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

ТЕОРЕТИЧЕСКАЯ И ПРИКЛАДНАЯ КРИПТОГРАФИЯ

Материалы международной
научной конференции

Минск, 20–21 октября 2020 г.

Минск
БГУ
2020

УДК 004.056.557(06)
ББК 32.811.4я431
Т33

Т33 **Теоретическая** и прикладная криптография : материалы междунар. науч. конф., Минск, 20–21 окт. 2020 г. / Белорус. гос. ун-т ; редкол.: Ю. С. Харин (гл. ред.) [и др.]. – Минск : БГУ, 2020. – 131 с.
ISBN 978-985-566-924-2.

Освещены 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, стеганография, криптография на основе sponge-функций, разделение секрета, нейронные сети в криптологии, доказательства с нулевым разглашением, блокчейн-системы, эффективная реализация криптографических примитивов, средства криптографической защиты информации, инфраструктура открытых ключей и электронный документооборот, массовая аутентификация, ID-карты и другие направления криптологии.

УДК 004.056.557(06)
ББК 32.811.4я431

ISBN 978-985-566-924-2

Содержание

К 20-летию
НИИ прикладных проблем
математики и информатики

ПРЕДИСЛОВИЕ

Международная научная конференция “Теоретическая и прикладная криптография”, организованная Белорусским государственным университетом и Научно-исследовательским институтом прикладных проблем математики и информатики (НИИ ППМИ БГУ) 20–21 октября 2020 года, посвящена актуальным проблемам современной криптографии и приурочена к двадцатилетнему юбилею НИИ ППМИ БГУ – ведущей в Беларуси научной организации в области криптологии.

Материалы конференции содержат 19 статей. Темы статей отвечают следующим направлениям: математические основы криптографии; булевы функции в криптографии; вероятностно-статистические методы криптологии; криптографические генераторы случайных и псевдослучайных чисел; оценка надёжности криптографических алгоритмов и протоколов; постквантовая криптография; стеганография; криптография на основе sponge-функций; разделение секрета; нейронные сети в криптологии; доказательства с нулевым разглашением; блокчейн-системы; эффективная реализация криптографических примитивов; средства криптографической защиты информации; инфраструктура открытых ключей и электронный документооборот; массовая аутентификация; ID-карты.

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

ВЫПУСК ПРОМЕЖУТОЧНЫХ ИМИТОВСТАВОК ПРИ АУТЕНТИФИЦИРОВАННОМ ШИФРОВАНИИ

С.В. Агиевич
НИИ прикладных проблем математики и информатики
Белорусский государственный университет
Минск, БЕЛАРУСЬ
e-mail: agievich@bsu.by

Выпуск промежуточных имитовставок в процессе аутентифицированного шифрования является удобным механизмом текущего контроля при обработке данных большого объема. В работе рассматриваются режимы аутентифицированного шифрования CHE и DWP из новой редакции СТБ 34.101.31. Обосновывается сохранение гарантий стойкости режимов при разрешении на выпуск промежуточных имитовставок.
Ключевые слова: аутентифицированное шифрование; имитовставка; оракул; неотличимость; преобладание

1 Введение

Аутентифицированное шифрование определяется алгоритмами установки защиты Wrap и снятия защиты Unwrap. Алгоритм Wrap принимает на вход открытый текст X, ассоциированные данные I, секретный ключ K и синхропосылку (служебные волатильные данные) S. Алгоритм возвращает шифртекст Y и имитовставку T. Шифртекст Y является результатом зашифрования X, имитовставка T — это контрольная характеристика пары (X, I), которая позволяет провести ее аутентификацию, т. е. проверку целостности и подлинности. Алгоритм Unwrap принимает на вход набор (Y, I, T, K, S) и возвращает либо открытый текст X, либо символ $\perp$ — признак ошибки аутентификации.

При приеме данных получатель расшифровывает последовательные фрагменты Y, но не может использовать результаты расшифрования вплоть до завершения приема, когда наконец открытый текст X будет определен полностью и можно будет провести аутентификацию (X, I). Такая ситуация недопустима, если речь идет об обработке данных большого объема, например, видеопотоков.

Одно из решений здесь — выпуск промежуточных имитовставок. Они вычисляются в процессе выполнения Wrap по мере обработки частей X. Точнее, если X' — префикс X, то соответствующие промежуточные шифртекст и имитовставки — это $(Y', T') = \mathrm{Wrap}(X', I, K, S)$. Пара (Y', T') проверяется с помощью алгоритма Unwrap. При успешной проверке определяется X'. Эта часть X может быть использована немедленно (например, отображена в случае видеоданных), не дожидаясь получения всего шифртекста. После определения X' проверяется следующая промежуточная имитовставка T'', определяется следующий префикс X''

(он является расширением X'), и так далее, до тех пор пока открытый текст X не будет определен полностью или не будет обнаружена ошибка аутентификации.

В современной криптографии системы аутентифицированного шифрования в основном строятся на основе блочных шифров или sponge-функций. При этом системы часто называют режимами, подразумевая способ использования шифра / функции. Выпуск промежуточных имитовставок является стандартной практикой для систем на основе sponge-функций, но редко разрешается в системах на основе блочных шифров. Например, для режима GCM [4], возможно самого распространенного на сегодняшний день, выпуск промежуточных имитовставок неприемлем: имитовставки вычисляются с повторяющимися синхропосылками, а повтор синхропосылок катастрофически снижает стойкость GCM.

Далее в работе мы обсуждаем режимы DWP и CHE, описанные в [3] и основанные на схеме аутентификации сообщений из [2]. Первый режим был введен в СТБ 34.101.31-2011 [1], второй — стандартизируется в новой редакции СТБ в настоящее время. В разделе 4 мы показываем, что выпуск промежуточных имитовставок в режимах DWP и CHE является безопасным. Предварительно в разделе 2 мы описываем режимы, а в разделе 3 вводим модель безопасности.

2 Режимы DWP и CHE

Пусть E — блочный шифр с длиной блока n и множеством ключей $\mathcal{K}$. Это мультимножество, составленное из подстановок $E_K \in \mathrm{Perm}(n)$, которые индексируются секретными ключами $K \in \mathcal{K}$. Здесь $\mathrm{Perm}(n)$ — множество всех подстановок на $\{0,1\}^n$. Элементы $\{0,1\}^n$ называются блоками. Обозначим через $N = 2^n$ их число.

Мы также будем обозначать через $\{0,1\}^*$ множество двоичных слов конечной длины. Длина слова $u \in \{0,1\}^*$ обозначается через $|u|$. Если u, v — слова одинаковой длины, то $u \oplus v$ есть их поразрядная сумма по модулю 2 (XOR).

Будем интерпретировать блоки из $\{0,1\}^n$ как элементы конечного поля $\mathbb{F}$ порядка N. Пусть используется обычное соответствие между $\mathbb{F}$ и $\{0,1\}^n$, когда $\oplus$ задает сложение в $\mathbb{F}$. Пусть

$$\mathtt{next}(\lambda) = a * \lambda \oplus b, \quad \lambda \in \mathbb{F},$$

где a — примитивный элемент $\mathbb{F}$, b — ненулевой элемент. Преобразование $\mathtt{next}$ является подстановкой на $\mathbb{F} \sim \{0,1\}^n$, причем эта подстановка является произведением независимых циклов длин 1 и $N-1$.

Алгоритмы режима CHE определяются ниже. В этих алгоритмах $X \in \{0,1\}^*$, $I \in \{0,1\}^*$, $K \in \mathcal{K}$, $S \in \{0,1\}^n$, $Y \in \{0,1\}^{|X|}$, $T \in \{0,1\}^n$. Используется фиксированное ненулевое слово $T_0 \in \{0,1\}^n$. Операция $\overset{n}{\leftarrow}$ означает разбиение двоичного слова на n-битовые блоки, причем разбиению предшествует дополнение слова до границы блока нулями. Обратная операция $\underset{m}{\leftarrow}$ означает сборку слова из нескольких блоков, причем после сборки выполняется обрезка слова (справа) до m битов.

Алгоритм Wrap	**Алгоритм** Unwrap
Вход: X, I, K, S.	**Вход**: Y, I, K, S, T.
Выход: Y, T.	**Выход**: X или $\perp$ (ошибка).
Шаги:	**Шаги**:
1. $H \leftarrow E_K(S)$, $C \leftarrow H$, $T \leftarrow T_0$.	1. $H \leftarrow E_K(S)$, $C \leftarrow H$, $T' \leftarrow T_0$.
2. $(I_1, \ldots, I_{r'}) \xleftarrow{n} I$.	2. $(I_1, \ldots, I_{r'}) \xleftarrow{n} I$.
3. Для $i = 1, 2, \ldots, r'$:	3. Для $i = 1, 2, \ldots, r'$:
(a) $T \leftarrow (T \oplus I_i) * H$.	(a) $T' \leftarrow (T' \oplus I_i) * H$.
4. $(X_1, \ldots, X_r) \xleftarrow{n} X$.	4. $(Y_1, \ldots, Y_r) \xleftarrow{n} Y$.
5. Для $i = 1, 2, \ldots, r$:	5. Для $i = 1, 2, \ldots, r$:
(a) $C \leftarrow \texttt{next}(C)$;	(a) $T' \leftarrow (T' \oplus Y_i) * H$;
(b) $Y_i \leftarrow X_i \oplus E_K(C)$;	(b) $C \leftarrow \texttt{next}(C)$;
(c) $T \leftarrow (T \oplus Y_i) * H$.	(c) $X_i \leftarrow Y_i \oplus E_K(C)$.
6. $Y \underset{\lvert X\rvert}{\leftarrow} (Y_1, \ldots, Y_r)$.	6. $X \underset{\lvert Y\rvert}{\leftarrow} (X_1, \ldots, X_r)$.
7. Кодировать $\lvert I\rvert$ и $\lvert X\rvert$ словом $W \in \{0,1\}^n$.	7. Кодировать $\lvert I\rvert$ и $\lvert X\rvert$ словом $W \in \{0,1\}^n$.
8. $T \leftarrow (T \oplus W) * H$.	8. $T' \leftarrow (T' \oplus W) * H$.
9. $T \leftarrow E_K(T)$.	9. $T' \leftarrow E_K(T')$.
10. Возвратить (Y, T).	10. Возвратить X если $T = T'$ или $\perp$ в противном случае.

Предполагается, что на шаге 7 каждого из алгоритмов различные пары $(|I|, |X|)$ дают различные слова W, и слово W является нулевым тогда и только тогда, когда $|I| = |X| = 0$.

Режим DWP отличается от CHE тем, что `next` является полноцикловой подстановкой. Кроме этого, меняется шаг 1. Он принимает вид:

$$C \leftarrow E_K(S), H \leftarrow E_K(C), T' \leftarrow T_0.$$

Режим DWP лучше совместим со стандартными реализациями режима шифрования CTR2 (описание можно найти в [3]), позволяя легко дополнить шифрование аутентификацией. Режим CHE более эффективен: он требует на один вызов E_K меньше.

3 Модель безопасности

Для обоснования надежности режима $\mathrm{Mode} \in \{\mathrm{CHE}, \mathrm{DWP}\}$ мы используем стандартный подход (см. напр. [5]), описываемый ниже.

1. Противник (вероятностный алгоритм) A получает доступ к оракулу аутентифицированного шифрования O. Противник отправляет оракулу запросы (X, I, S) и получает ответы (Y, T). Противник соблюдает один из двух

контрактов: синхропосылки в запросах либо случайные независимые равновероятные, либо произвольные неповторяющиеся. Противнику разрешается указывать в запросах пустые X и I.

2. Оракул O может быть реализован двумя способами. В первой (штатной) реализации оракул реализует аутентифицированное шифрование режима Mode, в котором используется подстановка E_K, выбранная случайно равновероятно из E. Эта реализация обозначается через $\mathrm{Mode}[E_K]$. Во второй (идеальной) реализации при ответе на каждый новый запрос (X, I, S) оракул выбирает (Y, T) случайно равновероятно из $\{0,1\}^{|X|} \times \{0,1\}^n$. Идеальная реализация обозначается через ρ.

3. Противник посылает оракулу O запросы, получает и анализирует ответы. Задача противника — отличить штатную реализацию от идеальной. Противник возвращает 1 (штатная реализация) или 0 (идеальная). Пусть A^O — ответ A.

4. Возможности A по распознаванию реализаций характеризует преобладание

$$\mathbf{Adv}^{\mathtt{priv}}_{\mathrm{Mode}[E]}(A) = \left|\mathsf{P}\left\{A^{\mathrm{Mode}[E_K]} = 1\right\} - \mathsf{P}\left\{A^{\rho} = 1\right\}\right|.$$

   Здесь вероятности определяются случайным выбором K, а также случайной лентами, которые A и ρ используют в своей работе. Аббревиатура `priv` является устоявшейся.

   Если преобладание $\mathbf{Adv}^{\mathtt{priv}}_{\mathrm{Mode}[E]}(A)$ мало для любого противника A с разумными ограничениями на его ресурсы, то режим Mode на основе E признается стойким.

Выполним стандартное упрощение, заменив E_K, случайного представителя шифра E, на π, случайную подстановку из $\mathrm{Perm}(n)$. Эта замена превращает $\mathbf{Adv}^{\mathtt{priv}}_{\mathrm{Mode}[E]}(A)$ в преобладание

$$\mathbf{Adv}^{\mathtt{priv}}_{\mathrm{Mode}[\mathrm{Perm}(n)]}(A) = \left|\mathsf{P}\left\{A^{\mathrm{Mode}[\pi]} = 1\right\} - \mathsf{P}\left\{A^{\rho} = 1\right\}\right|.$$

Замена мотивирована общим представлением о том, что подстановки надежного шифра E трудноотличимы от случайных подстановок. Замена сопровождается штрафом (еще одним преобладанием), который характеризует трудноотличимость случайных представителей E и $\mathrm{Perm}(n)$. Этот штраф носит формальный характер — он оценивается лишь косвенно в рамках общей оценки стойкости E. Для надежного шифра E штраф считается малым. Мы не вводим штраф для простоты.

Для заданных неотрицательных q, r и положительного d нас интересует оценки сверху для преобладания $\mathbf{Adv}^{\mathtt{priv}}_{\mathrm{Mode}[\mathrm{Perm}(n)]}(A)$, в котором фигурирует противник со следующим ограничениями: разрешается выполнить q запросов к оракулу, общее число блоков X в этих запросах не должно превосходить r, суммарное число блоков в каждой отдельной паре (X, I) должно быть меньше d. Учитываются, в том числе, последние, возможно неполные блоки X и I.

Искомые оценки для преобладания получены в [3]. Они имеют вид

$$\mathbf{Adv}^{\mathtt{priv}}_{\mathrm{Mode}[\mathrm{Perm}(n)]}(A) \le \frac{(r+q)(r+q-1)}{2N} + \alpha - \beta + \alpha\beta,$$

где $\alpha = \alpha(q, r, d)$, $\beta = \beta(q, r)$. Выражения для α и β (довольно громоздкие) можно найти в [3].

4 Стойкость при выпуске имитовставок

Разрешение на выпуск промежуточных имитовставок требует уточнения модели безопасности. Теперь противник дополнительно к регулярным запросам (X, I, S) может делать *вложенные* запросы (X', I, S), в которых X' является префиксом X. В запрос (X', I, S) может быть вложен другой запрос или (X', I, S) может быть вложен в запрос (X'', I, S), в свою очередь вложенный в (X, I, S).

Штатная реализация оракула определяется как и прежде. Идеальная реализация ρ корректируется: ответ $(Y', T') = \rho(X', I, S)$ вкладывается в ответ $(Y, T) = \rho(X, I, S)$ в том смысле, что Y' является префиксом Y. Как и прежде, T' и T выбираются случайно равновероятно независимо, а Y либо является случайным расширением случайного Y' из предыдущего ответа, либо, наоборот, Y' получен в результате укорачивания случайного Y из предыдущего ответа. Оракул распознает вложения и не выполняет бесполезные вычисления, повторно используя результаты обработки одного запроса при обработке другого. В частности, вложенные запросы не изменяют величины r — общего числа блоков открытых текстов X. Однако, вложенные запросы учитываются в q — общем числе запросов.

Теорема. *Оценки теорем 2 и 4 из [3] для* $\mathbf{Adv}^{\mathtt{priv}}_{Mode[\mathrm{Perm}(n)]}(A)$ *остаются справедливыми, если противник кроме регулярных запросов* (X, I, S) *может делать вложенные запросы* (X', I, S) *с выпуском промежуточных имитовставок* T'.

Доказательство. Доказательства теорем незначительно корректируются. Сохраняются обозначения, построения и общий ход рассуждений.

В контексте доказательств, вложенный запрос (X', I, S) может быть интерпретирован как запрос с пустым открытым текстом. Действительно, X' может быть обработан неявно: выходной шифртекст Y' является префиксом шифртекста Y для регулярного запроса (X, I, S). Однако, промежуточная имитовставка T' должна быть вычислена явно. Имитовставка определяется как $T' = \pi(Z')$, где Z' является результатом полиномиального хэширования:

$$Z' = f_{(Y', I)}(H).$$

Здесь $H = \pi(S)$ (в режиме CHE) или $H = \pi^2(S)$ (в DWP).

Если Y'' — это другой префикс Y и $Z'' = f_{(Y'', I)}(H)$, то

$$\mathsf{P}\left\{Z' = Z''\right\} = \mathsf{P}\left\{(f_{(Y', I)} - f_{(Y'', I)})(H)\right\} \le \frac{d}{N}.$$

Таким образом, оценка сверху вероятности коллизии $Z_i = Z_j$ сохраняется. Оценки вероятностей всех других коллизий, всех событий и, таким образом, итоговые оценки преобладаний также сохраняются. □

Библиографические ссылки

[1] СТБ 34.101.31-2011. Информационные технологии. Защита информации. Криптографические алгоритмы шифрования и контроля целостности. Стандарт Республики Беларусь. Мн.: Госстандарт, 2011.

[2] Agievich, S. EHE: nonce misuse-resistant message authentication. Прикладная дискретная математика. 39 (2018), pp. 33–41. Avail. at: `https://eprint.iacr.org/2017/231`.

[3] Agievich, S. The CTR mode with encrypted nonces and its extension to AE. Cryptology ePrint Archive, Report 2020/331, 2020. Avail. at: `https://eprint.iacr.org/2020/331`. An extended abstract of the paper published in Preproceedings of the 8th Workshop on Current Trends in Cryptology (CTCrypt-2019, Svetlogorsk, Russia, June 4–7, 2019), 2019, pp. 199—215.

[4] McGrew, D.A., Viega, J. The security and performance of the Galois/Counter Mode (GCM) of operation. In: Progress in Cryptology — INDOCRYPT 2004. Ed. by A. Canteaut and K. Viswanathan. Vol. 3348. Lecture Notes in Computer Science. Berlin, Heidelberg: Springer, 2005, pp. 343–355.

[5] Rogaway, P. Evaluation of Some Blockcipher Modes of Operation. Evaluation carried out for the Cryptography Research and Evaluation Committees (CRYPTREC) for the Government of Japan. University of California, Davis, 2011. Avail. at: `url:http://www.cs.ucdavis.edu/~rogaway/papers/modes.pdf`.

СТОЙКОСТЬ ПАРОЛЬНЫХ СИСТЕМ АУТЕНТИФИКАЦИИ В СОЦИАЛЬНЫХ СЕТЯХ

М.Н. Бобов
Белорусский государственный университет информатики и радиоэлектроники
Минск, БЕЛАРУСЬ
e-mail: bobov-mn@agat.by

В статье исследуется стойкость парольных систем аутентификации в социальных сетях. Получен критерий стойкости к атаке «день рождения», рекомендуемый к использованию в парольных системах аутентификации, используемых в больших распределённых сетях.
Ключевые слова: аутентификация; социальная сеть; парольная система; атака «день рождения»

В настоящее время широкое распространение получили распределённые информационные сети, созданные для обеспечения потребностей широкого круга пользователей и имеющие условное наименование «социальные сети». Каждый пользователь для получения доступа к такой сети на первом этапе проходит процедуру регистрации, в процессе которой сообщает системе своё учётное имя и пароль, а также другие учётные персональные данные. В дальнейшем, при обращении к сети для получения её услуг пользователь вводит свои учётное имя и пароль и при их совпадении с именем и паролем, введённым при регистрации, получает доступ сети.

Являясь средствами защиты каналов доступа к телекоммуникационным системам, механизмы аутентификации должны обладать рядом специфических качеств, обеспечивающих их стойкость к взлому, который может происходить путём подбора пароля, компрометации пароля или кражи файла паролей [1]. Вероятность подбора пароля зависит в основном от двух параметров: длины пароля и объёма алфавита и, если пароль выбирается случайно и равновероятно, то для её оценки используются формулы, широко применяемые для парольных механизмов аутентификации [3]:

а) вероятность подбора пароля с первой попытки

$$\mathrm{P}_{\mathrm{П}_1} = \frac{1}{A^S}, \text{ где } A \text{ – объём алфавита, } S \text{ – длина пароля.}$$

б) вероятность подбора пароля с i-ой попытки

$$\mathrm{P}_{\mathrm{П}_i} = \frac{1}{A^S + 1 - i}$$

в) вероятность подбора пароля за k попыток

$$\mathrm{P}_{\mathrm{П}_k} = \frac{k}{A^S}$$

г) вероятность подбора пароля в период его безопасного времени действия

$\mathrm{P}_{T_\text{Б}} = \dfrac{3600 T_\text{Б}}{A^S t_\text{П}}$, где $T_\text{Б}$ – безопасное время действия, $t_\text{П}$ – время набора пароля.

Вместе с тем, широко известные современные социальные сети объединяют огромное количество пользователей и поэтому оценку стойкости используемых в них парольных систем аутентификации к атакам подбора пароля, компрометации пароля и кражи файла паролей недостаточно. В данном случае, парольные системы аутентификации необходимо оценивать на стойкость к атакам «день рождения». Атака «дней рождения» — используемое в криптоанализе название для метода взлома шифров или поиска коллизий хеш-функций на основе парадокса дней рождения [4]. Парадокс дней рождения — положение, утверждающее, что если дана группа из 23 или более человек, то вероятность того, что хотя бы у двух из них дни рождения (число и месяц) совпадут, превышает 50 %. Для группы из 60 или более человек, вероятность совпадения дней рождения хотя бы у двух её членов составляет более 99 %, хотя 100 % она достигает, только когда в группе не менее 367 человек (с учётом високосных лет).

Определим вид формального выражения для расчёта вероятности совпадения хотя бы двух паролей размерности n в группе из m пользователей. Рассчитаем сначала, какова вероятность $\overline{p}(m)$ того, что в группе из m пользователей все их пароли будут различными. Если $N > m$ ($N = A^n$), то в силу принципа Дирихле вероятность равна нулю. Если же $N \leq m$, то будем рассуждать следующим образом. Возьмём наугад одного пользователя из группы и запомним его пароль. Затем возьмём наугад второго пользователя, при этом вероятность того, что его пароль не совпадёт с паролем первого пользователя, равна $1-1/N$. Затем возьмём третьего пользователя, при этом вероятность того, что его пароль не совпадёт с паролями первых двух, равна $1 - 2/N$. Рассуждая по аналогии, мы дойдём до последнего пользователя, для которого вероятность несовпадения его пароля со всеми предыдущими будет равна $1-(m-1)/N$. Перемножая все эти вероятности, получаем вероятность того, что все пароли в группе будут различными:

$$\begin{aligned} \overline{p}(m) &= 1 \cdot \left(1 - \frac{1}{N}\right)\left(1 - \frac{2}{N}\right) \cdots \left(1 - \frac{m-1}{N}\right) = \\ &= \frac{N(N-1)\cdots(N-m+1)}{N^m} = \frac{N!}{(N-m)!N^m}. \end{aligned} \tag{1}$$

Тогда вероятность того, что, по крайней мере, один пользователь имеет тот же пароль, что и любой другой из группы m, равна:

$$P(m) = 1 - \frac{N!}{(N-m)!N^m} \tag{2}$$

Воспользуемся формулой Стирлинга для приближенного вычисления значения

факториала $n! \sim \sqrt{2\pi n}\left(\frac{n}{e}\right)^n$ для расчета полученной функции:

$$P(m) = 1 - \frac{N!}{N^m}\frac{1}{(N-m)!} \sim 1 - \frac{\sqrt{2\pi N}\left(\frac{N}{e}\right)^N}{N^m * \sqrt{2\pi\,(N-m)}\left(\frac{N-m}{e}\right)^{(N-m)}} =$$
$$= 1 - \sqrt{\frac{N}{N-m}}\cdot\frac{1}{e^m}\cdot\left(\frac{N}{N-m}\right)^{(N-m)}$$

Таким образом, имеем:

$$P\,(m) \sim 1 - \sqrt{\frac{N}{N-m}}\cdot\frac{1}{e^m}\cdot\left(\frac{N}{N-m}\right)^{(N-m)} \tag{3}$$

Ниже на рисунках 1–3 приведены графики вероятности появления одинаковых паролей у двух пользователей из предположения, что пароли выбираются случайно и равновероятно. Расчет выполнен в программе Mathematica для следующих исходных условий:

количество знаков в алфавите N – 32, 42,57;

длина пароля n – 6,7,8;

количество пользователей m – от 1 до $1,7 \cdot 10^7$

По отношению к атаке «день рождения» сформулируем следующий критерий стойкости парольной системы аутентификации. Парольная система аутентификации считается стойкой, если величина вероятности совпадения двух назначаемых в ней паролей меньше 0,5, т.е.

$$P(m) < 0,5. \tag{4}$$

Другими словами, парольная система аутентификации считается не стойкой, если величина вероятности совпадения двух назначаемых в ней паролей $P(m) \geq 0,5$.

Данные о количестве пользователей, соответствующих принятому критерию, на рисунках 1-3 отмечены вертикальными линиями и приведены в таблице 1.

Таблица 1

№ п/п	Размер алфавита	$P(m) = 0,5$			$P(m) = 0,9$		
		n			n		
		6	7	8	6	7	8
1	36	$3,7 \cdot 10^4$	$4,0 \cdot 10^5$	$1,8 \cdot 10^6$	$1,1 \cdot 10^5$	$6,0 \cdot 10^5$	$3,5 \cdot 10^6$
2	42	$9,5 \cdot 10^4$	$6,0 \cdot 10^5$	$3,5 \cdot 10^6$	$1,8 \cdot 10^5$	$1,2 \cdot 10^6$	$7,2 \cdot 10^6$
3	57	$2,2 \cdot 10^5$	$1,6 \cdot 10^6$	$1,3 \cdot 10^7$	$4,0 \cdot 10^5$	$3,0 \cdot 10^6$	$\sim 10^9$

Тогда для указанных параметров системы с числом пользователей, расположенных слева от прямых, являются не стойкими.

В качестве примера оценим стойкость наиболее распространённых социальных сетей, данные по которым приводятся в исследовании компании «WebCanape» от

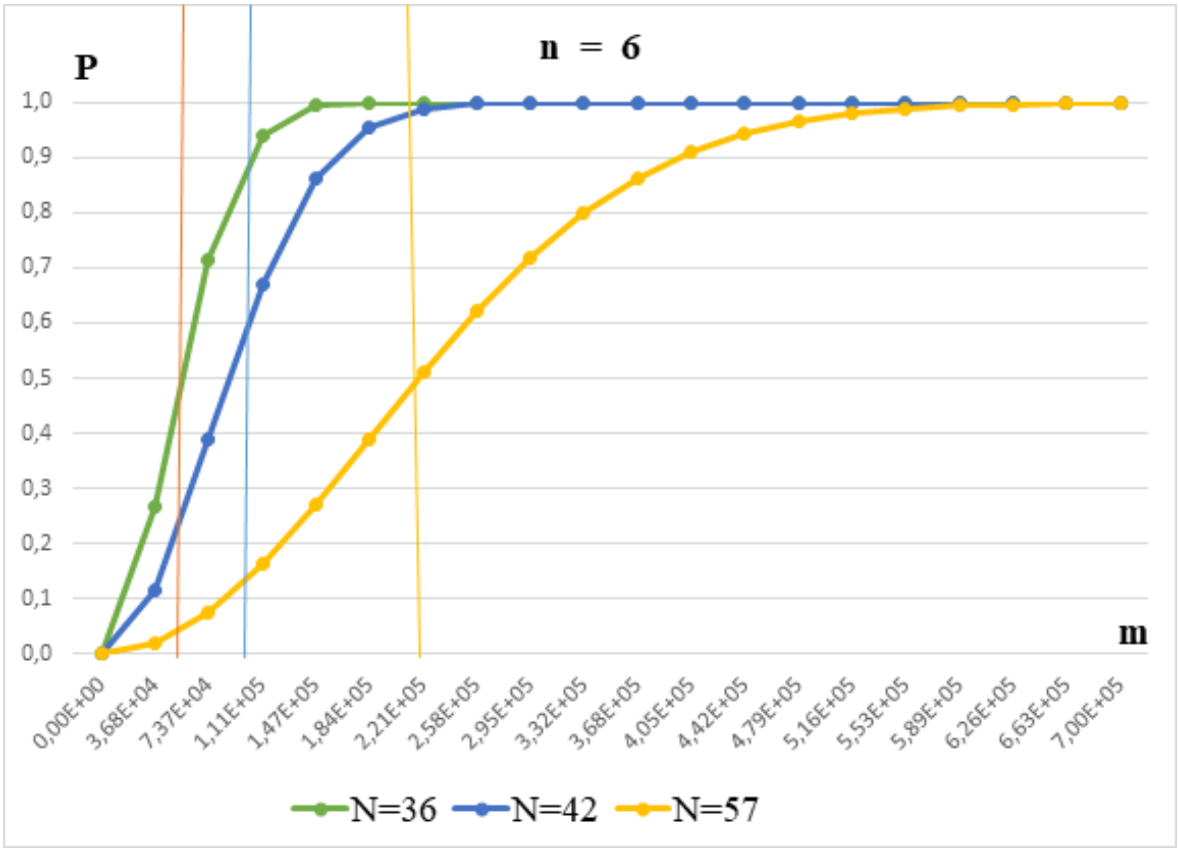


Рис. 1. Графики вероятности $P(m)$ при длине пароля $n = 6$

Таблица 2

№ п/п	Наименование сети	Количество пользователей
1	Facebook	2,27млрд. $= 2,27 \cdot 10^9$
2	Youtube	1,9 млрд. $= 1,9 \cdot 10^9$
3	Instagram	1,0 млрд. $= 1,0 \cdot 10^9$
4	Ozone	536 млн. $= 5,31 \cdot 10^8$
5	Twitter	326 млн. $= 3,26 \cdot 10^8$
6	Linkedn	303 млн. $= 3,03 \cdot 10^8$

января 2019 года [5]. Так, количество учётных записей пользователей наиболее известных социальных сетей составляет (Таблица 2):

При регистрации указанные сети предъявляют различные требования к парольным системам аутентификации, параметры которых приведены в таблице 3.

Сравнительные данные по существующему и допустимому числу пользователей в анализируемых социальных сетях, использующих парольные системы аутентификации с указанными при регистрации параметрами, в соответствии с критерием стойкости к атаке «день рождения» приведены в таблице 4.

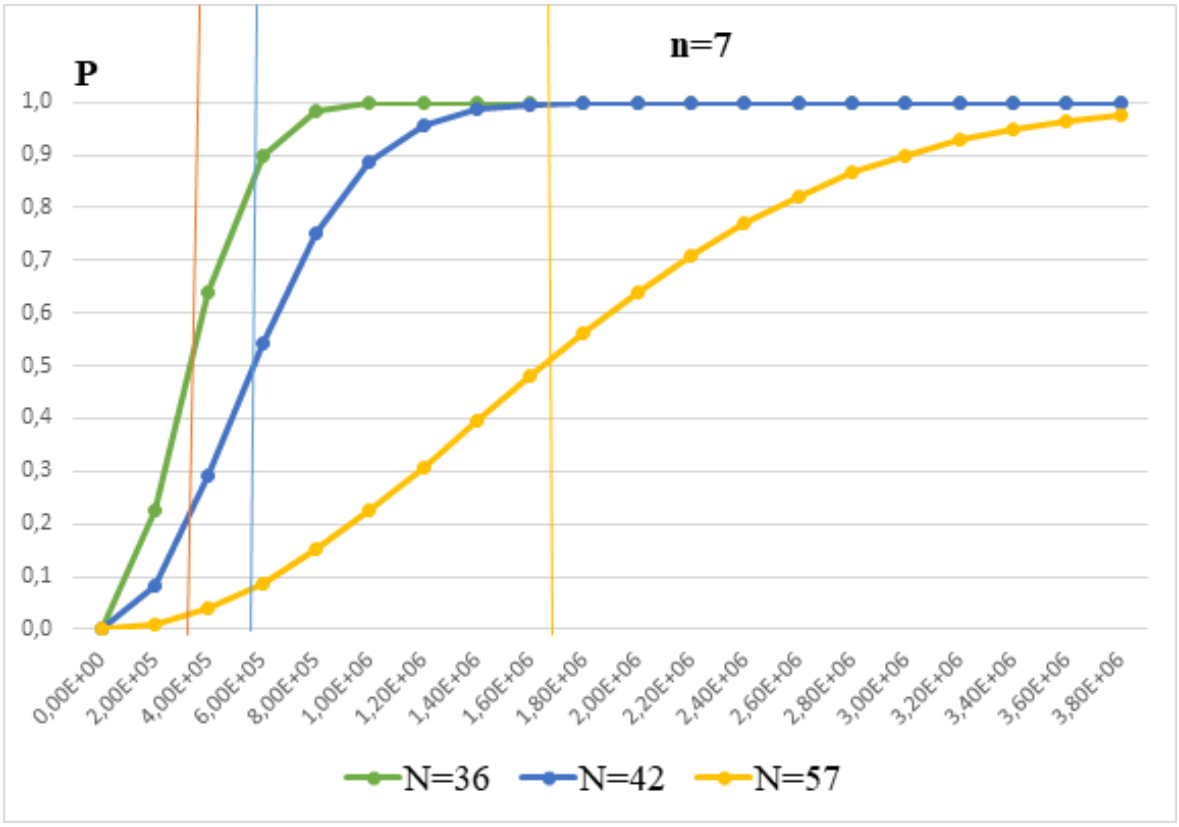


Рис. 2. Графики вероятности $P(m)$ при длине пароля $n = 7$

Таблица 3

№ п/п	Наименование сети	Количество пользователей	Алфавит A	Длина пароля n	$\mathrm{P}_{\mathrm{П}_1}$
1	Facebook	$2,27 \cdot 10^9$	42	6	$5,5 \cdot 10^9$
2	Youtube	$1,9 \cdot 10^9$	42	8	$9,6 \cdot 10^{12}$
3	Instagram	$1,0 \cdot 10^9$	62	15	$4,8 \cdot 10^{28}$
4	Ozone	$5,31 \cdot 10^8$	36	6	$2,1 \cdot 10^9$
5	Twitter	$3,26 \cdot 10^8$	36	6	$2,1 \cdot 10^9$
6	Linkedn	$3,03 \cdot 10^8$	36	6	$2,1 \cdot 10^9$

Как следует из данных, приведенных в таблице 4, из анализируемых социальных сетей только сеть Инстаграм является стойкой по отношению к атаке «день рождения». Определим теперь аналитическое выражение для практического рас-

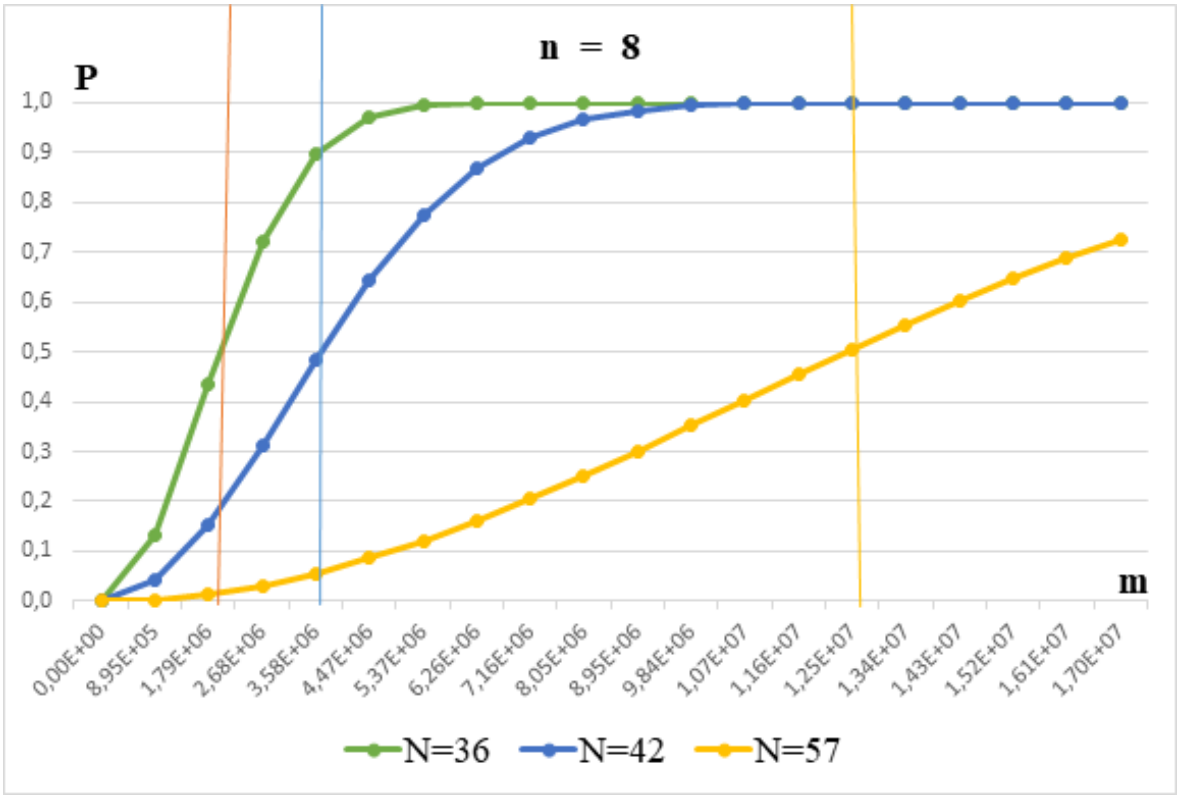


Рис. 3. Графики вероятности $P(m)$ при длине пароля $n = 8$

Таблица 4

№ п/п	Наименование сети	Количество пользователей	Допустимое количество пользователей по критерию $P(m) = 0,5$	$P_{П_1}$	
1	Facebook	$2,27 \cdot 10^9$	$9,5 \cdot 10^4$	$5,5 \cdot 10^9$	-
2	Youtube	$1,9 \cdot 10^9$	$3,6 \cdot 10^6$	$9,6 \cdot 10^{12}$	-
3	Instagram	$1,0 \cdot 10^9$	$\sim 10^{12}$	$4,8 \cdot 10^{28}$	Соотв.
4	Ozone	$5,31 \cdot 10^8$	$3,7 \cdot 10^4$	$2,1 \cdot 10^9$	-
5	Twitter	$3,26 \cdot 10^8$	$3,7 \cdot 10^4$	$2,1 \cdot 10^9$	-
6	Linkedn	$3,03 \cdot 10^8$	$3,7 \cdot 10^4$	$2,1 \cdot 10^9$	-

чёта стойкости сети к атаке «день рождения». Из выражения (1) получим [2]:

$$P(m) = 1 - 1 \cdot \left(1 - \frac{1}{N}\right)\left(1 - \frac{2}{N}\right) \cdots \left(1 - \frac{m-1}{N}\right) = 1 - \prod_{i=1}^{m-1}\left(1 - \frac{i}{N}\right) \approx$$

$$\approx 1 - \prod_{i=1}^{m-1} e^{-\frac{i}{N}} = 1 - e^{-\frac{m(m-1)}{N}}$$

Согласно критерия (4) имеем:

$$1 - e^{-\frac{m(m-1)}{N}} = \frac{1}{2}, \quad 2 = e^{\frac{m(m-1)}{2N}}, \quad \ln 2 = \frac{m(m-1)}{2N}.$$

Принимая $m(m-1) \approx m^2$, получим

$$m = \sqrt{2N \ln 2} = 1,17\sqrt{N} = \sqrt{A^n} = A^{\frac{n}{2}}.$$

Таким образом, парольные системы аутентификации, используемые в больших распределённых сетях, в которых число пользователей m сравнимо или больше возможного количества выбираемых ими для доступа к услугам аутентификаторов N, должны оцениваться на стойкость к атаке «день рождения» в соответствии с критерием

$$m = A^{\frac{n}{2}}.$$

Библиографические ссылки

[1] Бобов М.Н., Конопелько В.К. *Основы аутентификации в телекоммуникационных системах: Учеб. пособие* – Мн.: БГУИР, 2008. – 130 с.

