varepsilon}{\varepsilon_+} \right)^2 + o\left(\varepsilon_+^2\right). \tag{27}$$

Обозначим $\Phi^{-1}(\cdot)$ квантильную функцию стандартного нормального закона.

Теорема 2. *В условиях Теоремы 1, если*

$$n > \frac{(\Phi^{-1}(1-\alpha_0))^2}{2K\varepsilon_+^2},$$

то заданный асимптотический размер $0 < \alpha_0 < 1/2$ *решающего правила* (22) *достигается при пороговом значении:*

$$\triangle_n = \frac{K\varepsilon_+^2}{2} + \frac{(\Phi^{-1}(1-\alpha_0))^2}{2n}. \tag{28}$$

Библиографические ссылки

1. *Харин Ю.С. [и др.].* Криптология. Минск: БГУ, 2013.
2. NIST SP 800-22: Documentation and Software [Electronic resource].
   URL: `https://csrc.nist.gov/projects/random-bit-generation/documentation-and-software`
   (date of access: 03.08.2023).
3. *Zubkov A.M., Serov A.A.* Testing the NIST Statistical Test Suite on artificial pseudorandom sequences // Математические вопросы криптографии. 2019. Том. 10, Вып. 2. С. 89–96.
4. *Мальцев М.В., Харин Ю.С.* О тестировании выходных последовательностей криптографических генераторов на основе цепей Маркова условного порядка // Информатика. 2013. Ном. 4. С. 104–111.

5. *Харин Ю.С., Палуха В.Ю.* Статистические оценки энтропии Реньи и Тсаллиса и их использование для проверки гипотез о “чистой случайности” // Известия Национальной академии наук Беларуси. Серия физико-математических наук. 2016. ном. 2. С. 37–47.

О СТОЙКОСТИ СЕМЕЙСТВА АЛГОРИТМОВ NEA/NIA

К.Д. Царегородцев[1], С.А. Давыдов[2],
А.А. Чичаева[3]
[1,2,3]*АО "НПК Криптонит"*
Москва, РОССИЯ
e-mail: [1]k.tsaregorodtsev@kryptonite.ru,
[2]s.davydov@kryptonite.ru,
[3]a.chichaeva@kryptonite.ru

В настоящей работе исследуется стойкость семейства алгоритмов обеспечения конфиденциальности (NEA) и целостности (NIA) совместно с процедурой выработки производных ключей, используемых в сетях подвижной радиотелефонной связи пятого поколения 5G. Хотя в общем виде композиция *Encrypt and MAC*, используемая при комбинации алгоритмов NEA и NIA, не является надежной, добавление уникального счетчика $COUNT$ в вектор инициализации IV, а также использование двух (вычислительно) независимых ключей позволяет свести изучение стойкости исходного семейства к анализу стойкости используемой псевдослучайной функции (для выработки производных ключей) и схем шифрования и выработки имитовставки в стандартных моделях безопасности. Схема указанного сведения представлена в настоящей работе.

Ключевые слова: доказуемая стойкость; конфиденциальность; целостность; 5G; NEA; NIA

1 Введение

Алгоритмы из семейства NEA/NIA (new encryption algorithm, new integrity algorithm, далее алгоритмы

NEA/NIA) используются в сетях подвижной радиотелефонной связи пятого поколения (5G) [1]. На текущий момент спецификации 3GPP [1, 2] позволяют использовать алгоритмы указанного семейства в следующих модификациях: NEA1/NIA1 на основе шифра SNOW 3G, NEA2/NIA2 на основе шифра AES, NEA3/NIA3 на основе шифра ZUC. В Российской Федерации ведется разработка алгоритмов NEA/NIA на основе блочного шифра "Кузнечик" [3].

В рамках фиксированного типа трафика (подробнее см. раздел 2) обработка данных P осуществляется следующим образом:

$$NEA(P) \parallel NIA(P) = ENC(K_e, IV, P) \parallel MAC(K_i, IV \parallel P),$$

где ключи K_e, K_i — некоторые производные от мастер-ключа K_{AMF} (см. рис. 2), вектор инициализации IV зависит от счетчика $COUNT$ (числа соединений для фиксированного ключа) и других параметров трафика (подробное описание работы алгоритмов см. в [1]). Используемая композиция *Encrypt and MAC* в общем виде является нестойкой [6, 8], однако подмешивание счетчика в вектор IV позволяет добиться неповторяемости обрабатываемых сообщений $IV \parallel P$, что помогает свести анализ исходной конструкции к анализу используемых базовых блоков.

В настоящей работе мы изучаем безопасность семейства алгоритмов NEA/NIA в парадигме "доказуемая стойкость". В разделе 2 формально описаны изучаемые алгоритмы, раздел 3 посвящен описанию модели противника; анализ модели и схема доказательства стойкости приведены в разделе 4.

2 Описание алгоритмов NEA/NIA

2.1 Предварительные определения

Определение 1. Схема шифрования $\mathcal{SE}$ — тройка $(\mathbf{KGen}, \mathbf{Enc}, \mathbf{Dec})$: $\mathbf{KGen}$ — вероятностный алгоритм, возвращающий случайно выбранный ключ K (из некоторого пространства ключей $Keys$); алгоритм $\mathbf{Enc}$ ($\mathbf{Dec}$) принимает на вход ключ K, вектор инициализации IV и сообщение m (шифртекст ct) и возвращает шифртекст $ct \leftarrow \mathbf{Enc}_K^{IV}(m)$ (открытый текст $m \leftarrow \mathbf{Dec}_K^{IV}(ct)$). Алгоритмы должны удовлетворять свойству корректности: для любого $K \leftarrow^{\$} \mathbf{KGen}$ и для любых допустимых IV и m выполнено $\mathbf{Dec}_K^{IV}\left(\mathbf{Enc}_K^{IV}(m)\right) = m$.