[2] Мао, Венбо *Современная криптография: теория и практика* / Венбо Мао // Пер с англ. – М.: Издательский дом «Вильямс», 2005. – 768с.

[3] Смит, Ричард Э. *Аутентификация: от паролей до открытых ключей* / Ричард Э. Смит. – М.: Издательский дом “Вильямс”, 2002. – 432 с.

[4] Харин Ю.С., Берник В.И., Матвеев Г.В., Агиевич С.В. *Математические и компьютерные основы криптологии.* – Мн.: Новое знание, 2003. – 382с.

[5] *Вся статистика интернета на 2019 год – в мире и в России*. https://www.web-canape.ru/business/vsya-statistika-interneta-na-2019-god-v-mire-i-v-rossii/.

ОБ АППРОКСИМАЦИИ СЛУЧАЙНЫХ БУЛЕВЫХ ФУНКЦИЙ ПОРОГОВЫМИ ФУНКЦИЯМИ

В.А. Волошко
НИИ прикладных проблем математики и информатики
Белорусский государственный университет
Минск, БЕЛАРУСЬ
e-mail: valeravoloshko@yandex.ru

В статье исследуются аппроксимирующие свойства класса пороговых булевых функций от n переменных. Показано, что при $n \to \infty$ функция расстояния от случайной булевой функции до элементов некоторого кода сходится к гауссовому случайному полю с корреляционным ядром, зависящим от метрических свойств кода. Разработан алгоритм построения аппроксимации функцией из кода случайной булевой функции. Исследованы метрические свойства кода, образованного пороговыми функциями, и энтропийные свойства соответствующего корреляционного ядра.
Ключевые слова: случайная булева функция; пороговая функция; аппроксимация; гауссовское случайное поле; корреляционное ядро

1 Пороговые булевы функции

Для удобства будем рассматривать булевы функции вида $f : \{\pm 1\}^n \to \{\pm 1\}$ (их множество обозначим Φ_n) и центрированное расстояние Хэмминга между ними (скалярное произведение):

$$\Delta(f, f') = \langle f, f' \rangle = \sum_{x \in \{\pm 1\}^n} f(x) f'(x) \in [-2^n, 2^n]. \tag{1}$$

Максимальное значение $\Delta = 2^n$ означает, что функции совпадают, минимальное значение $\Delta = -2^n$ отвечает наиболее удаленным (взаимно инвертированным) функциям.

Зафиксируем некоторый базис действительнозначых функций на булевом кубе $\Psi = \{\psi_i\}_{i=1}^m$, $\psi_i : \{\pm 1\} \to \mathbb{R}$, и рассмотрим соответствующий класс пороговых булевых функций:

$$\Pi_\Psi = \{f_w\}_w, \ f_w(x) = \operatorname{sign} \langle w, \Psi(x) \rangle, \ x \in \{\pm 1\}^n, \tag{2}$$

где

$$w \in \mathbb{R}^m \setminus \{0\}, \ \Psi(x) = (\psi_i(x))_{i=1}^m \in \mathbb{R}^m.$$

Вектор w называется вектором весов и неоднозначно определяет булеву функцию вида (2). В классическом случае базис $\Psi = \Lambda = \{\lambda_i\}$ состоит из $m = n+1$ функций:

$$\lambda_i(x) = x_i, \ i = 1, 2, \ldots, n, \ \lambda_{n+1}(x) \equiv 1. \tag{3}$$

Очевидно, умножение вектора весов w на положительную константу не меняет функцию f_w в (2), а умножение w на отрицательную константу инвертирует функцию f_w. Поэтому в дальнейшем будем в основном рассматривать вектора весов w, лежащие на единичной сфере $\mathbb{S}^{m-1} \subset \mathbb{R}^m$. Множество пороговых функций (2) определяется частями, на которые евклидово пространство весовых векторов $\{w\} = \mathbb{R}^m$ (и сфера $\mathbb{S}^{m-1}$) разбивается 2^n гиперплоскостями $\langle \Psi(x), w\rangle = 0$, $x \in \{\pm 1\}^n$. Каждой такой части отвечает одна пороговая функция. В случае общего положения этих 2^n гиперплоскостей число частей соответствующего разбиения установлено формулой Шлефли [5], которая служит верхней оценкой мощности множества пороговых функций:

$$\#\Pi_\Psi \leq 2\sum_{i=0}^{m-1}\binom{2^n-1}{i} = 2^{mn(1+o(1))}, \tag{4}$$

где соответствующая асимптотика имеет место при $m, n \to \infty$ и $\log m = o(n)$. В случае стандартного линейного базиса (3) эта асимптотика оказывается точной [1]:

$$\#\Pi_\Lambda = 2^{n^2(1+o(1))},\ n \to \infty. \tag{5}$$

Данная статья посвящена двум вопросам: алгоритму построения и свойствам аппроксимации случайной булевой функции в классе пороговых функций (2). Для начала кратко рассмотрим эти вопросы при аппроксимации в классе функций из некоторого кода $C \subset \Phi_n$ общего вида.

2 Общие свойства кодовых расстояний до случайной булевой функции

Лемма 1. *Пусть $f \in \Phi_n$ — равномерно распределенная случайная булева функция и $d \in \mathbb{N}$ фиксировано. Тогда при $n \to \infty$ вектор расстояний* (1) *между f и некоторыми d функциями $c_1, \ldots, c_d \in \Phi_n$ имеет асимптотически нормальное распределение:*

$$\delta(f, c) = 2^{-n/2}(\Delta(f, c_i))_{i=1}^d \sim \mathcal{N}_d(0_d, 2^{-n}(\Delta(c_i, c_j))_{i,j=1}^d) \tag{6}$$

при сходимости соответствующей асимптотической матрицы ковариаций.

Таким образом, случайный процесс $\delta : C \to \mathbb{R}$, образованный нормированными расстояниями (1) между чисто случайной булевой функцией $f \in \Phi_n$ и элементами кода C:

$$\delta(c) = 2^{-n/2}\Delta(f, c),\ c \in C, \tag{7}$$

является центрированным асимптотически нормальным и имеет асимптотическое корреляционное ядро:

$$\mathcal{K}(c, c') = 2^{-n}\Delta(c, c'),\ c, c' \in C, \tag{8}$$

с единичной диагональю $\mathcal{K}(c,c) \equiv 1$, зависящее лишь от метрических свойств кода C (набора попарных расстояний).

Описанные вполне элементарные свойства позволяют в первом приближении получить некоторые известные результаты о предельном распределении кодового расстояния $\max_{c\in C} \delta(c)$ от кода C до чисто случайной булевой функции. В частности, для кода Рида-Маллера первого порядка $C = \mathrm{RM}_n^1$, состоящего из 2^{n+1} аффинных функций, процесс (7) состоит из 2^n некоррелированных случайных величин и их "минус-копий". Распределение соответствующего кодового расстояния $\max_{c\in C} \delta(c)$ аппроксимируется распределением случайной величины $\max_{1\le i\le 2^n} |\xi_i|$, где $\xi_i \sim \mathcal{N}(0,1)$ независимы. Для кода, состоящего только из линейных функций (аффинных с нулевым свободным членом), случайный процесс $\delta(\cdot)$ не содержит минус-копий, и распределение кодового расстояния аппроксимируется распределением случайной величины $\max_{1\le i\le 2^n} \xi_i$. В обоих случаях, используя теорию экстремумов случайных величин [2], приходим к так называемым дважды экспоненциальным пределам.

3 Идея алгоритма аппроксимации случайной булевой функции

Как правило, задача нахождения наилучшего приближения булевой функции $f \in \Phi_n$ в классе функций из некоторого кода C, затруднена большой величиной используемых на практике кодов. Покажем, как для построения алгоритма аппроксимации можно использовать тот факт, что на вход подается булева функция, имеющая свойства чисто случайной. Пусть нам уже известны некоторые $d = \#S$ значений $\delta(S) = (\delta(s))_{s\in S\subset C}$ максимизируемого процесса (7). Тогда, принимая во внимание асимптотическую нормальность указанного процесса, мы можем построить гауссовскую линейную регрессию (прогноз) остальных значений:

$$\hat{\delta}(c|S) ::= \mathsf{E}_{\delta\sim\mathcal{N}}\{\delta(c)|\delta(S)\} = \sum_{s\in S} \mathbf{a}_S(s,c)\delta(s). \tag{9}$$

Далее, чтобы каждый раз не делать оговорки, будем считать процесс (7) в точности гауссовским с корреляционным ядром (8). Если матрица ковариаций $\mathcal{K}(S) ::= \mathcal{K}(S,S)$ вектора известных значений $\delta(S)$ невырождена, вектор коэффициентов прогнозирования (9) допускает следующее явное выражение:

$$|\mathbf{a}_S(S,c)\rangle = \mathcal{K}(S)^{-1}\,|\mathcal{K}(S,c)\rangle\,, \tag{10}$$

и (9) перепишется в виде:

$$\hat{\delta}(c|S) = \langle\delta(S)|\,\mathcal{K}(S)^{-1}\,|\mathcal{K}(S,c)\rangle\,. \tag{11}$$

При этом в силу свойств нормального закона условное корреляционное ядро $\mathcal{K}(t,t'|S)$, $t,t' \in T$, на $T = C \setminus S$ не зависит от значений $\delta(S)$:

$$\mathcal{K}(t,t'|S) ::= \mathsf{Cov}(\delta(t),\delta(t')|\delta(S)) = \mathcal{K}(t,t') - \langle\mathcal{K}(t,S)|\,\mathcal{K}(S)^{-1}\,|\mathcal{K}(t',S)\rangle\,. \tag{12}$$

Как видим, для построения прогноза в (11) необходимо обратить матрицу размера $d \times d$, что имеет вычислительную сложность $\mathcal{O}(d^3)$ (наилучший известный алгоритм Копперсмита-Винограда [4] и его вариации имеют сложность $\mathcal{O}(d^{2.37})$, которая достигается только при очень больших d). Однако обращаемая матрица $\mathcal{K}(S)$ симметрична, положительно определена и при итеративном расширении множества S (добавлении элемента $s \in C \setminus S$) входит в качестве подматрицы в $\mathcal{K}(S \cup \{s\})$. В таком случае для вычислительной оптимизации применим процесс ортогонализации Грама-Шмидта, который предполагает хранение $\mathcal{O}(d^2)$ вспомогательных коэффициентов на шаге d: обратной матрицы Грама $\mathbf{Q}^d ::= \mathcal{K}(S)^{-1} \in \mathbb{R}^{d \times d}$ и ее разложения Холецкого $\mathbf{Q}^d = R'R$, где $R = (\mathbf{R}_{i,j})_{i,j=1}^d$ — нижнетреугольная матрица. Ее коэффициенты определены следующими соотношениями:

$$\xi_i ::= \sum_{j=1}^{i} \mathbf{R}_{i,j}\delta_j, \ i = 1, \ldots, d. \tag{13}$$

Здесь $\{\xi_i\}_{i=1}^d$ представляет собой ортогонализованную ($\mathsf{Cov}(\xi_i, \xi_j) = \mathbb{1}\{i = j\}$) последовательность случайных величин $\{\delta_i ::= \delta(s_i)\}_{i=1}^d$, $S = \{s_i\}_{i=1}^d$. Кроме того, на каждом новом шаге вычисляется d-вектор коэффициентов прогнозирования:

$$\left\langle \mathbf{f}^d \right| ::= \langle \delta(S) | \, \mathcal{K}(S)^{-1}, \tag{14}$$

который может быть рекурсивно построен по $\mathbf{f}^{d-1}$ за $\mathcal{O}(d)$ операций:

$$\mathbf{f}^d = \mathbf{f}^{d-1} + \xi_d \mathbf{R}_d, \ \mathbf{f}_i^d = \mathbf{f}_i^{d-1} + \mathbf{R}_{d,i} \sum_{j=1}^{d} \mathbf{R}_{d,j}\delta_j, \ i = 1, \ldots, d, \tag{15}$$

где полагаем $\mathbf{f}_j^i \equiv 0$ при $j > i$. Формула (11) приводится к простому виду:

$$\hat{\delta}(c|S) = \left\langle \mathbf{f}^d | \mathcal{K}(S, c) \right\rangle = \sum_{i=1}^{d} \mathbf{f}_i^d \mathcal{K}(c, s_i). \tag{16}$$

Рекуррентные формулы ортогонализации требуют $\mathcal{O}(d^2)$ операций на d-м шаге (всюду $\mathcal{K}_{i,j} ::= \mathcal{K}(s_i, s_j)$):

$$\mathbf{R}_{d,d} = \left(1 - \sum_{i=1}^{d-1} \left(\sum_{j=1}^{i} \mathbf{R}_{i,j}\mathcal{K}_{d,j} \right)^2 \right)^{-1/2}, \tag{17}$$

$$\mathbf{R}_{d,j} = -\mathbf{R}_{d,d} \sum_{j'=1}^{d-1} \mathcal{K}_{d,j'} \mathbf{Q}_{j,j'}^{d-1}, \ j = 1, \ldots, d-1, \tag{18}$$

$$\mathbf{Q}_{j,j'}^d = \mathbf{Q}_{j,j'}^{d-1} + |\mathbf{R}_d\rangle \langle \mathbf{R}_d|, \ \mathbf{Q}_{j,j'}^d = \mathbf{Q}_{j,j'}^{d-1} + \mathbf{R}_{d,j}\mathbf{R}_{d,j'}, \ j, j' = 1, \ldots, d, \tag{19}$$

где считаем $\mathbf{Q}_{j,j'}^{d-1} \equiv 0$ при $\max\{j, j'\} = d$. Начальные значения при $d = 1$ задаются так:

$$\mathbf{Q}^1 = 1, \ \mathbf{R}_{1,1} = 1, \ \mathbf{f}^1 = \delta(s_1). \tag{20}$$

Предлагается следующая **схема алгоритма максимизации** функции δ на коде C:

1: Некоторым способом выбираем начальный элемент $s_1 \in C$, инициализируем величины (20), полагаем $S = \{s_1\}$, $d = 1$, $\delta_* = \delta(s_1)$, $c_* = s_1$, переходим к шагу 2;

2: Если $d > 1$, вычисляем величины $\mathbf{Q}^d$, $\mathbf{R}_d$ и $\mathbf{f}^d$ по формулам (15), (17)-(19), переходим к шагу 3;

3: Максимизируем прогноз (16) среди $c \in T = C \setminus S$ и полагаем

$$s_{d+1} = \arg\max_{c \in T} \hat{\delta}(c|S),$$

если выполнено некоторое **условие остановки** — выходим из программы и возвращаем пару (c_*, δ_*), иначе вычисляем $\delta_{d+1} = \delta(s_{d+1})$, в случае $\delta_{d+1} > \delta_*$ обновляем значения $\delta_* = \delta_{d+1}$ и $c_* = s_{d+1}$, полагаем $S = S \cup \{s_{d+1}\}$, $d = d + 1$ и переходим к шагу 2.

Замечание 1. Описанный алгоритм имеет смысл только при наличии статистических зависимостей между случайными величинами $\delta(c)$, $c \in C$, другими словами, когда корреляционное ядро $\mathcal{K}$ существенно отличается от единичной матрицы. В частности, как было отмечено ранее, это условие **не выполняется** для кода Рида-Маллера первого порядка $C = \mathrm{RM}_n^1$.

Покажем, что для кода $C = \Pi_\Psi$, образованного пороговыми булевыми функциями (2), корреляционное ядро $\mathcal{K}$ существенно отличается от единичной матрицы при довольно общих ограничениях на базис Ψ.

4 Сферическая структура множества пороговых функций

Рассмотрим множество весовых векторов $\{w\} = \mathbb{S}^{m-1}$ с нормированной сферической метрикой $\mathbf{d}$ и корреляционным ядром K вида:

$$\mathbf{d}(w, w') = \frac{1}{\pi} \arccos \langle w, w' \rangle, \ \mathsf{K}(w, w') = \frac{2}{\pi} \arcsin \langle w, w' \rangle = 1 - 2\mathbf{d}(w, w'). \tag{21}$$

Нетрудно проверить, что ядро (21) действительно является корреляционным, то есть неотрицательно определенным, поскольку представимо в виде квадрата другого симметрического ядра:

$$\mathsf{K} = \mathsf{L}^2, \ \mathsf{K}(w, w') = \int_{\mathbb{S}^{m-1}} \mathsf{L}(w, v)\mathsf{L}(v, w')\mu(dv), \ \mathsf{L}(w, w') = \operatorname{sign} \langle w, w' \rangle. \tag{22}$$

Здесь μ — равномерная вероятностная мера на сфере $\mathbb{S}^{m-1}$.

Оказывается, при некоторых довольно общих ограничениях на базис Ψ метрика и корреляционное ядро (21) хорошо аппроксимируют метрику Хэмминга на множестве $C = \Pi_\Psi$ пороговых функций и соответствующее ядро (8):

$$\mathcal{K}(f_w, f_{w'}) \approx \mathsf{K}(w, w'), \ w, w' \in \mathbb{S}^{m-1}. \tag{23}$$

Возьмем для начала аффинный базис $\Psi = \Lambda$ и два весовых вектора $w, u \in \mathbb{S}^{m-1} = \mathbb{S}^n$. Тогда по определению для пороговых булевых функций f_w и f_u имеем:

$$\mathcal{K}(f_w, f_u) = \mathsf{E}\left\{\operatorname{sign}\langle w, \Lambda(x)\rangle \operatorname{sign}\langle u, \Lambda(x)\rangle\right\} = \mathsf{E}\left\{\operatorname{sign}(\alpha\beta)\right\},$$

где $\alpha = \langle w, \gamma\Lambda(x)\rangle$, $\beta = \langle u, \gamma\Lambda(x)\rangle$, $x \in \{\pm 1\}^n$ равномерно распределен, $\gamma \in \{\pm 1\}$ — вспомогательный случайный равновероятный элемент, не зависящий от x. Вектор $\gamma\Lambda(x) = (y_1, \ldots, y_{n+1})$ очевидно равномерно распределен на $\{\pm 1\}^{n+1}$, и для суммы

$$(\alpha, \beta) = \sum_{i=1}^{n+1} y_i(w_i, u_i)$$

справедлива ЦПТ, если выполнено условие Линдеберга [3]:

$$\forall \varepsilon > 0,\ \sum_{i=1}^{n+1}(w_i^2 + u_i^2)\mathbb{1}\left\{w_i^2 + u_i^2 > \varepsilon\right\} \underset{n\to\infty}{\longrightarrow} 0. \tag{24}$$

В этом случае α и β имеют асимптотически (при $n \to \infty$) нормальное совместное распределение с корреляцией $\langle w, u\rangle$, откуда

$$\mathcal{K}(f_w, f_u) = \mathsf{E}\left\{\operatorname{sign}(\alpha\beta)\right\} \underset{n\to\infty}{\longrightarrow} \frac{2}{\pi}\arcsin\langle w, u\rangle = \mathsf{K}(w, u).$$

При $n \to \infty$ условие (24) выполнено почти для всех пар w, u. В самом деле, зададим независимые равномерно распределенные $w, u \in \mathbb{S}^n$ в виде: $w = W/\|W\|$, $u = U/\|U\|$, где W и U — независимые стандартные гауссовские $(n+1)$-векторы. Тогда почти наверное $\|W\|^2 \sim \|U\|^2 \sim n$ и сумма в (24) эквивалентна величине

$$\frac{1}{n}\sum_{i=1}^{n+1}(W_i^2 + U_i^2)\mathbb{1}\left\{W_i^2 + U_i^2 > n\varepsilon\right\} \sim \mathsf{E}\left\{2\zeta \cdot \mathbb{1}\left\{2\zeta > n\varepsilon\right\}\right\} \sim n\varepsilon e^{-n\varepsilon/2} \to 0,$$

где $\zeta = \chi_2^2/2$ — стандартная экспоненциальная случайная величина.

Для произвольного базиса Ψ аппроксимация (23) тем точнее, чем более "равномерно" распределены на сфере $\mathbb{S}^{m-1}$ векторы $\pm\Psi(x)$, $x \in \{\pm 1\}^n$ (не ограничивая общности, можем считать $\|\Psi(x)\| \equiv 1$). Разобранный пример аффинного базиса $\Psi = \Lambda$ показывает, что векторы $\pm\Lambda(x)$ (2^{n+1} вершин гиперкуба, вписанного в $\mathbb{S}^n$) достаточно равномерно заполняют $\mathbb{S}^n$ при больших n. Будем далее считать, что имеем дело именно с таким "равномерным" базисом Ψ.

Задача максимизации функции δ на коде $C = \Pi_\Psi$ с помощью описанной аппроксимации ядер заменяется задачей максимизации гауссовского случайного поля $\delta : \mathbb{S}^{m-1} \to \mathbb{R}$ с нулевым средним и корреляционным ядром (21). Как уже было отмечено, соответствие $w \mapsto f_w$ весовых векторов и пороговых функций не биективно. В исходной задаче сфера $\mathbb{S}^{m-1}$ разбита на конечное число частей (каждая часть — одна пороговая функция), и поле δ кусочно постоянно на этих частях. Число частей $\#\Pi_\Psi$ ограничено сверху оценкой Шлефли (4), а их условным средним размером (диаметром), согласно аппроксимации (23), можно считать величину $\mathbf{d} = 2^{-n}$, поскольку, переходя по большой дуге от $w \in \mathbb{S}^{m-1}$ к $-w$, мы переходим от пороговой функции f_w к ее инверсии f_{-w}, преодолевая расстояние Хэмминга 2^n (число пересеченных частей), что в нормированной сферической метрике (21) отвечает расстоянию $\mathbf{d}(w, -w) = 1$.

5 Анализ энтропийных характеристик корреляционного ядра K

Для гауссовских процессов энтропия напрямую связана со среднеквадратической ошибкой аппроксимации. При последовательном дискретном наблюдении значений ζ_t такого процесса каждое новое значение при известных предыдущих имеет неопределенность $\mathsf{D}\{\zeta_t|\zeta_s, s<t\} = D_t$. Среднее геометрическое этих неопределенностей не зависит от того, в каком порядке наблюдались случайные величины ζ_t, и выражается через удельную энтропию h, приходящуюся на одно наблюдение:

$$\mathcal{D} = (D_1 \dots D_t)^{1/t} = \frac{e^{2h-1}}{2\pi}. \tag{25}$$

Нас будет интересовать энтропия дискретных подмножеств сферы $\mathbb{S}^{m-1}$ относительно корреляционного ядра (21), поскольку от этой энтропии зависит скорость уменьшения "оставшейся неопределенности" в ходе наблюдения новых значений процесса, а также время работы предложенного алгоритма максимизации, если, к примеру, в качестве условия остановки выбрать достижение некоторого порога средней неопределенности:

$$\mathcal{D} \leq \varepsilon.$$

Рассмотрим два дискретных множества на $\mathbb{S}^{m-1}$ — булев куб $\mathcal{C}_m$ и двойственный ему ортогональный канонический базис $\mathcal{B}_m$:

$$\mathcal{C}_m = \{w = (\pm m^{-1/2}, \dots, \pm m^{-1/2})\},\ \mathcal{B}_m = \{w = (\mathbb{1}\{i=j\})_{j=1}^m, i = 1, \dots, m\}. \tag{26}$$

Очевидно $\#\mathcal{C} = 2^m$, $\#\mathcal{B}_m = m$. Подмножество из 2^{m-1} векторов $w \in \mathcal{C}_m$ с положительной последней компонентой $w_m > 0$ обозначим $\mathcal{C}_m^+$, дополнительное к нему $\mathcal{C}_m^- = \mathcal{C}_m \setminus \mathcal{C}_m^+$.

Замечание 2. Булев куб $\mathcal{C}_m$ представляет собой множество точек сферы $\mathbb{S}^{m-1}$, наиболее удаленных от базиса $\mathcal{B}_m$ и его инверсии $-\mathcal{B}_m$, и наоборот. При этом ввиду инвариантности ядра (21) к ортогональным преобразованиям сферы $\mathbb{S}^{m-1}$ выбор любого другого ортогонального базиса и двойственного ему булева куба не повлияет на исследуемые энтропийные характеристики.

Лемма 2. *Пусть $S \subset \mathbb{S}^{m-1}$ — конечное множество m-векторов единичной длины. Тогда матрица $\mathsf{K}(S)$ вырождена тогда и только тогда, когда S содержит пару $\{w, -w\}$.*

Следствие 1. *Ядро K невырождено в ограничении на половину булева куба $\mathcal{C}_m^+$, и вырождено в ограничении на весь $\mathcal{C}_m$.*

Невырожденность ядра K в ограничении на базис $\mathcal{B}_m$ очевидна и без Леммы 2, поскольку $\mathsf{K}(\mathcal{B}_m) = \mathsf{I}_m$.

Следствие 2. *Ядро K бесконечномерно.*

Последнее понимается в том смысле, что существуют невырожденные конечные миноры $\mathsf{K}(S)$ любого размера.

Теорема 1. *Пусть w — любая из вершин булева куба $\mathcal{C}_m$. Тогда условная дисперсия значения поля $\delta(w)$ в этой точке при m известных значениях поля δ на множестве $\mathcal{B}_m$ при $m \to \infty$ имеет следующую асимптотику:*

$$\mathsf{K}(w, w|\mathcal{B}_m) \sim 1 - \left(\frac{2}{\pi}\right)^2. \tag{27}$$

Другими словами, если мы знаем значения гауссовского поля $\delta \sim \mathsf{K}$ в точках множества $\mathcal{B}_m$, то при больших m максимальная условная дисперсия среди оставшихся точек $w \in \mathbb{S}^{m-1}$ (в самых удаленных от $\mathcal{B}_m$ точках w — на булевом кубе $\mathcal{C}_m$) достигает значения $\sim 1 - 4/\pi^2$. Опишем теперь зеркальную ситуацию.

Теорема 2. *В случае 2^m известных значений поля δ на булевом кубе $\mathcal{C}_m$ условное ядро K на множестве $\mathcal{B}_m$ имеет следующую асимптотику при $m \to \infty$:*

$$\mathsf{K}(\mathcal{B}_m|\mathcal{C}_m) \sim \kappa \cdot \mathsf{I}_m, \;\; \kappa = 1 - \frac{2}{\pi}. \tag{28}$$

Как видим, при m известных значениях поля δ на $\mathcal{B}_m$ наибольшая условная неопределенность среди остальных точек асимптотически равна $1 - 4/\pi^2 \approx 0.59$, в то время как при 2^m известных значениях на $\mathcal{C}_m$ этот показатель снижается до $1 - 2/\pi \approx 0.36$.

Отметим, что матрица $\mathsf{K}(S) = \mathsf{L}^2(S)$ для достаточно "равномерных" и больших конечных множеств $S \subset \mathbb{S}^{m-1}$ может быть приближена матрицей $(\mathsf{L}(S))^2$. Это позволяет получить оценку величины (25) для множества $\mathcal{C}_m^+$ при $m \to \infty$:

$$\mathcal{D}(\mathcal{C}_m^+) \sim \frac{4\sqrt{e}}{\pi m}.$$

Другими словами, средняя неопределенность (25) в случае наблюдения 2^{m-1} значений поля $\delta \sim \mathsf{K}$ на $\mathcal{C}_m^+$ асимптотически пропорциональна m^{-1}.

Библиографические ссылки

[1] Зуев Ю. А. Комбинаторно-вероятностные и геометрические методы в пороговой логике. Дискретная математика (1991) 3, No 2, 47-57.

[2] Лидбеттер, М., Линдгрен, Г., Ротсен, Х. Экстремумы случайных последовательностей и процессов. М.: Мир, 1989. — 392 с.

[3] Ширяев, А. Н. Вероятность / А. Н. Ширяев. — М.: МЦНМО, 2011. — 416 с.

[4] Coppersmith, D., Winograd, S. Matrix multiplication via arithmetic progressions // J. Symbolic Computation. — 1990. — Vol 9. — p. 251-280.

[5] Schlafli L. Gesammelte mathematische Abhandlugen, Band 1. Birkhauser, Basel, 1850.

СРАВНИТЕЛЬНЫЙ АНАЛИЗ КРИПТОГРАФИЧЕСКИХ АРХИТЕКТУР РАСПРОСТРАНЕННЫХ СИСТЕМ МГНОВЕННОГО ОБМЕНА СООБЩЕНИЯМИ

М.А. Казловский
Белорусский государственный университет
Минск, БЕЛАРУСЬ
e-mail: kazlovski@bsu.by

Для организации конфиденциального общения между клиентами можно использовать доверенный сервер. Но такой сервер не может предоставить гарантии того, что он придерживается предписанного ему поведения. Поэтому в современных информационных системах, в первую очередь в системах мгновенного обмена сообщениями, используется концепция сквозного шифрования, которая позволяет гарантировать, что расшифровать передаваемые сообщения могут только клиенты, участвующие в общении. В работе рассматриваются известные протоколы сквозного шифрования, а также проводится сравнительный анализ безопасности популярных систем мгновенного обмена сообщениями.
Ключевые слова: сквозное шифрование; OTR; Signal Protocol; MTProto; система мгновенного обмена сообщениями

1 Введение

Большинство современных криптографических протоколов основано на взаимодействии клиентов с сервером. Как правило, в таких системах общение клиентов между собой сводится к отправке адресантом сообщений на сервер, который затем пересылает их адресату. При этом декларируется абсолютное доверие к серверу: считается, что он корректно выполняет протокол, не делая ничего иного. Такой подход не всегда устраивает клиентов, поскольку сервер не может предоставить гарантии того, что он придерживается предписанного ему поведения.

Поэтому возникла альтернативная концепция организации защищенного взаимодействия – сквозное шифрование (end-to-end encryption – E2EE): только клиенты, участвующие в общении, имеют возможность расшифровать передаваемые сообщения, а сервер лишь помогает в организации защищенного канала для общения, не обладая информацией, достаточной для раскрытия переписки. В данной работе рассматриваются криптографические архитектуры известных протоколов сквозного шифрования: Off-the-Record Messaging (OTR), Signal Protocol и MTProto. Также формулируются критерии безопасности систем мгновенного обмена сообщениями, с помощью которых проводится сравнительный анализ наиболее популярных из систем: Telegram, Signal, Viber, WhatsApp, FB Messenger и Skype.

2 Протоколы сквозного шифрования

Рассматриваются несколько известных протоколов сквозного шифрования. Протокол OTR [3] был предложен в 2004 году для использования в системах мгновенного обмена сообщениями Никитой Борисовым и Ианом Голдбергом. Протокол MTProto [2] был разработан в 2013 году Николаем Дуровым специально для системы мгновенного обмена сообщениями Telegram. Протокол Signal [1] (ранее — TextSecure) начал создаваться в 2013 году Тревором Перрином и Мокси Марлинспайком для обеспечения сквозного шифрования мгновенных сообщений, аудио и видеозвонков.

Каждый из этих протоколов может быть условно разделен на три фазы.

1. Запрос на установление соединения — стороны согласуют используемые криптонаборы.

2. Выработка общего ключа — стороны выполняют протокол, результатом которого является общий ключ.

3. Обмен сообщениями — выполняется протокол обмен сообщениями, в котором используемый для шифрования сообщения ключ постоянно меняется.

Вторая фаза во всех трех протокола основана на протоколе Диффи-Хеллмана, причем в Signal он выполняется три раза [4]. При этом используются различные группы: в OTR и MTProto это мультипликативная группа кольца вычетов, а в Signal — группа точек эллиптической кривой. Протоколы имеют механизмы, позволяющие убедиться, что построенный общий ключ совпадает: в OTR используется механизм, основанный на выработке имитовставок, в MTProto — на сравнении полученных хэш-значений общего ключа, в Signal — на результатах расшифрования зашифрованного в AEAD режиме сообщения. Все три протокола подвержены атаке типа «противник посередине». Для защиты от данной атаки в OTR предлагается использовать протокол «миллионеров-социалистов», который позволяет сторонам проверить подлинность друг друга при наличии у них общего секрета. В протоколах MTProto и Signal предусмотрено создание и визуальное отображение отпечатков (сформированных с помощью односторонних функций значений) общего ключа (MTProto) или открытых идентификационных ключей пользователей (Signal).

На третьей фазе передаваемые клиентами сообщения шифруются с помощью симметричного алгоритма шифрования (как правило, AES-256). Дополнительно выполняется контроль целостности с помощью имитовставки. В OTR шифрование выполняется в режиме CTR (схема Encrypt-then-mac), в MTProto — в режиме IGE (схема Mac-then-encrypt), в Signal — режимы CBC или AEAD (схема Encrypt-then-mac) [5]. Для защиты от «чтения назад» (Perfect Forward Secrecy) с помощью протокола Диффи-Хеллмана периодически формируется новый общий ключ. В OTR и Signal предусмотрена смена общего ключа после отправки или получения одного сообщения, а в MTProto — после 100 сообщений или через 7 дней существования старого общего ключа. При этом секретный ключ для шифрования

передаваемых сообщений всегда разный (в OTR и Signal меняется общий ключ по которому строится секретный, а в MTProto секретный ключ формируется в том числе с использованием открытого текста и случайных данных).

3 Критерии безопасности

Сравнительный анализ систем мгновенного обмена сообщения был проведен по девяти критериям, характеризующим безопасность системы. Результаты сравнительного анализа сведены в таблицу 1.

Ниже приведены сформулированные критерии и правила заполнения сводной таблицы:

1. *Открытость исходного кода*
   Позволяет независимым специалистам убедиться в корректности реализации протоколов сквозного шифрования, а также в отсутствии в исходном коде уязвимостей и незадекларированных возможностей, позволяющих раскрывать переписку. При заполнении таблицы если исходный код приложения проприетарный ставился «−», если открыта только клиентская часть – «+/−», если исходный код полностью открыт – «+».

2. *Децентрализация*
   Использование децентрализованной схемы организации работы системы мгновенного обмена сообщениями положительно сказывается на его безопасности, так как снимаются вопросы отказа в обслуживании, хранения зашифрованной переписки и других злонамеренных действий сервера. При заполнении таблицы если приложение работает в централизованной сети ставился «−», если в федеративной или P2P – «+».

3. *Анонимность*
   В большинстве систем мгновенного обмена сообщениями регистрация осуществляется по номеру мобильного телефона, то есть существует однозначная привязка клиента к номеру его телефона. Наличие альтернативных способов регистрации и поиска контактов усиливает безопасность общения. При заполнении таблицы если приложение обязательно требует номер мобильного телефона, ставился «−», если можно зарегистрироваться альтернативным способом (например, с помощью электронной почты – «+»).

4. *Сквозное шифрование (E2EE) чатов*
   Основной критерий, обеспечивающий конфиденциальность обмена сообщениями в системе без доверенных сторон. При заполнении таблицы если приложение не поддерживает сквозное шифрование, ставился «−», если поддерживает, но не по умолчанию – «+/−», если все чаты по умолчанию используют сквозное шифрование – «+».

5. *Проверка личности участников чата с E2EE*
   Большинство систем мгновенного обмена сообщениями не принуждают

участников проводить проверку личности друг друга по сторонним каналам (например, сверяя отпечатки ключей) или через знание общего секрета (с помощью протокола «миллионеров-социалистов»). Поэтому возможно осуществление атаки типа «противник посередине». При заполнении таблицы если приложение не поддерживает проверку личности ставился «−», если поддерживает, но ее осуществление необязательно – «+/−», если проверка личности осуществляется в обязательном порядке – «+».

6. *Уведомление о смене отпечатка общего ключа*
   В системах мгновенного обмена сообщениями смена общего ключа может быть следствием осуществления атаки типа «противник посередине». Поэтому в такой ситуации обязательно следует уведомлять клиента о смене отпечатка. При заполнении таблицы если приложение не поддерживает уведомления о смене отпечатка ставился «−», если поддерживает, но их необходимо включать в настройках – «+/−», если уведомление клиента осуществляется в обязательном порядке – «+».

7. *Групповые чаты с E2EE*
   Обычно в протоколе сквозного шифрования рассматривается защищенное общение между двумя сторонами: Алисой и Бобом. Но существует необходимость создания чатов с большим числом участников. При корректном расширении протокола сквозного шифрования защищенное общение возможно и в этом случае. При заполнении таблицы если приложение не поддерживает создание групповых чатов со сквозным шифрованием ставился «−», если поддерживает – «+».

8. *Защита социальноого графа*
   Многие системы мгновенного обмена сообщениями сохраняют информацию о круге общения своих клиентов, имея таким образом в своем распоряжении социальный граф, вершинами в котором выступают клиенты, а дугами – факт общения между двумя клиентами. При этом иногда сам факт общения двух конкретных абонентов может представлять интерес для противника. Более того, такой подход позволяет деанонимизировать клиента, проанализировав его круг общения. При заполнении таблицы если приложение не принимает мер для обеспечения секретности самого факта общения клиентов ставился «−», если такие меры принимаются – «+».

9. *Используемые криптографические примитивы*
   Большинство систем мгновенного обмена сообщениями используют стандартный набор надежных криптографических примитивов, обеспечивающий заданный уровень стойкости При этом существуют системы, использующие альтернативные алгоритмы или протоколы (например, вычисление имитовставки в MTProto). Некоторые системы продолжают использовать алгоритмы, признанные криптографическим сообществом недостаточно безопасными (RSA-1280 для асимметричного шифрования, SHA-1 для хэширования). При заполнении таблицы если приложение использует небезопасные крип-

тографические примитивы ставился «−», если приложение использует альтернативные криптографические примитивы – «+/−», если приложение использует стандартные криптографические примитивы – «+».

Таблица 1 Сравнительный анализ систем мгновенного обмена сообщениями

Система	(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)	(9)
Telegram	+/−	−	−	+/−	+/−	−	−	−	+/−
Signal	+	−	−	+	+/−	+	+	+	+
Viber	−	−	−	+	+/−	+	+	−	+
WhatsApp	−	−	−	+	+/−	+/−	+	−	+
FB Messenger	−	−	+	+/−	+/−	−	−	−	+
Skype	−	−	+	+/−	+/−	−	−	−	−

Библиографические ссылки

[1] Cohn-Gordon K., Cremers C., Dowling B. et al. A Formal Security Analysis of the Signal Messaging Protocol, 2019. Avail. at: `https://eprint.iacr.org/2016/1013.pdf`

[2] Durov N. End-to-End Encryption, Secret Chats, 2016. Avail. at: `https://core.telegram.org/api/end-to-end`

[3] Goldberg I., Borisov N. Off-the-Record Messaging Protocol version 3, 2012. Avail. at: `https://otr.cypherpunks.ca/Protocol-v3-4.0.0.html`

[4] Marlinspike M., Perrin T. The X3DH Key Agreement Protocol, 2016. Avail. at: `https://signal.org/docs/specifications/x3dh/x3dh.pdf`

[5] Perrin T., Marlinspike M. The Double Ratchet Algorithm, 2016. Avail. at: `https://signal.org/docs/specifications/doubleratchet/doubleratchet.pdf`

ЗАЩИТА ИНФОРМАЦИИ В СЕТЯХ БЕСПРОВОДНОГО ДОСТУПА, НА ОСНОВЕ СТАНДАРТА БЕЗОПАСНОСТИ IEEE 802.11ac

А.Н. Ковалевич[1,a], Т.Н. Ковалевич[1,b]
[1]*БИП-Институт правоведения*
Минск, БЕЛАРУСЬ
[2]*Университет им.Казимира Великого*
Быдгощ, ПОЛЬША
e-mail: [a]zzz805712@gmail.com, [b]thgilnoom384@yandex.ru

Информатизация современного общества привела к формированию новых видов преступлений, при совершении которых используется сквозное шифрование данных, средства беспроводной связи, негласного получения информации. Необходимость рассмотрения информационной безопасности как обособленного нормативного института, является одним из направлений концепции информационной безопасности в Республике Беларусь.
Защита информации в сетях беспроводного доступа, от несанкционированного воздействия, требует совершенствования, в частности контроля за использованием радиочастотного спектра беспроводной сети Wi-Fi.
Ключевые слова: беспроводные сети; шифрование данных; Wi-Fi; WPA; WPA2

1 Введение

Сети беспроводного доступа используются гражданами в торговых, офисных центрах, Интернет-кафе. Доступ в сеть Интернет, с использованием общедоступных сетей Wi-Fi осуществляется посредством СМС регистрации на телефонный номер, указанный в пользовательском соглашении. Данная мера аутентификации обусловлена созданием условий для безопасного использования сети Интернет. Идентификация выполняет функцию профилактики действий пользователей в сети Интернет, поскольку понимание пользователем того, что он может быть идентифицирован, будет сдерживать его от совершения противоправных действий.
Проблемным вопросом идентификации пользователей, является возможность использования сетевой карты в режиме мониторинга, позволяющим производить захват передаваемых сигналов в диапазоне радиочастотного спектра беспроводных сетей стандарта IEEE 802.11ac. Сохранение информации о частной жизни физических лиц и неразглашение персональных данных, содержащихся в информационных системах является целью защиты информации в Республике Беларусь [1].

2 Уязвимость беспроводных сетей стандарта IEEE 802.11ac

Определение 1. Совершенствование правового регулирования, связанного с несанкционированным доступом к компьютерной информации необходимо для обеспечения комплексной защиты передачи данных в сетях беспроводного доступа, информационной безопасности граждан и государства. Торговая марка Wi-Fi Alliance, имеет большой ряд стандартов для передачи информации. В 1997 году институтом инженеров электротехники впервые был разработан алгоритм WEP предназначенный для передачи данных в сетях беспроводного доступа. Алгоритм WEP основывается на подсчете контрольной суммы, проверки целостности данных. Защита информации в сетях Wi-Fi, основывается на протоколе WPA и WPA2. Беспроводная точка доступа, выполняет функцию базовой станции, которая имеет ограниченный радиус действия стандарта 802.11ax и работает в диапазоне частоты 2,4 ГГц. Вышеуказанный диапазон пришел на замену стандарту IEEE 802.11ac функционирующему на частоте 5 ГГц. Поддержка протокола WPA2 является обязательной для сертифицированных устройства Wi-Fi, поскольку в нем реализован алгоритм шифрования AES и протокол блочного шифрования данных CCMP с поддержкой увеличения размера ключа. Основная цель любой системы информационной безопасности заключается в предотвращении угроз от несанкционированного воздействия. Доступ к информации, осуществляемый с нарушением ее правового режима, рассматривается как несанкционированный доступ, таковым он становится, если лицо не имеет права доступа к информации, однако осуществляет его помимо установленного порядка. Перехват компьютерной информации - это неправомерное получение информации с использованием технических средств, осуществляющих обнаружение, прием и обработку информативных сигналов в сетях беспроводного доступа [3]. Сетевая карта в режиме мониторинга, фиксирует MAC адрес базовой станции, объем полученных данных, алгоритм шифрования, открытые сетевые порты. Вышеуказанные сведения находятся в основе принципов, правового регулирования общественных отношений в сфере информатизации и защиты информации в Республике Беларусь и подлежат защите, поскольку относятся к персональным данным распространение или предоставление которых ограничено. Разрешение на сбор, обработку, хранение информации о частной жизни физического лица и персональных данных, а также пользование ими осуществляется с письменного согласия данного физического лица [1]. Перехват компьютерной информации осуществляется на основе деаунтефикации направленной на разъединение клиента и точки доступа в сетях беспроводной связи. Сигналы деаунтефикации не шифруются стандартом безопасности 802.11ac и обусловлены уязвимостью направленной на обмен данными между маршрутизатором и подключенным клиентом. В момент разъединения базовой станции и клиента, маршрутизатор принимает сетевые пакеты "deauth"после чего происходит разъединение сетевого оборудования. При повторном подключении сетевые пакеты, подвержены перехвату с расшифровкой сетевого трафика. Снижение уровня защиты информации в сетях беспроводного доступа, обусловлено отсутствием записи параметров

работы маршрутизатора. Выбор алгоритма шифрования в сетях беспроводного доступа, является важным фактором, обеспечения информационной безопасности. Числовой код без специальных символов подвержен расшифровке, с последующей возможностью подключения к сетевому протоколу "telnet"предназначенному для самотестирования оборудования, а также удаленной настройке маршрутизатора.
В большинстве составов преступлений против информационной безопасности предметом является компьютерная информация, хранящаяся в компьютерной сети, системе, на компьютерных носителях либо передаваемая сигналами, распространяемыми по проводам, оптическим волокнам или радиосигналами. С целью совершенствования технических нормативно-правовых актов в Республике Беларусь, и обеспечения комплексной информационной безопасности в области сетей беспроводного доступа, необходимо рассмотреть вопрос о внесении термина мониторинг компьютерной сети в "Положение о технической и криптографической защите информации в Республике Беларусь от 29.11.2013 г. №529"Существенный недостаток отсутствия контроля в открытой сети Wi-Fi, связан с тем что при отсутствии в модеме алгоритма шифрования, все данные будут передаваться в незашифрованном виде, и могут быть подвержены перехвату со стороны злоумышленников, которые в последующем могут быть использованы в целях личной заинтересованности.
Усиление защиты беспроводной точки доступа, возможно реализовать путем создания сложного ключа идентификации, либо применением фильтра по MAC адресу. Однако обнаружение беспроводной сети в режиме мониторинга ставит под угрозу персональные данные, содержащиеся в сетях беспроводного доступа.

Библиографические ссылки

[1] Об информации, информатизации и защите информации: Закон Республики Беларусь, от 10.11.2008 №455-З // [Электронный ресурс] / Национальный центр правовой информации Республики Беларусь - Минск, 2020 г.

[2] О некоторых мерах по совершенствованию защиты информации: Указ Президента Республики Беларусь, от 16.04.2013 г. №196 // Национальный центр правовой информации Республики Беларусь - Минск, 2020 г.

[3] Положение о технической и криптографической защите информации в Республике Беларусь (в ред.Указа Президента Республики Беларусь от 29.11.2013 №529)

АГРЕГИРОВАННАЯ ПОДПИСЬ НА ЭЛЛИПТИЧЕСКИХ КРИВЫХ

Г.Л. Козина
Национальный университет "Запорожская политехника"
Запорожье, УКРАИНА
e-mail: ainc00@gmail.com

Предлагается протокол агрегированной подписи набора электронных документов на эллиптических кривых. Размер агрегированной подписи равен размеру подписи одного документа. Для проверки подписи используются открытые ключи всех участников подписания. Проверка осуществляется с помощью спаривания Вейля.
Ключевые слова: эллиптическая кривая; агрегированная подпись; билинейное спаривание Вейля

1 Введение

В случае, когда необходимо заверить набор электронних документов единой подписью, применяют механизм агрегированной подписи [1,2,3]. В отличие от мультиподписи, когда подписывается один документ группой подписантов и после этого координатором формируется единая подпись, в протоколе агрегированной подписи каждый участник подписания подписывает свой документ, и после этого формируется единая подпись. Размер агрегированной подписи набора документов равен размеру подписи одного документа.

В предлагаемом протоколе в качестве математического аппарата используются эллиптические кривые и спаривание точек эллиптической кривой. Для формивания агрегированной подписи используются секретные ключи подписантов. Проверка агрегированной подписи осуществляется с помощью спаривания Вейля [4] подписи и открытых ключей участников подписания.

2 Спаривание Вейля

Рассмотрим эллиптическую кривую над конечным полем $GF(p)$:

$$y^2 = x^3 + ax \, mod \, p,$$

где $p = 3 \, mod \, 4$, $a \in GF(p)$, G - аддитивная группа точек эллиптической кривой простого порядка n с базовой точкой P, $nP = O$, O - бесконечно удаленная точка; V - мультипликативная группа простого порядка n с нейтральным элементом 1.

Билинейным спариванием точек называется функция

$$e : G \times G \to V,$$

для которой выполняются следующие свойства:
1. $e(P+Q,R) = e(P,R) \cdot e(Q,R)$, $e(P,Q+R) = e(P,Q) \cdot e(P,R)$.
2. $e(k \cdot P, Q) = e(P,Q)^k$, $e(P, k \cdot Q) = e(P,Q)^k$.
3. $e(k \cdot P, Q) = e(P, k \cdot Q)$.
4. $e(k \cdot P, m \cdot Q) = e(P,Q)^{k \cdot m}$.
5. $e(P,P) \neq 1$.

Спаривайние Вейля $e(P,Q)$ точек P, Q эллиптической кривой задается формулой

$$e(P,Q) = \frac{F(P, Q+S) \cdot F(Q, -S)}{F(P,S) \cdot F(Q, P-S)} \quad \forall S \in G,$$

где $F(T,Q) =$ - функция Вейля точек T, Q.

Функцию Вейля точек T, Q порядка n можно вычислить с помощью рекурсивного алгоритма Миллера:

$f_{1,T}(Q) = 1 \quad \forall Q \in G$

$f_{i+j,T}(Q) = f_{i,T}(Q) \cdot f_{j,T}(Q) \cdot \frac{l_{i,j}}{v_{i+j}}(Q) \quad i + j < n$

$F(T,Q) = f_{n,T}(Q)$.

где $l_{i,j} = \alpha x + \beta y + \gamma$ - уравнение прямой, проходящей через точки $i \cdot T$, $j \cdot T$, $v_{i+j} = x - x_R$, $R = (i+j) \cdot T = (x_R, y_R)$.

Для обеспечения свойств 1-5 будем использовать искажающее отображение $\varphi(x,y) = (-x, y \cdot i)$.

В предлагаемом ниже протоколе спаривание Вейля точек эллиптической кривой вычисляется по правилу: $e(P,Q) \to e(P, \varphi(Q))$.

3 Протокол агрегированной подписи

В протоколе участвуют группа подписантов, каждый из которых подписывает свой документ, доверительный центр, координирующий работу подписантов и формирующий агрегированную подпись, и верификатор.

Общесистемными параметрами являются эллиптическая кривая над простым полем $GF(p)$: $GF(p)$:

$$y^2 = x^3 + ax \, mod \, p,$$

где $p = 3 \, mod \, 4$, $a \in GF(p)$, базовая точка P простого порядка n, выбранная хеш-функция H.

3.1 Генерация ключей

Пусть в протоколе участвуют t подписантов. Каждый подписант i выбирает секретный ключ d_i - целое число, меньшее n. Открытый ключ вычисляется по формуле $Q_i = d_i P$.

3.2 Формирование агрегированной подписи

Перед подписанием каждый подписант i хеширует свой документ M_i. Хеш-образ документа $H(M_i)$ подписант преобразовывает в точку H_i эллиптической кривой. Подписью документа M_i является точка эллиптической кривой $S_i = d_i H_i$.

Пара $< M_i, S_i >$ - документ и подпись - отправляется в доверительный центр, где проходит проверку правильности подписи с использованием спаривания Вейля: $e(S_i, P) = e(H_i, Q_i)$. Если подпись каждого подписанта i верна, доверительный центр формирует агрегированную подпись $S = \sum_{i=1}^{t} S_i$.

3.3 Проверка агрегированной подписи

Для проверки агрегированной подписи S документов $M_1, M_2, ..., M_t$ верификатор запрашивает открытые ключи подписантов $Q_1, Q_2, ..., Q_t$, хеширует полученные документы, преобразует каждый хеш-образ $H(M_i)$ в точку H_i эллиптической кривой. Если выполняется соотношение $e(S, P) = \prod_{i=1}^{t} e(H_i, Q_i)$, верификатор признает подпись правильной.

Покажем корректность процедуры проверки.

Поскольку $e(H_i, Q_i) = e(S_i, P)$, то

$\prod_{i=1}^{t} e(H_i, Q_i) = \prod_{i=1}^{t} e(S_i, P) = e(\sum_{i=1}^{t} S_i, P) = e(S, P)$.

4 Пример

В протоколе участвуют группа из $t = 3$ подписантов - A_1, A_2, A_3, каждый из которых подписывает свой документ - M_1, M_2, M_3 соответственно, доверительный центр, координирующий работу подписантов и формирующий агрегированную подпись, и верификатор B.

Общесистемными параметрами являются эллиптическая кривая над простым полем $GF(2383)$: $y^2 = x^3 - 3x \, mod \, 2383$, базовая точка $P = (81, 787)$ простого порядка $n = 149$, хеш-функция H. Для вычисления спаривания Вейля выбрано $S = (O, O)$.

4.1 Генерация ключей

Каждый подписант A_i выбирает секретный ключ $d_i < 149$:

$d_1 = 46$, $d_2 = 102$, $d_3 = 40$.

Открытымий ключами соответственно являются

$Q_1 = (1890, 1038)$, $Q_2 = (134, 303)$, $Q_3 = (929, 873)$.

4.2 Формирование агрегированной подписи

Перед подписанием каждый подписант A_i хеширует свой документ M_i. Хеш-образ документа $H(M_i)$ подписант преобразовывает в точку H_i эллиптической кривой: $H_1 = (195, 1426)$, $H_2 = (134, 2080)$, $H_3 = (931, 1400)$ соответственно.

Подписью документа M_i является точка эллиптической кривой $S_i = d_i H_i$:

$S_1 = (695, 320)$, $S_2 = (379, 1068)$, $S_3 = (1273, 2045)$.

Пары $< M_i, S_i >$ - документ и подпись - отправляются в доверительный центр, где проходят проверку правильности подписи с использованием спаривания Вейля:

$e(S_1, P) = e(H_1, Q_1) = 1686 + 18 \cdot i$,
$e(S_2, P) = e(H_2, Q_2) = 698 + 2076 \cdot i$,
$e(S_3, P) = e(H_3, Q_3) = 247 + 898 \cdot i$.

Поскольку подпись каждого подписанта A_i верна, доверительный центр формирует агрегированную подпись $S = (387, 289)$.

4.3 Проверка агрегированной подписи

Для проверки агрегированной подписи $S = (387, 289)$ документов M_1, M_2, M_3 верификатор B запрашивает открытые ключи подписантов $Q_1 = (1890, 1038)$, $Q_2 = (134, 303)$, $Q_3 = (929, 873)$, хеширует полученные документы, преобразует каждый хеш-образ $H(M_i)$ в точку H_i эллиптической кривой: $H_1 = (195, 1426)$, $H_2 = (134, 2080)$, $H_3 = (931, 1400)$ соответственно.

Далее верификатор B вычисляет произведение $\prod_{i=1}^{3} e(H_i, Q_i) = 1118 + 1991 \cdot i$, а также спаривание Вейля точек S и P: $e(S, P) = 1118 + 1991 \cdot i$.

Поскольку выполняется соотношение

$$e(S, P) = \prod_{i=1}^{3} e(H_i, Q_i),$$

верификатор B признает подпись правильной.

Библиографические ссылки

[1] Макаров А.О. (2019). Схема пост-квантовой агрегированной подписи на основе теории алгебраического кодирования. *Вопросы кибербезопасности.* № **2(30)**, С. 69–76.

[2] Boneh D., Gentry C., Lynn B. and Shacham H. (2003). Aggregate and Verifiably Encrypted Signatures from Bilinear Maps. *Advances in Cryptology EUROCRYPT 2003, May 4-8.* P. 416–432.

[3] Zhao Yunlei (2018). Aggregation of Gamma-Signatures and Applications to Bitcoin. *Cryptology ePrint Archive.* https://eprint.iacr.org/2018/414/20180510:203542.

[4] ISO/IEC 14888-3:2006(E)(2006). *Information Technology — Security Techniques – Digital signatures with appendix – Part 3: Discrete logarithm based mechanisms.*

КРИПТОГРАФИЧЕСКИЕ ПРОТОКОЛЫ НА ОСНОВЕ БЛОКЧЕЙНА, СТОЙКОГО В ТЕОРЕТИКО-ИНФОРМАЦИОННОМ СМЫСЛЕ: ИДЕИ, РЕАЛИЗАЦИЯ, ОЦЕНКИ СТОЙКОСТИ И НАДЕЖНОСТИ

А.М. Кудин[1,a]
[1]*Национальный банк Украины, НТУУ "КПИ имени Игоря Сикорского"*
Киев, УКРАИНА
e-mail: [a]pplayshner@gmail.com

Решение задач анализа и синтеза стойких к криптоанализу криптографических протоколов привело к исследованию свойств фундаментальных криптографических блоков, из которых можно построить криптографический протокол произвольной сложности. Назовем такие блоки примитивными криптографическими протоколами. В настоящее время основными примитивными криптографическими протоколами считаются протоко-лы разделения секрета (secret sharing) и протоколы не интерактивных доказательств (non-interactive). В работах R. Goyal и V. Goyaly было показано, что все примитивные криптографические протоколы можно заменить блокчейном. В этом случае интересен вопрос существования аналога стойким в теоретико-информационном смысле примитивным протоколам протоколов, использующих блокчейн. В докладе показан утвердительный ответ на этот вопрос и рассмотрен метод построения протоколов соглашения блокчейнов, стойких в теоретико-информационном смысле. Идея построения протоколов основана на принципиальной невозможности вычисления обратной функции с требуемой точностью. Предложенные протоколы обладают эффективностью по быстродействию на уровне «византийских» протоколов, но менее требовательны к соотношению количества честных/нечестных участников протокола. Рассмотрены вопросы получения оценок стойкости протокола к известным атакам подмены блока, реализации протокола и оценки его надежности для различных сценариев практического применения.
Ключевые слова: системы неинтерактивных доказательств; блокчейн; информационная неопределенность; радиус информации

1 Введение

Идеи аксиоматического построения криптографических преобразований из небольшого количества криптографических примитивов известны достаточно давно [4]: любой, сколь угодно сложный криптографических алгоритм есть суперпозиция однонаправленных генераторов псевдослучайной последовательности, хеш-функций, функций односторонней перестановки и т.д.). Подобно этому криптографический протокол любой сложности – суперпозиция примитивных криптографических протоколов, основными из которых являются протоколы распреде-

ления секрета (secret sharing), протоколы интерактивных и неинтерактивных доказательств (аргументации), протоколы привязки к биту (bit commitment), протоколы передачи с забыванием (oblivious transfer), протоколы передачи с секретом (англ. - trapdoor commitment) и тому подобное.

С появлением блокчейнов быстро возникла идея использования их как ядра принципиально новой формальной теории криптографических протоколов, а именно, использования блокчейнов вместо протоколов аргументации и доказательств с нулевыми знаниями [6].

В таком подходе, правда существует одна фундаментальная проблема: известны протоколы доказательств с нулевыми знаниями с теоретико-информационной (или безусловной) стойкостью [3], в то время как считалось стойкость протоколов консенсуса блокчейнов относится максимум к теоретико-сложностной (или практической по Шеннону) стойкости. В следующем разделе приводится протокол консенсуса блокчейна, стойкого к атакам централизации в теоретико-информационном смысле.

2 Протокол консенсуса, основанный на потере точности вычислений

Основной идеей нового протокола консенсуса является изменение подхода к расчету консенсусной функции и уничтожения взаимосвязей между ценным ресурсом, который используется в консенсусном протоколе и вознаграждения за победу в консенсусе. В качестве ценного ресурса можно использовать такой ресурс, накопление которого было бы нецелесообразно с экономического или технологического смысла (например, реальные IP-адреса), а алгоритм добавления нового блока в блокчейн при применении протокола соглашения «proof-of-works» изменить таким образом, чтобы необходимая для работы алгоритма исходная информация была задана неполно и неточно.

Значение целевой функции консенсуса вычисляется с точностью, которая задается некоторым порогом. Исходная информация располагаются на нескольких ресурсах за доступ к которым конкурируют участники протокола соглашения. Последнее свойство позволяет сравнивать шансы участников протокола с высокопроизводительными и малопроизводительными вычислительными ресурсами в борьбе за право генерации нового блока.

Теоретической основой построения и оценки устойчивости протокола согласования на основании «потери точности» предлагается выбрать общую теорию оптимальных алгоритмов [2], которая связывает существование и сложность алгоритмов с точностью задания входных данных алгоритма.

Пошаговое описание протокола, основанного на вышеупомянутых принципах и оценку его стойкости к известным атакам рассмотрены автором совместно с Ковальчук Л.В. и Коваленко Б.А. в работе [1].

3 Вопросы надежности функционирования блокчейн систем

В дополнении к стойкости блокчейна к атакам генерации ложного блока и разветвления, можно рассматривать понятие надежности и живучести функционирования блокчейн систем. Надежность целесообразно ввести как возможность сохранения правильного функционирования блокчейна под влиянием случайных, стихийных явлений. Вопросы надежности функционирования блокчейн систем рассмотрены автором совместно с К.С. Горняк в работе [5].

Библиографические ссылки

[1] Кудін, А. М., Ковальчук, Л. В., Коваленко, Б. А. (2019) Теоретичні засади та застосування блокчейн-технологій: імплементація нових протоколів консенсусу та краудсорсінг обчислень. *Математичне та комп'ютерне моделювання. Серія: Технічні науки.*. Вип. **19**,С. 56-62.

[2] Трауб, Д., Васильковский, Г., Вожьняковский, Х. (1988). *Информация, неопределенность, сложность*. Мир, Москва.

[3] Feige, U., Shamir, A. (1990) Witness indistinguishable and witness hiding protocols. *STOC*, P. 416–426.

[4] Goldreich, O. (2001). *Foundations of Cryptography Vol.1 Basic Tools.*. Cambridge University Press, London.

[5] Gorniak, K. S., Kudin, A. M. (2020) Aspects of blockchain reliability considering its consensus algorithms. *Theoretical and Applied Cybersecurity*. V. **2**, P. 5-9.

[6] Goya, R., Goyaly, V. (2017) Overcoming cryptographic impossibility results using blockchains. *eprint.iacr.org*. T. **935**.

НЕПОРОГОВОЕ МОДУЛЯРНОЕ РАЗДЕЛЕНИЕ СЕКРЕТА

Г.В. Матвеев[a], В.В. Матулис
Белорусский государственный университет
Минск, БЕЛАРУСЬ
e-mail: [a]matveev@bsu.by

В статье исследуется вопрос об эффективной реализации общих (непороговых) структур доступа (разделения секрета). На основе таких характеристик эффективности алгоритма разделения секрета, как информационный уровень и длина ключа, получены оценки эффективности GM-алгоритма. Предложен метод частичных объединений, более эффективный в сравнении с GM-алгоритмом.
Ключевые слова: структура доступа; разделение секрета; модулярный подход; информационный уровень; длина ключа

1 Введение

Большинство результатов в теории модулярного разделения секрета относится к пороговым структурам доступа. Несмотря на свою важность, пороговые структуры являются достаточно узким классом структур. В данной работе мы рассмотрим вопрос об эффективной реализации общих структур доступа. Следующая теорема, полученная Н. Н. Шенцом [1], описывает одно ограничение модулярного подхода.

Теорема 1. *Идеально с помощью модулярного разделения секрета возможно реализовать только пороговую структуру доступа.*

Таким образом, в общем случае модулярная реализация разделения секрета идеальной не будет. В связи с этим нас интересует эффективность неидеальной реализации разделения секрета. Для этого существуют различные характеристики, основными из которых являются *информационный уровень* и *длина ключа*.

Пусть S – множество значений разделяемого секрета, а S_i – множество значений частичного секрета i-го участника.

Определение 1. Информационным уровнем схемы разделения секрета называется минимальное отношение ρ размера хранимого секрета к размеру частичного секрета в битах [5]

$$\rho = \min_{i \in I} \left\{ \frac{\log_2 |S|}{\log_2 |S_i|} \right\}.$$

Определение 2. Длиной ключа схемы разделения секрета ss называется длина наибольшего из ключей при условии хранения секрета размером 1 бит [2].

$$ss = \max_{i \in I} \log_2 |S_i|.$$

Имеются следующие оценки для этих характеристик, не зависящие от конкретного алгоритма разделения секрета.

Теорема 2. *Для любой структуры доступна на множестве k участников существует схема разделения секрета с длиной ключей порядка $O(2^{0.994k})$ [4].*

Теорема 3. *Для любого числа участников k существует структура доступа, любая реализация которой имеет информационный уровень порядка $O(\log k/k)$ [2].*

Теорема 4. *Наименьшая возможная длина ключей для пороговой структуры доступа есть $O(\log k)$ [2].*

Для модулярного разделения секрета ранее Н. Н. Шенцом был получен следующий результат [1].

Теорема 5. *Информационный уровень модулярного разделения секрета выражается через степени модулей участников*

$$\rho = \frac{M_2 - M_1}{\max\limits_{i \in I} \deg m_i(x)}.$$

Как видно, для непороговой модулярной реализации нет оценок эффективности. Далее мы пытаемся восполнить этот пробел.

2 Оценка эффективности GM-алгоритма

Из работы [3] известно, что любую структуру доступа можно реализовать модулярно. Описанный в этой работе способ генерации подходящих модулей будем называть *GM-алгоритмом*. Ниже приведено его краткое описание.

Алгоритм 1.
Вход: Базис структуры отказа Γ_{max}.
Выход: Модули участников $m_1(x),\ m_2(x),\ \ldots,\ m_t(x) \in \mathbb{F}_q[x]$.
Шаг 0. Положим $m_1(x),\ m_2(x),\ \ldots,\ m_t(x) = 1,\ s = |\Gamma_{max}|$. Сгенерируем различные неприводимые многочлены $p_i(x) \in \mathbb{F}_q[x],\ i = 1,\ s$.
Шаг k, $(1 \le k \le s)$. Рассматриваем подмножество $A_k \in \Gamma_{max}$. Все модули участников, не входящих в A_k, домножаем на многочлен $p_k(x)$.
Конец алгоритма.

Теорема 6. *Информационный уровень, получаемый при генерации модулей участников (t,k)-пороговой схемы с помощью GM-алгоритма составляет*

$$\rho = \frac{1}{C_{k-1}^{t-1}}.$$

Доказательство. По определению, для модулярного разделения секрета

$$\rho = \frac{M_2 - M_1}{\max\limits_{i \in I} \deg m_i(x)}.$$

Сначала оценим M_2. Для этого рассмотрим произвольное разрешённое множество s участников, $|s| = t$. Нас интересует значение $\deg LCM(\{m_i(x), i \in s\})$. Заметим, что модуль каждого из участников представляет собой произведение какого-то подмножества многочленов из $\{p_1(x),\ p_2(x),\ \ldots\}$. Пусть S – множество индексов этих многочленов. Тогда каждому участнику соответствует некоторое подмножество $s_i \subset S$ множества S и модуль участника может быть записан в следующем виде

$$m_i(x) = \prod_{j \in s_i} p_j(x).$$

Тогда

$$\deg LCM(\{m_i(x), i \in s\}) = n \left| \bigcup_{i \in s} s_i \right|,$$

что можно переписать в виде

$$\deg LCM(\{m_i(x), i \in s\}) = n(|S| - |h|),$$
$$h = \textstyle\bigcap_{i \in s} \overline{s_i}.$$

Очевидно, что $|S| = |\Gamma_{\max}|$, поскольку каждый многочлен $p_i(x)$ соответствует какому-то элементу из базиса структуры отказа. Нас интересует значение $|h|$. Оно соответствует мощности подмножества таких многочленов $p_j(x),\ j \in h$, что ни один из ключей $m_i(x),\ i = 1,\ 2,\ \ldots,\ k$, не содержит многочлен $p_j(x)$. Это означает, что все $m_i(x),\ i \in s$, не делятся на $p_j(x)$ одновременно, что возможно, только если $s \in \Gamma_{max}$. Противоречие. Следовательно, $h = 0$.

Осталось оценить $|\Gamma_{\max}|$. Это есть количество способов выбора $t-1$ участника из k, то есть C_k^{t-1}.

Для вычисления M_1 можно применить аналогичные рассуждения для любого множества участников из базиса структуры отказа. В этом случае множество h не пусто. Оно состоит из всех элементов базиса структуры отказа, в которые включено s, то есть только из одного элемента, поэтому $M_1 = C_k^{t-1} - 1$.

Получаем, что $M_2 - M_1 = n$. Осталось оценить степени модулей участников.

Без ограничения общности, рассмотрим первого участника. Его модуль домножался на многочлен степени n всякий раз, когда встречался элемент $x \in \Gamma_{\max}, 1 \notin x$. Количество таких элементов подсчитать несложно – оно соответствует количеству подмножеств мощности $t-1$, не содержащих первого участника. Это количество есть C_{k-1}^{t-1}.

В итоге имеем

$$\rho = \frac{M_2 - M_1}{\max\limits_{i \in I} \deg m_i(x)} = \frac{n}{nC_{k-1}^{t-1}} = \frac{1}{C_{k-1}^{t-1}}.$$

□

3 Метод частичных объединений

Недостатком GM-алгоритма является то, что он неэффективно реализует пороговые схемы, которые с помощью модулярного подхода можно реализовать идеально. Предлагаемый ниже метод частичных объединений лишен этого недостатка.

Алгоритм 2.

1. Вход – система из m многочленов $q_i(x),\ i = 1, \ldots, m$.
2. Конечное количество раз делается одна из следующих операций:
3. Объединить два существующих многочлена в один, равный их наименьшему общему кратному.
4. Добавить в систему копию одного из находищихся в ней многочленов.
5. Выход – система из l многочленов $f_i(x),\ i = 1, \ldots, l$.

Нас интересует, какие структуры доступа можно реализовать с помощью такого подхода и насколько эффективно это можно сделать.

Теорема 7. *С помощью метода частичных объединений можно реализовать любую структуру доступа.*

Доказательство. Как уже упоминалось, модуль $m_i(x),\ i = 1, \ldots, k$ каждого из участников после работы GM-алгоритма представляет собой произведение какого-то подмножества многочленов из $\{p_1(x), p_2(x), \ldots\}$ и представим в виде

$$m_i(x) = \prod_{j \in s_i} p_j(x).$$

Рассмотрим следующие операции над системой многочленов $m_i(x),\ i = 1, \ldots, k$.

1. Замена некоторого многочлена на два новых, таким образом, что исходный многочлен равен НОК новых.
2. Удаление из системы некоторого многочлена, который присутствует в нескольких экземплярах.

Сначала с помощью операции 1) разложим все модули $m_i(x)$ на их примарные составляющие $p_j(x)$. В получившейся системе некоторые $p_j(x)$ встречаются больше одного раза. С помощью операции 2) добьёмся, чтобы каждый многочлен встречался только один раз. Таким образом, мы пришли к множеству $p_j(x)$ попарно взаимно простых многочленов одной степени. □

Теперь нас интересует насколько эффективно это можно сделать.

Для пороговых структур задача тривиальна, поскольку пороговая структура является начальным состоянием метода частичных объединений.

Теорема 8. *Длина ключей в результате склеивания составляет* $O(\log m/\rho)$*, где* m *– количество многочленов в начале работы метода частичных объединений, а* ρ *– уровень информации полученной с его помощью реализации.*

Доказательство. Пусть размер секрета составляет один бит. Тогда размер максимального ключа равен как минимум $1/\rho$. В действительно он будет больше, потому что в общем случае не существует m попарно взаимно простых многочленов 1-ой степени. Тогда размер ключа будет α/ρ, где α – минимальный размер ключа (степень многочлена), при которой над полем $\mathbb{F}_q$ существует m попарно взаимно простых многочленов степени α. Эта величина имеет порядок $O(\log m)$. □

Следствие. *С помощью склеивания модулей пороговую схему можно реализовать с длиной ключей порядка* $ss = O(t \log(kt))$.

Библиографические ссылки

[1] Шенец Н.Н. Об информационном уровне модулярных схем разделения секрета // *Докл. Нац. акад. наук Беларуси, сер. физ.-мат. наук*, т. 54 №6, 2010, с. 9–12.

[2] Bogdanov, A., Guo, S., Komargodski, I. Threshold secret sharing requires a linear size alphabet. // *Theory of Cryptography - 14th International Conference, TCC.* – 2016, Beijing, China, October 31 - November 3, 2016, Proceedings, Part II, pages 471–484, 2016

[3] Galibus T. Matveev G. Generalized Mignotte Sequences in Polynomial Rings // *ENTCS* – 2007. – Vol. 186, P. 43–48. – DOI: 10.1016/j.entcs.2006.12.044.

[4] Liu, T., Vaikuntanathan, V. Breaking the circuit-size barrier in secret sharing. // *Proceedings of the 50th Annual ACM SIGACT Symposium on Theory of Computing.* – 2018. – P. 699–708.

[5] Stinson, D. R. *Cryptography: Theory and Practice.* // CRC Press. – 1995.

ГРУППОВЫЕ СВОЙСТВА SH-ОБОБЩЕНИЯ АЛГОРИТМА БЛОЧНОГО ШИФРОВАНИЯ ФЕЙСТЕЛЯ

М.А. Пудовкина
Московский государственный технический университет им. Н.Э. Баумана
Москва, РОССИЯ
e-mail: maricap@rambler.ru

Описываются свойства группы G, порожденной частичными функциями переходов автоматной модели неавтономного регистра сдвига над произвольной конечной абелевой группой. Такой регистр сдвига применяется в SH-обобщение алгоритма блочного шифрования Фейстеля. Дана характеризация группы G через операцию экспоненцирования, приведены условия ее примитивности.
Ключевые слова: операция экспоненцирования; сплетение групп; импримитивная группа; примитивная группа; неавтономный регистр сдвига

1 Введение

Пусть $(X,+)$ — конечная абелева группа, в частности, $(X,+)$ может являться аддитивной группой поля $GF(p)$ или кольца $\mathbb{Z}_p$, $p \geq 2$. Рассмотрим неавтономный регистр сдвига (НРС) длины $m \geq 2$ над группой X с функцией обратной связи $X^m \to X$, заданный условием

$$(\alpha_1, ..., \alpha_m) \mapsto \alpha_1 + h(\alpha_2, ..., \alpha_m), h : X^{m-1} \to X.$$

Неавтономный регистр сдвига реализует преобразование множества X^m с частичными функциями переходов $g_{h,k} : X^m \to X^m$,

$$g_{h,k} : (\alpha_1, ..., \alpha_m) \mapsto (\alpha_2, ..., \alpha_m, \alpha_1 + h(\alpha_2, ..., \alpha_m) + k)\,, k \in X.$$

Он совпадает с одним из вариантов обобщения алгоритма блочного шифрования Фейстеля, а именно, обобщенного SH-алгоритма (source-heavy) (см., [5]) с частичной раундовой функцией

$$g_{k,h} : (\alpha_1, ..., \alpha_m) \mapsto (\alpha_2, ..., \alpha_m, \alpha_1 + h(\alpha_2, ..., \alpha_m) + k)\,, k \in X,\ h : X^{m-1} \to X.$$

Группа $G^{(m)}(h) = \langle g_{h,k} | k \in X \rangle$, порожденная всеми частичными функциями, называется *группой неавтономного регистра сдвига*, а в некоторых криптографических приложениях — *группой алгоритма шифрования*. Она является важной характеристикой алгоритма шифрования, который при ее интранзитивности, импримитивности или унипримитивности может иметь разные слабости. Если группа $G^{(m)}(h)$ импримитивна, то при криптоанализе алгоритма шифрования возможно

применение естественных гомоморфизмов, связанных с существованием нетривиальной системы импримитивности (разбиение алфавита текстов на равномощные блоки). В [2,4] описаны разные случаи при импримитивных групп алгоритмов блочного шифрования. Если же группа $G^{(m)}(h)$ унипримитивна и описывается с помощью операции экспоненцирования, то она может являться подгруппой группы изометрий некоторой нетривиальной метрики, что для криптографических приложений означает сохранение соотношений между парами открытого и соответствующего шифрованного текстов. Первый такой пример приведен в [1] для двоичного неавтономного регулярного регистра сдвига. В настоящей работе получено его обобщение для неавтономного регистра сдвига над произвольной конечной абелевой группы $(X, +)$. Дана характеризация группы $G^{(m)}(h)$ через операцию экспоненцирования, приведены условия ее примитивности.

2 Основные результаты

Пусть $S(X)$ — симметрическая группа на множестве X, $\alpha^g = \alpha g = g(\alpha)$ — образ элемента $\alpha \in X$ при действии на него подстановкой $g \in S(X)$, $B^U = \{f | f : U \to B\}$ для произвольных множеств B, U.

Напомним следующие понятия (см., например, [1,3]).

Определение 1. Пусть $G \leq S(X)$, $H \leq S(J)$, $G^J = \{g | g : J \to G\}$. Тогда множество $\left\{(g,h) | (g,h) \in G^J \times H\right\}$ относительно операции

$$(g_1, h_1)(g_2, h_2) = (g, h_1 h_2),$$

где $(g_1, h_1), (g_2, h_2) \in G^J \times H$, $g \in G^J$,

$$g(j) = g_1(j) g_2\left(j^{h_1}\right) \text{ для каждого } j \in J,$$

является группой, которая называется сплетением группы G группой H и обозначается $G \wr H$.

Определение 2. Экспоненцированием группы G группой H называется группа подстановок степени $|X|^{|J|}$ множества $X^J = \{\varphi | \varphi : J \to X\}$, обозначаемая $G \uparrow H$, абстрактно изоморфная сплетению $G \wr H$ и задаваемая следующим действием на множестве X^J:

$$(g,h) : \varphi(j) \mapsto \varphi\left(j^{h^{-1}}\right)^{g\left(j^{h^{-1}}\right)} \text{ для каждого } j \in J,$$

где $(g,h) \in G \wr H$, $\varphi \in X^J$.

Группа $G \uparrow H$ имеет нормальный делитель

$$N = \left\{(g,1) | g \in G^J\right\} \cong \overbrace{G \times \ldots \times G}^{|J|},$$

причем $G \uparrow H/N \cong H$.

Известно (см., например, лемма 2.7.A [3]), что группа $G \uparrow H$ примитивна тогда и только тогда, когда группа G примитивна и нерегулярна, а группа H транзитивна. В терминах подгрупп группы экспоненцирования в классификационной теореме О'Нэна-Скотта описывается ряд классов примитивных групп.

Пусть $v_\beta^{(i,m)} : X^m \to X^m$,

$$v_\beta^{(i,m)} : (\alpha_1, ..., \alpha_m) \mapsto (\alpha_1, ..., \alpha_{i-1}, \alpha_i + \beta, \alpha_{i+1}, ..., \alpha_m),\ \beta \in X,\ i = 1, ..., m,$$

$J(h) = \left\{j_1, ..., j_{q(h)}\right\}$ — множество номеров всех существенных переменных $x_{j_1}, ..., x_{j_{q(h)}}$ функции $h(x_1, ..., x_{m-1})$, $J(h) \subset \{1, ..., m-1\}$, $q(h) = |J(h)|$, и

$$d = d(h) = \text{НОД}\left\{j_1, ..., j_{q(h)}, m\right\}.$$

Если $d > 1$, то положим $l = l(h) = m/d$, и функцию $h^{(d)} : X^{l-1} \to X$ зададим условием

$$h^{(d)}(\beta_1, ..., \beta_{l-1}) = h(\beta'_1, ..., \beta'_{m-1}) \text{ для каждого набора } (\beta_1, ..., \beta_{l-1}) \in X^{l-1},$$

где

$$\beta'_j = \begin{cases} \beta_i, & \text{если } j/d = i,\ \ i \in \{1, 2, ..., l-1\}, \\ 0, & \text{если } j/d \notin \{1, 2, ..., l-1\}. \end{cases}$$

Рассмотрим множество функций $\Phi = \left\{\varphi | \varphi : \{1, ..., d\} \to X^l\right\}$. Для каждого $\alpha = (\alpha_1, ..., \alpha_m) \in X^m$ положим $\psi : \alpha \to \varphi_\alpha$, где

$$\varphi_\alpha : i \mapsto \left(\alpha_i, \alpha_{i+d}, ..., \alpha_{i+(l-1)d}\right).$$

Очевидно, что ψ есть биекция между множествами Φ и X^m. Заметим, что

$$g_{h,k}^{-1} : (\alpha_1, ..., \alpha_m) \mapsto (\alpha_m - h(\alpha_1, ..., \alpha_{m-1}) - k, \alpha_1, ..., \alpha_{m-1}),$$

$$g_{h,0}^{-1} g_{h,k} = v_k^{(m,m)}.$$

Поэтому $v_k^{(m,m)} \in G^{(m)}(h)$. Очевидно, что $g_{h,k} = g_{h,k-\beta} v_\beta^{(m,m)}$ для всех $\beta, k \in X$.

Пусть 0 — нулевой элемент группы $(X, +)$, $\langle (d, d-1, ..., 1) \rangle$ – циклическая группа, порожденная циклом $\langle (d, d-1, ..., 1) \rangle$.

Основным результатом работы является следующая теорема.