Определение 2. Схема выработки имитовставки $\mathcal{MA}$ — тройка $(\mathbf{KGen}, \mathbf{Tag}, \mathbf{Vfy})$: $\mathbf{KGen}$ — вероятностный алгоритм, возвращающий случайно выбранный ключ K (из некоторого пространства ключей $Keys$); алгоритм $\mathbf{Tag}$ ($\mathbf{Vfy}$) принимает на вход ключ K, сообщение m (а также имитовставку τ) и возвращает имитовставку $\tau \leftarrow \mathbf{Tag}_K(m)$ (результат проверки имитовставки $b \leftarrow \mathbf{Vfy}_K(m, \tau) \in \{0, 1\}$). Алгоритмы должны удовлетворять свойству корректности: для любого $K \leftarrow^{\$} \mathbf{KGen}$ и для любых допустимых m выполнено $\mathbf{Vfy}_K\left(m, \mathbf{Tag}_K(m)\right) = 1$.

2.2 Описание протокола для фиксированного типа трафика

Пусть заданы некоторые схема шифрования $\mathcal{SE}$ и схема выработки имитовставки $\mathcal{MA}$. Под **алгоритмами NEA/NIA** $\mathcal{AE}$ будем понимать следующую тройку алгоритмов, построенную на основе схем $\mathcal{SE}$ и $\mathcal{MA}$.

– **Алгоритм генерации ключа** $\mathcal{AE}$.**KGen** выбирает пару независимых ключей $K_e \xleftarrow{\$} \mathcal{SE}$.**KGen**, $K_i \xleftarrow{\$} \mathcal{MA}$.**KGen** и возвращает $K \leftarrow (K_e, K_i)$.

– **Алгоритм зашифрования** $\mathcal{AE}.\mathbf{Enc}_K^{IV}(m)$ и **алгоритм расшифрования** $\mathcal{AE}.\mathbf{Dec}_K^{IV}(ct)$: псевдокод алгоритмов приведен на рис. 1.

$\mathcal{AE}.\mathbf{Enc}_K^{IV}(m)$	$\mathcal{AE}.\mathbf{Dec}_K^{IV}(ct)$
$K_e, K_i \leftarrow K$	$K_e, K_i \leftarrow K$
$ctxt \leftarrow \mathcal{SE}.\mathbf{Enc}_{K_e}^{IV}(m)$	$ctxt, \tau \leftarrow ct$
$\sigma \leftarrow \mathcal{MA}.\mathbf{Tag}_{K_i}(IV \,\|\| m)$	$m \leftarrow \mathcal{SE}.\mathbf{Dec}_{K_e}^{IV}(ctxt)$
$ct \leftarrow ctxt \,\|\, \sigma$	$\sigma \leftarrow \mathcal{MA}.\mathbf{Tag}_{K_i}(IV \,\|\| m)$
return ct	**if** $\sigma \neq \tau$
	return $\perp_{MAC}$
	fi
	return m

Рис. 1. Псевдокод алгоритма NEA/NIA (для фиксированного ключа)

Вектор инициализации IV длины 64 бита формируется следующим образом:

$$IV = COUNT \,\|\, BEARER \,\|\, DIR \,\|\, 0^{26} \in \{0,1\}^{64},$$

где $COUNT$ — 32-битовый счетчик соединений (инкрементируется после обработки очередного сообщения),

$BEARER$ — 5-битовый параметр, зависящий от технических характеристик соединения, DIR — однобитовый параметр, задающий направление передачи данных (к абоненту, от абонента). Для упрощения обозначений введем также функцию **Parse**(IV), которая по вектору инициализации IV однозначно (в силу фиксированности длины полей) восстанавливает параметры $par = (COUNT, BEARER, DIR)$.

2.3 Описание протокола для нескольких типов трафика

Алгоритмы NEA/NIA используются для защиты нескольких типов трафика: NAS, RRC, UP [1]. Дерево ключей для разных типов трафика приведено на рис. 2. N3IWF трафик защищается с использованием алгоритма IPSec [1], его анализ выходит за рамки анализа алгоритмов NEA/NIA. Стрелка $K_X \to K_Y$ на дереве означает, что ключ K_Y по-

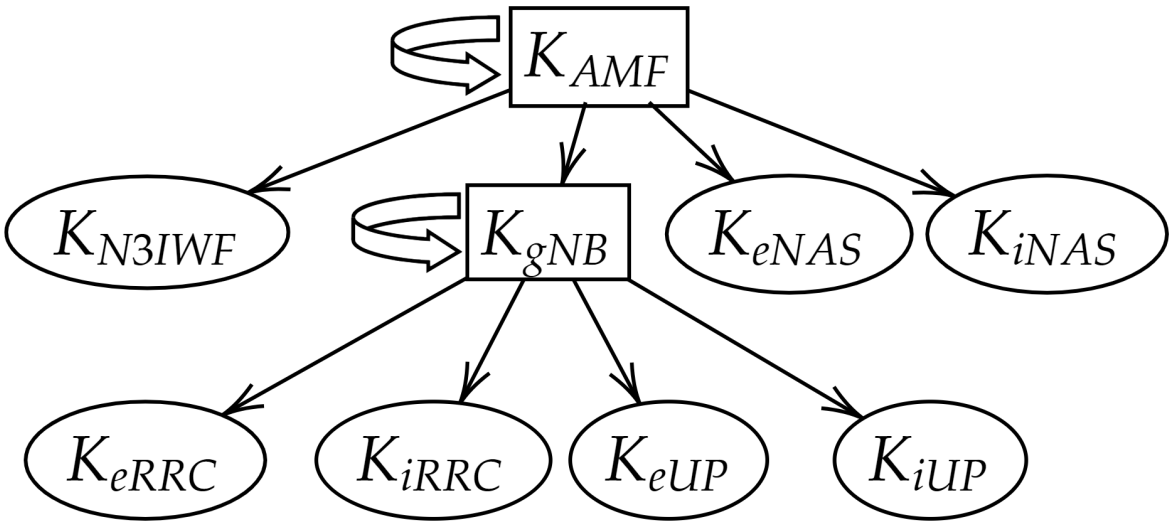

Рис. 2. Ключевое дерево для алгоритма NEA/NIA

лучается как производный от K_X с помощью некоторой

псевдослучайной функции $\mathcal{F}$: $K_Y \leftarrow \mathcal{F}(K_X, S_X)$, где S_X — уникальная константа, зависящая от технических характеристик соединения и типа трафика. В овал обведены ключи, используемые непосредственно для защиты трафика. В прямоугольник обведены ключи, используемые в качестве внутреннего состояния генератора ключей (могут сменяться на производные). Общий вид обработки сообщений алгоритмами NEA/NIA изображен на рис. 3.