Теорема 1. *Пусть $m \geq 3$, $d = d(h) > 1$, $l = l(h) \geq 1$, $m = l(h)d(h)$. Тогда:*

- *$\psi^{-1} G^{(m)}(h) \psi \leq G^{(l)}\left(h^{(d)}\right) \uparrow \langle (d, d-1, ..., 1) \rangle$, группа $G^{(m)}(h)$ подобна подгруппе экспоненцирования групп $G^{(l)}\left(h^{(d)}\right)$ и $\langle (d, d-1, ..., 1) \rangle$;*

- *группа*

$$Q = \left\langle g_{h,0}^{-j} v_\beta^{(m,m)} g_{h,0}^j, g_{h,0}^d | j \in \{0, ..., d-1\}, \beta \in X \right\rangle,$$

индуцирует на множествах

$$\Omega_i = \left\{(\delta_i, \delta_{i+d}, ..., \delta_{i+(l-1)d}) | (\delta_i, \delta_{i+d}, ..., \delta_{i+(l-1)d}) \in X^l\right\}$$

группы Q_i подобные $G^{(l)}\left(h^{(d)}\right)$, $i = 1, ..., d$;

- $Q \lhd G^{(m)}(h)$ *и* $G^{(m)}(h)/Q \cong \langle (d, d-1, ..., 1) \rangle$*;*
- *если* M *— минимальный нормальный делитель группы* $G^{(l)}\left(h^{(d)}\right)$*, содержащий элемент* $v_\beta^{(l,l)}$ *для каждого* $\beta \in X$*, то*

$$\left|G^{(m)}(h)\right| = d|M|^d \left|G^{(l)}\left(h^{(d)}\right)/M\right|;$$

- *группа* $G^{(m)}(h)$ *примитивна, если примитивна и нерегулярна группа* M*.*

Библиографические ссылки

[1] Погорелов Б.А. (1986). *Основы теории групп подстановок. Часть 1. Общие вопросы*. М.: в/ч 33965, 316 с.

[2] Caranti A., Dalla V.F., Sala M. (2008). On some block ciphers and imprimitive groups. http://arxiv. org/abs/math/0806.4135.

[3] Dixon J., Mortimer B. (1996). *Permutation groups*. Carleton University, 346 p.

[4] Paterson K.G. (1999). Imprimitive Permutation Groups and Trapdoors in Iterated Block Ciphers. *FSE'99, LNCS*. **1636**, pp. 201 – 214.

[5] Shingo Y., Tetsu I. (2011). On Permutation Layer of Type 1, Source-Heavy, and Target-Heavy Generalized Feistel Structures. *CANS 2011, LNCS*. **7092**, pp. 98 – 117.

ЭФФЕКТИВНАЯ МНОГОРАЗРЯДНАЯ АРИФМЕТИКА ДЛЯ ПАРАЛЛЕЛЬНОЙ МОДЕЛИ ВЫЧИСЛЕНИЙ

А.Н. Терещенко[1,a], В.К. Задиракa[1,b]
[1]*Института кибернетики НАН Украины*
Киев, УКРАИНА
e-mail: [a]teramidi@ukr.net, [b]zvk140@ukr.net

Работа посвящена реализации многоразрядной арифметики в параллельной модели вычислений. Для этого приведено описание модели параллельных вычислений. Дается описание путей оптимизации при построении алгоритмов в параллельной модели и приведены критерии эффективности, которым должны соответствовать такие алгоритмы. Приведены ограничения, которые нужно учитывать каждый раз, когда возникает необходимость задействовать большее число параллельных процессоров
Ключевые слова: многоразрядная арифметика; параллельная модель вычислений

1 Введение

Как известно, большая часть прикладных задач может быть разделена на меньшие задачи (подзадачи), что позволяет большую задачу привести к решению меньших по сложности задач. Существует много методов реализации и выполнения меньших задач на разных устройствах одновременно (большая часть таких методов является дублированием выполнения на разных процессорах или дублированием данных на разных процессорах). Наиболее сложной проблемой является локализация и оптимизация всех последовательных задач, то есть локализация и оптимизация шагов, которые не могут быть распараллелены. Последующей проблемой является реализация задачи в виде алгоритма для определенных устройств.

Первые попытки сформулировать критерии ускорения за счет использования параллельных вычислений относят к работе Джина Амдала [7]. В своей работе Амдал сформулировал закон, который утверждает, что небольшая часть программы, которая не поддаётся распараллеливанию, ограничит общее ускорение от распараллеливания. Для коэффициента ускорения S_p процесса в целом имеет место зависимость [7] $S_p = 1/(\alpha + \frac{1-\alpha}{p})$, где α – часть последовательных вычислений, p – количество процессоров. Зависимость S_p от доли последовательных вычислений и количества задействованных процессоров приведена на рис. 1.

Любая большая математическая или инженерная задача обычно будет состоять из нескольких частей, которые могут выполняться параллельно или только последовательно. Сформулированный закон определяет верхнюю границу полезности от увеличения количества процессоров в вычислительной системе. Амдал обосновал, что дополнительные усилия не дают никакого эффекта, если задача не

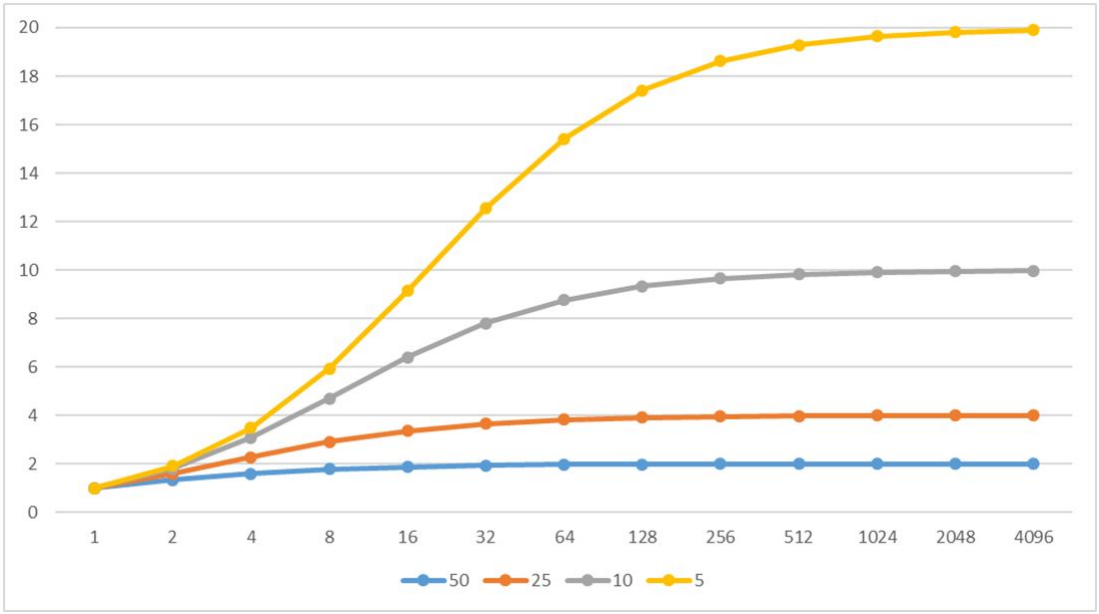


Рис. 1. Зависимость коэффициента ускорения от доли последовательных вычислений и количества задействованных процессоров

может быть распараллелена в последовательной части. На рис. 1 видно, что при общей доле в 5 процентов последовательных шагов, программа не может быть ускорена более чем в 20 раз, несмотря на количество задействованных процессоров. При разработке параллельных систем необходимо также учитывать время, необходимое для передачи данных между узлами. Зависимость времени вычислений от числа узлов будет иметь максимум, и с определенного момента добавление новых узлов в систему будет увеличивать время работы программы.

2 Параллельная модель вычислений

Под параллельной моделью вычислений рассматривается модель GPU (Graphics Processing Unit) видеокарты. Физически это отдельное устройство, которое устанавливается в компьютер дополнительно. GPU построена по технологии SIMD (Single Instruction–Multiple Data), где потоковые процессоры могут выполнять одну инструкцию одновременно, оперируя с различными данными. В такой модели GPU имеет собственную память, которая значительно быстрее памяти основного процессора. Иногда используют специальную (искусственно сгенерированную) модель вычислений, в которой рассматривается модель GPU основного процессора. Физически это отдельное ядро на основном процессоре. Такая модель отличается от модели GPU видеокарты тем, что она не имеет собственной памяти, а использует память основного процессора. В этой модели, с практической точки зрения, операции с памятью медленнее, чем в модели GPU видеокарты. С теоретической точки зрения анализ сложности алгоритмов в параллельной и специальной (искусственно сгенерированной) моделях вычислений дает одинаковые оценки.

Разделение на последовательную и параллельную модели вычислений связано с тем, что эффективность алгоритма зависит от максимального учета архитектурных особенностей вычислительной системы, для которой этот алгоритм реализуется. Так, например, алгоритмы реализации вычислений должны учитывать, что операции изменения содержимого любой ячейки памяти в последовательной и параллельной моделях вычислений выполняются только последовательно. А считывать содержмое ячейки памяти могут одновременно несколько пара разными процессорами в параллельной модели вычислений.

3 Пути оптимизации

Появление новых параллельных систем вызвало необходимость разработки нового программного обеспечения, которое должно было выполняться параллельно. Это было значительным импульсом к разработке новых параллельных алгоритмов (в отличие от традиционных последовательных алгоритмов) и их реализации для различных вычислительных систем. Появились алгоритмы и программные пакеты, способные работать на суперкомпьютерах и с данными большого размера.

В работах рассматривают пути оптимизации арифметических операций при построении алгоритмов в параллельной модели вычислений, а именно

1. Уменьшение связанных шагов за счет замены их более простыми и однотипными, но несвязанными операциями, что обычно увеличивает количество задействованных процессоров, но дает возможность уменьшить общее количество операций, выполняемых каждым из параллельных процессоров.

2. Уменьшение объема обрабатываемых данных, что позволяет уменьшить количество задействованных параллельных процессоров, сохраняя общее количество операций, выполняемых каждым из параллельных процессоров.

3. Использование резервов оптимизации вычислений (не увеличивая количество шагов алгоритма).

Приведенный перечень путей оптимизации не является исчерпывающим.

Распараллеливание арифметических операций можно осуществить, в основном, тогда, когда удается уменьшить количество сильно связанных между собой шагов, поэтому особое внимание уделяется первому методу оптимизации. Метод оптимизации за счет уменьшения общей разрядности входных данных используется, например, при реализации алгоритма многоразрядного умножения на основе быстрого преобразования Фурье (БПФ).

4 Критерии эффективности

Разработка эффективных параллельных алгоритмов для GPU невозможна без тщательного изучения этих алгоритмов для одного процессора. Эффективными алгоритмами в параллельной модели будут алгоритмы, при реализации которых:

- используется кэш-память максимально;
- построены на векторных операциях;

- задействуют небольшое число параллельных процессоров, чтобы уменьшить объем электроэнергии необходимой для выполнения многоразрядной операции.

Большая задача в параллельной модели вычислений разбивается на подзадачи для выполнения на одном процессоре, где вычисления рассматривается как вычисления в последовательной модели вычислений. Чем больше алгоритмов проанализировано для последовательной модели, тем больше вероятность того, что выбранная последовательная модель для каждого параллельного процессора при сохранении баланса между кэш-памятью, векторными операциями и количеством задействованных процессоров даст максимальный эффект.

5 Ограничения при реализации алгоритмов

Операция умножения является составляющей операции возведения в степень по модулю. От быстродействия операции умножения зависит быстродействие асимметричных криптографических программно-аппаратных комплексов. Если в последовательной модели вычислений именно общее число однословных операций умножения влияет на выбор метода реализации многоразрядной операции и общую оценку сложности, то переход в параллельную модель вычислений требует использования дополнительной логики для учета знака переноса, что увеличивает сложность вычисления не менее чем в два раза, хотя в последовательной модели знак переноса учитывается на лету (автоматически). Кроме того, знак переноса нужно учитывать и переносить между данными для разных процессоров.

Если при умножении двух 256-разрядных чисел задействовать 65536 параллельных процессоров, то сложность выполнения многоразрядной операции по количеству однословных операций умножения равна $O^*(N) = 1$. Т.е. каждый из 65536 процессоров выполнит только одну однословную операцию умножения. Это возможно только теоретически. На практике, чем больше параллельных процессоров задействуется, тем больше ограничений нужно учитывать. Если рассматривать GPU, то одним из первых ограничений является размер кэш-памяти рабочей группы процессоров. Вычисления на GPU разбиваются на группы процессоров. Каждая группа имеет свою кэш-память, которая значительно быстрее локальной или глобальной памяти GPU. Преимуществом кэш-памяти является то, что если хотя бы один процессор группы читает данные из локальной или глобальной памяти, то остальным процессорам нет необходимости выполнять операцию считывания с той же ячейки памяти. Данные считываются уже из кэш-памяти.

Следующим ограничением является число процессоров в рабочей группе, в которой все операций выполняются синхронно. При увеличении количества задействованных процессоров все вычисления необходимо разбивать на несколько рабочих групп, между которыми необходимо выполнять синхронизацию, которая является очень затратной операцией. При последующем увеличении параллельных процессоров возникает уже вопрос затрат энергии на выполнения одной многоразрядной операции, так как каждый задействованный процессор потребляет энергию. Также преимуществом GPU является то, что GPU поддерживает векторные операции, которые имеют ограничение по длине 2, 4, 8 и 16.

6 Вывод

Разнообразие существующих методов распараллеливания вычислений операций многоразрядной арифметики обусловлено отличием практических задач и устройств, для которых реализуются параллельные алгоритмы. Как следствие, это требует включения библиотеки программ, которая выполняет операции над многоразрядными числами, в штатное математическое обеспечение современных многопроцессорных систем с заданными характеристиками качества по точности и быстродействию. Существует проблема разработки универсальных алгоритмов реализации операций многоразрядной арифметики, которые выполнялись бы эффективно на различных устройствах и различных системах (последовательных и параллельных) для различной длины многоразрядных чисел.

Из этого следует, что оговоренные задачи являются недостаточно исследованными как с теоретической точки зрения, так и с точки зрения практического применения. Отдельной проблемой существующих подходов является сложность практической реализации. Таким образом, разработка новых, более эффективных по быстродействию алгоритмов выполнения операций многоразрядные арифметики в последовательной и параллельной моделях вычислений является актуальным научно-техническим заданием, что имеет важное прикладное значение.

Библиографические ссылки

[1] Анісімов А.В. (2001). *Алгоритмічна теорія великих чисел. Модулярна арифметика великих чисел.* Видавничий дім “Академперіодика”, 153 с.

[2] Задирака В.К. (1983). *Теория вычисления преобразования Фурье.* Наук. Думка, Киев, 213 с.

[3] Задірака В., Олексюк О. (2003). *Комп'ютерна арифметика багаторозрядних чисел.* Наукове видання, Київ, 263 с.

[4] Карацуба А.А., Офман Ю.П. (1962). Умножение многоразрядных чисел на автоматах. *ДАН СССР.* Т. 14, С. 293-–294.

[5] Николайчук Я.М., Возна Н.Я., Пітух І.Р. (2010). *Проектування спеціалізованих комп'ютерних систем.* Терно-Граф, Тернопіль, 392 с.

[6] Хіміч О.М. (2018). Суперкомп'ютерні технології та математичне моделювання складних систем. *Вісник НАНУ.* Т. 5, С. 69-–72.

[7] Gene M. Amdahl (1967). Validity of the single processor approach to achieving large-scale computing capabilities. *AFIPS Conf Proc.* V. **30**, P. 483-–485.

[8] Leighton F.T. (1992). *Introduction to Parallel Algorithms and Architectures: Arrays, Trees, Hypercubes*

РАЗРАБОТКА МЕТОДИКИ СТАТИСТИЧЕСКОГО ТЕСТИРОВАНИЯ ПСЕВДОСЛУЧАЙНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ С ПРИМЕНЕНИЕМ ЗАКОНА ПОВТОРНОГО ЛОГАРИФМА

А.И. Трубей[a], М.В. Мальцев[b], В.Ю. Палуха[c], И.К.Пиршток[d]
НИИ прикладных проблем математики и информатики
Белорусский государственный университет
Минск, БЕЛАРУСЬ
e-mail: [a]trubeia@mail.ru, [b]maltsew@bsu.by, [c]palukha@bsu.by, [d]pirshtuk@bsu.by

В статье исследуется возможность применения закона повторного логарифма для статистического тестирования генераторов псевдослучайных последовательностей. Разработана двухэтапная процедура проверки гипотез с применением закона повторного логарифма для теста Монобит с использованием статистики хи-квадрат согласия. Проведено тестирование известных физических и программных генераторов.
Ключевые слова: статистический тест; псевдослучайная последовательность; криптографическая стойкость; закон повторного логарифма

1 Введение

Для оценки качества генераторов, применяемых в целях защиты данных, часто используется набор тестов (батарея) NIST SP800-22 [4], чтобы обнаружить отклонения двоичной последовательности от модели независимых симметричных испытаний Бернулли. Однако батарея имеет существенные недостатки, связанные с ошибками 2 рода. Генератор, который, в основном, генерирует случайные последовательности, с вероятностью β будет также генерировать смещенные на некоторую величину Δ от равновероятного распределения последовательности (например, последовательности, состоящие, в основном, из нулей или единиц). При этом генератор будет оцениваться как «хороший» тестами NIST SP800-22, хотя выходные последовательности несложно отличить от равномерного распределения.

Кроме того, батарея не охватывает некоторые основополагающие законы случайности. Существуют две фундаментальные предельные теоремы о случайных двоичных последовательностях – это центральная предельная теорема и закон повторного логарифма (ЗПЛ). Несколько тестов в NIST SP800-22 включают центральную предельную теорему, в то время как ни один тест не охватывает закон повторного логарифма, который определяет (при некоторых условиях) точный порядок роста сумм независимых случайных величин при увеличении числа слагаемых.

В докладе авторы попытались восполнить данный пробел. В работе приводятся преимущества тестирования случайных последовательностей, основанные на статистических расстояниях и законе повторного логарифма [5,6]. Описывается методика принятия решений о качестве последовательностей на основе статистического расстояния с использованием статистики хи-квадрат согласия. В докладе также представлены результаты экспериментов по тестированию генераторов псевдослучайных последовательностей и физических генераторов, в ходе которых были выявлены слабости в некоторых обычно используемых генераторах псевдослучайных последовательностей и подтверждено удовлетворительное качество последовательностей, вырабатываемых физическими генераторами.

2 Тестирование генераторов псевдослучайных последовательностей. Батарея NIST SP800-22

Проведем сравнительное статистического тестирования генераторов псевдослучайных последовательностей и физических генераторов.

Линейный конгруэнтный генератор определяется рекуррентным соотношением $X_{n+1} = aX_n + c \ (\mod m)$, где X_n – последовательность псевдослучайных чисел, m – модуль, $a, c < m$.

Для любого начального значения X_0 псевдослучайная последовательность имеет вид $X_0,\ X_1, \ldots, X_i \ldots$, где X_i – двоичное представление целого числа X_i.

Линейные конгруэнтные генераторы были включены в различные языки программирования, например, в C и C++. Функции drand48(), lrand48(), mrand48() и rand48() генерируют равномерно распределенные случайные числа по формуле:

$$X_{n+1} = \text{0x343FD} \cdot X_n + \text{0x269EC3} \ (\mod 2^{32}) \text{ (выбираются 16–30 биты)}.$$

В компьютерных экспериментах использовались двоичные последовательности, полученные с помощью линейного конгруэнтного генератора, используемого в Microsoft Visual C++ с указанными выше параметрами. В дальнейших экспериментах используются последовательности, состоящие из 7–14 бит чисел X_n

Были проведены две сессии тестирования с количеством выборок 1000 и 5000, а также следующими параметрами тестирования:

– объём выборки – 10^6 бит (125 000 байт);

– уровень значимости на первом этапе – 0,01;

– уровень значимости на втором этапе – 0,0001;

В результате было установлено:

– при числе выборок 1000 – тестирование пройдено успешно;

– при числе выборок 5000 – тестирование пройдено успешно.

Для сравнения было проведено также тестирование последовательностей, выработанных физическим генератором на основе шумового диода «Ключ-04», которое также не выявило отклонений от нулевой гипотезы.

3 Закон повторного логарифма

Первый вариант усиленного закона больших чисел был сформулирован и доказан Э. Борелем применительно к схеме Бернулли. Пусть независимые случайные величины $X = (x_1, \ldots, x_n)$ одинаково распределены и принимают два значения 0 и 1 с вероятностью 1/2. Тогда $S_n = \sum_{i=0}^{n-1} x_i$ есть число успехов в схеме Бернулли с вероятностью успеха 1/2. Э. Борель доказал, что $S_m/n \to 1/2$ при $n \to \infty$ с вероятностью 1.

Впоследствии (1914) Г. Харди и Дж. Литлвуд (G. Hardy, J. Littlewood) показали, что почти наверное

$$\lim_{\mathrm{n}\to\infty} \sup \frac{\left|S_n - \frac{n}{2}\right|}{\sqrt{n \ln n}} < \frac{1}{\sqrt{2}}.$$

Затем А. Я. Хинчин (1924) доказал более сильный результат, называемый законом повторного логарифма [3]:

$$P\left(\lim_{n\to\infty} \sup \frac{\left|S_n - \frac{n}{2}\right|}{\sqrt{n \ln \ln n}} = \frac{1}{\sqrt{2}}\right) = 1. \tag{1}$$

В более общем виде закон повторного логарифма можно сформулировать следующим образом. Если задана схема независимых испытаний Бернулли (p – вероятность положительного исхода в одном испытании, $1 - p$ – вероятность отрицательного исхода), также справедлива формула:

$$\lim_{n\to\infty} \sup \frac{\frac{S_n - np}{\sqrt{np(1-p)}}}{\sqrt{2 \ln \ln n}} = \lim_{n\to\infty} \sup \frac{S_n - np}{\sqrt{2np\,(1-p) \ln \ln n}} = 1. \tag{2}$$

Закон повторного логарифма занимает промежуточное положение между законом больших чисел и центральной предельной теоремой. Дальнейшие существенные продвижения в исследовании условий приложения закона повторного логарифма связаны с работами А. Н. Колмогорова (1929) и В. Феллера (1943) [2]. Экспериментальная иллюстрация закона повторного логарифма представлена на рисунке 1.

4 Статистические процедуры множественной проверки гипотез

Многие криптографические задачи (например, генерация ключей, анализ стойкости криптографических алгоритмов) требуют применения статистических критериев для обнаружения большого числа отклонений от гипотетической модели (например, от модели независимых симметричных испытаний Бернулли). Каждый статистический критерий предназначен для проверки конкретной гипотезы H_0 и позволяет выявить только определенные типы отклонений от H_0. Поэтому для проверки набора гипотез и увеличения точности обнаружения альтернативных

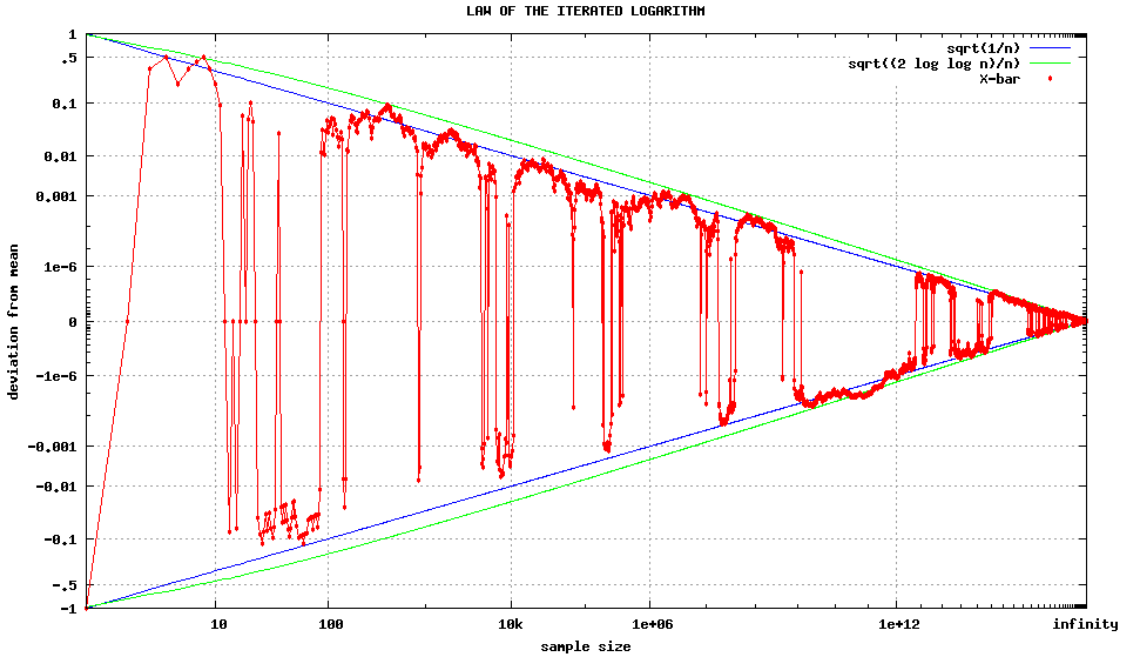


Рис. 1. Экспериментальная иллюстрация закона повторного логарифма

гипотез при статистическом тестировании последовательностей следует использовать определенный набор статистических критериев, а для принятия итогового решения – процедуры множественной проверки гипотез.

Одноэтапные процедуры, в первую очередь, предназначены для проверки качества тестируемой выборки. К недостаткам одноэтапных процедур можно отнести слабо поддающееся контролю уменьшение вероятности ошибки 1 рода α и мощности. Двухэтапные процедуры позволяют увеличить мощность критерия и удерживать вероятность «ложной тревоги» на должном уровне.

Каждый одноэтапный тест предоставляет одно или несколько p-значений. Двухэтапные тесты измеряют однородность полученных p-значений для фиксированного одноэтапного теста. Двухэтапный тест часто более эффективен, чем одноэтапный, но иногда он отклоняет даже «хорошие» генераторы, когда размер выборки на втором этапе слишком велик, поскольку он обнаруживает ошибки аппроксимации при вычислении p-значений.

5 Статистика закона повторного логарифма для теста Монобит

Очевидно, что бинарную последовательность можно представить в виде реализации схемы Бернулли. Для последовательности $x \in \Sigma^n$определим:

$$S(n) = \sum_{\mathrm{i}=0}^{\mathrm{n}-1} x_i;\ S(n)^* = \frac{2S(n) - n}{\sqrt{n}}, \tag{3}$$

где Σ^n – множество двоичных последовательностей длины n.

Вспомним, что закон больших чисел, справедливый для бесконечного значения n, по существу, говорит о невероятности отклонения экспериментально наблюдаемого числа κ от математического ожидания этой величины. В нашем случае он гласит, что для случайной последовательности x: $S_m/n \to 1/2$, что соответствует частотному тесту (Монобит) в NIST SP800-22.

Закон повторного логарифма дает оптимальную верхнюю оценку $\sqrt{2\ln\ln n}$ для колебаний $S(n)^*$. Основываясь на этом факте, мы будем использовать следующую статистику:

$$S_{\text{зпл}}(n) = \frac{S(n)^*}{\sqrt{2\ln\ln n}} = \frac{2S(n) - n}{\sqrt{2n\ln\ln n}}. \tag{4}$$

Случайные последовательности удовлетворяют общим статистическим законам, в том числе закону повторного логарифма. В соответствии с предельной теоремой Муавра-Лапласа для заданных z_1 и z_2:

$$\lim_{n\to\infty} P\ [z_1 \le S(n)^* \le z_2] = \Phi(z_2) - \Phi(z_1).$$

Скорость роста в указанном приближении ограничена $\max\left\{\frac{k^2}{n^2}, \frac{k^4}{n^3}\right\}$, где $k = S(n) - \frac{n}{2}$. То есть:

$$|\,[z_1 \le S(n)^* \le z_2] - (\Phi(z_2) - \Phi(z_1))\,| \le \max\left\{\frac{k^2}{n^2}, \frac{k^4}{n^3}\right\} \text{ для всех } n > 0$$

.

Распределение, порожденное $S_{\text{зпл}}(n)$, определяет вероятностную меру на вещественной прямой $\mathbb{R}$. Пусть $\mathcal{R} \in \Sigma^n$ – набор из m последовательностей со стандартным определением вероятности на нем. То есть, для каждой последовательности $x_0 \in \mathcal{R}$ положим $P[x = x_0] = 1/m$. Тогда каждый набор $\mathcal{R} \in \Sigma^n$ порождает вероятностную меру $\mu_n^{\mathcal{R}}$ на R

$$\mu_n^{\mathcal{R}}(I) = P[S_{\text{зпл}}(n) \in I, x \in \mathcal{R}]$$

для каждого измеримого по Лебегу множества I на $\mathbb{R}$. Для U =Σ^n введем μ_n^U – соответствующую вероятностную меру, порожденную равномерным распределением.

Для случайной последовательности распределение статистики $S(n)^*$ может быть аппроксимировано нормальным распределением с математическим ожиданием 0 и дисперсией 1 с ошибкой, не превышающей $1/n$. Другими словами, меру μ_n^U можно рассчитать следующим образом:

$$\mu_n^U\{(-\infty, z]\} = \Phi\left(z\sqrt{2\ln\ln n}\right) = \sqrt{\Phi\ln\ln n}\int_{-\infty}^{z}\Phi\left(y\sqrt{2\ln\ln n}\right)dy. \qquad (5)$$

6 Процедура принятия решения

На первом этапе двухэтапной процедуры по каждой выборке вычисляется статистика критерия. На втором этапе по полученной на первом этапе последовательности значений статистик, как правило, проверяется гипотеза согласия с теоретическим распределением статистики. Таким образом, двухэтапные процедуры позволяют избегать грубых ошибок при принятии/отвержении гипотезы H_0.

Мы будем проверять гипотезу согласия последовательности значений статистики $S_{\text{зпл}}(n)$ с нормальным распределением на вещественной прямой $\mathbb{R}$ $(-\infty, \infty)$. Процедура принятия решения основана на критерии χ^2 согласия. Для построения критерия χ^2 будем использовать в качестве дискретного разбиения вещественной прямой $\mathbb{R}$ множество $\mathcal{B}$, определяемое следующим образом:

$$\mathcal{B} = \cup I = \{(-\infty, -1), [1, \infty)\} \cup \{[0.05r - 1,\ 0.05r - 0.95) : 0 \le r \le 39\}. \qquad (6)$$

На основании формулы (5) на рисунке 2 приведены функции плотности распределений μ_n^U для различных объемов выборок.

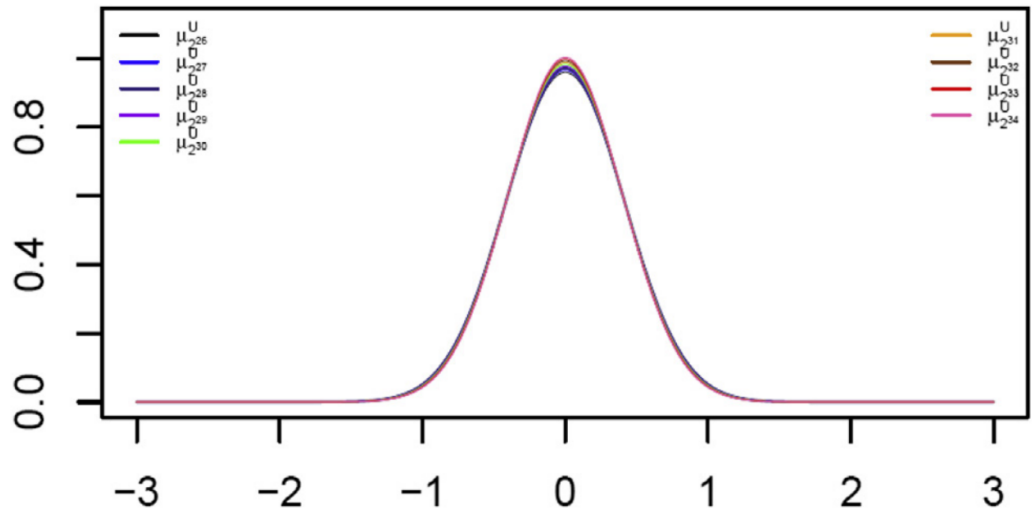


Рис. 2. Функции плотности распределений μ_n^U

Чтобы оценить генератор G с применением закона повторного логарифма для теста Монобит, необходимо:

1. Осуществить генерацию набора $\mathcal{R} \in \Sigma^n$ из $m = 10\ 000$ последовательностей возможно большей длины.

2. На первом этапе двухэтапной процедуры проверки гипотез вычислить значения статистики $S_{\text{зпл}}(n)$ по всем m последовательностям.

3. На втором этапе двухэтапной процедуры проверки гипотез сравнить между собой вероятностные меры $\mu_n^{\mathcal{R}_n}$ и μ_n^U. Для сравнения будем использовать следующую статистику χ^2 согласия [1]:

$$\chi^2 = \sum_{j=1}^{|\mathcal{B}|} \frac{\left[v_n^{\mathcal{R}_n}(I_j) - mp_n^{\mathrm{U}}(I_j)\right]^2}{mp_n^{\mathrm{U}}(I_j)}, \tag{7}$$

где $v_n^{\mathcal{R}_n}(I_j)$ – частоты попадания значений статистики $S_{\text{зпл}}(n)$ в интервал I_j по всем m последовательностям; $p_n^{\mathrm{U}}(I_j)$ – теоретические вероятности попадания $S_{\text{зпл}}(n)$ в интервал I_j. То есть, необходимо проверить гипотезу о том, что выборка

$$\left\{v_n^{\mathcal{R}_n}(I_1), \ldots, v_n^{\mathcal{R}_n}(I_j), \ldots, v_n^{\mathcal{R}_n}\left(I_{\lfloor\mathcal{B}\rfloor}\right)\right\}$$

извлечена из некоторой нормальной совокупности с математическим ожиданием 0 и среднеквадратичным отклонением $\sigma = \frac{1}{\sqrt{2\ln\ln n}}$.

Полагаем, что генератор G прошел тестирование по тесту Монобит с применением закона повторного логарифма, если P-значение статистики χ^2 согласия превышает заданный уровень значимости α, то есть, $P \geq \alpha$.

7 Экспериментальные результаты

Для проверки гипотезы проведено тестирование 10 000 последовательностей, выработанных соответственно линейным конгруэнтным генератором и физическим генератором «Ключ-ВС». Результаты сравнений выборок, полученных в результате применения закона повторного логарифма, с нормальным распределением по критерию χ^2 согласия приведены в таблице 1.

Из таблицы 1 видно, что для **всех** последовательностей (объемом от 0.5 GB до 10 GB), выработанных физическим генератором, выполняется гипотеза H_0 согласия с моделью независимых симметричных испытаний Бернулли на уровне значимости $\alpha = 0.01$. В то время как последовательности, вырабатываемые линейным конгруэнтным генератором, согласуются с моделью независимых симметричных испытаний Бернулли только при объемах от 0.5 GB до 4 GB. Для последовательностей большего объема (5 GB, 10 GB) гипотеза H_0 не выполняется. Причем с увеличением объема статистическое расстояние (статистика χ^2) постепенно увеличивается. Хотя при этом P-значения статистик стандартного теста Монобит для всех объемов последовательностей согласуются с гипотезой H_0 на уровне значимости $\alpha = 0.01$. Это означает, что уязвимости, характерные для линейного конгруэнтного генератора, проявляются только в последовательностях, объемом не

Таблица 1 Результаты тестирования последовательностей, выработанных ЛКГ и физическим генератором «Ключ-ВС»

Объем (GB)	ЛКГ		«Ключ-ВС»	
	29 степ. свободы (объед. групп)		29 степ. свободы (объед. групп)	
	χ^2	P-знач.	χ^2	P-знач.
0.5 GB	29,97	0,4151	25,72	0,6402
1 GB	23,28	0,7631	30,88	0,3708
2 GB	18,82	0,9256	41,30	0,0647
3 GB	23.59	0,7488	30,22	0,4028
4 GB	30.37	0,3956	32,76	0,2876
5 GB	59.79	0,0006	22.78	0,7864
10 GB	98.98	$3{,}8\text{e}^{-10}$	27,40	0,4423

менее 5 GB и традиционным тестом Монобит не выявляются (P-значение данного теста для последовательности объемом 5 GB равно 0.971, то есть справедлива нулевая гипотеза).

В настоящее время существует немало генераторов псевдослучайных последовательностей, реализованных в соответствии с различными принципами (в основном – на базе блочных криптоалгоритмов, функций хеширования и т.д.). Поэтому с целью проверки качества таких генераторов было также проведено тестирование псевдослучайных последовательностей (объемом 5 GB и 10 GB), сгенерированных в соответствии с разработанным сотрудниками НИИ ППМИ стандартом СТБ 34.101.47-2012 (в режиме счетчика. Результаты сравнений выборок, полученных в результате применения закона повторного логарифма, с нормальным распределением по критерию χ^2 согласия приведены в таблице 2.

Таблица 2 Результаты тестирования последовательностей, выработанных в соответствии с СТБ 34.101.47-2012 (в режиме счетчика)

Объем (GB)	Степ. своб. (объед. групп)	χ^2	P-знач.	Степ. своб.	χ^2	P-знач.
5 GB	29	25,90	0,6303	41	37,03	0,6474
10 GB	27	23,36	0,6650	41	38,52	0,5812

Из таблицы 2 видно, что для последовательностей (объемом 5 GB и 10 GB), сгенерированных в соответствии с СТБ 34.101.47-2012 (в режиме счетчика), как и для физического генератора «Ключ-ВС», выполняется гипотеза H_0 согласия с моделью независимых симметричных испытаний Бернулли на уровне значимости $\alpha = 0.01$. Это означает, что в алгоритме генерации псевдослучайных последовательностей слабостей не выявлено. То есть этот алгоритм, в отличие от линейного конгруэнтного генератора, является криптографически стойким.

Разработанная методика тестирования последовательностей с применением статистического расстояния и закона повторного логарифма в дальнейшем позволит повысить полноту и качество проводимых тематических исследований СКЗИ, в особенности, при проектировании и разработке новых генераторов случайных последовательностей.

Гистограммы частот выборок, полученных с применением закона повторного логарифма, для линейного конгруэнтного генератора, физического генератора «Ключ-ВС» и алгоритма генерации псевдослучайных последовательностей в соответствии с СТБ 34.101.47-2012, построенные с использованием программы «Статистика», приведены на рисунках 3 – 6.

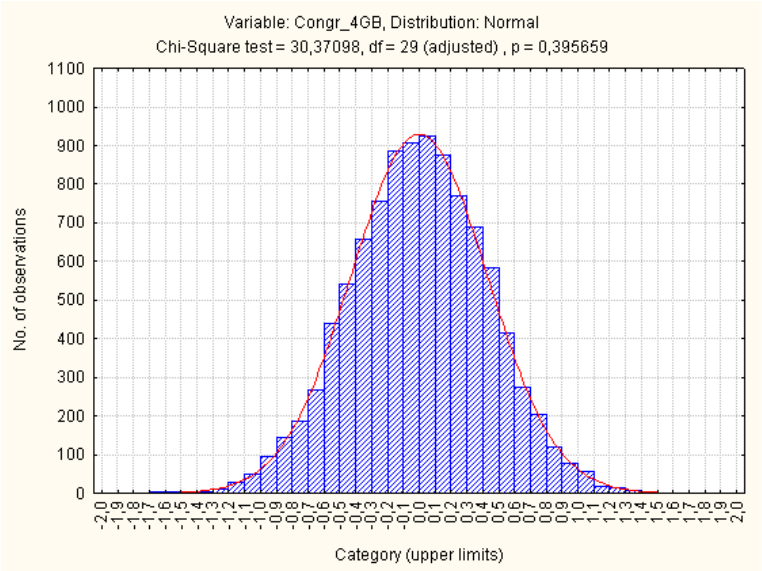


Рис. 3. Гистограмма частот линейного конгруэнтного генератора, 4 GB (после объединения групп)

8 Заключение

1. Установлено, что уязвимости в некоторых часто используемых реализациях генераторов псевдослучайных последовательностей не выявляются инструментами тестирования NIST SP800-22, в основном, из-за недостаточной длины тестируемых последовательностей.

2. Разработана двухэтапная процедура проверки гипотез с применением закона повторного логарифма для теста Монобит с использованием статистики хи-квадрат согласия.