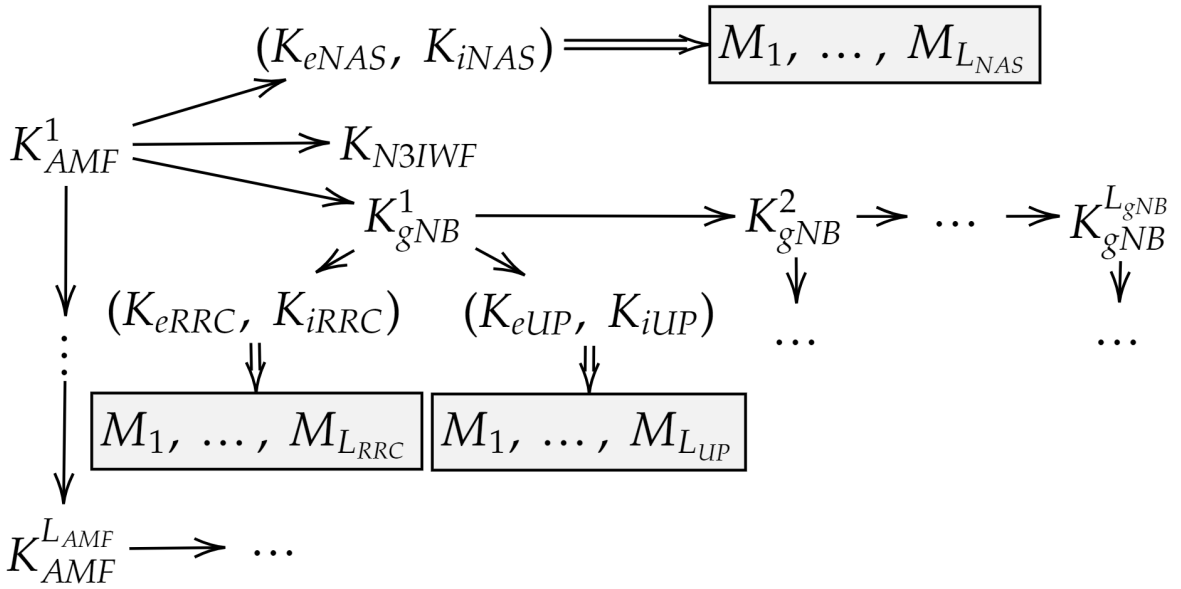

Рис. 3. Развертка ключевого дерева для схемы NEA/NIA

3 Модель противника

Для анализа схемы $\mathcal{AE}$ будем использовать подход “доказуемая стойкость”. В рамках этого подхода возможности противника по взаимодействию с системой формализуются в виде предоставления противнику доступа к различным оракулам, а угрозы — в виде специфических условий, при ко-

торых противник достигает успеха в формальной модели. Так, в рассматриваемой ниже модели IND-CCA3 (см. также [9]) противнику дается доступ к оракулам $\mathcal{O}^b_{\text{enc}}$ (зашифрование сообщений) и $\mathcal{O}^b_{\text{dec}}$ (расшифрование сообщений). Противник может адаптивно подбирать векторы инициализации IV, пары сообщений (m_0, m_1) и шифртексты ct, которые будут подаваться на вход соответствующих оракулов.

Для исключения возможности тривиальных атак вводятся множества $params$ и $sent$. Множество $params$ необходимо для отбраковки запросов с повторяющимися параметрами par; при отсутствии такой проверки противник может тривиально нарушить свойство конфиденциальности, подав дважды на вход оракулу $\mathcal{O}_{\text{enc}}$ сообщения с одинаковым IV и воспользовавшись перекрытием гаммы для нарушения конфиденциальности. В реальных условиях повтор par при зашифровании сообщений исключен за счет вхождения в состав IV монотонно возрастающего счетчика $COUNT$. Множество $sent$ необходимо для исключения возможности "тривиальных" атак, при которых противник сначала получает шифртекст, а затем перенаправляет его оракулу расшифрования. При этом проверяется уникальность пары (par, ct); если противник может навязать шифртекст ct для расшифрования с другими значениями параметров $par' \neq par$, то это считается в рамках модели допустимой атакой.

Определение 3. Преобладание противника $\mathcal{A}$ в модели IND-CCA3 для схемы $\mathcal{AE}$ определяется как:

$$\mathbf{Adv}^{\text{IND-CCA3}}_{\mathcal{AE}}(\mathcal{A})$$

$$= \mathbb{P}\left[\mathbf{Exp}_{\mathcal{AE}}^{\text{IND-CCA3-1}}(\mathcal{A}) \to 1\right] - \mathbb{P}\left[\mathbf{Exp}_{\mathcal{AE}}^{\text{IND-CCA3-0}}(\mathcal{A}) \to 1\right].$$

Псевдокод эксперимента $\mathbf{Exp}_{\mathcal{AE}}^{\text{IND-CCA3-}b}$, $b \in \{0, 1\}$, приведен на рис. 4.