3. Проведено тестирование последовательностей большого объема, сгенерированных линейным конгруэнтным генератором, а также физическим генератором на основе шумового диода «Ключ-ВС» по тесту Монобит. При этом

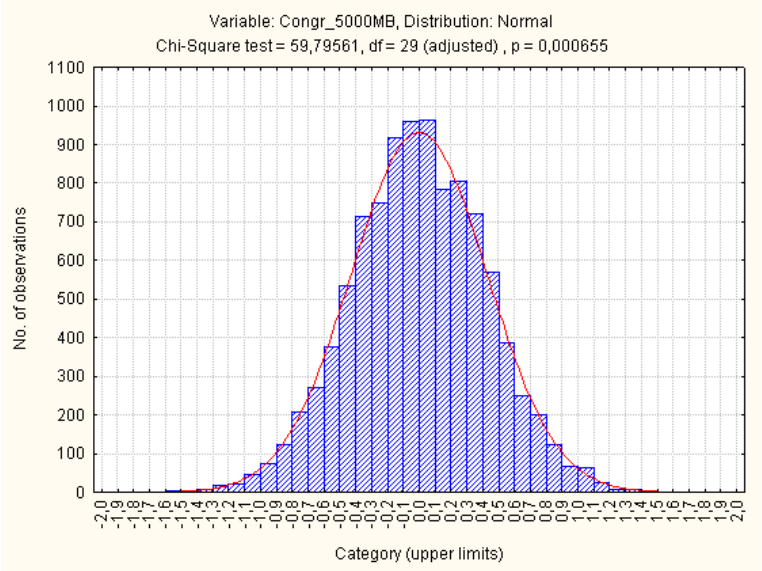


Рис. 4. Гистограмма частот линейного конгруэнтного генератора, 4 GB (после объединения групп)

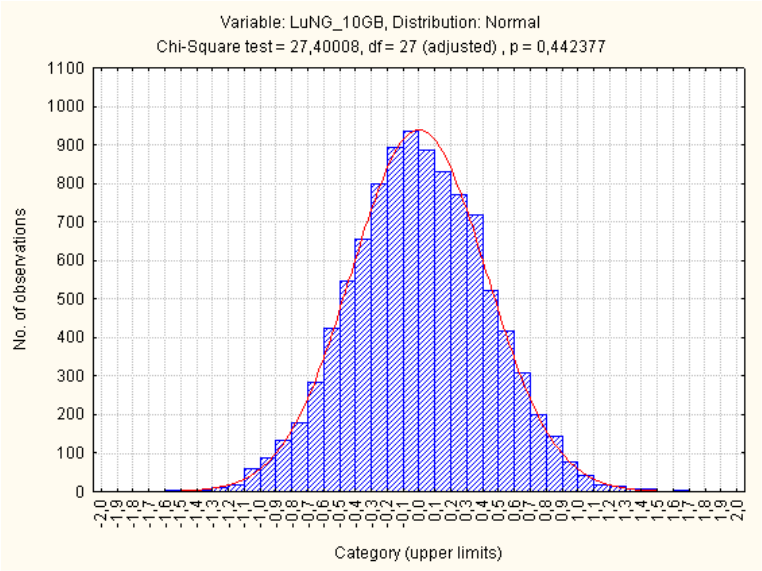


Рис. 5. Гистограмма частот физического генератора «Ключ-ВС», 10 GB (после объединения групп)

физический генератор успешно прошел тестирование, а линейный конгруэнтный генератор тестирование провалил.

4. Тестирование с применением закона повторного логарифма показало, что алгоритм генерации псевдослучайных последовательностей согласно СТБ 34.101.47-2012 (в режиме счетчика) является криптографически стойким при

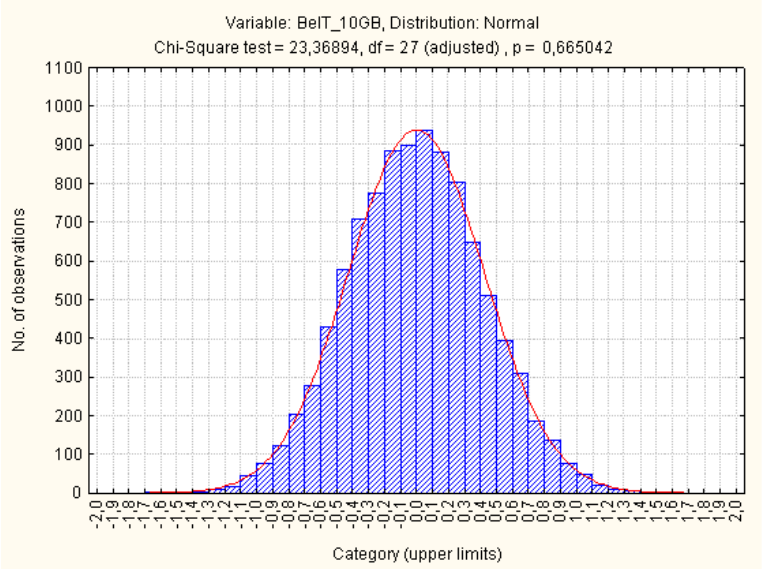


Рис. 6. Гистограмма частот алгоритма СТБ 34.101.47-2012, 10 GB (после объединения групп)

атаке с применением закона повторного логарифма для теста Монобит.

Библиографические ссылки

[1] Крамер, Г. *Математические методы статистики* / Г. Крамер – М.: Мир, 1976.

[2] Feller, W. *Introduction to probability theory and its applications, vol. I.* New York: John Wiley & Sons, Inc.; 1968.

[3] Khintchin, A. Über einen Satz der Wahrscheinlichkeitsrechnung / *Fundamenta Mathematicae.* – 1924. – 6. – P. 9–20.

[4] Rukhin, A. et al. *A statistical test suite for random and pseudorandom number generators for cryptographic applications NIST Special Publication 800-22*, 2010.

[5] Wang, Y. *On the Design of LIL Tests for (Pseudo) Random Generators and Some Experimental Results* / Dept. SIS, UNC Charlotte Charlotte, NC 28223, USA. – [Electronic resource]. – 2014. – Mode of access: https://arxiv.org/abs/1401.3307. – Date of access: 01/03/2020.

[6] Wang, Y., Nicol, T. On statistical distance based testing of pseudorandom sequences and experiments with PHP and Debian OpenSSL / *Computers & Security.* – Volume 53. – September 2015. – P 44–64.

ИСПОЛЬЗОВАНИЕ СИСТЕМНЫХ СВОЙСТВ И ПАРАМЕТРОВ ТЕКСТОВЫХ ФАЙЛОВ В СТЕГАНОГРАФИЧЕСКИХ ПРИЛОЖЕНИЯХ

П. П. Урбанович, Д. Э. Юрашевич[b]
Белорусский государственный технологический университет
Минск, БЕЛАРУСЬ
e-mail: [a]pav.urb@yandex.by, [b]dima.yurashevich32155@gmail.com

Стеганографические методы и инструментальные средства применяются для хранения и/или передачи скрытой информации. При использовании электронных текстовых документов в качестве контейнеров скрытое размещение такой информации обычно основывается на модификации цветовых или пространственно-геометрических параметров символов текста-контейнера. В статье исследуются и анализируются системные свойства и параметры электронных текстовых документов как потенциальных элементов стеганографической системы, в которые осаждается тайная информация. Основная задача исследования – оценка стеганографической стойкости текста-контейнера при модификации указанных свойств и параметров файлов в процессе осаждения тайной информации.
Ключевые слова: защита информации; текстовая стеганография; системные свойства и атрибуты фалов; стеганографическая стойкость

1 Введение

Проблема зашиты информации и защиты авторских прав в IT-сфере приобретает все большую актуальность. Одно из направлений решения проблемы предусматривает использование стеганографии, которая, в отличие от криптографии, основана даже на сокрытии самого факта использования преобразования [3,4]. Вместе с тем известно, что моделирование стеганографических и криптографических систем основывается на тех же базовых принципах [4,5,11].

Современная стеганография, как правило, «имеет дело» с электронными средствами. Это может объясняться следующими причинам. Во-первых, так как объем осаждаемой информации, как правило, довольно небольшой по сравнению с размером контейнера, в котором она будет скрыта, то в электронные контейнеры гораздо проще скрывать данные и извлекать их. Во-вторых, процедура осаждения/извлечения может быть автоматизирована с помощью специальных программных средств. В-третьих, электронный формат данных характеризуется информационной избыточностью, которой можно управлять, чтобы скрыть сообщения. Эти общие для всех электронных документов особенности, на наш взгляд, ставят знак равенства между цифровой и компьютерной стеганографией.

Основу электронного контента составляют текстовые документы, базы данных, коды компьютерных программ, а также объекты мультимедиа. Защита указанных средств от подделки или несанкционированного использования стеганографическими методами предусматривает выполнение нескольких важных условий.

К основным из них относят трудность обнаружения отличий между параметрами исходного (пустого) файла-контейнера и стеганоконтейнера – файла с осажденной информацией, а также устойчивость (неизменность) осажденной в контейнер информации при его модификации. Оба указанных условия относятся к известной характеристике методов рассматриваемого класса – стеганографической стойкости.

Для стеганоконтейнеров в виде текстовых файлов разработаны методы осаждения/извлечения тайной информации (или цифровых водяных знаков), основанные на модификации различных пространственно-геометрических (пробелы между словами, пробелы меду строками, использование невидимых символов, модификация апроша, кернинга, масштаба и др.) или цветовых параметров символов текста на основе RGB-модели [2,3,4,7,8,9,10].

На сегодняшний день задача поиска методов преобразования контейнеров, в том числе – текстовых, и встраивания в них тайной информации по-прежнему является актуальной. Часто наиболее устойчивые к атакам стеганоалгоритмы не позволяют встроить достаточный объем секретной информации в файл-контейнер. Разработка таких алгоритмов встраивания, которые, с одной стороны, повышают стеганостойкость системы, а с другой – сохраняют объем осажденных секретных данных, может быть отнесена к числу важных задач.

Одно из новых направлений в анализируемой предметной области связано с использованием так называемых альтернативных потоков файловой системы NTFS [1]. При этом стеганографическое преобразование не затрагивает собственно содержимое файла-контейнера. В настоящей статье анализируются особенности и возможности использования подхода на основе альтернативных потоков данных в приложении к текстовым документам-контейнерам. Здесь аналогом альтернативных потоков служат системные свойства и параметры файлов.

2 Системные свойства и параметры текстового файла

В качестве объекта исследования использовался файл с расширением DOCX. Причем для получения и анализа его свойств и параметров файл не должен быть пустым. Исследования проводились с использованием библиотеки *Microsoft. WindowsAPICodePack.Shell.*

Встроенные средства ОС *Windows* позволяют обычному пользователю получить информацию о следующих системных свойствах и параметрах:

- свойства описания: *название*, *тема*, *теги*, *категории*, *комментарии*;
- свойства источника: *авторы*, *кем сохранен*, *редакция*, *номер версии*, *имя программы*, *организация*, *руководитель*; *дата создания содержимого*, *дата последнего сохранения*, *последний вывод на печать*, *общее время редактирования*

- свойства содержимого: *состояние содержимого*, *тип содержимого*, *количество страниц*, *количество слов*, *количество знаков*, *количество строк*, *количество абзацев*, *шаблон*, *шкала*, *ссылки*, *язык*;

- свойства файла: *размер*, *дата создания*, *дата изменения*, *дата доступа*, *доступность*, *автономность*, *компьютер*.

Из числа приведенных свойств поддерживают модификацию следующие 13: *язык*, *тип содержимого*, *состояние содержимого*, *руководитель*, *организация*, *номер версии*, *редакция*, *авторы*, *комментарии*, *категории*, *теги*, *тема*, *название*.

Для выявления и анализа других свойств и параметров файла разработана программная реализация метода, принимающего в качестве параметра путь доступа к документу. Метод возвращает лист пар ключ–значение. Методом создаются переменные, которые представляют собой набор родительских элементов, которые, в свою очередь, содержат дочерние системные свойства и параметры. В данном методе также используется вызов другого метода, принимающего на вход объект родителя системных свойств для заполнения результирующего листа полученными ключ–значениями. В результате нами выявлено 208 свойств. Каждое значение свойства обладает своим типом данных. Этот тип данных не является уникальным. Указанные свойства по принадлежности к типу данных распределены следующим образом: *String* – 83, *UInt32* – 26, *Boolean* – 23, *String[]* – 23, *DateTime* – 13, *Object* – 12, *UInt16* – 8, *UInt64* – 8, I*nt32* – 5, *IntPtr* – 3, *Byte[]* – 2, *IntPtr[]* – 1, *IStream* – 1.

Для получения свойств, основанных на родительском свойстве, использовался метод, обладающий модификатором доступа «private» и не возвращающий никакого значения. Это обусловлено теми обстоятельствами, что его роль заключается в получении и заполнении переменной листа, и доступ к методу должен осуществляться исключительно из метода, находящегося в одном классе с данным методом.

Родительские свойства логически объединяют некоторые системные свойства. Все нижеперечисленные свойства описаны в классе *ShellProperties*. Данный класс определяет другой класс, который реализует вспомогательные методы для извлечения свойств оболочки, используя каноническое имя, ключ свойства или строго типизированное свойство. Он также обеспечивает доступ ко всем строго типизированным системным свойствам и коллекциям свойств по умолчанию.

Для модификации свойств, подразумеющей стеганографическое осаждение информации, разработано специальное приложение, функционал которого заключается в том, что оно обрабатывает действие нажатия на кнопку изменения свойств. При этом проводится проверка на валидность ввода данных.

3 Анализ результатов модификации системных свойств и параметров файла-контейнера

Выявлено, что не все свойства допускают возможностью их изменения. К ним относятся: *ItemFolderPathDisplay*, *ItemType*, *ParsingPath*, *FileName*. При попытке

модификации такого свойства файл не завершает свою работу ошибкой, а работает в штатном режиме. Однако есть такие свойства, при изменении которых документ утратит свою работоспособность (например, свойство *ItemNameDisplay*).

Кроме модификации свойств файла изменениям подвергались его атрибуты: *Archive*, *Compressed*, *Device*, *Directory*, *Encrypted*, *Hidden*, *IntegrityStream*, *Normal*, *NoScrubData*, *NotContentIndexed*, *Offline*, *ReadOnly*, *ReparsePoint*, *SparseFile*, *System*, *Temporary*. Для изменения атрибута документа был разработан метод, позволяющий производить необходимые манипуляции.

Проверка хеш-суммы. Хеш вычислялся с использованием стандартных алгоритмов MD5 и SHA256. Для реализации проверки была использована библиотека C# *System.Security.Cryptography*. При этом вычисления были основаны на использовании разработанного метода, принимающего на вход в качестве параметра массив байтов, а затем из массива байтов формирующего строку. Значение атрибута устанавливается в *Archive*.

Установлено, что изменение любого из свойств документа влечет за собой изменение хеш– суммы, изменение атрибута документа не влияет на его хеш. Кроме того, переформатирование файла (DOCX, DOC, TXT) также не изменяет хеш.

Проверка объема файла. Для подтверждения корректности оценки объема файла при использовании модификаций их свойств использовались два метода: с помощью объекта класса *FileInfo* и с объекта класса *ShellFile*. Нами анализировались следующие текстовые свойства: *Comment*, *Copyright*, *FileDescription*, *FileVersion*, *FullText*, *IdentityProperty*, *InfoTipText*, *InternalName*, *ItemClassType*, *ItemFolderNameDisplay*, *ItemNamePrefix*, *ItemUrl*, *KindText*, *Language*, *MileageInformation*, *MIMEType*, *OriginalFileName*, *OwnerSid*, *ParentalRating*, *ParentalRatingsOrganization*, *ParsingName*, *PriorityText*, *Project*, *ProviderItemID*, *RatingText*, *SensitivityText*, *SoftwareUsed*, *SourceItem*, *Status*, *Subject*, *Title*, *Trademarks* – всего – 32.

В результате многочисленных опытов и сопоставительного анализа получены следующие основные результаты:

- свойства *Title*, *Language*, *Subject* типа *String* допускают запись в значение свойства без изменения размера документа до 444 символов латинского алфавита, знаков препинания и знаков пробелов;

- свойство *Comment* допускает запись 464 символов латинского алфавита, знаков препинания и пробелов без изменения размера документа;

- первое изменение значения всех системных свойств (кроме 4-х вышеперечисленных) влечет за собой изменение размера документа-контейнера, в котором производится такое изменение; причем увеличение размера документа происходит таким образом, что этот показатель увеличивается каждые 12–20 операций по модификации свойств: например, первое изменение свойства *Copyright* приводит к увеличению объема файла сразу увеличивается на 610 байт, затем изменения не наблюдаются в течении 12 модификаций, после чего объем файла возрастает в среднем на 250 байт;

- выявлена зависимость чувствительности объема файла при модификации некоторых свойств от алфавита, на основе которого генерируется осаждаемая информация: так, например, свойство *Comment* даже при размещении в нем 5000 арабских цифр не сказывается на объеме файла;

- любая модификация свойства на основе данных типа *Bool* приводит к изменению объема файла.

4 Обсуждение результатов

Предлагается использовать системные свойства текстовых документов-контейнеров в качестве среды для осаждения тайной информации стеганографическими методами, наряду с известным использованием собственно содержимого документа. Для документов, созданных на основе процессора MS Word, выявлено существование более 200 различных системных свойств, содержание многих из которых нельзя извлечь и проанализировать встроенными стандартными средствами операционной системы и используемого приложения MS Word.

К числу наиболее подходящих для использования в стеганографических приложениях следует отнести такие свойства фалов, как *Title*, *Language*, *Subject, Comment*, модификация которых путем размещения (осаждения) дополнительно до 50 байт информации типа *String* не приводит к увеличению объема файла. Важно также, что изменение любого атрибута файла (*Archive*, *Compressed*, *Device*, *Directory*, *Encrypted*, *Hidden* и др.) также не может выявлено в процессе стеганоанализа файла-контейнера на основе, например, сопоставления объемов и хешей исходного и модифицированного (с осажденной информацией) файлов.

Со всей очевидностью можно утверждать, что предложенный подход может быть реализован не только по отношению к файлам текстовых форматов.

Доступ к системным свойствам файлов и их атрибутов, а также анализ параметров свойств и атрибутов при выполнении описанных стеганографических операций производился с использованием авторского программного продукта [6].

Библиографические ссылки

[1] Колмаков М. В., Блинова Е.А. (2018). Особенности применения стеганографических методов в альтернативных потоках файловой системы NTFS. *Информационные технологии: тезисы докладов 82-й МНТК БГТУ*. БГТУ, Минск. С. 23–24.

[2] Сущеня А. А., Блинова Е.А., Урбанович П.П. (2018). Модификация стеганографического метода изменения междустрочного расстояния электронного документа. *Технические средства защиты информации: тезисы докладов XVI Белорусско-российской научно-технической конференции, Минск, 5 июня 2018 г.* БГУИР. Минск. С. 90.

[3] Урбанович П. П. (2016). *Защита информации методами криптографии, стеганографии и обфускации: учеб.-метод. пособие для студ.* БГТУ, Минск.

[4] Харин Ю. С., Берник В. И., Матвеев Г. В., Агиевич С. В. (2003). *Математические и компьютерные основы криптологии.* Новое Знание, Минск / Москва.

[5] Шутько Н. П., Романенко Д. М., Урбанович П. П. (2015). Математическая модель системы текстовой стенографии на основе модификации пространственных и цветовых параметров символов текста. *Труды БГТУ.* № 6 (179), С. 152–156.

[6] Юрашевич Д.Э., Урбанович П.П. *Прикладное программное обеспечение для сокрытия информации в текстовых документах.* Государственный реестр информационных ресурсов РБ. Регистрационное свид. № 1142022658 от 28.05.2020.

[7] Brassil J.T., Low S., Maxemchuk N.F., O'Gorman L. (1995). Electronic Marking and Identification Techniques to Discourage Document Copying. *IEEE Journal on Selected Areas in Communications.* V. 13. №. 8. P. 1495–1503.

[8] Shutko N. A., Urbanovich P.P., Zukowski P. (2018). A method of syntactic text steganography based on modification of the document-container aprosh. *Przegląd Elektrotechniczny.* R. 94, № 6. P. 82–85.

[9] Taleby M., Li Q., Jun Hou, Mazraeh H., Jing Zhang. (2018). AITSteg: An Innovative Text Steganography Technique for Hidden Transmission of Text Message via Social Media. *IEEE Access.* V.6. P. 65981–65995.

[10] Urbanovich P., Chourikov K., Rimorev A., Urbanovich N. (2010). Text steganography application for protection and transfer of the information. *Przegląd Elektrotechniczny.* R. 86, № 7. P.95–97.

[11] Urbanovich P., Shutko N. (2016). Theoretical Model of a Multi-Key Steganography System. *Recent Developments in Mathematics and Informatics. Contemporary Mathematics and Computer Science.* Vol. 2, Chapter 11. KUL, Lublin. P. 181–202.

АНАЛИЗ АЛГОРИТМА ШИФРОВАНИЯ КАЛИНА 128/256 С УМЕНЬШЕННЫМ ЧИСЛОМ РАУНДОВ ИНТЕГРАЛЬНЫМ МЕТОДОМ

Д.А. Федченко
Оперативно-аналитический центр при Президенте Республики Беларусь
Минск, БЕЛАРУСЬ
e-mail: zmicier.fied@yandex.ru

В данной работе описывается применение интегрального метода криптоанализа к шифру «Калина 128/256». Результатом является построение наилучшей на данный момент по совокупности показателей атаки уменьшенной до 7 раундов версии шифра. Для проведения атаки требуется подбор 2^{98} пар блоков открытого и шифрованного текстов, 2^{56} бит оперативной памяти и выполнения объёма работ, эквивалентного 2^{242} операциям зашифрования.
Ключевые слова: блочный симметричный шифр; Калина; AES; интегральный криптоанализ; метод частичных сумм

1 Введение

Одним из актуальных методов криптографического анализа блочных шифров является интегральный криптоанализ. Он зарекомендовал себя в результате применения к таким XSLP схемам как SQUARE [2] и AES [5].

Настоящая работа посвящена изучению возможности применения интегрального методов криптоанализа к блочному шифру «Калина», лежащему в основе национального стандарта шифрования Республики Украина ДСТУ 7624:2014 [1]. «Калина» представляет из себя блочный шифр, выполненный по XSLP схеме, во многом аналогичной AES, однако с рядом существенных изменений, направленных на повышение его стойкости.

2 Общие сведения

Блочный шифр «Калина» имеет пять возможных вариантов работы. Под «Калина 128/256» всюду в данной работе подразумевается вариант, при котором длина блока в байтах (N_b) равна 16, а длину ключа в байтах (N_k) – 32. Количество раундов (r) при этом равно 14, а матрица состояний содержит 8 строк и 2 столбца.

Каждый раунд состоит из четырёх базовых операций, рассмотренных далее:

1. *SubBytes (SB)* – операция, определяемая четырьмя 8-битными S-боксами: π_0, π_1, π_2 и π_3 следующим образом: ко всем элементам каждой строки матрицы состояний с номером $j \in \overline{0,7}$ применяется S-бокс π_{jmod4}.

2. *ShiftRows (SR)* – линейная операция перестановки элементов матрицы состояний. Строка с номером $j \in \overline{0,7}$ представляется как последовательность байт, к которой применяется циклический сдвиг вправо на δ_j бит, где $\delta_j = \left\lfloor \frac{j \cdot N_b}{64} \right\rfloor$.
3. *MixColumns (MC)* – линейное преобразование, задаваемое умножением каждого столбца матрицы состояний на МДР-матрицу размера 8×8 над полем $GF(2^8)$, задаваемую с помощью неприводимого многочлена $x^8+x^4+x^3+x^2+1$.
4. *AddRoundKey (ARK, $\boxplus$ либо $\oplus$)* – операция прибавления раундового ключа. Начальное и заключительное прибавление раундовых ключей осуществляется сложением по модулю 2^{64} ($\boxplus$) частей ключа с различными столбцами матрицы состояний. Прибавление остальных ключей происходит с применением операции побитового сложения XOR ($\oplus$).

Функции, реализующую применение данных операций к l-битовому внутреннему состоянию шифра ($l = N_b \cdot 8$) обозначим через π_l', τ_l, ψ_l , $\eta_l^{(k_v)}$ и $\kappa_l^{(k_v)}$, соответственно. Во введённых обозначениях базовое шифрующее преобразование шифра «Калина» $T_{l,k}^{(K)}$ можно определить следующим образом:

$$T_{l,k}^{(K)} = \eta_l^{(k_0)} \cdot \prod_{\nu=1}^{r-1} (\pi_l' \cdot \tau_l \cdot \psi_l \cdot \kappa_l^{(k_\nu)}) \cdot \pi_l' \cdot \tau_l \cdot \psi_l \cdot \eta_l^{(k_r)},$$

где K – ключ шифрования длины $k = N_k \cdot 8$ бит.

3 Интегральный криптоанализ

Будем считать, что алфавит открытого и шифрованного текстов равен V_n, где $n = m \cdot d$. Пусть $X \subset V_n$, тогда под j-тым подблоком блока $\alpha = (\alpha_0, \ldots, \alpha_{d-1}) \in V_n, \alpha_i \in V_m, i = 0, \ldots, d-1$, будем понимать вектор α_j. Подблоки множества X с номерами i образуют мультимножество X_i.

Удобно использовать следующие условные обозначения:

$\mathcal{C}$: обозначение мультимножества X_i символом $\mathcal{C}$ означает, что $\exists \alpha \in V_m : \forall \beta \in X_i$ верно $\alpha = \beta$. Важно отметить, что для двух мультимножеств обозначенных символом $\mathcal{C}$ значение α, принимаемое подблоками, может отличаться.

$\mathcal{A}$: Если мультимножество X_i обозначено символом $\mathcal{A}$, то $\forall \alpha, \beta \in X_i : \alpha \neq \beta$. В случае, когда мощность мультимножества равна максимальному количеству подблоков длины m, выполнение свойства $\mathcal{A}$ равносильно тому, что все возможные значения подблока появляются в мультимножестве ровно один раз. Помимо этого, ясно, что сумма всех элементов такого мультимножества равна нулю.

$\mathcal{S}$: Если мультимножество обозначено символом $\mathcal{S}$, значит сумма всех его элементов может быть заранее найдена при построении атаки. Заметим, что такие мультимножества предоставляют атакующему меньше информации, чем обозначенные символами $\mathcal{C}$ или $\mathcal{A}$. Действительно, свойством $\mathcal{S}$ обладают как мультимножества чётной мощности, обладающие свойством $\mathcal{C}$, так и мультимножества элементов из V_m, обладающие свойством $\mathcal{A}$.

Будем говорить, что множество $X \in V_n$ обладает структурой $\mathcal{R} = (\mathcal{R}_0, \ldots, \mathcal{R}_{d-1})$, где $\mathcal{R}_i \in \{\mathcal{C}, \mathcal{A}, \mathcal{S}\}$, если для мультимножества X_i выполняется свойство $\mathcal{R}_i, i = 0, \ldots, d-1$.

r-раундовым интегральным соотношением (интегралом) для некоторого алгоритма шифрования будем называть такой набор структур $(\mathcal{R}^{(0)}, \ldots, \mathcal{R}^{(r)})$, что существует вектор $(X^{(0)}, X^{(1)}, \ldots, X^{(r)}) \in V_n^{r+1}$, элементы $X^{(j)}$ которого являются множествами промежуточных шифрованных текстов после j раундов работы алгоритма, и обладают структурой $\mathcal{R}^{(j)}, j = 0, \ldots, r$. Множество $X^{(0)}$ будем называть входом интегрального соотношения, а $X^{(r)}$ – выходом.

Адаптация основного интегрального соотношения (трёхраундового интеграла для AES) к данному шифру приводят к построению интеграла, приведённого на Рисунке 1.

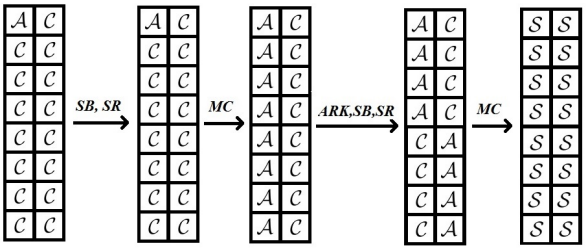


Рис. 1. 2-раундовый интеграл для шифра «Калина 128/256»

4 Описание атаки

Для удобства, обозначим символами $m^{(i)}, b^{(i)}$ и $t^{(i)}$ блоки промежуточного шифрованного текста, получаемые после преобразования *MixColumns* (ψ), прибавления раундового ключа k_{i-1} (η или κ) и *ShiftRows* (τ), соответственно, $i-$го раунда. Индексы l и k будут опущены в связи с тем, что обсуждается конкретная версия шифра «Калина» с $l = 128$, $k = 256$.

На первом этапе проведения атаки необходимо подобрать 2^8 открытых текстов так, чтобы множество $m^{(1)}$ обладало структурой $\mathcal{R} = (\mathcal{R}_1, \mathcal{R}_2, \ldots, \mathcal{R}_{16})$, такой что $\exists i \in \overline{1,16} : (\mathcal{R}_i = \mathcal{A}) \wedge (\forall j \in \{1, \ldots, 16\} \backslash \{i\} : \mathcal{R}_j = \mathcal{C})$. Из свойств рассеивания преобразований *ShiftRows* и *MixColumns* следует, что всякий байт состояния $m^{(1)}$ может быть выражен с помощью восьми байт состояния $b^{(1)}$, содержащихся в двух столбцах матрицы состояний (по четыре в каждом). При этом, в одном из столбцов интересующие нас байты являются младшими, а в другом – старшими. Младшие четыре байта выражаются с помощью четырёх байт открытого текста и четырёх байт ключа k_0. В свою очередь старшие, в связи с особенностями операции $\eta^{(k_0)}$, могут быть выражены через восемь байт открытого текста и восемь байт ключа $k^{(0)}$. Отсюда следует, что любой байт состояния $m^{(1)}$ может быть выражен при помощи двенадцати байт открытого текста и двенадцати байт ключа k_0.

Атакующий выбирает 26 множеств $X_i^{pt}, i = 1, \ldots, 26$ из 2^{96} открытых текстов обладающих структурой $(\mathcal{A}_0^{12}, \mathcal{A}_0^{12}, \ldots, \mathcal{A}_0^{12}, \mathcal{C}, \mathcal{C}, \mathcal{C}, \mathcal{C})$. Множества соответству-

ющих X_i^{pt} зашифрованных блоков обозначим X_i^{ct}. В результате, при любом ключе k_0 множества промежуточных шифрованных текстов $m^{(1)}$, соответствующих X_i^{pt} могут быть представлены в виде разбиения на 2^{88} множеств структуры $\mathcal{R}$.

Согласно основному интегральному тождеству для шифра «Калина 128/256», если входом интеграла является множество обладающее структурой $\mathcal{R}$, то выход интеграла обладает структурой $\mathcal{S}^{16} = (\mathcal{S}, \ldots, \mathcal{S})$. В частности, это означает что упомянутому ранее разбиению соответствует разбиение множества промежуточных шифрованных текстов $b^{(4)}$ на 2^{88} множеств обладающих структурой $\mathcal{S}^{16}$. Отсюда следует, что и множество $b^{(4)}$ обладает структурой $\mathcal{S}^{16}$.

Для удобства дальнейшего проведения атаки, запишем функцию зашифрования алгоритма «Калина 128/256», уменьшенного до 7 раундов в эквивалентной форме:

$$T^{(K)} = \eta^{(k_0)} \cdot \pi' \cdot \tau \cdot \psi \cdot \kappa^{(k_1)} \cdot \ldots \cdot (\pi' \cdot \tau \cdot \kappa^{(k_4')} \cdot \psi \cdot \pi' \cdot \tau \cdot \kappa^{(k_5')} \cdot \psi) \cdot \pi' \cdot \tau \cdot \psi \cdot \kappa^{(k_6)} \cdot \pi' \cdot \tau \cdot \psi \cdot \eta^{(k_7)},$$

где для k_i' выполняются соотношения $\kappa^{(k_i')} = \psi\kappa^{(k_i)}\psi^{-1}, i = 4, 5$.

Любой байт состояния $b^{(4)}$ может быть выражен с помощью восьми байт промежуточного состояния $b^{(6)}$, восьми байт ключа k_5' и одного байта ключа k_4'. Любой байт состояния $b^{(6)}$ выражается через шифртекст и ключи k_6 и k_7. Учитывая, что ключи k_6 и k_7 связаны между собой операцией побитового циклического сдвига, трудоёмкость их совместного перебора составит 2^{128}.

Пусть $k_i[i_1, \ldots, i_t]$ – множество байт раундового ключа k_i с номерами $i_1, \ldots, i_t$, где $i_j = 0, \ldots, 15$, и $1 \le t \le 16$.

Символом S будем обозначать промежуточную сумму, служащую для проверки выполнения свойства $\mathcal{C}$ для мультимножества X_0 подблоков множества промежуточных шифрованных текстов $b^{(4)}$, получаемых из X_i^{pt}. При этом, согласно интегральному соотношению верно $S = 0$.

Сформулируем Алгоритм 1, позволяющий определить некоторые байты раундовых ключей уменьшенной до 7 раундов версии шифра «Калина 128/256»:

Вход: $X_i^{pt}, i = 1, \ldots, 26$;
Выход: $k_7[0, \ldots, 15], k_6[0, \ldots, 15], k_5'[0, \ldots, 3], k_5'[12, \ldots, 15], k_4'[0]$;
1: $S := 0$;
2: для всех $(k_7[0, \ldots, 15], k_5'[0, \ldots, 3, 12, \ldots, 15], k_4'[0]) \in V_8^{16} \times V_8^8 \times V_8$
3: $k_6[0, \ldots, 15] := (k_7[0, \ldots, 15] \ggg 56)$;
4: i := 1;
5: для всех $c \in X_i^{ct}$
6: $b^{(7)} = \big(c\big)(\eta^{(k_7)})^{-1} \cdot \psi^{-1} \cdot (\pi' \cdot \tau)^{-1}$;
7: $b^{(6)} = \big(b^{(7)}\big)\kappa^{(k_6)} \cdot \psi^{-1} \cdot (\pi' \cdot \tau)^{-1}\psi^{-1}$;
8: $m^{(4)}[0, \ldots, 11] = \big(b^{(6)}[0, \ldots, 3, 12, \ldots, 15]\big)\kappa^{(k_5'[0,\ldots,3,12,\ldots,15])} \cdot (\pi' \cdot \tau)^{-1}$;
9: $b^{(5)}[0, \ldots, 11] = \big(m^{(4)}[0, \ldots, 11]\big)\psi^{-1}$;
10: $b^{(4)}[0] = \big(b^{(5)}[0]\big)\kappa^{(k_4'[0]} \cdot (\pi' \cdot \tau)^{-1}$;
11: $S := S \oplus b^{(4)}[0]$;
12: если $S = 0$ то
13: если $i < 26$ то

14: i := i + 1;
15: Перейти на Шаг 5;
16: иначе
17: Опробуемый набор байт считается истинным;
18: иначе
19: Опробуемый набор байт отбраковывается;

Таблица 1 Эффективность некоторых атак на уменьшенные версии шифров

Шифр	Раунды	Материал	Память	Трудоёмкость	Источник
«Калина 128/256»	7	2^{98}	2^{56}	2^{242}	Новая
«Калина 128/256»	7	2^{89}	$2^{202,64}$	$2^{230,2}$	[4]
AES 128/256	7	$2^{36,39}$	2^{24}	2^{172}	[3]

5 Заключение

В данной работе была построена интегральная атака на уменьшенный до 7 раундов шифр «Калина 128/256». Предлагаемый алгоритм атаки требует значительно меньших затрат оперативной памяти, по сравнению с атаками, опубликованными ранее, однако является более трудоёмким и требует больший объём подобранных открытых текстов.

Библиографические ссылки

[1] Горбенко І.Д., Долгов В.І., Олійников Р.В. (2007). Перспективний блоковий симетричний шифр «Калина». Основні положення та специфікація. *Прикладная радиоэлектроника*. Т. **6**, №2. С. 195–208.

[2] Daemen J., Knudsen L., Rijmen V. (1997). The block cipher Square. *Fast Software Encryption*. С. 149–165.

[3] Ferguson N., Kelsey J., Lucks S., Schneier B., Stay M., Wagner D., Whiting D. (2001). Improved Cryptanalysis of Rijndael.

[4] Riham AlTawy, Abdelkhalek A., Amr M.Youssef (2015). A Meet-in-the-Middle Attack on Reduced-Round Kalyna-b/2b. *Concordia University, Montreal, Quebec, Canada*.

[5] Federal Information Processing Standards Publication (2001). Specification for the advanced encryption standard (AES).

КОМПОНЕНТНАЯ ПРИМИТИВНОСТЬ ОРГРАФОВ

В.М. Фомичев
Финансовый университет при Правительстве Российской Федерации
ООО «Код Безопасности»
Институт проблем информатики ФИЦ «Информатика и управление» РАН
Москва, РОССИЯ
e-mail: fomichev.2016@yandex.ru

Для конечных орграфов, все вершины которых имеют ненулевые полустепени захода и исхода, введены понятия компонентной примитивности и компонентного экспонента. Эти понятия распространяют известные понятия с множества примитивных орграфов на более широкое множество не сильно связных и не связных орграфов, что существенно расширяет область приложений матрично-графового подхода к оценке перемешивающих и нелинейных свойств преобразований информации. Получен критерий компонентной примитивности орграфа и оценки компонентного экспонента орграфа. С использованием полученных результатов оценена допустимая длина холостого хода двухкаскадных генераторов, построенных основе последовательного соединения нелинейных регистров сдвига.
Ключевые слова: компонента сильной связности; примитивный орграф; экспонент орграфа; расстояние от вершины до множества вершин

Основные обозначения

$\mathbb{N}$	множество натуральных чисел
$\mathbb{N}_n$	$= \{0, \ldots, n-1\}$, $n \in \mathbb{N}$
$F(l_1, \ldots, l_m)$	число Фробениуса для аргументов $l_1, \ldots, l_m \in \mathbb{N}$, где $(l_1, \ldots, l_m) = 1$
$w(u, v)$	путь в орграфе из вершины u в вершину v
$w \bullet w'$	конкатенация путей w и w', где совпадают последняя вершина пути w и первая вершина пути w'
V_n	пространство всех двоичных векторов длины n, $n \in \mathbb{N}$
$\Leftrightarrow$	тогда и только тогда, когда...

Введение

В криптографических алгоритмах сложные функции часто построены с помощью композиции относительно несложных функций, допускающих удобную аппаратную и/или программную реализацию. Итерации однотипных нелинейных преобразований векторного пространства применяются как в поточных, так и в блочных

шифрах, где зашифрование и расшифрование выполняется с помощью нескольких раундов однотипных вычислений. Важной задачей анализа таких шифрсистем является определение таких характеристик координатных функций композиции преобразований, как множества существенных и нелинейных переменных, степень нелинейности и др. Не только точное определение, но и оценка этих характеристик координатных функций композиции преобразований является в общем случае нетривиальной задачей.

Для исследования множества существенных и нелинейных переменных композиций нелинейных преобразований векторных пространств разработан и активно применяется обоснованный в научной литературе матрично-графовый подход (МГП) [7,8]. Математическую основу МГП составляют критерии примитивности и локальной примитивности множеств неотрицательных матриц и орграфов, а также оценки их экспонентов и локальных экспонентов.

История получения до 2018 года основных результатов по этим направлениям отражена в [7]. Введенные Фробениусом [10] в 1912 году изначальные понятия впоследствии были развиты рядом авторов [4 – 12], в том числе в работах прикладного характера [13 – 15]. Понятия примитивности и экспонентов неотрицательных матриц и орграфов обобщены для множеств матриц и орграфов и для их локальных характеристик.

В данной работе введены понятия компонентной примитивности и компонентного экспонента орграфа, распространяющие известные понятия с множества примитивных орграфов на более широкое множество орграфов, у которых каждая вершина имеет ненулевые полустепени захода или исхода. К таким орграфам относятся некоторые не сильно связные и не связные графы. Компонентную примитивность можно рассматривать как частного вида локальную примитивность орграфа.

Использование введенных понятий существенно расширяет область приложений МГП к изучению существенных и нелинейных переменных итеративных функций.

1 Определяющие свойства компонентного экспонента орграфа

Пусть конечный орграф Γ имеет множество вершин $\mathbb{N}_n = \{0, \ldots, n-1\}$. Назовем орграф Γ особенным, если он имеет вершину с нулевой полустепенью захода или исхода. В противном случае назовем орграф неособенным. Далее рассматриваются неособенные орграфы.