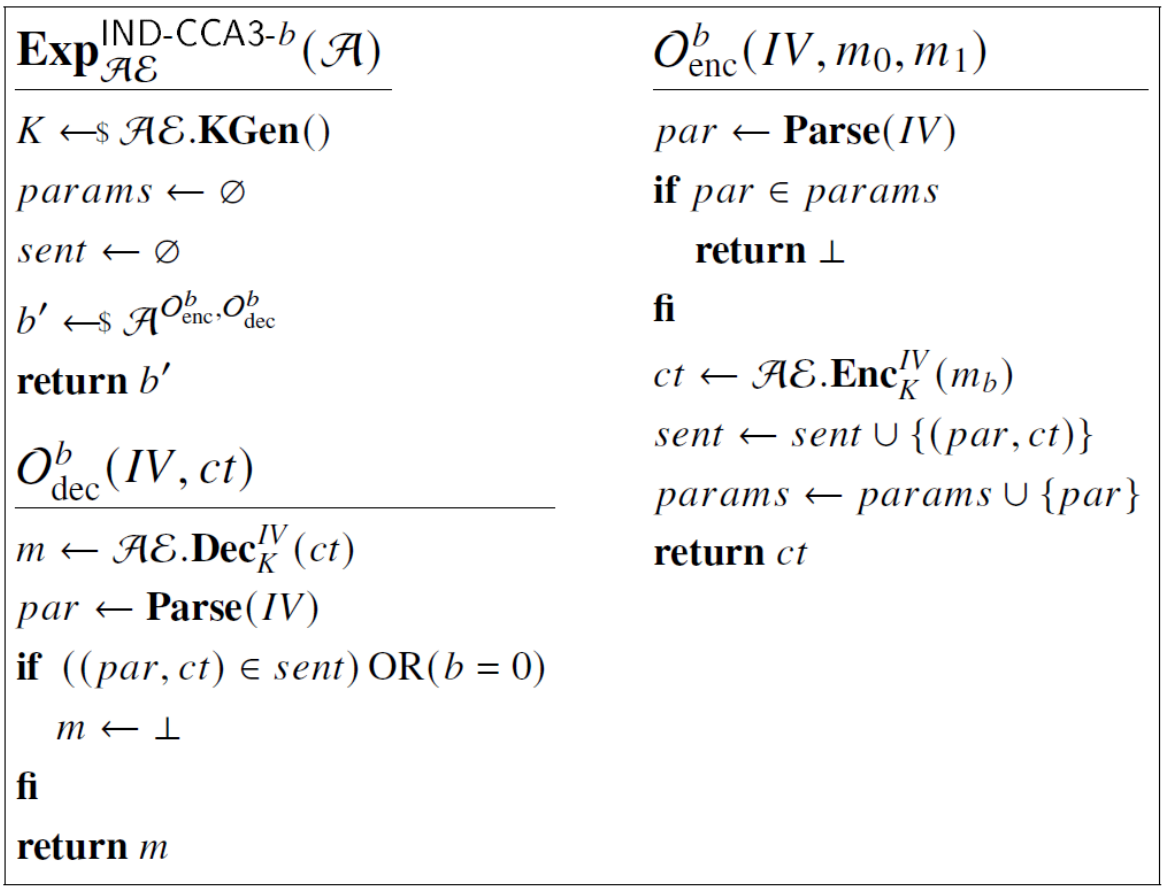

Рис. 4. Модель противника для схемы $\mathcal{AE}$ (для фиксированного ключа)

Перечислим угрозы, которые могут быть формализованы в рамках модели.

– **Нарушение конфиденциальности:** противник, который может извлечь частичную информацию об открытом тексте m_b из шифртекста ct, способен восстановить значение бита b (с помощью ответов оракула $\mathcal{O}_{\text{enc}}^b$).

– **Нарушение целостности:** противник, который может корректно модифицировать шифртекст (с проверкой целостности), способен восстановить значение бита b (с помощью ответов оракула $\mathcal{O}^b_{\mathrm{dec}}$).

– **Криптографическая привязка** параметров par, от которых зависит вектор инициализации IV, к шифртексту: если противник может реализовать ситуацию, в которой ранее сформированный для параметров par шифртекст ct будет принят как корректный шифртекст для параметров $par' \neq par$, то он сможет определить бит b, зафиксированный внутри оракула $\mathcal{O}^b_{\mathrm{dec}}$.

Также приведем некоторые (стандартные) свойства протоколов передачи данных, которые **не рассматриваются** как угрозы безопасности в модели IND-CCA3.

– **Порядок сообщений:** подробнее см., например, [5, 7]. Следующие угрозы не рассматриваются как нарушение свойств безопасности в изучаемой модели: перемешивание сообщений (out-of-order delivery), удаление части сообщений, повторный прием сообщений (replay-атаки).

– **Устойчивость к повторам вектора инициализации (misuse resistance):** подробнее см., например, [4]. Конфиденциальность при повторе IV зависит от свойств схемы $\mathcal{SE}$.

– **Целостность при возможности получать расшифрование частей шифртекста (INT-RUP).** При этом режимы аутентифицированного шифрования вида гаммирование + имитовставка на открытый текст

совместно с уникальным вектором инициализации IV и независимыми ключами являются стойкими в модели INT-RUP (см. [10]).

– **Атаки с использованием побочных каналов** и **атаки, связанные с анализом трафика.**

4 Анализ модели

Можно выделить следующие этапы анализа алгоритмов NEA/NIA (см. рис. 5).

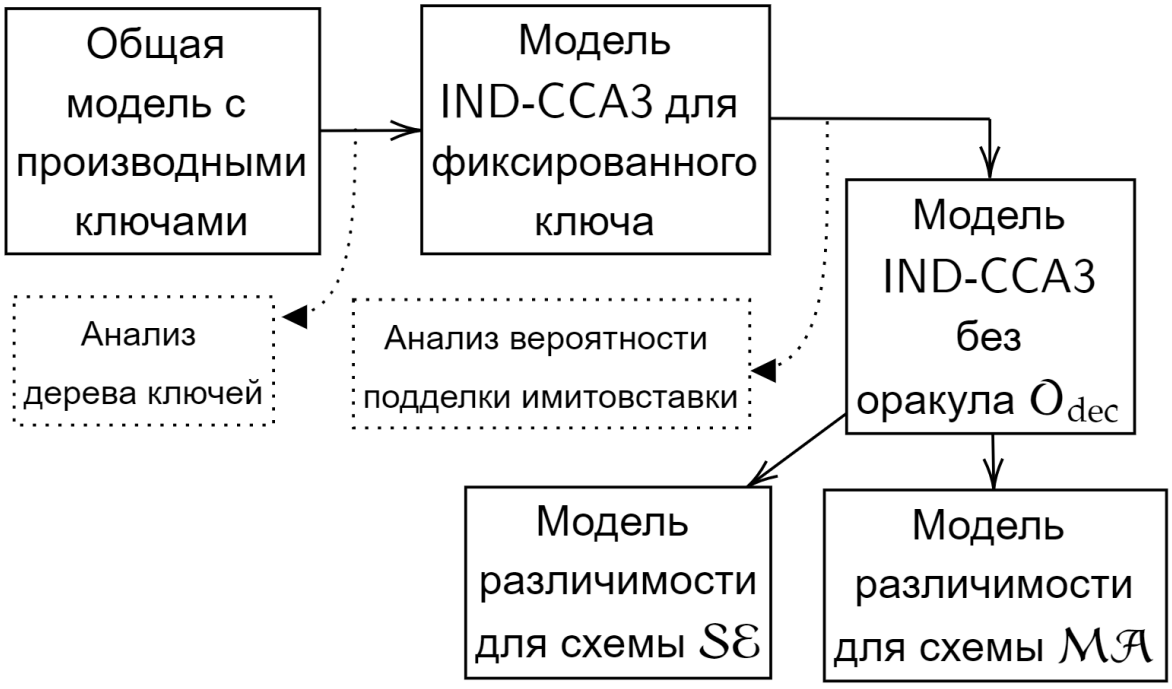

Рис. 5. Анализ алгоритмов NEA/NIA

– Отделить выработку производных ключей от процесса обработки сообщений и проанализировать полученное ключевое дерево в модели неотличимости вырабатываемых ключей от случайных двоичных равновероятных

строк соответствующей длины. Стойкость в указанной модели следует из стойкости используемой псевдослучайной функции $\mathcal{F}$.

– С помощью техники "гибридного аргумента" перейти к рассмотрению фиксированного ключа для конкретного типа трафика (модель IND-CCA3).

– Исключить оракул $\mathcal{O}_{\text{dec}}$ в модели IND-CCA3 из рассмотрения: оракул выдает тривиальные ответы до тех пор, пока противнику не удастся подделать имитовставку на некотором "новом" шифртексте. Вероятность этого события оценивается через стойкость используемой схемы имитовставки $\mathcal{MA}$.

– С помощью техники "гибридного аргумента" разбить полученную модель на две подмодели: (стандартная) модель LOR-CPNA для неразличимости шифртекстов для схемы $\mathcal{SE}$ и модель для неразличимости имитовставок для схемы $\mathcal{MA}$, которая, в свою очередь, сводится к (стандартной) модели PRF неотличимости кода имитовставки от случайной равновероятной двоичной строки.

Библиографические ссылки

1. Security architecture and procedures for 5G system. V18.0.0 [Electronic resourse].
URL: `https://www.etsi.org/deliver/etsi_ts`
(date of access: 30.06.2023).

2. System Architecture Evolution (SAE). Security architecture. V17.4.0 [Electronic resourse].
URL: `https://www.etsi.org/deliver/etsi_ts`
(date of access: 30.06.2023).

3. ГОСТ Р 34.12 – 2018. Информационная технология. Криптографическая защита информации. Блочные шифры [Электронный ресурс].
URL: `https://internet-law.ru/gosts/gost/70509`
(дата обращения: 30.06.2023).

4. Misuse-resistant MGM2 mode / L. Akhmetzyanova [et al.] // International Journal of Open Information Technologies. 2021. Vol. 20, Iss. 1. P. 6–14.

5. *Bellare M., Kohno T., Namprempre C.* Authenticated encryption in SSH: provably fixing the SSH binary packet protocol // Proc. 9th ACM Conf. Comp. Comm. Sec. Ass. Comp. Machinery. 2002. P. 1–11.

6. *Bellare M., Namprempre C.* Authenticated Encryption: Relations among Notions and Analysis of the Generic Composition Paradigm // J. Cryptology. 2000. Vol. 21. P. 469–491.

7. From stateless to stateful: Generic authentication and authenticated encryption constructions with application to TLS / C. Boyd [et al.] // Proc. Crypt. Track RSA Conf. 2016. P. 55–71.

8. *Krawczyk H.* The Order of Encryption and Authentication for Protecting Communications (or: How Secure Is SSL?) // Proc. Adv. Crypt. 2001. P. 310–331.

9. A Characterization of Authenticated-Encryption as a Form of Chosen-Ciphertext Security [Electronic resourse]. URL: https://eprint.iacr.org/2004/272 (date of access: 30.06.2023).

10. О свойстве безопасности RUP для схем аутентифицированного шифрования [Электронный ресурс]. URL: https://www.ruscrypto.ru/resource/archive/rc2023/files/02/_babuyeva_alekseyev_akhmetzyanova_bozhko.pdf (дата обращения: 30.06.2023).

EXTENDING THE FUNCTIONALITY OF BLIND ACCUMULATORS: CONTEXTS

Sergey Agievich[1], Maksim Kazlouski[2]
[1]*Research Institute for Applied Problems of Mathematics and Informatics*
[2]*Belarusian State University*
Minsk, BELARUS
e-mail: [1]agievich@{bsu.by,gmail.com},
[2]maksim.a.kazlouski@gmail.com

Blind accumulators collect private keys of eligible entities in a decentralized manner not getting information about the keys. Once the accumulation is complete, an entity processes the resulting accumulator deriving a public key that refers to the private key previously added by this entity. We extend the blind accumulator scheme with the context functionality so that the derived public key is bound to a specific context and it is hard to associate this key with other public keys of the same entity derived in different contexts. Blind accumulators with contexts are useful in various e-voting scenarios, for example in revoting. We provide an implementation of the extended blind accumulator scheme and justify its security.
Keywords: e-voting; revoting; cryptographic accumulator; blind accumulator; decisional Diffie–Hellman problem

1 Preliminaries

A blind accumulator is a cryptographic container that collects private keys and outputs (derives) the corresponding public keys. A private key is added to the accumulator in a provably correct manner while remaining secret, that is, known only to its owner.