Говорят, что в орграфе из вершины u достижимо множество вершин A (вершина v), если существует путь длины $t > 0$ из вершины u в некоторую вершину множества A (в вершину v). Вершина орграфа называется циклической (ациклической), если она принадлежит некоторому контуру (не принадлежит какому-либо контуру). Компонентой сильной связности (ксс) орграфа называется его максимальный подграф с множеством взаимно достижимых вершин.

Обозначим: $V(K)$ - множество вершин ксс K; $K(u)$ — ксс, содержащая циклическую вершину u; $\boldsymbol{K}(\Gamma)$ — множество всех ксс орграфа Γ; для вершины u через I_u и O_u — соответственно множества всех вершин орграфа, из которых u достижима, и вершин, достижимых из u.

Любой контур является частью некоторой ксс. В частности, ксс может состоять из единственной вершины с петлей. Из определения ксс следует единственность ксс $K(u)$.

Если $\boldsymbol{K}(\Gamma) = \{K_1, \ldots, K_r\}$, то в силу определения ксс $V(K_s) \cap V(K_l) = \varnothing$ и ксс K_s и K_l не являются взаимно достижимыми при $s \neq l$, $s, l \in \{1, \ldots, r\}$.

Лемма 1. *В неособенном орграфе*

$$I_u \cap O_u = \begin{cases} V(K(u)), & u - \textit{циклическая вершина,} \\ \varnothing, & \textit{в противном случае.} \end{cases}$$

Доказательство. Для любой вершины $i \in I_u$ существует путь $w(i, u)$, и для любой вершины $j \in O_u$ существует путь $w(u, j)$. Значит, для любой пары вершин $(i, j) \in I_u \times O_u$ существует путь $w(i, j)$, проходящий через u.

Пусть вершина u циклическая, тогда для любых вершин $i, j \in V(K(u))$ имеется обратный путь $w(j, i)$, отсюда $i, j \in I_u \cap O_u$. Если хотя бы одна из вершин i, j не принадлежит $V(K(u))$, то эта вершина не принадлежит $I_u \cap O_u$, так как обратный путь не существует. Значит, равенство для циклической вершины u верно.

Пусть вершина u ациклическая. Тогда $u \notin I_u \cup O_u$ иначе в вершине u имеется петля, что противоречит ацикличности вершины u. Если $i \in I_u \cap O_u$, где $i \neq u$, то существует путь $w(i, u)$ и обратный путь $w(u, i)$, что противоречит ацикличности вершины u. Следовательно, множества I_u и O_u не содержат общих вершин. □

Неособенный орграф Γ назовем компонентно примитивным (кратко — компримитивным), если при некотором $t \in \mathbb{N}$ в орграфе Γ^t имеются дуги (u, v) для любого $u \in \mathbb{N}_n$ и любого $v \in O_u$. Наименьшее такое t назовем компонентным экспонентом орграфа Γ и обозначим com-expΓ. Выполнены свойства:

1) если орграф Γ примитивный, то он состоит из единственной ксс и является компримитивным, при этом com-expΓ = expΓ;

2) если компримитивный орграф Γ состоит из компонент связности $K_1, \ldots, K_r$, то

$$\text{com-exp}\Gamma = \max_{1 \leq s \leq r} \{\text{com-exp}K_s\}.$$

Пример. Компримитивным, но не примитивным орграфом является связный орграф Γ, имеющий петлю в вершине 0, примитивный подграф Γ' с множеством вершин $\{1, \ldots, n-1\}$ и дугу $(i, 0)$, где $i \in \{1, \ldots, n-1\}$. Такой орграф имеет ксс Γ' и ксс с единственной вершиной 0.

В силу свойства 2 ограничимся изучением только связных неособенных орграфов.

Расстоянием в Γ от вершины u до множества вершин V, обозначается $\rho(u, V)$, называется длина кратчайшего пути из u в ближайшую вершину множества V. Если множество V не достижимо из вершины u, то $\rho(u, V) = \infty$.

Обобщим понятие эксцентриситета вершины и диаметра орграфа на не сильно связные орграфы. Псевдоэксцентриситетом вершины u орграфа Γ (обозначается $\mathrm{pex}(u)$) назовем наибольшее из расстояний от u до вершин множества O_u (положим $\rho(u,u)=0$):

$$\mathrm{pex}(u)=\max_{v\in O_u}\rho(u,V).$$

Псевдодиаметром орграфа Γ (обозначается $\mathrm{pdm}\Gamma$) назовем величину:

$$\mathrm{pdm}\Gamma=\max_{0\le u<n}\mathrm{pex}(u).$$

Теорема 1. *(критерий компримитивности). Неособенный орграф компримитивный $\Leftrightarrow$ каждая его ксс примитивная и любые две ациклические вершины не являются смежными. Если орграф Γ компримитивный, то*

$$\text{com-exp}\Gamma\le\mathrm{pdm}\Gamma+\max_{K\in\boldsymbol{K}(\Gamma)}\exp K.$$

Доказательство. Необходимость. Пусть ксс K не примитивная. Тогда при любом $t\in\mathbb{N}$ имеются вершины $u,v\in V(K)$ такие, что не существует пути длины t из u в v. Так как $v\in O_u$, то отсюда следует, что орграф Γ не компримитивный.

Если в Γ ациклические вершины u и v являются смежными, то при любом $t>1$ в орграфе Γ^t нет дуги (u,v), иначе в Γ вершина v принадлежит контуру длины $t-1$, что противоречит ее ацикличности. Так как $v\in O_u$, то отсюда следует, что орграф Γ не компримитивный.

Достаточность. Для любой вершины u в Γ есть путь $w(u,v)$ при $v\in O_u$. Пусть $K\in\mathrm{K}(\Gamma)$.

Если $u,v\in V(K)$, то в силу примитивности K имеются пути $w(u,v)$ любой длины $\gamma\ge\exp K$.

Если вершина u ациклическая и $v\in V(K)$, то для некоторой вершины $j\in V(K)$ существует путь $w(u,j)$ длины $\rho(u,V(K))$, и при любом $\gamma\ge\exp K$ существует путь $w(j,v)$ длины γ. Следовательно, так как $\mathrm{pex}(u)\ge\rho(u,V(K))$, то при любом $\gamma\ge\exp K$ существует путь $w(u,v)$ длины $\mathrm{pex}(u)+\gamma$, являющийся конкатенацией путей $w(u,j)\bullet w(j,v)$.

Если вершина v ациклическая и $u\in V(K)$, то для некоторой вершины $j\in V(K)$ существует путь $w(j,v)$ длины $\rho(V(K),v)$, и при любом $\gamma\ge\exp K$ существует путь $w(u,j)$ длины γ. Следовательно, так как $\mathrm{pex}(u)\ge\rho(V(K),v)$, то при любом $\gamma\ge\exp K$ существует путь $w(u,v)$ длины $\gamma+\mathrm{pex}(u)$, являющийся конкатенацией путей $w(u,j)\bullet w(j,v)$.

Если вершины u и v ациклические, то по условию они не смежные, значит, любой путь $w(u,v)$, в частности, кратчайший путь, проходит через некоторую ксс K. Отсюда для некоторых вершин $s,j\in V(K)$, принадлежащих кратчайшему пути $w(u,v)$, имеются пути $w(u,s)$ и $w(j,v)$, сумма длин которых не более $\mathrm{pex}(u)$, и при любом $\gamma\ge\exp K$ существует путь $w(s,j)$ длины γ. Значит, при любом $\gamma\ge\exp K$ существует путь $w(u,v)$ длины $\gamma+\mathrm{pex}(u)$, являющийся конкатенацией путей $w(u,s)\bullet w(s,j)\bullet w(j,v)$.

Обобщая все случаи, получаем, что в Γ для любой вершины u и любой вершины $v \in O_u$ имеются пути $w(u,v)$ любой длины $\gamma \geq \mathrm{pex}(u) + \max\limits_{K \in \boldsymbol{K}(\Gamma)} \exp K$. Следовательно, орграф Γ компримитивный и оценка com-expΓ верна. $\square$

Следствие 1. *Пусть* Γ *— связный компримитивный орграф, содержащий ксс* $K_1, \ldots, K_r$ *порядка* $k_1, \ldots, k_r$ *соответственно,* $r > 1$, *тогда*

$$\text{com-exp}\Gamma \leq (n-r)^2 + n.$$

Доказательство. Пусть $\max\limits_{K \in \boldsymbol{K}(\Gamma)} \exp K = \exp K_1$. По условию $|K_1| \leq n-r+1$. Отсюда в соответствии с универсальной оценкой Виландта $\exp K_1 \leq (n-r+1)^2 - 2(n-r+1) + 2$. Учитывая, что $\mathrm{pdm}\Gamma \leq n-1$, получаем по теореме 1: com-exp$\Gamma \leq \exp K_1 + n - 1$. После упрощения выражения получается нужная оценка. $\square$

2 Свойства одного класса генераторов двоичной гаммы

Генераторы псевдослучайных последовательностей используются в системах шифрования для формирования псевдослучайных ключевых последовательностей, инициальных параметров и др. Важным свойством поточного шифра является зависимость знаков выходной последовательности генератора $\{y_t, t = 0, 1, \ldots\}$ от всех знаков начального состояния (ключа). Электронные схемы криптографических генераторов обычно реализуются с использованием элементов памяти, обуславливающих так называемую «задержку» при вычислении используемых знаков выхода. В силу этого существует граница t_0 такая, что при $t < t_0$ знаки y_t зависят не от всех знаков начального состояния. Эти знаки часто не используются для шифрования во избежание риска, связанного с эффективностью некоторых криптоаналитических атак. Определяемая разработчиком характеристика генератора, обычно несколько превышающая границу t_0, называется длиной холостого хода генератора и определяет количество начальных тактов, в которых знаки выходной последовательности игнорируются (не используются).

Граница t_0 определяется в основном перемешивающими свойствами преобразования $g(x)$ внутренних состояний генератора и оценивается с помощью определенного локального экспонента перемешивающего орграфа $\Gamma(g)$ преобразования $g(x)$. Получим эту оценку для одного класса генераторов с помощью com-exp$\Gamma(g)$.

Пусть $x = (x_0, \ldots, x_{n-1})$ — начальное состояние генератора. Для преобразования $g(x)$ множества V_n с координатными функциями $g_0(x), \ldots, g_{n-1}(x)$ перемешивающим графом называется орграф $\Gamma(g)$ с множеством вершин $\mathbb{N}_n$, где (u,v) есть дуга $\Leftrightarrow$ $g_v(x)$ существенно зависит от x_u, $0 \leq u, v < n$.

Оценим границу t_0 для двухкаскадных генераторов, построенных с помощью последовательного соединения нелинейных регистров левого сдвига, длины которых равны n и m. Пусть обратные связи регистров заданы соответственно функциями $f_0(x_0, \ldots, x_{n-1})$ и $f_1(x_n, \ldots, x_{n+m-1})$. При $x = (x_0, \ldots, x_{n+m-1}) \in V_{n+m}$ пре-

образование $g(x)$ множества V_{n+m} внутренних состояний генератора зададим координатными функциями:

$$g(x) = \{x_1, \ldots, x_{n-1}, f_0(x_0, \ldots, x_{n-1}), \\ x_{n-1} \oplus x_{n+1}, x_{n+2}, \ldots, x_{n+m-1}, f_1(x_n, \ldots, x_{n+m-1})\}. \quad (1)$$

Из (1) следует, что орграф $\Gamma(g)$ состоит из соединенных дугой $(n-1, n)$ ксс K_0 и K_1 (примитивных при некоторых функциях f_0 и f_1) с множествами вершин $\{0, \ldots, n-1\}$ и $\{n, \ldots, n+m-1\}$ соответственно. Отсюда $\max\limits_{0 \le u < n} \rho(u, K_0) = 0$, $\max\limits_{0 \le u < n} \rho(u, K_1) = n$.

В силу теоремы 1 com-exp$\Gamma(g) \le n + m - 1 + \max\{\exp K_0, \exp K_1\}$. Пусть для определенности $n \le m$. Тогда, используя абсолютную оценку Виландта и оценку pdm$\Gamma \le n + m - 1$, получаем:

$$\text{com-exp}\Gamma \le n + m^2 - m + 1.$$

Параметры обратных связей регистров позволяют уточнить оценки com-exp$\Gamma(g)$, используя оценки, данные в [6].

Библиографические ссылки

[1] Berger T., Minier M., Thomas G. (2014). Extended generalized Feistel networks using matrix representation. *SAC http://sac2013.irmacs.sfu.ca/slides/s16.pdf*

[2] Berger T., Francq J., Minier M., Thomas G. (2016). Extended generalized Feistel networks using matrix representation to propose a new lightweight block cipher: Lilliput. *IEEE Trans. Comput.* Vol. 65, No. 7. P. 2074–2089.

[3] Brualdi R. A., Liu B. (1990). Generalized exponents of primitive directed graphs. *J. Graph Theory.* Vol. 14, No. 4. P. 483–499.

[4] Dulmage A. L., Mendelsohn N. S. (1962). The exponent of a primitive matrix. *Can. Math. Bull.* Vol. 5, No. 3. P. 241–244.

[5] Dulmage A. L., Mendelsohn N. S. (1964). Gaps in the exponent set of primitive matrices. *Ill. J. Math.* Vol. 8, No. 4. P. 642–656.

[6] Fomichev V.M., Avezova Ya.A. (2020). Exact Formula for Exponents of Mixing Digraphs of Register Transformations. *Journal of Applied and Industrial Mathematics.* 14 (2), P. 308–320.

[7] Fomichev V. M., Avezova Ya. E., Koreneva A. M., Kyazhin S. N. (2018). Primitivity and Local Primitivity of Digraphs and Nonnegative Matrices. *J. Appl. Ind. Math.* №12(3), P. 453–469.

[8] Fomichev V. M., Koreneva A. M. (2020). Encryption Performance and Security of Certain Wide Block Ciphers. *J Comput Virol Hack Tech.* 16, P. 197–216.

[9] Fomichev V. M., Kyazhin S. N. (2017). Local Primitivity of Matrices and Graphs. *J. Appl. Ind. Math.* P. 26–39. DOI 10.1134/ S1990478917010045.

[10] Frobenius G. (1912). Uber Matrizen aus nicht negativen Elementen. *Berl. Ber.* P. 456–477. [German].

[11] Liu B. (2003). Generalized exponents of Boolean matrices. *Linear Algebra Appl.* Vol. 373. P. 169–182.

[12] Neufeld S. W. (1996). A diameter bound on the exponent of a primitive directed graph. *Linear Algebra Appl.* Vol. 245. P. 27–47.

[13] Perkins P. (1961). A theorem on regular graphs. *Pac. J. Math.* Vol. 2. P. 1529–1533.

[14] Sachkov V. N., Tarakanov V. E. (2002). Combinatorics of nonnegative matrices. *Translations of Mathematical Monographs American Mathematical Society* Vol. 213, 269 p.

[15] Suzaki T., Minematsu K. (2010). Improving the generalized Feistel. *Lect. Notes Comput. Sci.* Vol. 6147. P. 19–39.

[16] Wielandt H. (1950). Unzerlegbare nicht negative Matrizen. *Math. Z.* Bd. 52. P. 642–648. [German].

ДИСКРЕТНЫЕ ВРЕМЕННЫЕ РЯДЫ В КРИПТОЛОГИИ

Ю.С. Харин
НИИ прикладных проблем математики и информатики
Белорусский государственный университет
Минск, Беларусь
e-mail: kharin@bsu.by

Рассматривается актуальная в криптологии проблема построения и статистического анализа (оценивание параметров, проверка гипотез) моделей дискретных временных рядов, адекватно описывающих выходные последовательности криптографических генераторов и узлов систем криптографической защиты информации.
Ключевые слова: «чистая случайность»; дискретный временной ряд; цепь Маркова высокого порядка; малопараметрическая модель; статистический анализ

1 Введение

Случайные и псевдослучайные последовательности, а также порождающие их физические и программные генераторы являются неотъемлемыми элементами современных систем криптографической защиты информации (СКЗИ) для решения следующих основных задач: генерация гаммы в поточных криптосистемах; генерация сеансовых и других ключей в криптосистемах; генерация «случайных значений» параметров для многих систем ЭЦП; формирование «случайных запросов» при реализации большинства существующих криптографических протоколов выработки общего секретного ключа и аутентификации.

Математической моделью последовательностей, порождаемых генераторами, а также последовательностей, возникающих в различных узлах СКЗИ, является дискретный временной ряд (ДВР). Дискретный временной ряд (ДВР) – это случайный процесс $x_t \in A$ на вероятностном пространстве $(\Omega, F, \mathbf{P})$ с дискретным временем $t \in \mathbb{N} = \{1, 2, \ldots\}$ и дискретным множеством состояний мощности $|A| = N$, $2 \le N < +\infty$. Без потери общности полагаем пространство состояний (алфавит) $A = \{0, 1, \ldots, N-1\}$.

В криптологии в связи с Шенноновской теорией совершенных криптосистем большое внимание уделяется так называемому «чисто случайному» ДВР – равномерно распределенной случайной последовательности (РРСП).

РРСП – это последовательность дискретных случайных величин $x_1, x_2, \ldots \in A = \{0, 1, \ldots, N-1\}$, обладающая двумя свойствами [2]:

C_1) для любого числа $n \in \mathbb{N}$ и произвольных индексов $1 < t_1 < \ldots < t_n$ случайные элементы $x_{t_1}, \ldots, x_{t_n}$ независимы в совокупности;

C_2) для любого $t \in \mathbb{N}$ случайная величина x_t имеет равномерное на A распределение вероятностей:

$$\mathbf{P}\{x_t = i\} = N^{-1}, \quad i \in A.$$

В настоящее время известно более сотни методов и алгоритмов генерации последовательностей, по своим свойствам приближающихся к РРСП. Еще больше разработано методов статистического тестирования криптографических генераторов, заключающихся в проверке простой гипотезы $H_0 = \{\{x_t\}\,\text{есть РРСП}\}$ против сложной альтернативы $H_1 = \bar{H}_0 = \{\text{нарушены свойства}\, C_1, C_2\}$. Проведенный обзор существующих статистических тестов показывает:

1) многие из существующих тестов не ориентированы на проверку главного свойства C_1, а лишь частных случаев свойств C_1, C_2, т.е. частных случаев альтернативы $H_1 = \bar{H}_0$;

2) многие из известных тестов построены «эвристически» и не фиксируют семейство альтернатив H_1;

3) многие тесты не имеют оценок мощности;

4) при включении нескольких тестов в батарею не удается оптимизировать «составной» тест.

В связи с этим актуальна рассматриваемая в этой статье проблема разработки адекватных вероятностных моделей для описания отклонений H_1 от модели РРСП, построения статистических тестов для обнаружения и оценивания таких отклонений.

2 Модели ДВР на основе уклонений от s-мерной равномерности и их энтропийный анализ

Определим вложенное в H_1 семейство «альтернатив s-мерной неравномерности»:

$$H_{1(s)} = \{\{x_1, x_2, \ldots\} = \{X_1, X_2, \ldots\}\} \subset H_1,$$

где $X_1, X_2, \ldots \in A^s$ – независимые одинаково распределенные s-фрагменты (слова) над алфавитом A с некоторым s-мерным дискретным распределением вероятностей

$$\mathbf{P}_{i_1,\ldots,i_s} = \mathbf{P}\{x_1 = i_1, \ldots, x_s = i_s\}, \quad i_1, \ldots, i_s \in A,$$

отличным от равномерного:

$$\Delta_s = \textstyle\sum_{i_1,\ldots,i_s \in A} |\mathbf{P}_{i_1,\ldots,i_s} - N^{-s}| > 0, \ \sum_{i_1,\ldots,i_s \in A} \mathbf{P}_{i_1,\ldots,i_s} \equiv 1.$$

Это семейство моделей ДВР обладает двумя свойствами:

1) при $s \to \infty$ семейство этих альтернатив имеет в пределе альтернативу $H_1 = \bar{H}_0$ общего вида;

2) чем меньше Δ_s, тем ближе альтернатива $H_{1(s)}$ к нулевой гипотезе H_0.

Обозначим: $\{x_1, x_2, \ldots, x_T\} = \{X_1, X_2, \ldots, X_M\}$ – наблюдаемая реализация выходной последовательности длиной $T = M \cdot s$, разбитая на M непересекающихся фрагментов длины s, $\mathrm{I}\{B\}$ – индикатор события B,

$$\hat{\mathbf{P}}_{i_1,\ldots,i_s} = \frac{1}{M} \sum_{m=1}^{M} \mathrm{I}\{X_m = (i_1, \ldots, i_s)\}, \quad i_1, \ldots, i_s \in A, - \tag{1}$$

– статистическая оценка для $\mathbf{P}_{i_1,\ldots,i_s}$.

Тест обобщенного отношения правдоподобия для проверки H_0, $H_{1(s)}$ на основе статистик (1) имеет вид:

$$\text{принимается} \begin{cases} H_0, \text{ если } \hat{H}_s - s\ln N > -\dfrac{1}{2M} G^{-1}_{N^s-1}(1-\varepsilon), \\ H_{1(s)} \text{ в противном случае,} \end{cases} \tag{2}$$

$$\hat{H}_s = -\sum_{i_1,\ldots,i_s \in A} \hat{\mathbf{P}}_{i_1,\ldots,i_s} \ln \hat{\mathbf{P}}_{i_1,\ldots,i_s}$$

– статистическая оценка s-мерной энтропии Шеннона, $G^{-1}_K(\cdot)$ – обратная функция распределения хи-квадрат с K степенями свободы, $\varepsilon \in (0,1)$ – заданный уровень значимости теста.

Тест (1), (2) удобно использовать для визуализации процесса принятия решений в виде так называемого «энтропийного профиля (портрета)» – графика зависимости нормированного уклонения оценки s-мерной энтропии от ее математического ожидания при H_0 (см. рис. 1, 2, где штриховые линии обозначают границы области решений):

$$\alpha(s) = 2M\left(\hat{H}_s - s\ln N\right)/G^{-1}_{N^s-1}(1-\varepsilon),\ s \in \{s_{min}, s_{min}+1, \ldots, s_{max}\}. \tag{3}$$

Заметим, что для теста (1), (2) «опасными» оказываются искусственно сформированные «выходные последовательности», являющиеся $s\cdot 2^s$-периодическим повторением фрагмента, полученного конкатенацией последовательности 2^s всевозможных s-цепочек; для таких последовательностей решение всегда будет в пользу H_0. Во избежание этой «бреши» теста необходимо: а) строить энтропийный профиль (3) при различных значениях s; б) оценку $\hat{H}_s$ строить по пересекающимся s-фрагментам.

Отметим еще, что вместо энтропии Шеннона в (1) – (3) могут использоваться энтропийные функционалы Реньи и Тсаллиса [4].

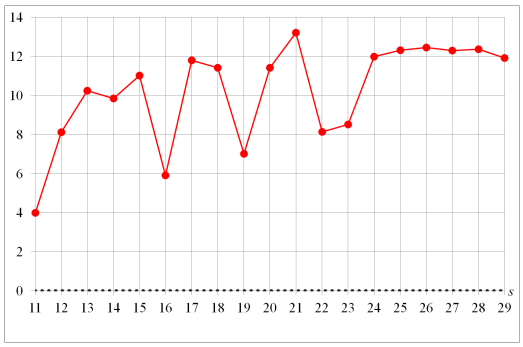


Рис. 1. Энтропийный профиль $\ln|\alpha(s)|$ нелинейного регистра сдвига порядка 24 ($N=2$, $\varepsilon=0.05$, $T=2^{32}/s$)

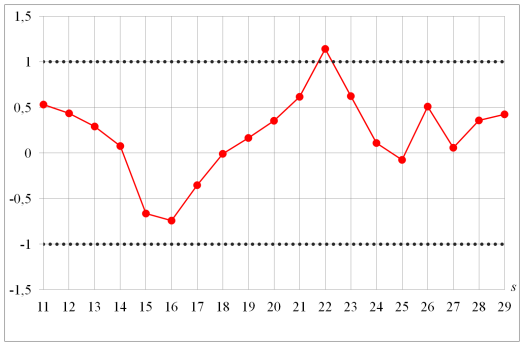


Рис. 2. Энтропийный профиль $\alpha(s)$ генератора BelT (СТБ 34.101.27-2011, $N=2$, $\varepsilon=0.05$, $T=2^{29}/s$)

3 Модели ДВР на основе цепей Маркова высокого порядка

Учитывая, что универсальной моделью стохастической зависимости элементов выходной последовательности $\{x_t\}$ криптографического генератора является цепь Маркова достаточно высокого порядка s, определим вложенное в $H_1 = \bar{H}_0$ семейство альтернатив марковской зависимости: $H_1^{(s)} = \{\{x_t\}$ – однородная цепь Маркова порядка s с матрицей переходов $\mathbf{P}\}$, где $\mathbf{P}=\left(p_{i_1,\ldots,i_s,i_{s+1}}\right)$, $i_1,\ldots,i_{s+1} \in A$, – $(s+1)$-мерная матрица,

$$p_{i_1,\ldots,i_{s+1}}=\mathbf{P}\{x_{t+1}=i_{s+1}|x_t=i_s,\ldots,x_{t-s+1}=i_1\}, \Delta_s=\sum_{i_1,\ldots,i_{s+1}\in A}\left|p_{i_1,\ldots,i_{s+1}}-N^{-1}\right|>0. \quad (4)$$

Семейство альтернатив $H_1^{(s)} : s=1,2,\ldots\}$ обладает тремя важными свойствами:
1) свойство полноты $H_1^{(s)} \to H_1 = \bar{H}_0$ при $s \to \infty$;
2) свойство монотонности: $H_1^{(s)} \subset H_1^{(s+1)}$;
3) свойство близости к H_0: $H_1^{(s)} \to H_0$, если $\Delta_s \to 0$.

Тест обобщенного отношения правдоподобия для проверки гипотез H_0, $H_1^{(s)}$ основан на статистической оценке $\hat{h}_s$ условной энтропии $h_s = H\left\{x_t|x_{t-1},\ldots,x_{t-s}\right\}$:

$$\text{принимается} \begin{cases} H_0, \text{ если } \hat{h}_s - \ln N > -G_f^{-1}(1-\varepsilon)/(2(T-s)),\ f=N^s(N-1), \\ H_{1(s)} \text{ в противном случае.} \end{cases} \quad (5)$$

Аналогично (3) с помощью $\hat{h}_s$ строится энтропийный профиль для $\{x_1,\ldots,x_T\}$.

К сожалению, тесты (2), (5), анализирующие стохастические зависимости глубины s в выходной последовательности $\{x_t\}$, требуют экспоненциально растущей с ростом s длины анализируемой последовательности $T = O\left(N^{s+1}\right)$. Для преодоления этой трудности целесообразно использовать так называемые «малопараметрические модели цепей Маркова высокого порядка», т.е. модели цепей Маркова s-го порядка, для которых $(N^s \times N)$-матрица вероятностей переходов зависит от «малого» числа параметров $D \ll N^s(N-1)$; $\varkappa = D/\left(N^s(N-1)\right) \ll 1$ – коэффициент сжатия, равный относительному числу параметров модели.

4 Подходы к построению малопараметрических цепей Маркова высокого порядка

Подход I

Этот подход состоит в «сжатии множества значений элементов матрицы» $\mathbf{P}$. Пусть $Q = (q_{j_1,\ldots,j_r,j_{r+1}})$ – некоторая $(r+1)$-мерная матрица, $1 \le r < s$,

$$\sum_{j_{r+1}\in A} q_{j_1,\ldots,j_r,j_{r+1}} \equiv 1,\ 0 \le q_{j_1,\ldots,j_r,j_{r+1}} \le 1;$$

$B(\cdot) : A^s \to A^r$ – некоторая дискретная функция. С помощью $B(\cdot)$ $(s+1)$-мерная матрица $\mathbf{P}$ «сжимается» в $(r+1)$-мерную матрицу Q преобразованием:

$$p_{i_1,\ldots,i_s,i_{s+1}} = q_{B(i_1,\ldots,i_s),i_{s+1}};\ \varkappa_{\mathrm{I}} = N^{r-s} \le 1. \tag{6}$$

Примеры малопараметрических ДВР в рамках подхода I: MC(s,r), MCCO(s,L), VLMC [5].

Подход II

Этот подход заключается в использование порождающего уравнения для условного распределения вероятностей (4) будущего состояния $x_t \in A$ при условии предыстории $X_{t-s}^{t-1} = \left(x_{t-1}\ldots, x_{t-s}\right)' \in A^s$:

$$p_{i_1,\ldots,i_s,i_{s+1}} = q_{i_{s+1}}(\theta(i_1,\ldots,i_s;a)),\ i_1,\ldots,i_{s+1} \in A, \tag{7}$$

где $\{q_j(\theta) : j{\in}A\}$ – некоторое вероятностное распределение на A, зависящее от параметра $\theta{=}(\theta_j){\in}\Theta{\subseteq}R^L$; $\theta{=}\theta(i_1,\ldots,i_s;a)$ – некоторая функция, известная с точностью до вектора параметров $a = (a_k) \in R^m$. Относительное число параметров:

$$\varkappa_{\mathrm{II}} = \frac{m}{N^s(N-1)} \le 1.$$

Примеры малопараметрических ДВР в рамках подхода II: модель Джекобса – Льюиса, MTD-модель, DAR(s), BCNAR(s), BiCNAR(s), PCNAR(s).

5 Малопараметрические модели ДВР на основе подхода I и их статистический анализ

5.1 Цепь Маркова MC(s,r) порядка s с r частичными связями

Эта модель определяется формулой (6) с $B(j_1,\ldots,j_s) = \left(j_{m_1^0},\ldots,j_{m_r^0}\right)$ [1,2]:

$$p_{J_1^{s+1}} = p_{j_1,\ldots,j_s,j_{s+1}} = q_{j_{m_1^0},\ldots,j_{m_r^0},j_{s+1}},\ J_1^{s+1} \in A^{s+1}, \tag{8}$$

где $J_i^k = (j_i, j_{i+1},\ldots,j_k){\in}A^{k-i+1}$ – последовательность $k-i+1$ индексов; r – число связей; $M_r^0 = (m_1^0,\ldots,m_r^0)$ – вектор с r упорядоченными целыми компонентами $1 = m_1^0 < m_2^0 < \ldots < m_r^0 \le s$, называемый шаблоном связей; $Q = \left(q_{J_1^{r+1}}\right)_{J_1^{r+1}\in A^{r+1}}$ – $(r+1)$-мерная стохастическая матрица. Если $r = s$, то получаем полносвязную цепь Маркова порядка s.

Теорема 1. *ДВР, определенный моделью (8), является эргодической цепью Маркова тогда и только тогда, когда существует $i \in \mathbb{N}$ такое, что*

$$\min_{J_1^s, J_{s+i+1}^{2s+i}\in A^s} \sum_{J_{s+1}^{s+i}\in A^i} \prod_{k=1}^{s+i} q_{j_{k+m_1^0-1},\ldots,j_{k+m_r^0-1},j_{k+s}} > 0. \tag{9}$$

Стационарное распределение вероятностей $(\pi^*_{J_1^s})_{J_1^{s+1}\in A^s}$ *удовлетворяет уравнениям:*

$$\pi^*_{J_2^{s+1}} = \sum_{j_1\in A} \pi^*_{J_1^s}\, q_{j_{m_1^0},\ldots,j_{m_r^0},j_{s+1}},\ J_1^{s+1}\in A^s. \tag{10}$$

Следствие 1. *Пусть ДВР (8) – стационарная цепь Маркова. Стационарное распределение вероятностей имеет мультипликативную форму*

$$\pi^*_{J_1^s} = \prod_{i=1}^{s} \pi^*_{j_i},\ J_1^s\in A^s,$$

тогда и только тогда, когда $\pi^*_{j_{r+1}} = \sum_{j_1\in A} \pi^*_{j_1}\, q_{J_1^{r+1}},\ J_2^{r+1}\in A^r,\ \sum_{j\in A}\pi^*_j = 1.$

Следствие 2. *В условиях Следствия 1, если матрица* Q *– дважды стохастическая:*

$$\sum_{j_1\in A} q_{J_1^{r+1}} \equiv 1,\ \sum_{j_{r+1}\in A} q_{J_1^{r+1}} \equiv 1,$$

то s*-мерное стационарное распределение вероятностей – равномерное:* $\pi^*_{J_1^s} \equiv N^{-s}$.

Примем обозначения: $X_1^n{=}(x_1,\ldots,x_n)\ \in\ A^n$ – реализация $\mathrm{MC}(s,r)$ длины n; $F\big(J_i^{i+s-1};M_r\big){=}(j_{i+m_1-1},\ldots,j_{i+m_r-1})$ – функция-селектор r-го порядка; $\delta_{J_1^k,I_1^k}{=}\prod_{l=1}^{k}\delta_{j_l,i_l}$ – символ Кронеккера для мультииндексов $J_1^k,\ I_1^k\in A^k$;

$$\nu_{J_1^{r+1}}(X_1^n;M_r) = \sum_{t=1}^{n-s} \delta_{F\left(X_t^{t+s-1};M_r\right),J_1^r}\delta_{x_{t+s},j_{r+1}} - \tag{11}$$

– частотная статистика $\mathrm{MC}(s,r)$ для шаблона $M_r\in\mathrm{M}$;

$$\mu_{J_1^{r+1}}(M_r) = \mathbf{P}\big\{F\big(X_t^{t+s-1};M_r\big) = J_1^r, x_{t+s} = j_{r+1}\big\} -$$

– распределение вероятностей $(r+1)$-граммы; точка вместо любого индекса означает суммирование по всем его значениям: $\mu_{J_1^r\cdot}(M_r){=}\sum_{j_{r+1}\in A}\mu_{J_1^{r+1}}(M_r)$.

Статистическое оценивание Q

Теорема 2. *Если шаблон связей* M_r^0 *известен, то оценка максимального правдоподобия (ОМП) для матрицы* Q *имеет вид:*

$$\hat{Q} = (\hat{q}_{J_1^{r+1}})_{J_1^{r+1}\in A^{r+1}},$$

$$\hat{q}_{J_1^{r+1}} = \begin{cases} \hat{\mu}_{J_1^{r+1}}(M_r^0)/\hat{\mu}_{J_1^r\cdot}(M_r^0),\ \textit{если}\ \hat{\mu}_{J_1^r\cdot}(M_r^0)>0, \\ 1/N,\ \textit{если}\ \hat{\mu}_{J_1^r\cdot}(M_r^0)=0, \end{cases} \tag{12}$$

где $\hat{\mu}_{J_1^{r+1}}(M_r){=}\nu_{J_1^{r+1}}(X_1^n;M_r)/(n-s)$ *– частотная оценка* $\mu_{J_1^{r+1}}(M_r)$, $J_1^{r+1}\in A^{r+1}$, $M_r{\in}\mathrm{M}$.

Теорема 3. *Для стационарной $MC(s,r)$ статистики $\{\hat{q}_{J_1^{r+1}} : J_1^{r+1} \in A^{r+1}\}$, определенные (12), – асимптотически ($n \to \infty$) несмещенные и состоятельные оценки с ковариациями, удовлетворяющими асимптотическому разложению:*

$$\mathrm{Cov}\{\hat{q}_{J_1^{r+1}}, \hat{q}_{K_1^{r+1}}\} = \sigma^{\hat{q}}_{J_1^{r+1},K_1^{r+1}}/(n-s) + \mathcal{O}(1/n^2), \tag{13}$$

где

$$\sigma^{\hat{q}}_{J_1^{r+1},K_1^{r+1}} = \delta_{J_1^r,K_1^r} \frac{q_{J_1^{r+1}}(\delta_{j_{r+1},k_{r+1}} - q_{K_1^{r+1}})}{\mu_{J_1^r\cdot}(M_r^0)},\ J_1^{r+1},\ K_1^{r+1} \in A^{r+1}.$$

Вдобавок, вероятностное распределение N^{r+1}-мерного случайного вектора $\big(\sqrt{n-s}$
$(\hat{q}_{J_1^{r+1}} - q_{J_1^{r+1}})\big)_{J_1^{r+1}\in A^{r+1}}$ *при $n\to\infty$ сходится к нормальному распределению с нулевым средним и ковариационной матрицей*

$$\Sigma^{\hat{q}} = \big(\sigma^{\hat{q}}_{J_1^{r+1},K_1^{r+1}}\big)_{J_1^{r+1},K_1^{r+1}\in A^{r+1}}.$$

Состоятельный статистический тест для проверки гипотез H_0: $Q{=}Q^0$, $H_1{=}\overline{H}_0$, с фиксированной (гипотетической) матрицей $Q^0 = (q^0_{J_1^{r+1}})_{J_1^{r+1}\in A^{r+1}}$ состоит из следующих четырех шагов.

1. Вычисление статистик $\nu_{J_1^{r+1}}(X_1^n; M_r^0)$, $J_1^{r+1} \in A^{r+1}$ согласно (11).

2. Вычисление статистики $\big(D_{J_1^r} = \{j_{r+1} \in A : q^0_{J_1^{r+1}} > 0\}\big)$

$$\rho = \sum_{J_1^r\in A^r,\ j_{r+1}\in D_{J_1^r}} \nu_{J_1^r\cdot}(X_1^n; M_r^0) \left(\hat{q}_{J_1^{r+1}} - q^0_{J_1^{r+1}}\right)^2 / q^0_{J_1^{r+1}}.$$

3. Вычисление P-значения: $P{=}1 - G_U(\rho)$, где $G_U(\cdot)$ – функция распределения χ^2 распределения с $U = \sum\limits_{J_1^r\in A^r} (|D_{J_1^r}| - 1)$ степенями свободы.

4. Решающее правило (ε – асимптотический уровень значимости): если $P \ge \varepsilon$, то заключаем, что гипотеза H_0 верна; в противном случае верна H_1.

Следствие 3. *Если $MC(s,r)$ стационарна и рассматривается семейство контигуальных альтернатив H_{1n}: $Q{=}Q^{1n}$,*

$$Q^{1n} = (q^{1n}_{J_1^{r+1}})_{J_1^{r+1}\in A^{r+1}},\ q^{1n}_{J_1^{r+1}} = q^0_{J_1^{r+1}}(1 + d_{J_1^{r+1}}/\sqrt{n-s}\,), \tag{14}$$

$\sum\limits_{j_{r+1}\in A} d_{J_1^{r+1}} q^0_{J_1^{r+1}} = 0$, $\sum\limits_{J_1^{r+1}\in A^{r+1}} |d_{J_1^{r+1}}| > 0$, *то при $n \to \infty$ мощность разработанного теста*

$$w \to 1 - G_{U,a}\big(G_U^{-1}(1-\varepsilon)\big),$$

где $G_{U,a}(\cdot)$ – функция распределения нецентрального χ^2 распределения с U степенями свободы и параметром нецентральности $a = \sum\limits_{J_1^{r+1}\in A^{r+1}} \mu_{J_1^{r+1}}\left(M_r^0\right)\ d^2_{J_1^{r+1}}$.

Уравнение (14) означает свойство контигуальности альтернатив H_{1n}: при увеличении длины n альтернатива H_{1n} приближается к H_0 со скоростью $\mathcal{O}(1/\sqrt{n}\,)$.

Статистическое оценивание шаблона связей M_r^0

Примем обозначения: M – множество допустимых шаблонов M_r;

$$H(M_r) = -\sum_{J_1^{r+1}\in A^{r+1}} \mu_{J_1^{r+1}}(M_r)\ln\Big(\mu_{J_1^{r+1}}(M_r)/\mu_{J_1^{r}\cdot}(M_r)\Big) \geq 0 - \qquad (15)$$

– условная энтропия будущего символа $x_{t+s}\in A$ при условии предыстории, выделяемой селектором $F\left(X_t^{t+s-1};\, M_r\right)\in A^r$, $M_r\in$ M; $\hat{H}(M_r)$ – «подстановочная» оценка условной энтропии, получающаяся подстановкой вместо истинных вероятностей $\mu_{J_1^{r+1}}(M_r)$ в (15) их оценок $\hat{\mu}_{J_1^{r+1}}(M_r)$, $J_1^{r+1}\in A^{r+1}$.

Теорема 4. *Если s, r известны, то ОМП для шаблона связей M_r^0 минимизирует оценку условной энтропии:*

$$\hat{M}_r = \arg\min_{M_r\in \mathrm{M}} \hat{H}(M_r).$$

Если $MC(s,r)$ стационарна, то $\hat{M}_r$ при $n\to\infty$ состоятельна: $\hat{M}_r \xrightarrow{\mathbf{P}} M_r^0$.