The derived public key is accompanied by a proof that it refers to some of the collected private keys while it is computationally hard to determine which one. With all this, blind accumulators are managed in the decentralized manner.

Blind accumulators are introduced in [1] as a tool for organizing decentralized electronic voting (e-voting). Voters use accumulated private keys to sign ballots, the derived public keys are used to verify signatures. The voter's public key acts as a immutable pseudonym which can be used to prevent double voting or, conversly, allow multiple ballots to be cast with only the last one to be counted.

The last possibility, the so-called revoting, is an important feature of modern e-voting systems. The direct revoting based on blind accumulators have the following drawback: by observing ballots, an adversary can track the change in the opinions of voters (while not violating their anonymity). It is desirable to organize revoting in such a way that it is difficult to relate the original and subsequent ballots of the same voter.

This motivates us to extend the functionality of blind accumulators. In Section 2, we enrich interfaces of the blind accumulator algorithms by adding to some of them a parameter that describes a target context: regular voting, revoting, second round voting, etc. To maintain guarantees that voter's object in different contexts are hard to associate with each other, we introduce an additional security requirement called severance. In Section 3, we propose an implementation of the extended blind accumulator scheme. In Section 4, we discuss the security of the proposed implementation.

2 Contexts

Cryptographic accumulators are special encodings of tuples of objects. We write $\mathbf{a} = [S]$ to denote that an accumulator $\mathbf{a}$ encodes a tuple S. We interpret tuples as ordered multisets bringing standard set notations such as the curly braces, the membership ($\in$) and union ($\cup$) symbols.

A *blind accumulator scheme* introduced in [1] is a tuple of polynomial-time algorithms $\mathsf{BAcc} = (\mathsf{Init}, \mathsf{Add}, \mathsf{PrvAdd}, \mathsf{VfyAdd}, \mathsf{Der}, \mathsf{PrvDer}, \mathsf{VfyDer})$ that are defined as follows.

1. The probabilistic algorithm $\mathsf{Init}\colon 1^l \mapsto \mathbf{a}_0$ takes a security level $l \in \mathbb{N}$ (in the unary form) and outputs an initial accumulator $\mathbf{a}_0 = [\varnothing]$.

   We assume that $\mathbf{a}_0$ implicitly refers to l and public parameters (such as a description of an elliptic curve) and that these parameters implicitly define a set of private keys SKeys and a set of public keys PKeys.

2. The deterministic algorithm $\mathsf{Add}\colon (\mathbf{a}, sk) \mapsto \mathbf{a}'$ takes an accumulator $\mathbf{a} = [S]$ and a private key sk, and outputs an updated accumulator $\mathbf{a}' = [S \cup \{sk\}]$.

   We assume that every accumulator $\mathbf{a}$ that is input to Add is an output of either Init or some previous call to Add. This ensures the *consistency* of $\mathbf{a}$, i.e. that it is constructed as

   $$\mathbf{a} \leftarrow \mathsf{Add}(\ldots(\mathsf{Add}(\mathsf{Add}(\mathbf{a}_0, sk_1), sk_2), \ldots), sk_n),$$
   $$\mathbf{a}_0 \leftarrow \mathsf{Init}(1^l), \quad sk_i \in \mathsf{SKeys},$$

   and therefore is an incrementally built encoding $[S]$ of the multiset $S = \{sk_1, sk_2, \ldots, sk_n\}$.

We also assume that public parameters referenced in the initial accumulator $\mathbf{a}_0$ are passed to all accumulators incrementally built from it.

3. The probabilistic algorithm $\mathsf{PrvAdd}\colon (\mathbf{a}, \mathbf{a}', sk) \mapsto \alpha$ takes accumulators $\mathbf{a}$, $\mathbf{a}'$ and a private key sk, and generates a proof α that $\mathbf{a}' = \mathsf{Add}(\mathbf{a}, sk)$.

4. The deterministic algorithm $\mathsf{VfyAdd}\colon (\mathbf{a}, \mathbf{a}', \alpha) \mapsto b$ takes accumulators $\mathbf{a}$, $\mathbf{a}'$ and a proof α that $\mathbf{a}' = \mathsf{Add}(\mathbf{a}, sk)$ for some private key sk. The algorithm verifies the proof and outputs either $b = 1$ for acceptance or $b = 0$ for rejection.

5. The deterministic algorithm $\mathsf{Der}\colon (\mathbf{a}, sk) \mapsto pk \mid \perp$ takes an accumulator $\mathbf{a}$ and a private key sk, and either derives a public key pk or outputs the error symbol $\perp$.

   We require that for a consistent $\mathbf{a} = [S]$, $\mathsf{Der}(\mathbf{a}, sk) = \perp$ if and only if $sk \notin S$.

6. The probabilistic algorithm $\mathsf{PrvDer}\colon (\mathbf{a}, pk, sk) \mapsto \delta$ takes an accumulator $\mathbf{a}$, a private key sk and a public key pk, and generates a proof δ that $pk = \mathsf{Der}(\mathbf{a}, sk)$.

7. The deterministic algorithm $\mathsf{VfyDer}\colon (\mathbf{a}, pk, \delta) \mapsto b$ takes an accumulator $\mathbf{a}$, a public key pk and a proof δ that $pk = \mathsf{Der}(\mathbf{a}, sk)$ for some private key sk. The algorithm verifies the proof and outputs either $b = 1$ for acceptance or $b = 0$ for rejection.

Further details on the algorithms and additional requirements for them are presented in [1].

To support contexts, we extend the interfaces of the last 3 algorithms. We describe a context with a non-empty binary

word (string) c and use it as an additional input parameter of Der, PrvDer and VfyDer. Denote the resulting extension of BAcc by BAcc1.

The algorithm Der of BAcc1 takes a triple $(\mathbf{a}, sk, c)$ and outputs a public key pk bound to the context c. We require that if $sk \xleftarrow{\$} \mathsf{SKeys}$, $sk \in S$ and $\mathbf{a} = [S]$, then $pk \leftarrow \mathsf{Der}(\mathbf{a}, sk)$ has a fixed distribution D over PKeys regardless of S and c.