Статистическое оценивание r, s

Пусть $s\in[s_-,s_+]$, $r\in[r_-,r_+]$, $1\leq s_-<s_+<\infty$, $1\leq r_-<r_+<s_+$.

Для оценивания r, s мы используем Байесовский Информационный Критерий (Bayesian Information Criterion), который имеет вид:

$$BIC(s,r) = 2(n-s)\hat{H}(\hat{M}_r) + U\ln(n-s)\,, \qquad (16)$$

$$U = \sum_{J_1^r\in A^r} (|D_{J_1^r}| - 1 + \delta_{\hat{\mu}_{J_1^r\cdot}(\hat{M}_r),0}),\ D_{J_1^r} = \{j_{r+1}\in A : \hat{\mu}_{J_1^{r+1}}(\hat{M}_r) > 0\}.$$

Статистические оценки s, r определяются при минимизации:

$$BIC(s,r) \to \min_{s_-\leq s\leq s_+,\, r_-\leq r\leq r_+}\,. \qquad (17)$$

Теорема 5. *Если $MC(s,r)$ стационарна, то BIC-оценки $\hat{r}$, $\hat{s}$ определяемые (16), (17), при $n\to\infty$ состоятельны.*

Статистическую оценку $\hat{Q}$ удобно использовать для визуализации уклонения от гипотезы H_0 (для которой $q_{i_1,\ldots,i_{r+1}} = N^{-1}$). На рис. 3, 4 представлены результаты такой визуализации для генератора со случайной обратной связью и генератора BelT (СТБ 34.101.27-2011 в режиме гаммирования) соответственно; здесь красный цвет – оценка условной вероятности перехода в «0» $\hat{q}_{K_1^r,0}$, зеленый – в «1» $\hat{q}_{K_1^r,1}$); здесь по оси абсцисс откладывается $K_1^r = F\left(J_1^s;\hat{M}_r\right)\in A^r$.

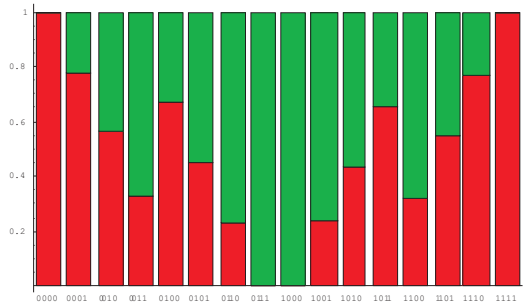


Рис. 3. Оценка $\hat{Q}$ (s=63, r=4, T=10^5)

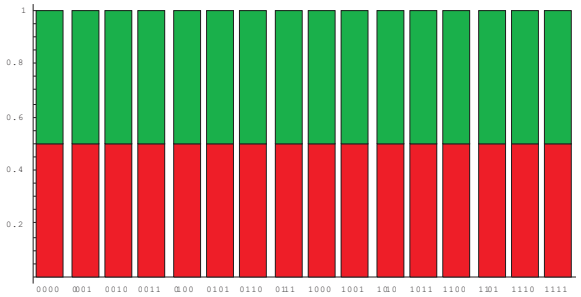


Рис. 4. Оценка $\hat{Q}$ (s=32, r=4, $T = 8{\cdot}10^6$)

5.2 Цепь Маркова условного порядка MCCO(s, L)

Примем обозначения: $l \in \{1, 2, \ldots, s{-}1\}$, $K{=}N^l{-}1$; $Q^{(1)}, \ldots, Q^{(M)}$ $(1{\leq}M{\leq}K{+}1)$ – M-различных квадратных стохастических матриц порядка N:

$$Q^{(m)} = \left(q_{i,j}^{(m)}\right),\ 0 \leq q_{i,j}^{(m)} \leq 1,\ \sum_{j \in A} q_{i,j}^{(m)} \equiv 1,\ i, j \in A,\ 1 \leq m \leq M;$$

$< J_n^m >= \sum_{k=n}^{m} N^{k-n} j_k$ – числовое представление мультииндекса $J_n^m \in A^{m-n+1}$; $\mathrm{I}\{C\}$ – индикаторная функция; $1 \leq m_k \leq M$, $1 \leq b_k \leq s - L$, $0 \leq k{\leq}K$.

Последовательности $\{m_k\}$, $\{b_k\}$ фиксированы, $\min\limits_{0 \leq k \leq K} b_k{=}1$, и все элементы множества $\{1, 2, ..., M\}$ представлены в последовательности $m_0, \ldots, m_K$.

Цепь Маркова $\{x_t \in A : t \in \mathbb{N}\}$ называется цепью Маркова условного порядка (MCCO(s, L)), если одношаговые вероятности переходов имеют следующее малопараметрическое представление:

$$p_{J_1^{s+1}} = \sum_{k=0}^{K} \mathrm{I}\{< J_{s-L+1}^{s} >= k\} q_{j_{b_k}, j_{s+1}}^{(m_k)}; \tag{18}$$

величина $s_k = s - b_k + 1$ называется условным порядком цепи Маркова. Согласно (18) условное распределение состояния x_{t+1} в момент $t + 1$ зависит не от всех s предыдущих состояний, а лишь от $L{+}1$ избраных $\left(j_{b_k}, J_{s-L+1}^{s}\right)$. Заметим, что если $L = s - 1$, $s_0 = s_1 = \ldots = s_K = s$,то мы получаем полносвязную цепь Маркова порядка s: MC(s).

Методы и алгоритмы статистического анализа MCCO(s, L) представлены в [7].

6 Малопараметрические модели ДВР на основе подхода II и их статистический анализ

6.1 Модель Джекобса – Льюиса

Эта модель порождается стохастическим разностным уравнением [6]:

$$x_t = \mu_t x_{t-\eta_t} + (1-\mu_t)\xi_t, \tag{19}$$

где $t > s$, $\{\xi_t, \eta_t, \mu_t\}$ – независимые в совокупности случайные величины с вероятностными распределениями:

$$\mathbf{P}\{\mu_t = 1\} = 1 - \mathbf{P}\{\mu_t = 0\} = \rho;$$

$$\mathbf{P}\{\eta_t = i\} = \lambda_i,\ i \in \{1, 2, \ldots, s\},\ \sum_{i=1}^{s} \lambda_i = 1,\ \lambda_s \neq 0; \tag{20}$$

$$\mathbf{P}\{\xi_t = k\} = \pi_k,\ k \in A,\ \sum_{k \in A} \pi_k = 1;$$

$$\mathbf{P}\{x_1 = k\} = \ldots = \mathbf{P}\{x_s = k\} = \pi_k,\ k \in A.$$

Относительное число параметров этой модели линейно (а не экспоненциально!) зависит от s:

$$\varkappa_{JL} = \frac{N + s - 1}{N^s(N-1)}.$$

Теорема 6. *ДВР x_t, определяемый (19), (20), – это однородная цепь Маркова порядка s с начальным распределением $\pi_{i_1,\ldots,i_s} = \pi_{i_1} \cdot \ldots \cdot \pi_{i_s}$ и $(s+1)$-мерной матрицей вероятностей одношаговых переходов $P(\pi, \lambda, \rho) = (p_{i_1,\ldots,i_{s+1}})$:*

$$p_{i_1,\ldots,i_s,i_{s+1}} = (1-\rho)\pi_{i_{s+1}} + \rho \sum_{j=1}^{s} \lambda_j \delta_{i_{s-j+1},i_{s+1}},\ i_1, \ldots, i_{s+1} \in A. \tag{21}$$

Следствие 4. *ОМП $(\hat{\pi}, \hat{\lambda}, \hat{\rho})$ параметров π, λ, ρ по наблюдениям $x_1, \ldots, x_n$ определяются как решение задачи максимизации:*

$$l(\pi, \lambda, \rho) = \sum_{t=1}^{s} \ln \pi_{x_t} + \sum_{t=s+1}^{n} \ln\left((1-\rho)\pi_{x_t} + \rho \sum_{j=1}^{s} \lambda_j \delta_{x_{t-j},x_t}\right) \to \max_{\pi,\lambda,\rho}. \tag{22}$$

Методы и алгоритмы статистического анализа модели Джекобса – Льюиса представлены в [2].

6.2 MTD-модели Рафтери

MTD (Mixture Transition Distribution)-модель [10] определяется следующим частным случаем уравнения (7):

$$p_{i_1,\ldots,i_s,i_{s+1}} = \sum_{j=1}^{s} \lambda_j q_{i_j,i_{s+1}},\ i_1, \ldots, i_{s+1} \in A,$$

где $Q = (q_{i,k})$ – некоторая стохастическая $(N \times N)$-матрица,

$$0 \leq q_{i,k} \leq 1,\ \sum_{k \in A} q_{i,k} \equiv 1,\ i, k \in A,$$

$\lambda = (\lambda_1, \ldots, \lambda_s)'$ – некоторое дискретное распределение вероятностей, $\lambda_1 > 0$. Обобщенная MTDg (generalized MTD)-модель определяется следующей параметризацией $(s+1)$-мерной матрицы $\mathbf{P}$:

$$p_{i_1,\ldots,i_s,i_{s+1}} = \sum_{j=1}^{s} \lambda_j q^{(j)}_{i_j,i_{s+1}},\ i_1,\ldots,i_{s+1} \in A, \tag{23}$$

где $Q^{(j)} = \left(q^{(j)}_{i,k}\right)$ – некоторая стохастическая матрица для j-го лага.

Относительное число параметров MTDg-модели:

$$\varkappa_{\text{MTDg}} = (s(N(N-1)/2+1)-1)/(N^s(N-1)).$$

Свойства стационарного распределения вероятностей

Теорема 7. *Для MTDg-модели (22), если* $\exists K \in \mathbb{N}$: $\left((Q^{(1)})^K\right)_{ij} > 0$, $\forall i,j \in A$, *то* s*-мерное стационарное распределение имеет вид* $(i_1,\ldots,i_s \in A)$*:*

$$\pi^*_{i_1,\ldots,i_s} = \prod_{l=0}^{s-1}\left(\pi^*_{i_s-l} + \sum_{j=l+1}^{s}\lambda_j\left(q^{(j)}_{i_{j-l},i_s-l} - \sum_{r=0}^{N-1} q^{(j)}_{r,i_s-l}\pi^*_r\right)\right).$$

Следствие 5. *Для эргодической MTD-модели 2-мерное стационарное распределение случайного вектора* $(x_{t-m}, x_t)'$, $1 \le m \le s$, *имеет вид:*

$$\pi^*_{ki}(m) = \pi^*_k\pi^*_i + \pi^*_k\lambda_{s-m+1}(q_{ki} - \pi^*_i),\ i,k \in A.$$

Используя свойства стационарного распределения вероятностей, установленные Теоремой 7 и Следствием 5, разработаны методы и алгоритмы статистического анализа MTD-модели, представленные в [2].

6.3 Биномиальная условно нелинейная авторегрессионная модель BiCNAR(s)

Эта модель порождается специальным (биномиальным) случаем порождающего уравнения (7):

$$p_{i_1,\ldots,i_s,i_{s+1}} = C^{i_{s+1}}_{N-1}\theta^{i_{s+1}}(1-\theta)^{N-1-i_{s+1}},\ i_{s+1} \in A = \{0,1,\ldots,N-1\}, \tag{24}$$

$$\theta = \theta\left(\mathrm{I}^s_1\right) = \mathrm{F}\left(a'\Psi\left(\mathrm{I}^s_1\right)\right),\ \mathrm{I}^s_1 = (i_1,\ldots,i_s)' \in A^s,$$

где $\Psi\left(\mathrm{I}^s_1\right) = \left(\psi_1\left(\mathrm{I}^s_1\right),\ldots,\psi_m\left(\mathrm{I}^s_1\right)\right)'$: $A^s \to R^m$ – вектор-столбец $m \le N^s$ линейно независимых функций, например, полиномов; $\mathrm{F}(\cdot)$: $R^1 \to [0,1]$ – некоторая функция распределения, например, логистическая, нормальная или Коши:

$$\Lambda(\zeta) = \frac{1}{1+e^{-\zeta}},\ \Phi(\zeta) = \frac{1}{\sqrt{2\pi}}\int\limits_{-\infty}^{\zeta} e^{-\frac{x^2}{2}}dx,\ C(\zeta) = \frac{1}{2} + \frac{\arctan(\zeta)}{\pi},\ \zeta \in R^1;$$

$a = (a_1, \ldots, a_m)'$ – вектор-столбец m неизвестных параметров модели.

Относительное число параметров модели: $\varkappa = m\big(N^s(N-1)\big)^{-1} \le 1$.

Примем обозначения: $\mathrm{F}^{-1}(\cdot)$ – квантильная функция; $X_1^T = (x_1, \ldots, x_T)' \in A^T$ – наблюдаемый ДВР длины T;

$$\hat{\theta}(J) = \frac{1}{N-1} \cdot \frac{\sum\limits_{t=s+1}^{T} x_t \mathrm{I}\{X_{t-s}^{t-1} = J\}}{\sum\limits_{t=s+1}^{T} \mathrm{I}\{X_{t-s}^{t-1} = J\}}, \; J \in A^s; \tag{25}$$

$B = (b_J)$ – $(N^s \times 1)$-вектор-столбец, $b_J = \mathrm{F}^{-1}(\hat{\theta}(J))$; $H = (h_{J,J'})$ – некоторая фиксированная $(N^s \times N^s)$-симметричная неотрицательно определенная матрица; $\mathbf{\Psi} = (\Psi(J))$ – $(m \times N^s)$-матрица; O_m – нулевой m-вектор.

Теорема 8. *Если* $\mathrm{F}(\cdot)$ *удовлетворяет условиям гладкости:* $0<\mathrm{F}(\zeta)<1$, $0<\mathrm{F}'(\zeta)<+\infty$, $\mathrm{F}(\cdot)$ *и* $\mathrm{F}^{-1}(\cdot)$ *– дважды дифференцируемы, и* $|\mathbf{\Psi} H \mathbf{\Psi}'| \neq 0$, *то FBE-оценка (Frequencies Based Estimator)*

$$\hat{a} = (\mathbf{\Psi} H \mathbf{\Psi}')^{-1} \mathbf{\Psi} H B \tag{26}$$

состоятельна и асимптотически нормальна при $T \to +\infty$*:*

$$\hat{a} \xrightarrow{\mathbf{P}} a, \; \sqrt{T}(\hat{a} - a) \xrightarrow{\mathbf{D}} \mathcal{N}_m(O_m, \Sigma_H),$$
$$\Sigma_H = (\mathbf{\Psi} H \mathbf{\Psi}')^{-1} \mathbf{\Psi} H J^{-1} H (\mathbf{\Psi} H \mathbf{\Psi}')^{-1},$$

где J *– информационная матрица Фишера.*

Методы и алгоритмы статистического анализа BiCNAR(s)-модели, ее частных случаев и обобщений представлены в [3,8,9].

7 Заключение

1. В криптологии актуальна проблема построения и статистического анализа моделей дискретных временных рядов, адекватно описывающих отклонения от модели РРСП.
2. В статье представлены такие семейства моделей ДВР на основе уклонений от s-мерной равномерности и на основе цепей Маркова порядка s.
3. Для преодоления «проклятия размерности» в статье представлены два подхода к построению малопараметрических моделей цепей Маркова высокого порядка.
4. Разработаны методы и алгоритмы статистического анализа (оценивание параметров, проверка гипотез) малопараметрических моделей, построенных на основе предложенных подходов.
5. Теоретические результаты иллюстрируются результатами компьютерных экспериментов по тестированию выходных последовательностей известных криптографических генераторов.

Библиографические ссылки

[1] Харин Ю.С. (2004). Цепи Маркова с r-частичными связями и их статистическое оценивание. *Доклады НАН Беларуси*. Т. **48**, № 1, С. 40–44.

[2] Харин Ю.С., Агиевич С.В., Васильев Д.В., Матвеев Г.В. (2013). *Криптология*. БГУ, Минск.

[3] Харин Ю.С., Волошко В.А. (2019). Биномиальные условно нелинейные авторегрессионные модели дискретных временных рядов и их вероятностные и статистические свойства. *Труды Института Математики НАН Беларуси*. Т. **26**, № 1, С. 95–105.

[4] Харин Ю.С., Палуха В.Ю. (2017). Энтропийный анализ криптографических генераторов случайных и псевдослучайных последовательностей. *Веснік сувязі*. Т. **146**, № 1, С. 46–49.

[5] Buhlmann P., Wyner A.J. (1999). Variable length Markov chains. *The Annals of Statistics*. Vol. **27**, No. 2, pp. 480–513.

[6] Jacobs P.A., Lewis P.A.W. (1978). Discrete time series generated by mixtures I: correlational and runs properties. *Journal of the Royal Statistical Society. Ser. B*. Vol. **40**, No. 1, pp. 94–105.

[7] Kharin Yu., Maltsew M. (2017). Statistical analysis of high-order dependencies. *Acta et Commentationes Universitetas Tartuensis de Mathematica*. Vol. **21**, No. 1, pp. 37–45.

[8] Kharin Yu.S., Voloshko V.A., Medved E.A. (2019). Statistical estimation of parameters for binary conditionally nonlinear autoregressive time series. *Mathematical Methods of Statistics*. Vol. **26**, No. 2, pp. 103–118.

[9] Kharin Yu., Zhurak M. (2015). Statistical analysis of spatio-temporal data based on Poisson conditional autoregressive model. *INFORMATICA*. Vol. **26**, No. 1, pp. 67–87.

[10] Raftery A. (1985). A model for high-order Markov chains. *Journal of the Royal Statistical Society. Ser. B*. Vol. **47**, No. 3, pp. 528–539.

МЕТОД ДЕЛЕНИЯ НА ДВОИЧНУЮ ЭКСПОНЕНТУ ДЛЯ ВЫПОЛНЕНИЯ ДЕКОДИРУЮЩЕЙ ОПЕРАЦИИ В ПОРОГОВОМ МИМА-КРИПТОМОДУЛЕ РАЗДЕЛЕНИЯ СЕКРЕТА С МАСКИРУЮЩИМ ПРЕОБРАЗОВАНИЕМ

А.Ф. Чернявский[b], А.А. Коляда[a], С.Ю. Протасеня[b]
Институт прикладных физических проблем имени А.Н. Севченко
Минск, БЕЛАРУСЬ
e-mail: [a]razan@tut.by, [b]estellita@mail.ru

Представлена новая разработка метода выполнения в пороговом криптомодуле разделения секрета с маскирующим преобразованием декодирующей операции. Для решения рассматриваемой задачи применены рекурсивная схема деления на двоичную экспоненту и вычислительная технология на диапазонах больших чисел таблично-сумматорного типа, основанная на минимально избыточной модулярной арифметике (МИМА). Отличительной особенностью развиваемого подхода является использование в качестве области принадлежности секрета-оригинала конечных колец вычетов по модулям, имеющим вид степеней числа 2. Это существенно уменьшает сложность результирующей декодирующей МИМА-процедуры.
Ключевые слова: пороговое разделение секрета; криптосхемы разделения секрета; маскирующее преобразование; декодирующая операция; модулярный код; модулярные системы счисления; минимально избыточная модулярная арифметика

1 Введение

Важнейшей актуальной задачей современного процесса развития распределенных компьютерных и инфокоммуникационных систем является надежное обеспечение необходимого уровня безопасности при хранении, обработке и передаче данных [2,3]. При решении обозначенной задачи особую роль выполняет применяемая технология управления криптографическими ключами. В настоящее время к наиболее перспективным технологиям такого рода относят технологию активной безопасности [2,3], которая базируется на периодическом обновлении ключей, одноразовых паролях и пространственном разделении секрета. На практике разделение секретной информации обычно осуществляется в рамках пороговых схем [1,3,4,5].

Реализуемое (t, n)-пороговой системой решающее правило обеспечивает разделение секрета n абонентами с возможностью его восстановления по компонентам, принадлежащим любым l участникам сеанса связи ($2 \leq t \leq l \leq n$; t – пороговое число абонентов). При этом группы абонентов числом $k < t$ реконструировать секрет-оригинал по соответствующим компонентам не могут. Исходный и долевые

секреты представляют собой большие целые числа (ЦЧ), поэтому эффективность выполняемых в пороговых криптосистемах преобразований определяется реализационными свойствами используемой технологии перевода осуществляемых вычислений из диапазонов больших чисел в диапазоны ЦЧ стандартной разрядности. В свете сказанного в качестве компьютерно-арифметической основы для криптографических приложений рассматриваемого класса целесообразно принять модулярную арифметику – арифметику модулярных систем счисления (МСС). Фундаментальные преимущества МСС наиболее полно удается реализовать в рамках так называемого минимально избыточного кодирования [1,3].

Наиболее трудоемкой операцией в пороговых криптосистемах модулярной арифметики разделения секретной информации является реконструкция секрета-оригинала по модулярным кодам маскирующего аналога. Это обусловлено главным образом использованием в операциях данного класса вычислительных технологий, ориентированных на диапазоны больших чисел, а также соответствующих конфигураций интегрально-характеристической базы системы счисления в остатках. Настоящее сообщение посвящено разработке метода выполнения декодирующей операции в пороговом криптомодуле разделения секрета, базирующемся на минимально избыточной модулярной арифметике (МИМА) [1]. Применение вычислительной МИМА-технологии на диапазонах больших чисел для решения рассматриваемой задачи позволяет в значительной мере минимизировать необходимые временные и аппаратурные затраты.

2 Принципиальные основы пороговых МИМА-криптосхем разделения секрета с маскирующим преобразованием

Введем обозначения:

$\lfloor a \rfloor$ и $\lceil a \rceil$ – наибольшее и наименьшее ЦЧ соответственно не большее и не меньшее вещественной величины a;

НОД(A, B) – наибольший общий делитель целых чисел A и B;

$\mathbb{Z}_m = \{0, 1, \ldots, m-1\}$ – множество наименьших неотрицательных вычетов (остатков) по натуральному модулю $m > 1$;

$\chi = |A/B|_m = (A/B) \pmod m$ – элемент множества $\mathbb{Z}_m$, удовлетворяющий сравнению $B_\chi \equiv A \pmod m$ $(B \neq 0,\ \text{НОД}(B, m) = 1)$;

$\mathbf{M}\_l = \{m_1,\ m_2,\ \ldots,\ m_l\}$ – базис МСС, состоящий из $l > 1$ попарно простых модулей (оснований);

$(|X|_{m_1},\ |X|_{m_2},\ \ldots,\ |X|_{m_l})$ – представление ЦЧ X (модулярный код) в МСС с базисом $\mathbf{M}\_l$.

Пусть $p_1, p_2, \ldots, p_n$ – упорядоченные по возрастанию попарно простые большие натуральные числа $(n > 1)$; $P_i = \prod_{s=1}^{i} p_s \quad ; \ \_P_j = \prod_{s=1}^{j} p_{n-s+1} \ = /P_{n-j} \quad (i, j = \overline{1, n})$; $\mathbf{P} = \{p_1, p_2, \ldots, p_n\}$; $\mathbf{I}\_l = \{\forall\ (i_1,\ i_2,\ \ldots,\ i_l) | 1 \le i_1 < i_2 < \cdots < i_l \le n;\ 2 \le t \le l \le n\}$ (t – фиксированное натуральное число); $I\_l = (i_1,\ i_2,\ \ldots,\ i_l)$ – произвольный элемент множества $\mathbf{I}\_l$; $\mathbf{P}_{I\_l} = \{p_{i_1},\ p_{i_2},\ \ldots,\ p_{i_l}\}$; $P_{I\_l} = \prod_{j=1}^{l} p_{i_j}$.

Концептуальную основу (t, n)-пороговой схемы разделения секрета с модулярным базисом $\mathbf{P} = \mathbf{P}\_n = \{p_1,\ p_2,\ \ldots, p_n\}$ которая рассчитана на полное число n и пороговое число t абонентов распределенной системы, составляют нижеследующие определяющие положения.

А. Исходный секрет (секрет-оригинал) представляет собой ЦЧ $S \in \mathbf{Z}_p$ (p – большой модуль, взаимно простой с $p_1, p_2, \ldots, p_n$).

Б. Над S в МСС с базисом $\mathbf{P}$ выполняется маскирующее преобразование вида

$$\tilde{S} = S + C \cdot p, \tag{1}$$

где C – псевдослучайный целочисленный параметр.

Цифры $\tilde{\sigma}_i = \left|\tilde{S}\right|_{p_i} = \left|\sigma_i + |C \cdot p|_{p_i}\right|_{p_i}$ $(\sigma_i = |S|_{p_i};\ i = \overline{1, n})$ получаемого кода $(\tilde{\sigma}_1,\ \tilde{\sigma}_2,\ \ldots,\ \tilde{\sigma}_n)$ рассматриваются как долевые (частичные) секреты, принадлежащие одноименным абонентам.

В. Любые l абонентов $(t \le l \le n)$ могут восстановить секрет-оригинал S по принадлежащим им долевым (маскирующим) секретам. Но никакая группа абонентов количеством $k < t$ сделать этого не может.

Представляемые исследования нацелены на решение задачи восстановления секрета-оригинала Sпо кодам $(\tilde{\sigma}_{i_1},\ \tilde{\sigma}_{i_2},\ \ldots,\ \tilde{\sigma}_{i_l})$ МСС с базисами $\mathbf{P}_{I\_l}(I\_l \in \mathbf{I}\_l)$ маскирующего аналога (1) (см. пункт А) с обеспечением минимизации временных затрат на выполнение результирующей декодирующей процедуры при сохранении максимального уровня криптостойкости, присущего классическим пороговым схемам, таким, в частности, как схемы Шамира, Блэкли и другие [5]. При этом для синтеза искомого декодирующего алгоритма (алгоритма восстановления секрета-оригинала) используются метод деления на двоичную экспоненту, а также вычислительная МИМА-технология [4].

Основополагающая идея предлагаемой алгоритмизации преобразования $\tilde{S} > S$ состоит в использовании для кодирования секрета-маски $\tilde{S}$ семейства минимально избыточных МСС (МИМСС), определяемых базисами $\mathbf{P}I\_l$, которые отвечают группам абонентов числом l. Без нарушения общности изложение дальнейшего материала преимущественно проводится на примере группы абонентов, за которыми закрепляются основания $p_1, p_2, \ldots, p_l$ набора $\mathbf{P}\_l$ – представителя множества $\mathbf{P}_{\mathbf{I}\_l}$ с $I\_l = (1, 2, \ldots, l) \in \mathbf{I}\_l$. Долевые секрета, принадлежащие абонентам указанной группы являются цифрами кода $(\tilde{\sigma}_1,\ \tilde{\sigma}_2, \ldots,\ \tilde{\sigma}_l)$ МСС с модулями $p_1, p_2, \ldots, p_l$ секрета-маски $\tilde{S}$.

В компьютерных алгоритмах МИМА фундаментальную роль выполняет интервально-модулярная форма чисел. В случае ЦЧ $\tilde{S} = (\tilde{\sigma}_1,\ \tilde{\sigma}_2, \ldots,\ \tilde{\sigma}_l)$ она имеет вид

$$\tilde{S} = \sum_{i=1}^{l-1} P_{i,l-1}\tilde{\sigma}_{i,\ l-1} + P_{l-1}I_l\left(\tilde{S}\right), \tag{2}$$

где $P_{i,l-1} = \frac{P_{l-1}}{p_i},\ P_{l-1} = \prod_{s=1}^{l-1} p_s$;

$$\tilde{\sigma}_{i,\ l-1} = \left|P_{i,l-1}^{-1}\tilde{\sigma}_i\right|_{p_i}; \tag{3}$$

$I_l\left(\tilde{S}\right)$ – интервальный индекс числа $\tilde{S}$ по базису $\mathbf{P}\_l$. Принцип минимально избыточного модулярного кодирования раскрывает нижеследующая теорема [4].

Теорема 1. *Для того, чтобы в МСС с базисом* $\mathbf{P}\_l$ *интервальный индекс* $I_l\left(\tilde{S}\right)$ *каждого элемента* $\tilde{S}$ *диапазона* $\mathbb{Z} = \{0, 1, ..., P-1\}$ *($P = p_0 P_{l-1}$; p_0 – вспомогательный модуль) полностью определялся вычетом* $\hat{I}_l(\tilde{S}) = \left|I_l(\tilde{S})\right|_{p_l}$, *необходимо и достаточно выполнения условия*

$$p_l \geq 2p_0 + l - 2 \quad (p_0 \geq l - 2). \tag{4}$$

При этом для $I_l(\tilde{S})$ *верны расчетные соотношения:*

$$I_l(\tilde{S}) = \begin{cases} \hat{I}_l(\tilde{S}), \ \textit{если } \hat{I}_l(\tilde{S}) < p_0, \\ \hat{I}_l(\tilde{S}) - p_l, \ \textit{если } \hat{I}_l(\tilde{S}) \geq p_0; \end{cases} \tag{5}$$

$$\hat{I}_l(\tilde{S}) = \left| \sum_{\mathrm{i}=1}^{l} R_{i,l}(\tilde{\sigma}_i) \right|_{p_l}; \tag{6}$$

$$R_{i,l}(\tilde{\sigma}_i) = \left| -p_i^{-1} \mid P_{i,l-1}^{-1}\tilde{\sigma}_i \right|_{p_i}\Big|_{p_l} \ (i \neq l), \ R_{l,l}(\tilde{\sigma}_l) = \left| \frac{\tilde{\sigma}_l}{P_{l-1}} \right|_{p_l}. \tag{7}$$

Главное преимущество МИМСС с базисами $\mathbf{P}_{I\_l}$ ($I\_l \in \mathbf{I}\_l$) над неизбыточными аналогами обусловлено l-кратным сокращением реализационных затрат на вычисление интервального индекса, осуществляемое по формулам вида (5) – (7) [4].

Корректное согласование порогового принципа разделения секрета и минимально избыточного модулярного кодирования с обеспечением необходимого уровня криптостойкости результирующей МИМА-схемы дает нижеследующая теорема.

Теорема 2. *Для того, чтобы любые* l *абонентов* ($2 \leq t \leq l \leq n$; t – *фиксированное ЦЧ) могли восстановить* S *по соответствующему коду МСС маскирующего секрета* $\tilde{S}$, *удовлетворяющей условию вида* (4) *минимальной избыточности (см. теорему 1), но никакая группа абонентов числом* $k < t$ *не имела такой возможности, достаточно выполнения системы условий:*

$$\begin{cases} \tilde{S} \ \in \ \tilde{\mathbf{S}} = \left\{\tilde{S}_{нп}, \ \tilde{S}_{нп}+1, \ \ldots, \tilde{S}_{вп}\right\} \subseteq \{\_P_{t-1}, \_P_{t-1}+1, .., p_0 P_{t-1}-1\}, \\ C \in \widetilde{\mathbf{C}} = (\mathbf{C} \backslash \mathbf{C}_p), \end{cases}$$

где $\tilde{S}_{нп}$ *и* $\tilde{S}_{вп}$ – *используемые нижнее и верхнее пороговые значения секрета-маски* $\tilde{S}$; p_0 – *вспомогательный модуль, удовлетворяющий ограничению* $p_0 \leq p_t - t + 2$; $\mathbf{C} = \{C_{НП}, C_{НП}+1, \ldots, C_{ВП}\}$ $\left(C_{НП} = \left\lfloor \tilde{S}_{НП}/p \right\rfloor; \ C_{ВП} = \left\lfloor \tilde{S}_{ВП}/p \right\rfloor\right)$; $\mathbf{C}_p = \left\{\forall C \in \mathbf{C} | S + C \cdot p \ \in \ (\tilde{S}_{НП}; \tilde{S}_{ВП}); \ Q\left(\tilde{S}; j_1, \ j_2, \ \ldots, \ j_k\right) = \left\lfloor \frac{\tilde{S}}{\prod_{i=1}^{k} p_{j_i}} \right\rfloor \quad (1 \leq j_1 < j_2 < \cdots < j_k \leq n; \ 2 \leq k < t)\}$, p – *делитель ЦЧ* Q.

3 Метод выполнения декодирующей операции в пороговом МИМА-криптомодуле разделения секрета с маскирующим преобразованием

Реконструкция секрета-оригинала по модулярным кодам маскирующего аналога является наиболее трудоемкой операцией в пороговых МА-криптосистемах разделения секрета. Из (1) вытекает равенство $S = \left|\tilde{S}\right|_p$, указывающее на то, что для получения S по $\tilde{S}$ достаточно ЦЧ $\tilde{S}$ привести к остатку по модулю p.

Рассмотрим случай, когда p представляет собой двоичную экспоненту: $p = 2^{b\_p}$ и пусть $r = 2^{b\_r}$, $b\_r \le b\_p$, $\nu = \lceil b\_p/b\_r \rceil$, $(\tilde{s}_{\nu-1} \ \ \tilde{s}_{\nu-2} \ldots \ \tilde{s}_0)_r$ $(\tilde{s}_j \in \mathbb{Z}_r;\ j = \overline{0, \nu-1})$ – код числа $\left|\tilde{S}\right|_{r^\nu}$ в позиционной системе счисления (ПСС) с основанием r разрядностью ν цифр. Тогда основой для восстановления секрета-оригинала S по маскирующему секрету $\tilde{S}$ может служить формула

$$S = \left|\tilde{S}\right|_p = \left|\tilde{S}\right|_{2^{b\_p}} = (s_{\nu-1} \ s_{\nu-2} \ \ldots \ s_0)_r \tag{8}$$

где

$$s_j = \begin{cases} \tilde{s}_j \ \text{ при } j = \overline{0, \ \nu-2}, \\ \tilde{s}_{\nu-1} \,(\mathrm{mod} \ \ (\exp_2 (b\_p - (\nu-1)\, b\_r))) \ \text{ при } j = \nu-1. \end{cases} \tag{9}$$

Из (8), (9) следует, что в случае $p = 2^{b\_p}$ решение поставленной задачи: $\mathbf{P}\_l = \{p_1, p_2, \ldots, p_l\}$, сводится к преобразованию минимально избыточного модулярного кода (МИМК) $(\tilde{\sigma}_1, \ \tilde{\sigma}_2, \ \ldots, \ \tilde{\sigma}_l)$ в позиционный r-ичный код $(\tilde{s}_{\nu-1} \ \ \tilde{s}_{\nu-2} \ldots \ \tilde{s}_0)_r$. Это преобразование может быть осуществлено по методу деления на двоичную экспоненту [4]: маскирующего секрета $\tilde{S} = (\tilde{\sigma}_1, \tilde{\sigma}_2, \ldots, \tilde{\sigma}_l)$ на $r = 2^{b\_r}$, причем по упрощенному МИМА-алгоритму.

Преобразование минимально избыточного модулярного кода $(\tilde{\sigma}_1, \tilde{\sigma}_2, \ldots, \tilde{\sigma}_l)$ в позиционный r-ичный код $(\tilde{s}_{\nu-1} \ \ \tilde{s}_{\nu-2} \ldots \ \tilde{s}_0)_r$ числа $\tilde{S}$ методом деления на двоичную экспоненту $r = 2^{b\_r}$ базируется на операционном кортеже рекурсивного типа:

$$\begin{gathered} \left\langle \tilde{S}_0 = \tilde{S}, \ \tilde{s}_0 = \left|\tilde{S}_0\right|_r ; \tilde{S}_1 = \left\lfloor \tilde{S}_0/r \right\rfloor, \ \tilde{s}_1 = \left|\tilde{S}_1\right|_r ; \ \tilde{S}_2 = \left\lfloor \tilde{S}_1/r \right\rfloor, \ \tilde{s}_2 = \left|\tilde{S}_2\right|_r ; \ldots ; \right. \\ \left. \tilde{S}_{\nu-1} = \left\lfloor \tilde{S}_{\nu-2}/r \right\rfloor, \ \tilde{s}_{\nu-1} = \left|\tilde{S}_{\nu-1}\right|_r \right\rangle . \end{gathered} \tag{10}$$

На j-й итерации процесса реализации (10) сначала формируется минимально избыточный модулярной код $(\tilde{\sigma}_1^{(j)}, \ \tilde{\sigma}_2^{(j)}, \ \ldots, \ \tilde{\sigma}_l^{(j)})$ ЦЧ $\tilde{S}_j$, а затем находится цифра $\tilde{s}_j$ его r-ичного позиционного кода путем расширения полученного минимально избыточного модулярного кода на модуль $r = 2^{b\_r}$ согласно правилу:

$$\tilde{s}_j = \left|\tilde{S}_j\right|_r = \left| \sum_{i=1}^{l-1} \left| P_{i,l-1} \tilde{\sigma}_{i,\ l-1}^{(j)} \right|_r + \left| P_{l-1} I_l(\tilde{S}_j) \right|_r \right|_r \quad \left(j = \overline{0, \nu-1}\right), \tag{11}$$

где

$$\tilde{\sigma}_{i,\ l-1}^{(j)} = \left| P_{i,l-1}^{-1} \tilde{\sigma}_i^{(j)} \right|_{p_i} ; \tag{12}$$

интервально-индексная характеристика $I_l\left(\tilde{S}_j\right)$ числа $\tilde{S}_j$ определяется по расчетным соотношениям (5)-(7) при $\tilde{S}=\tilde{S}_j$ и $\tilde{\sigma}_i=\tilde{\sigma}_i^{(j)}$ $(i=\overline{1,l})$.

Что касается числа $\tilde{S}_j$, то в соответствии с (10) для цифр его минимально избыточного модулярного кода верна формула

$$\tilde{\sigma}_i^{(j)}=\left|\left\lfloor\frac{\tilde{S}_{j-1}}{r}\right\rfloor\right|_{p_i}=\begin{cases}\tilde{\sigma}_i \text{ при } j=0,\\ \left|\left|\tilde{\sigma}_i^{(j-1)}-\tilde{s}_{j-1}\right|_{p_i}\cdot|r^{-1}|_{p_i}\right|_{p_i} \text{ при } j=\overline{1,\ \nu-1}\end{cases} \tag{13}$$

$$\left(i=\overline{1,l}\right).$$

Конкретный выбор способа компьютерной реализации базовых расчетных соотношений (10) – (13) предлагаемого метода модулярно-позиционного кодового преобразования в первую очередь определяется необходимостью оперирования в диапазонах больших чисел – в конечных кольцах по большим модулям $p_1,p_2,\ldots,p_n$. В частности, это относится к нормированным остаткам (12), вычетам (7) и (13).

Сравнительный анализ эффективности разработанного метода с неизбыточными версиями показывает, что по производительности он превосходит аналоги как минимум в $l(19l-3)/(22l-6)$ раз. В частности, при $l=7\div 40$ достигается $(6\div 35)$-кратное повышение производительности.

4 Заключение

Предложена МИМА-конфигурация метода деления на двоичную экспоненту для выполнения декодирующей операции в пороговом криптомодуле разделения секрета с маскирующим преобразованием. Главные отличительные особенности разработанного подхода к решению рассматриваемой задачи обусловлены использованием колец принадлежности секрета-оригинала по модулям, имеющим вид степеней числа 2, а также вычислительной МИМА-технологии, согласованной с пороговым принципом. Это приводит к существенному сокращению реализационных затрат на этапе реконструкции исходного секрета по кодам маскирующего аналога.

Библиографические ссылки

[1] Коляда А.А., Кучинский П.В., Червяков Н.И. Пороговый метод разделения секрета на базе избыточных модулярных вычислительных структур// *Информационные технологии*. – Т. **25**, № 9. – М.: Новые технологии, 2019. – С. 553—561.

[2] Харин Ю.С. и др. *Криптология: учебник* // Мн.: БГУ, 2013. 511 с.

[3] Червяков Н.И., Коляда А.А., Ляхов П.А. и др. *Модулярная арифметика и ее приложения в инфокоммуникационных технологиях*. М.: ФИЗМАТЛИТ, 2017. 400 с.

[4] Jia Xingxing, Daoshun Wang, Daxin Nie, Xiangyang Luo, Jonathan Zheng Sun. A new threshold changeable secret sharing scheme based on the Chinese remainder theorem // *Information sciences*. 2019. Vol. **473**. P. 13–30.

[5] Shiong Jian Shyu, Ying-Ru Chen. Treshold secret image sharing by Chinese remainder theorem // *IEEE Asia – Pacific Services Computing conference*. – Yilan, Taiwan, 9 – 12 dec., 2008. – Vol. **1**. – P. 1332–1337.