Hereinafter we write $r_1, r_2, \ldots \xleftarrow{L} R$ to denote that $r_1, r_2, \ldots$ are chosen independently at random from a set R according to a probability distribution L and denote by \$ the uniform distribution.

The paper [1] defines 4 security requirements for blind accumulators: consistency, soundness, blindness, unlinkability. To reflect the transition from BAcc to BAcc1, the last 3 requirements are modified as follows:

– in the definition of soundness, the algorithms $\mathcal{A}$ and $\mathcal{E}$ take the additional input c that is transferred to VfyDer and Der respectively;

– in the definition of blindness, the algorithms $\mathcal{S}_2$ takes the additional input c that is transferred to Der and PrvDer;

– in the definition of unlinkability, the game G takes the additional input c that is repeated when calling Der.

The consistency, soundness, blindness, and unlinkability security requirements do not guarantee that public key derived in different contexts are hard to associate with each other. To support such guarantees, we introduce an additional requirement called *severance*.

Consider an algorithm $\mathcal{A}$ that takes a consistent accumulator $\mathbf{a} = [S]$ of security level l, different context strings c, c' and public keys pk, pk'. The first public key is derived from $\mathbf{a}$ using $sk \in S$ in the context c. The algorithm $\mathcal{A}$ guesses if the second public key is also derived from $\mathbf{a}$ using $sk \in S$ but in the context c'. The algorithm returns 1 (true) or 0 (false).

Definition 1. A scheme BAcc1 provides *severance* if for any probabilistic polynomial-time algorithm $\mathcal{A}$ described above it holds that

$$\begin{gathered}\mathbf{Adv}(\mathcal{A}) \\ = |\mathbf{P}\left\{\mathcal{A}(\mathbf{a}, c, c', pk, pk') = 1 \colon pk \leftarrow \mathsf{Der}(\mathbf{a}, sk, c), pk' \leftarrow U\right\} \\ -\mathbf{P}\left\{\mathcal{A}(\mathbf{a}, c, c', pk, pk') = 1 \colon pk \leftarrow \mathsf{Der}(\mathbf{a}, sk, c), pk' \stackrel{D}{\leftarrow} V\right\}\Big|, \\ U = \mathsf{Der}(\mathbf{a}, sk, c'), \quad V = \mathsf{PKeys}.\end{gathered}$$

is negligible in l.

3 Implementation

In [1], an implementation of the BAcc scheme, called BAcc-DH, is proposed. We modify BAcc-DH to support the BAcc1 functionality. The resulting implementation is called BAcc1-DH.

In BAcc1-DH, a cyclic group $\mathbb{G}_q$ of large prime order q is used. We write this group additively and denote by $\mathbb{G}_q^*$ the set of nonzero elements of $\mathbb{G}_q$. We also use the ring $\mathbb{Z}_q$ of residues of integers modulo q and the set $\mathbb{Z}_q^*$ of nonzero (invertible) residues. The group $\mathbb{G}_q$ is constructed in the algorithm BAcc1-DH.Init. An input security level l determines the bit length of q. Once $\mathbb{G}_q$ is constructed, the set of private keys SKeys and the set of public

keys PKeys are defined as $\mathbb{Z}_q^*$ and $\mathbb{G}_q^*$ respectively. The initial accumulator $\mathbf{a}_0$ and all subsequent accumulators are words in the alphabet $\mathbb{G}_q^*$. The set of non-empty words in an alphabet Σ is denoted by Σ^+. An empty word is denoted by $\perp$. The notation $(\mathbb{G}_q^*)^+$ is shortened to $\mathbb{G}_q^{*+}$. The notation $\{0,1\}^+ \cup \{\perp\}$ is shortened to $\{0,1\}^*$.

The algorithms Add, PrvAdd and VfyAdd of BAcc-DH are used unchanged in BAcc1-DH. The remaining algorithms are updated, corrections are highlighted in frames in the listings below.

Algorithm BAcc1-DH.Init

Input: 1^l (security level).

Output: $\mathbf{a}_0 \in \mathbb{G}_q^{*+}$ (initial accumulator).

Steps:

1. Construct a group $\mathbb{G}_q$ of prime order q such that $C_1 2^l < q < C_2 2^l$, where C_1, C_2 are some constants.
2. Constr. hash func-s. $H\colon \{0,1\}^* \to \mathbb{Z}_q$, $H_1\colon \{0,1\}^* \to \mathbb{G}_q^*$.
3. $G \leftarrow H_1(\perp)$.
4. $\mathbf{a}_0 \leftarrow G$.
5. Return $\mathbf{a}_0$.

The descriptions of $\mathbb{G}_q$ and G can be interpreted as additional outputs of the algorithm. We allow H to process arbitrary input data assuming they are pre-encoded into a binary word.

Algorithm BAcc1-DH.Der

Input: $\mathbf{a} \in \mathbb{G}_q^{*+}$ (accumulator), $u \in \mathbb{Z}_q^*$ (private key), $c \in \{0,1\}^+$ (context).

Output: $V \in \mathbb{G}_q^*$ (public key).

Steps:

1. Parse $\mathbf{a} = G_0 G_1 \dots G_n$.
2. Find $i \in \{1, 2, \dots, n\}$ such that $uG_i = G_0$. If such i does not exist, return $\perp$.
3. $\boxed{C \leftarrow H_1(c).}$
4. $\boxed{\text{Return } uC.}$

Algorithm BAcc1-DH.PrvDer

Input: $\mathbf{a} \in \mathbb{G}_q^{*+}$ (accumulator), $u \in \mathbb{Z}_q^*$ (private key), $V \in \mathbb{G}_q^*$ (public key), $\boxed{c \in \{0,1\}^+ \text{ (context)}}$.
Output: $\delta \in \mathbb{Z}_q^+ \times \mathbb{Z}_q^+$ (proof).
Steps:

1. Parse $\mathbf{a} = G_0 G_1 \dots G_n$.
2. Find $i \in \{1, 2, \dots, n\}$ such that $uG_i = G_0$. If such i does not exist, return $(0, 0)$.
3. $\boxed{C \leftarrow H_1(c).}$
4. For $j = 1, 2, \dots, n$, $j \neq i$:
   (a) $h_j, s_j \xleftarrow{\$} \mathbb{Z}_q$;
   (b) $\boxed{\mathbf{r}_j \leftarrow s_j(G_j G_0) + h_j(C\,V).}$
5. $k_i \xleftarrow{\$} \mathbb{Z}_q$.
6. $\mathbf{r}_i \leftarrow k_i(G_i G_0)$.
7. $h_i \leftarrow \left(H(\mathbf{a}, \mathbf{r}_1 \mathbf{r}_2 \dots \mathbf{r}_n, V) - \sum_{j \neq i} h_j\right) \bmod q$.
8. $s_i \leftarrow (k_i - u h_i) \bmod q$.
9. $\delta \leftarrow (h_1 h_2 \dots h_n, s_1 s_2 \dots s_n)$.
10. Return δ.

Algorithm BAcc1-DH.VfyDer

Input: $\mathbf{a} \in \mathbb{G}_q^{*+}$ (accumulator), $V \in \mathbb{G}_q^*$ (public key), $\delta \in \mathbb{Z}_q^+ \times \mathbb{Z}_q^+$ (proof), $\boxed{c \in \{0,1\}^+ \text{ (context)}}$.
Steps:

1. Parse $\delta = (\mathbf{h}, \mathbf{s})$. If $|\mathbf{h}| \neq |\mathbf{s}|$ or $|\mathbf{a}| \neq |\mathbf{h}| + 1$, return 0.
2. Parse $\mathbf{a} = G_0 G_1 \dots G_n$, $\mathbf{h} = h_1 h_2 \dots h_n$ and $\mathbf{s} = s_1 s_2 \dots s_n$.
3. $\boxed{C \leftarrow H_1(c).}$
4. For $j = 1, 2, \dots, n$:
   (a) $\boxed{\mathbf{r}_j \leftarrow s_j(G_j G_0) + h_j(C\,V).}$
5. If $H(\mathbf{a}, \mathbf{r}_1 \mathbf{r}_2 \dots \mathbf{r}_n, V) \not\equiv h_1 + h_2 + \dots + h_n \pmod{q}$, return 0.
6. Return 1.

4 Security

In this section, we justify the security of BAcc1-DH examining 5 security requirements stated in [1] and Section 2.

The security definitions in [1] allow runtime environments to be managed. We use this to replace the hash functions H and H_1 with a random oracle (see [2]) and permit this oracle to be programmed. The random oracle responds to a fresh input μ with a random output h and repeats a previous output when an input is repeated. Programming the oracle consists in assigning a given random output h to a given input μ. Collisions can potentially occur when programming: the input μ may already be associated with an output $h' \neq h$. Fortunately, we avoid collisions.

To justify the unlinkability and severance, we use the well-known DDH (Decisional Diffie–Hellman) problem [3]. The

DDH problem is specified with respect to a cyclic group $\mathbb{G}_q$ with a generator G and consists in deciding for a given tuple (G, uG, vG, wG), $u, v, w \in \mathbb{Z}_q^*$, if $w \equiv uv \pmod{q}$. The algorithm $\mathcal{B}$ that solves DDH guesses if this is indeed the case and outputs either 1 (true) or 0 (false).

Definition 2. Let $\mathcal{G}$ be an algorithm that constructs a cyclic group $\mathbb{G}_q$ and its generator G given an input 1^l. The DDH problem is *hard with respect to* $\mathcal{G}$ if for any polynomial-time algorithm $\mathcal{B}$ operating on $\mathbb{G}_q$ and G constructed by calling $\mathcal{G}(1^l)$ it holds that the advantage

$$\mathbf{Adv}(\mathcal{B}) = \Big|\mathsf{P}\left\{\mathcal{B}(G, uG, vG, uvG) = 1 \colon u, v \xleftarrow{\$} \mathbb{Z}_q^*\right\} - \mathsf{P}\left\{\mathcal{B}(G, uG, vG, wG) = 1 \colon u, v, w \xleftarrow{\$} \mathbb{Z}_q^*\right\}\Big|$$

is negligible in l. The probabilities here are over a random tape of $\mathcal{B}$ and $\mathcal{G}$ and over a random choice of u, v and w.

Theorem. *The* BAcc1-DH *implementation of the* BAcc1 *scheme satisfies the requirements of consistency, soundness, blindness, unlinkability and severance in the programmable random oracle model provided that DDH is hard with respect to* BAcc1-DH.Init.

References

1. *Agievich S.* Blind accumulators for e-voting // Central European Conference on Cryptology (CECC'22): Proceedings / Mathematical Institute, Slovak Academy of Sciences; editorial board: K. Nemoga (editor-in-chief), R. Ploszek, P. Zajac. Bratislava: Mathematical Institute, Slovak Academy of Sciences, 2022. P. 15–18.

2. *Bellare M., Rogaway P.* Random oracles are practical: a paradigm for designing efficient protocols // Proc. 1st ACM Conf. Comp. Comm. Security. 1993. P. 62–73.

3. *Boneh D.* The decision Diffie-Hellman problem // LNCS. 1998. Vol. 1423. P. 48–63.

Index

Научное издание

ТЕОРЕТИЧЕСКАЯ И ПРИКЛАДНАЯ КРИПТОГРАФИЯ

Материалы
II Международной научной конференции

Минск, 19–20 октября 2023 г.

В авторской редакции

Ответственный за выпуск *В. А. Волошко*

Подписано в печать 18.09.2023. Формат 60×84/16. Бумага офсетная.
Печать цифровая. Усл. печ. л. 17,21. Уч.-изд. л. 10,99.
Тираж экз. Заказ

Белорусский государственный университет.
Свидетельство о государственной регистрации издателя, изготовителя,
распространителя печатных изданий № 1/270 от 03.04.2014.
Пр. Независимости, 4, 220030, Минск.

Отпечатано с оригинал-макета заказчика