КЛЕПТОГРАФИЯ VS КРИПТОГРАФИЯ & СТЕГАНОГРАФИЯ

М.Е. Шелест[1,a], Б.А. Коваленко[2], А.И. Трубей[3,b]
[1]*Национальный университет "Черниговская политехника"*
Чернигов, УКРАИНА
[2]*Amazon-UA*
Киев, УКРАИНА
[3]*НИИ прикладных проблем математики и информатики*
Белорусский государственный университет
Минск, БЕЛАРУСЬ
e-mail: [a]mishel3141@gmail.com, [b]trubeia@mail.ru

В статье исследуется новое направления в защите информации – клептография, и ее связь с криптографией и стеганографией. Вводится понятие клептографического механизма и приводится их общая классификация. Демонстрируются некоторые известные криптопримитивы с встроенным клептографическим механизмом.
Ключевые слова: клептография; криптография; стеганография; канал утечки информации

1 Введение

При современном развитии информационных технологий и формировании киберпространства проблема защиты информации становится еще более актуальной. Особое место в ее решении играют криптографические и стеганографические методы защиты. Если с помощью криптографии скрывают содержимое защищаемой информации, то стеганографические методы (каналы скрытой передачи данных, цифровые отпечатки пальцев, цифровые водяные знаки и пр.) позволяют скрыть сам факт наличия такой информации.

Любое государство пытается контролировать, по крайней мере, свой сегмент киберпространства. Это возможно разными способами. Например, существует видимая коллаборация с государственными структурами (в первую очередь спецслужб США, Китая и России) крупных фирм-производителей микроэлектроники, вычислительной и телекоммуникационной техники с целью сбора информации о пользователях и доступе к их информации. В СМИ неоднократно появлялись данные о сотрудничестве со спецслужбами известных производителей средств телекоммуникаций (Cisco, Huawei), шифраторов (Crypto AG, Omnisec, Mils Electronic), программного обеспечения (Microsoft), социальных сетей (Facebook, Вконтакте, Одноклассники), антивирусных систем (Касперский, Radware, McAfee), поставщиков услуг электронной почты и сетевых Интернет-гигантов (Google, Yahoo, AT&T, CenturyLink, Verizon). Такое сотрудничество включает разработку и встраивание необходимых «бэкдоров» с последующей передачей спецслужбам тайных сведений о уязвимостях в аппаратном и программном обеспечении, в том числе и о действующих ключах шифрования.

2 Клептография и ее связь с криптографией, стеганографией

Вопросами разработки и встраивания закладок в системы защиты информации занимается клептография. Клептография изучает методы синтеза и анализа каналов скрытой передачи данных (embedded trapdoor, subliminal channel), которые позволяют лицу, внедрившего такой канал, получать чувствительную информацию относительно криптосистемы, ключей шифрования или организовывать выкачку защищаемых данных с информационных систем. Клептография стала системно развиваться в 70-х годах прошлого столетия с формированием рынка электронных шифраторов, а затем и открытого программного обеспечения, включая операционные системы. Методы клептографии в последнее время также успешно осваиваются и применяются хакерами.

Клептография, как направление информационной безопасности, тесно связана с криптографией и стеганографией (рис. 1).

Связь клептографии с криптографией обусловлена тем, что объектом ее исследований является клептографическая закладка (механизм), которая является частью криптосистемы. Методы криптоанализа часто используются для выявления закладок, то есть являются и инструментами клептоанализа.

Клептография близка также к стеганографии. Общей отправной точкой как клептографии, так и стеганографии можно считать работы Г.Саймонса, в которых сформулированы и исследованы «проблема узника» («the prisoner's problem») и скрытые каналы передачи («subliminal channels») [6,7].

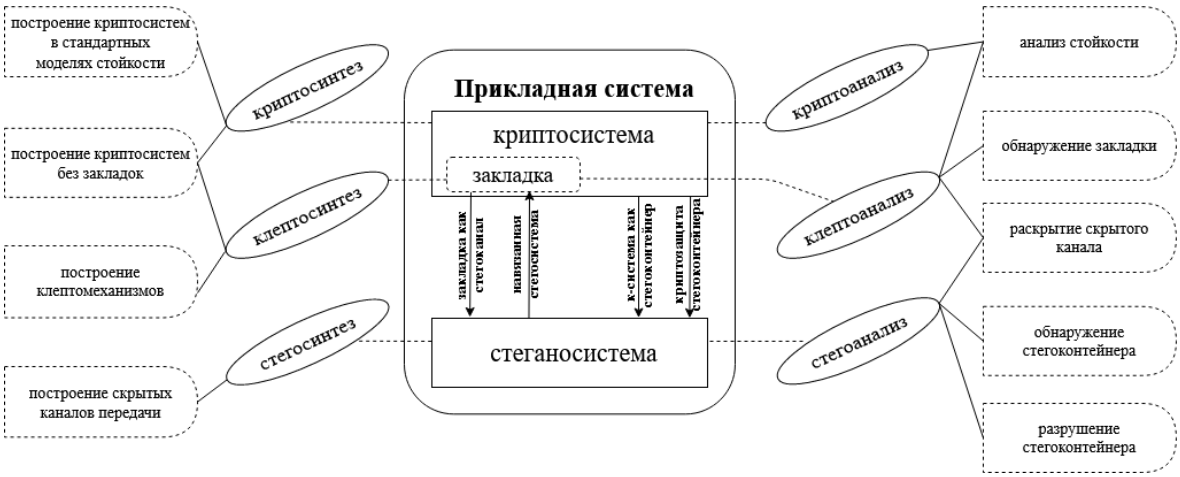


Рис. 1. Связь криптографии, стеганографии и клептографии

Функционирование клептографических и стеганографических механизмов в некоторых аспектах схожи или пересекаются:

1. Клептомеханизм, который выполняет передачу секрета, может рассматриваться как стеганографический канал.

2. Скрытно встроенный стеганографический механизм может использоваться разработчиком для клептографических атак передачи секрета.

3. Клептографический механизм и стеганосистема могут сосуществовать независимо. Например, в одной из модификаций SETUP, кроме схемы передачи ключа существуют также стегоканалы, которые базируются на временных задержках отправления, вероятностном контроле определенных бит открытых случайных параметров, имитации сбоев и пр.

3 Основные направления развития клептографии

На данный момент, основным направлением практической клептографии является синтез криптосистем и криптопримитивов с соответствующими закладками. Криптосистемой с клептозакладкой будем называть такую криптосистему, у которой:

1. Структура системы сгенерирована с использованием «секрета разработчика».

2. «Секрет разработчика» практически невозможно получить путем анализа криптосистемы или такой анализ вообще невозможный.

3. Криптографические свойства системы существенно ослабевают в случае знания “секрета разработчика”.

То есть, в клептографической модели криптосистемы добавляется роль «разработчика», цель которого состоит в модифицировании криптосистемы (либо построение ее с нуля) таким образом, чтобы она содержала закладку, которая бы позволяла в процессе работы системы незаметно передавать определенную секретную информацию разработчику или упрощала ему задачу понижения криптографических свойств системы.

Построение канала утечки путем модификации реализации стандартного протокола – одна из наиболее изученных клептографических проблем [4]. Первой попыткой формализации клептографического механизма является модель SETUP (Secretly Embedded Trapdoor with Universal Protection), предложенная Яном и Юнгом, которая позволяет организовать скрытую передачу секретного ключа криптосистем на базе RSA и задачи дискретного логарифма [8].

Учитывая широкое использование криптографической защиты в информационно-телекоммуникационных системах, особую остроту приобретают вопросы защиты самих криптосистем на всех уровнях их жизненного цикла: этапе проектирования, реализации, развертывания и использования. Актуальными в этом аспекте являются вопросы:

возможности построения криптосистем, устойчивых к различным типам клептографических атак;

разработки критериев наличия/отсутствия клептографических закладок примитивов;

Таблица 1 Классификация клептографических механизмов

Классификация	**Тип клептомеханизма**	**Примеры**
По степени закрытости реализации	Закрытые стандартизованные реализации	Программные библиотеки, схемотехнические описания, спецификации алгоритмов
	Закрытые реализации	Проприетарные программные продукты с обфускацией программного обеспечения и потоков данных
	Аппаратные реализации	Криптографические микроконтроллеры, аппаратные криптомодули
По результатам анализа	Недеструктивные (с возможностью дальнейшего использования)	Анализ программных компонентов, маскирующихся аппаратных компонентов, логический анализ спецификаций и т.д.
	Деструктивные (без возможности дальнейшего использования)	Анализ криптографических контролеров, встроенной EEPROM-памяти и т.д.
По уровню построения	Модификация готовых криптосистем	Добавления канала утечки в реализацию системы, например, атака BEAST протокола TLS1.0 і ниже
	Построение новых криптоалгоритмов со встроенными закладками	Примеры вероятно таких алгоритмов: DES, DualEC, DRGB
По способу внедрения	Открытое распространение клептографических модификаций реализации алгоритмов	Например, в виде программных компонентов
	Распространения проприетарных закрытых криптосистем в виде аппаратных модулей	
	Лоббирование стандартизации клептографических криптосистем, навязывание их использования через правовые механизмы, корпоративные политики или маркетинговые кампании	

синтеза криптографических систем и криптопримитивов с закладками с целью расширения множества шаблонов проектирования закладок для исследования методов их выявления и противодействия им.

Клептографические механизмы разнятся по сценарию построения, способу защиты канала разработчика, уровню абстракции и тому подобное. Известные работы, касающиеся проблем клептографии, фокусируются на отдельных алгоритмах с потенциальной закладкой или построением конкретных протоколов с каналами незаметной утечки секрета, поэтому разнообразие методов в определенной мере размывает общую картину направления. Классификация клептографических механизмов приведена в таблице 1.

Проблемой всех практических клептографических механизмов является то, что даже при нахождении закладки или канала утечки невозможно практически доказать «умышленность» ее построения, поскольку они также могут свидетельствовать лишь о недостаточности имеющихся методов или квалификации аналитиков. Поэтому под криптопримитивом с встроенным клептографическим механизмом мы понимаем такую схему, где только потенциально может быть намеренно организован канал утечки или нарушения криптографических свойств.

4 Обзор современных клептографических механизмов

Приведем несколько примеров, которые, по всей вероятности, содержат клептографические механизмы.

1. *Алгоритм шифрования DES.* Алгоритм симметричного шифрования DES был предложен в 1974 году фирмой IBM, базируется на сети Фейстеля, размер открытого текста и сообщения составляет 64 бит, размер ключа – 56 бит. В оригинальную схему АНБ США был внесен ряд изменений (уменьшение длины ключа с 64 до 56 бит, «помощь» сотрудников АНБ в генерации S-блоков), что снизило устойчивость алгоритма к атакам перебора и дифференциальных анализа. Это наводило на подозрения, что такие изменения были внесены преднамеренно для того, чтобы спецслужбы США, имевшие достаточные вычислительные возможности, могли проводить дешифрование сообщений без знания секретных ключей. В частности, есть подозрения, что они владели методами дифференциального криптоанализа до его публикации Бихамом [2].

2. *Российский стандарт хеширования ГОСТ Р34-11-2012*. Российский стандарт хеширования ГОСТ Р34-11-2012 пришел на смену устаревшему стандарту ГОСТ Р34-11-94. Данный алгоритм имеет размер блока 512 бит и длину хеш-кода 256/512 бит, заявленные сложности поиска прообраза и сильной коллизии были $2^{512}/2^{256}$ и $2^{256}/2^{128}$ соответственно. Однако после стандартизации появилось ряд работ, демонстрирующих методы построения коллизий и поиска прообраза усеченных версий. С точки зрения клептографии, важен тот факт, что методы генера-

ции большинства константных параметров являются неизвестными, что наводит на подозрение на то, что они могут быть секретом разработчика, что упрощает для владельца секрета определенные задачи криптоанализа.

3. *Российский стандарт симметричного шифрования ГОСТ Р34-12-2015*. Стандарт блочного симметричного шифра ГОСТ Р34-12-2015, разработанный Центром защиты информации и специальной связи ФСБ России, представляет собой SP-сеть со схемой Фейстеля для ключевого расписания. Было показано, что S-блок алгоритма сгенерирован не истинно случайным образом (как это указано в стандарте), а с использованием генератора, схему которого удалось восстановить. В свою очередь, этот факт хотя напрямую и не указывает наличие лазейки, однако наводит на подозрения о целенаправленном снижении стойкости примитива с целью упрощения криптоанализа разработчиками.

4. *Система аппаратного шифрования Skipjack и стандарт EES*. Стандарт EES (Escrowed Encryption Standard) аппаратного шифрования разработан АНБ США в рамках проекта Capstone для систем защищенной правительственной связи с закладкой. Стандарт включает в себя блочный алгоритм симметричного шифрования Skipjack и архитектуру LEAF (Law Enforcement Access Field – поле доступа для правоохранительных органов). Для имплементации стандарта использовался защищенный чип Clipper. Предполагалось, что стойкость шифратора будет базироваться на секретном алгоритме шифрования Skipjack, а процесс инициализации ключей будет производиться непосредственно разработчиком чипа. Архитектура LEAF позволяет использовать два ключа расшифрования: один – для пользователя, а другой – для правоохранительных органов. Поэтому разработчики могут расшифровывать перехваченное сообщение, в то время как обычные пользователи могут это делать только с помощью собственных секретных ключей, которые зашиты аппаратно.

5. *Канал утечки в системах на основе криптографии на эллиптических кривых*. Известны как минимум два принципиальных подхода к построению лазейки на базе криптографии на эллиптических кривых:

1. генерация криптографически слабой эллиптической кривой, построение и публикация изоморфной к ней (изоморфизм является секретным параметром разработчика);

2. использование стойкой эллиптической кривой такого вида, что отсутствие проверки того, что точка находится на кривой приводит к переводу операций над классом кривых, в котором разработчик может за приемлемое время решать задачу дискретного логарифмирования.

Идея первого подхода заключается в том, что разработчик сначала выбирает эллиптических кривую E_s, задачу дискретного логарифмирования которой можно свести к задаче дискретного логарифмирования в поле $\mathbb{F}_2^N$, используя определенную функцию спаривания Вейля так, что последняя практически решается раз-

работчиком. Далее, разработчик строит изоморфную кривую E_{pb}, используя секретное преобразование φ: $E_s \to E_{pb}$ методом, описанным в [3]. Затем кривая E_{pb} публикуется (например, как часть стандарта) и используется жертвой. В таком случае задача дискретного логарифмирования, например, поиск $x: \ xG = P$ по известным G и P, сложная для пользователя системы, однако разработчик может ее свести к задаче на кривой $E_s: \ P \to \varphi^{-1}(P), G \to \varphi^{-1}(G)$, что сведением к задаче дискретного логарифмирования над полем остатков по методу, описанному в [5] позволяет разработчику решить задачу ECDLP за приемлемое время.

Клептомеханизм второго похода продемонстрирован на примере схемы цифровой подписи на базе эллиптических кривых ECKCDSA [1]. Идея заключается в том, что в алгоритм генерации цифровой подписи жертвы вводится ошибка (секретный параметр разработчика), что позволяет разработчику, перехватив определенное количество подписей жертвы, получить ее секретный ключ.

6. *Каналы утечки секрета в протоколах*. Одним из известных примеров таких механизмов является метод SETUP, который позволяет организовать завладение секретным ключом путем преднамеренной модификации реализации криптосистемы на основе задачи факторизации больших чисел или задачи дискретного логарифмирования в конечных полях.

На данный момент этот метод является теоретическим (общеизвестных фактов его применения не известно), однако вполне реальный для использования на практике. Другой тип атаки – BEAST (CVE-2011-3389) на протокол SSL до версии TLS 1.0, который использует комбинации уязвимостей XSS (Cross Site Scripting) веб сервиса и Session Fixation в реализации CBC режима шифрования протокола SSL. Злоумышленник может принудить жертву выполнить браузерный код таким образом, что в полученной зашифрованной последовательности нарушается уникальность стартового вектора (CBC режим шифра) для кожного открытого сообщения, позволяя нападающему дешифровать секретную часть сообщения. В действительности, маловероятно, чтобы данная атака была спланированным клептографическим механизмом, однако она имеет определённые признаки такого: вследствие вмешательства в систему жертвы образуется канал скрытной утечки секрета.

Отдельное внимание следует обратить на атаки, которые направленные на открытые реализации криптопротоколов. Одной из их особенностей есть то, что изменения открытой реализации может делать практически любой разработчик, при этом процесс аудита безопасности не всегда идет должным образом.

5 Заключение

1. Обозначена актуальность нового направления в защите информации – клептографии и ее связь с криптографией и стеганографией.

2. Введено неформальное понятие клептографического механизма как расширение криптосистемы, которое дает дополнительные возможности разработ-

чику.

3. Приведена общая классификация клептографических механизмов.

4. Продемонстрированы некоторые известные криптопримитивы с встроенным клептографическим механизмом: алгоритм блочного шифрования DES, система аппаратного шифрования Skipjack, а также алгоритм хеширования с потенциальной лазейкой ГОСТ Р34-11-2012.

Библиографические ссылки

[1] Bernstein, DJ., Chou, T., Chuengsatiansup, C et al. How to Manipulate Curve Standards: A White Paper for the Black Hat Http://Bada55.Cr.Yp.To. //*Proceedings of the Second International Conference on Security Standardisation Research* – Volume 9497. SSR 2015. Tokyo, Japan: SpringerVerlag, 2015:109-139. doi: 10.1007/978-3-319-27152-1_6. url: https: //doi.org/10.1007/978-3-319-27152-1_6.

[2] Biham, E., Shamir, A. Differential cryptanalysis of DES-like cryptosystems. // *Journal of Cryptology* 1991;4 – P. 3-72.

[3] Galbraith, SD., Hess, F., Smart, NP. Extending the GHS Weil Descent Attack. // *Advances in Cryptology - EUROCRYPT 2002*. Под ред. Knudsen, LR. Berlin, Heidelberg: Springer Berlin Heidelberg, 2002. – P. 29-44.

[4] Kovalenko B., Kudin A. *«Kleptography trapdoor free cryptographic protocols»*, Cryptology ePrint Archive, Report 2018/989, https://eprint.iacr.org/2018/989.

[5] Menezes, A., Teske, E. *Cryptographic Implications of Hess' Generalized GHS Attack*. Cryptology ePrint Archive, Report 2004/235. https: // eprint. iacr.org/2004/235. 2004.

[6] Simmons GJ. The Prisoners' Problem and the Subliminal Channel. // *Advances in Cryptology: Proceedings of Crypto 83*. Под ред. Chaum, D. Boston, MA: Springer US, 1984. – P. 51-67. doi: 10.1007/978-1-4684-4730-9_5. url: https://doi.org/10.1007/978-1-4684-4730-9_5.

[7] Simmons GJ. The Subliminal Channel and Digital Signatures. *Advances in Cryptology*. Под ред. Beth, T., Cot, N., Ingemarsson, I. Berlin, Heidelberg: Springer Berlin Heidelberg, 1985. – P. 364-378.

[8] Young, A., Yung, M. The Dark Side of "Black-Box" Cryptography or: Should We Trust Capstone? // *Advances in Cryptology - CRYPTO '96: 16th Annual International Cryptology Conference Santa Barbara, California, USA August 18–22, 1996 Proceedings*. Под ред. Koblitz, N. Berlin, Heidelberg: Springer Berlin Heidelberg, 1996. – P. 89-103.

MODELS OF DISTRIBUTED PROOF GENERATION FOR ZK-SNARK-BASED BLOCKCHAINS

Yuri Bespalov[1,a], Alberto Garoffolo[2,b], Lyudmila Kovalchuk[3,c], Hanna Nelasa[4,d], Roman Oliynykov[3,e]
[1]*Bogolyubov Institute for Theoretical Physics*
Kiev, UKRAINE
[2]*Horizen*
Milan, ITALY
[3]*IOHK Research*
HONG KONG
[4]*Zaporizhzhia Polytechnic National University*
Zaporizhzhia, UKRAINE
e-mail:
{[a]yu.n.bespalov,[c]lusi.kovalchuk,[d]annanelasa,[e]roliynykov}@gmail.com,
[b]alberto@horizen.global

We model distributed proof generation for ZK-SNARKs-based blockchains via discrete Markov chains. Two different types of proof construction models are considered: those in which all the proofs to be built are independent (they can be considered as leaves on the Merkle tree) and those in which the proofs are located at all nodes of the Merkle tree, and hence form a partially ordered set.
Keywords: blockchain; Merkle tree; lumpable Markov chain; Stirling numbers; coupon collector's problem; classical occupancy distribution; Birkhoff duality

1 Introduction

The paper considers the problem of estimating the number of steps to build a complete set of SNARK proofs in the Merkle tree for blockchains. In doing so, we consider two different types of proof construction models: those in which all the proofs to be built are independent (they can be considered as leaves on the Merkle tree) and those in which the proofs are located at all nodes of the Merkle tree, and hence form a partially ordered set. The first one obviously is much more simpler, and we partially solved it.

The article is organized in the next way. The Chapter 3 illustrate the lumping of states technique for Markov chains on the sample of coupon collector's problem. This technique and this sample are used the further sections. Section 3 considers the problem of the number of steps to construct a complete set of proofs that are leaves of the Merkle tree. We proof that the model from Example 5 initially formulated as non-Markovian is stochastically equivalent to the Markov chain from Example 4, and study its lumped form from Example 6. The recurrent formulas for the expectation and variance of the number of steps are received. We show that dependence of expectation on two parameters the number of provers n and the number of leaves m can asymptotically

reduces to a function h of single parameter n/m and describe this function. Section 4 covers the construction of the entire Merkle tree. Moreover, it is convenient to generalize the models from Sections 2 and 3 to the case of a partially ordered set. This generalization leads to some useful ideas, such as a more appropriate probability distribution on poset items. We are interested in the case of a complete Merkle tree with $2^\ell - 1$ nodes. It is hardly possible to expect a complete analytical solution. The corresponding numerical results and their analysis are supposed to be considered in the expanded version of these theses.

This work was supported in part by the National Research Foundation of Ukraine under Grant 2020.01/0351.

2 Preliminary models

The *Stirling numbers of the second kind* can be defined in the context of the Stanley's twelvefold way [5,1.9]: $S(m,n) = \left\{ {m \atop n} \right\}$ is the number of partitions of the m labeled elements into n non-empty nonlabelled blocks. Denote $\mathbf{m} := \{1, 2, \dots, m\}$. Then the number of surjections $\mathbf{m} \twoheadrightarrow \mathbf{n}$ is $n!\left\{ {m \atop n} \right\}$. It can be calculated as a sum of multinomial coefficients $\binom{m}{m_1,\dots,m_n} := \frac{m!}{m_1!\cdots m_n!}$, using the forward difference operator Δ or the inclusion-exclusion principle:

$$n!\left\{ {m \atop n} \right\} = \sum_{\substack{m_1+\cdots+m_n=m \\ m_i \geqslant 1}} \binom{m}{m_1, \dots, m_n} = \Delta^n 0^m = \sum_{r=0}^{n} (-1)^r \binom{n}{r} (n-r)^m.$$

Here we assume that Markov chains are discrete-time, stationary and with finite or countable state-space S. We write elements of transition matrix in the form

$$p_{ij} = p(i,j) = \mathbf{P}(X(n+1) = j \mid X(n) = i), \qquad i, j \in S.$$

This a stochastic matrix with $\sum_{j \in S} p_{ij} = 1$.

Definition 1 ([2,§6.3])**.** Let $p = (p_{ss'})_{s,s' \in S}$ be a stochastic matrix over a state-space S. A surjection $\pi : S \twoheadrightarrow T$ is called a *lumping map* (and the corresponding partition $S = \coprod_{t \in T} \pi^{-1}(t)$ *lumpable*) if for any $t' \in T$ the sum $\sum_{s' \in \pi^{-1}(t')} p_{ss'}$ is locally constant on $s \in \pi^{-1}(t)$ for each $t \in T$.

Proposition 1. *Let $(p_{ss'})_{s,s' \in S}$ be a stochastic matrix and $\pi : S \twoheadrightarrow T$ a lumping map.*

1. *Then one can define a new stochastic matrix over a state-space T with entries $p^{\pi}_{tt'} := \sum_{s' \in \pi^{-1}(t')} p_{ss'}$, $s \in \pi^{-1}(t)$.*
2. *Let $v = (\delta_{\pi(s),t})_{\substack{s \in S, \\ t \in T}}$ be the incidence matrix corresponding to the lumping map π, and $u = (v^t v)^{-1} v^t$ the transpose matrix, normalized to stochastic, then the lumped k-fold transition matrix is*

$$(upv)^k = up^k v. \tag{1}$$

We describe a so called coupon collector model as a result of lumping constructions. It is closely related to the our further models, in particular leads to the classical occupancy distribution described via Stirling numbers of the second kind.

Example 1. Consider the asymmetric random walk on the n-dimensional hyperoctant $\mathbb{Z}^n_{\geqslant 0}$ with nonzero transition probabilities $p(a, a+e_i) = 1/n$ for each $a \in \mathbb{Z}^n_{\geqslant 0}$ and basic vectors $e_i = (\underbrace{0,\dots,0}_{i-1}, 1, \underbrace{0,\dots,0}_{n-i})$. Then nonzero entries of m-fold transition matrix are $p^m(a, a+h) = n^{-m}\binom{m}{h_1,\dots,h_n}$, where $h_1 \geqslant 0$ and $h_1 + \dots + h_n = m$.

Example 2. The type map conversion map $\overline{(\text{-})} : \mathbb{Z}_{\geqslant 0} \to \{0,1\}$, $\overline{a} = \begin{cases} 0, & \text{if } a = 0, \\ 1, & \text{if } a > 0, \end{cases}$ applied to each coordinate gets a lumping map $\mathbb{Z}^n_{\geqslant 0} \to \{0,1\}^n$ for the previous Markov chain. According to (1) for the obtained Markov chain on the hypercube $\{0,1\}^n$ m-step transition matrix p^m is the following: if $p^m(a,b)$ then $a_i \leqslant b_i$ for all i; and

$$p^m(a,b) = n^{-m} \sum_{\substack{m_1+\dots+m_n=m \\ m_i \geqslant 1}} \binom{m}{m_1,\dots,m_n} = \frac{r!}{n^m} \left\{ {m \atop r} \right\}, \text{ where } r = \sum_i (b_i - a_i), \text{ if } a \neq b.$$

$$p^m(a,a) = \Big(\sum_i a_i/n \Big)^m.$$

Example 3 (Coupon collector's problem)**.** The projection of hypercube to the main diagonal

$$\{0,1\}^n \to \{0,1,\dots,n\}, \qquad (a_i)_{1 \leqslant i \leqslant n} \mapsto \sum_i a_i$$

is a lumping map. Combining the states we get so called coupon collecting Markov chain [3,2.2], where nonzero m-step transition probabilities are the following:

$$p^m(k,k) = \frac{k^m}{n^m}, \qquad p^m(k,k+r) = \frac{1}{n^m} \binom{n-k}{r} r! \left\{ {m \atop r} \right\} = \frac{(n-k)_r}{n^m} \left\{ {m \atop r} \right\}, \qquad (2)$$

where $(n)_r = n(n-1)\cdots(n-r+1)$ is *the falling* factorial.

There are n distinct coupons in the urn. A collector draw with replacement one random coupon in a step. The number $\xi_m = \xi_0 p^m$ of distinct coupons selected after m steps has the classical occupancy distribution [4]: $\mathbf{P}(\xi_m = r) = p^m(0,r)$.

The expectation of number ζ^n_r of steps to obtain exactly r distinct coupons is described via harmonic numbers $H_n = 1 + 1/2 + \dots + 1/n$:

$$\mathbf{E}\, \zeta^n_r = n(H_n - H_{n-r}). \qquad (3)$$

3 Distributed generation of sets of proofs

Example 4. Suppose that there exist $m > 0$ nodes in a network called *provers* and a finite set N of proof-candidates for which they need to construct proofs. We model

this situation as a Markov chain, where states are subsets of $N' \subseteq N$ of candidates for which proofs are not yet constructed. On each step in the state N' each prover independently selects a single candidate from N' and construct its proof, i.e. selection is given by a function $g : \mathbf{m} \to N'$ uniformly distributed among all functions $\mathbf{m} \to N'$. For given selections the next state is obtained by removing all candidates proved in this step. So nonzero transition probabilities described via number of surjections:

$$p(N', N'') = |N' \smallsetminus N''|! \cdot \left\{ {m \atop |N' \smallsetminus N''|} \right\} \cdot |N'|^{-m}, \qquad N'' \subseteq N', \quad |N' \smallsetminus N''| \leqslant m. \quad (4)$$

Example 5. To force provers to act independently, rules are modified in the following way: Denote $\operatorname{ord} N$ the set of linear orderings of N i.e. bijections $\sigma : \{1, 2, \ldots, |N|\} \xrightarrow{\cong} N$. (Note that $|\operatorname{ord} N| = |N|!$.) Suppose that at the beginning each prover randomly selects its own priority ordering $\sigma_i \in \operatorname{ord} N$, $1 \leqslant i \leqslant m$ (We assume a uniform distribution on $\operatorname{ord} N$). After that the process becomes completely deterministic: In the first step all provers select candidates according to the function $g : \mathbf{m} \to N$ given by $g(i) := \sigma_i(1)$. The next state in $N' = N \smallsetminus \operatorname{Im}(g)$. There is a natural projection $\rho^N_{N'} : \operatorname{ord}(N) \to \operatorname{ord}(N')$, which removes foreign elements from an ordering. And provers can do the next step with priority orderings $\rho^N_{N'}(\sigma_i)$.

Proposition 2. *The model from Example 5 is stochastically equivalent to the Markov chain from Example 4.*

Доказательство. (Sketch.) Uniform distributions of σ_i imply 1) uniform distribution of the first selection function g, and 2) uniform distributions of $\rho^N_{N'}(\sigma_i)$, because the fiber of $\rho^N_{N'}$ over each point has the same cardinality $|\operatorname{ord} N|/|\operatorname{ord} N'| = |N|!/|N'|!$. □

Example 6. Note that the Markov chain from Example 4 admits a lumping map $N' \mapsto |N|$. For each $m, n > 0$ and we obtain a Markov chain with states $\{0, 1, \ldots, n\}$. Exactly from definition one can see that for fixed m and for $n' \leqslant n$, one Markov chain is included in other. So one can consider the colimit (union) of these chains for all n. So for each $m \in \mathbb{Z}_{>0}$ we obtain a Markov chain, where states are nonnegative integers and the only nonzero elements of transition matrix are the following

$$\begin{aligned} p(0,0) &= 1, \\ p(n, n-r) &= \frac{1}{n^m} \binom{n}{r} r! \left\{ {m \atop r} \right\} = \frac{(n)_r}{n^m} \left\{ {m \atop r} \right\}, \quad n > 0, \ 1 \leqslant r \leqslant m. \end{aligned} \quad (5)$$

The formula coincides with the classical occupancy distribution from Example 3.

So if we start from the state $\xi^{mn}_0 \equiv n$, then the evolution on the kth step is defined via kth power of transition matrix:

$$\xi^{mn}_k = \xi^{mn}_0 p^k.$$

The absorbing state is 0. All trajectories are strictly decreasing and $\xi^{mn}_k \equiv 0$ for $k \geqslant n$.

The subject of our interest is the *absorption time* τ^{mn}, a random variable which measure the exact number of steps m provers needs to obtain all n proofs. I.e. $\tau^{mn} = k + 1$ iff $\xi^{mn}_{k+1} = 0$ and $\xi^{mn}_k \neq 0$.

Taking into account the lower triangular form of our transition matrix we get recurrent and explicit formulas

$$\begin{aligned}
&\mathbf{P}(\tau^{mn}=0)=\delta_{n0},\\
&\mathbf{P}(\tau^{mn}=k+1)=\sum_{r=1}^{\min(m,n)} p_{n\,n-r}\,\mathbf{P}(\tau^{m\,n-r}=k)=\sum_{r=0}^{\min(m,n)}\frac{(n)_r}{n^m}\left\{{m\atop r}\right\}\mathbf{P}(\tau^{m\,n-r}=k) \qquad (6)\\
&\mathbf{P}(\tau^{mn}=k+1)=\sum_{n_k<\cdots<n_1<n_0=n} p_{n_0n_1}\cdots p_{n_{k-1}n_k}p_{n_k0}\\
&\qquad=\sum_{n_k<\cdots<n_1<n_0=n}\frac{n!}{(n_0n_1\cdots n_k)^m}\left\{{m\atop n_0-n_1}\right\}\cdots\left\{{m\atop n_{k-1}-n_k}\right\}\left\{{m\atop n_k}\right\}. \qquad (7)
\end{aligned}$$

Multiplying (6) by k^ℓ and taking a sum over k we get the recurrent formula for ℓth moment:

$$\mathbf{E}(\tau^{mn}-1)^\ell=\sum_{r=1}^{\min(n,m)} p_{m\,n-r}\,\mathbf{E}(\tau^{m\,n-r})^\ell.$$

In particular, this allows to calculate expectation and variance:

Proposition 3. *Let $m>0$. Then $\tau^{m0}\equiv 0$ and for $n>0$*

$$\begin{aligned}
\mathbf{E}\,\tau^{mn}&=1+\sum_{r=1}^{\min(n,m)}\frac{(n)_r}{n^m}\left\{{m\atop r}\right\}\mathbf{E}\,\tau^{m\,n-r},\\
\mathbf{E}(\tau^{mn})^2&=-1+2\,\mathbf{E}\,\tau^{mn}+\sum_{r=1}^{\min(n,m)}\frac{(n)_r}{n^m}\left\{{m\atop r}\right\}\mathbf{E}(\tau^{m\,n-r})^2,\\
\mathbf{V}\mathrm{ar}\,\tau^{mn}&=\mathbf{E}(\tau^{mn})^2-(\mathbf{E}\,\tau^{mn})^2.
\end{aligned}$$

Here we compare the values of $\mathbf{E}\,\tau^{mn}$ as results of analytic calculation using Wolfram Mathematica (3 last digits in numerator) and of 10^5 random tests of model from Example 5 (3 last digits in denominator):

$n\backslash m$	10	20	30	40	50	100	200	300
10	$2.16\frac{869}{787}$	$1.78\frac{542}{357}$	$1.37\frac{086}{051}$	$1.14\frac{190}{100}$	$1.05\frac{090}{099}$	$1.00\frac{027}{027}$	$1.00\frac{000}{000}$	$1.00\frac{000}{000}$
20	$3.47\frac{931}{927}$	$2.34\frac{507}{533}$	$2.00\frac{865}{842}$	$1.96\frac{422}{396}$	$1.83\frac{582}{516}$	$1.11\frac{346}{316}$	$1.00\frac{070}{055}$	$1.00\frac{000}{001}$
30	$4.67\frac{850}{932}$	$3.04\frac{330}{296}$	$2.48\frac{512}{367}$	$2.05\frac{429}{539}$	$2.00\frac{238}{236}$	$1.66\frac{514}{691}$	$1.03\frac{364}{183}$	$1.00\frac{115}{112}$
40	$5.80\frac{575}{489}$	$3.76\frac{690}{573}$	$2.99\frac{443}{496}$	$2.59\frac{552}{423}$	$2.13\frac{500}{559}$	$1.97\frac{687}{744}$	$1.22\frac{719}{433}$	$1.01\frac{995}{928}$
50	$6.89\frac{606}{594}$	$4.20\frac{784}{602}$	$3.27\frac{580}{637}$	$2.98\frac{450}{461}$	$2.68\frac{236}{375}$	$1.99\frac{990}{982}$	$1.60\frac{171}{019}$	$1.11\frac{091}{170}$
100	$12.16\frac{720}{615}$	$7.06\frac{755}{721}$	$5.24\frac{624}{792}$	$4.36\frac{879}{869}$	$3.98\frac{029}{051}$	$2.90\frac{527}{516}$	$2.00\frac{005}{003}$	$1.99\frac{585}{578}$
200	$22.47\frac{230}{252}$	$12.37\frac{230}{229}$	$9.00\frac{099}{246}$	$7.13\frac{489}{424}$	$6.06\frac{816}{896}$	$4.00\frac{045}{029}$	$2.99\frac{159}{165}$	$2.05\frac{752}{897}$
300	$32.65\frac{910}{976}$	$17.60\frac{450}{329}$	$12.50\frac{050}{043}$	$9.98\frac{039}{139}$	$8.27\frac{088}{058}$	$5.02\frac{111}{084}$	$3.30\frac{483}{400}$	$2.99\frac{925}{942}$

Conjecture 1. • There exists a monotone increasing function $h:\mathbb{R}_{>0}\to\mathbb{R}_{>0}$ given by the limit

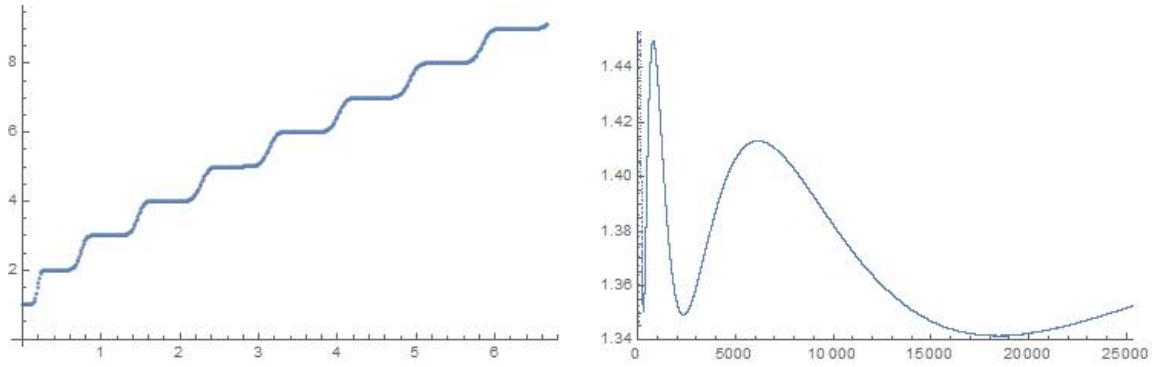
$$h(z):=\lim_{\substack{m,n\to\infty\\ n/m\to z}}\mathbf{E}\,\tau^{mn};$$

- $h(z) \searrow 1$ when $z \searrow 0$;
- $h(1) = 3$ (for example $\mathbf{E}\,\tau^{750\,750} \approx 3 - 1.1 \cdot 10^{-8}$);
- $h(z)/z \searrow 1$ and $h(z) = z + \frac{1}{2}\log z + O(1)$ when $z \to +\infty$;

Доказательство. We can proof only part of the above statements, other are results of numerical experiments. 1. For fixed $m, n \in \mathbb{Z}_{>0}$ the function $\mathbb{Z}_{>0} \to \mathbb{R}_{>0}$, $a \mapsto \mathbf{E}\,\tau^{am\,an}$ is monotone increasing. 2. The expectation $\mathbf{E}\,\tau^{mn}$ can be majorized by $\mathbf{E}\,\zeta_r^n$ form coupon collector model:

$$\begin{aligned}\mathbf{E}\,\tau^{m\,bm} - \mathbf{E}\,\tau^{m\,m} &\leqslant (\mathbf{E}\,\zeta_m^{bm} + \mathbf{E}\,\zeta_m^{(b-1)m} + \cdots + \mathbf{E}\,\zeta_m^{2m})/m \\ &= b(H_{bm} - H_{(b-1)m}) + (b-1)(H_{(b-1)m} - H_{(b-2)m}) + \cdots + 2(H_{2m} - H_m) \\ &\approx \log\frac{b^b}{(b-1)!} \underset{b\gg 1}{\approx} b + \frac{1}{2}\log\frac{b}{2\pi}.\end{aligned}$$ □

The graph of $h(x)$ for small x looks like a ladder. From other hand we can see the asymptotic of $h(x)$ for $x \to \infty$. On the figures bellow graphs of the functions $n/750 \mapsto \mathbf{E}\,\tau^{750\,n}$ and $n/50 \mapsto \mathbf{E}\,\tau^{50\,n} - n/50 - \ln(n/50)/2$ give suitable approximations:



The behaviour of the variance $\mathbf{V}\mathrm{ar}\,\tau^{mn}$ is more complicated. Our numerical calculations allows to suppose that $\mathbf{V}\mathrm{ar}\,\tau^{mn} < 1$ if $m \geqslant 10$ and $n/m < 10000$.

Remark 1. Example 5 allows to obtain rough but very quick estimation of proof construction success. Note that $\xi_k^{mn} \geqslant n - r$ implies that $\#\{\sigma_i(j) | 1 \leqslant i \leqslant m, 1 \leqslant j \leqslant r\}$. So calculating probabilities we have $\mathbf{P}(\xi_k^{mn} \geqslant n - r) \leqslant \binom{n}{\ell}\left(\frac{(r)_k}{(n)_k}\right)^m$. In particular, $\mathbf{P}(\tau^{mn} > k) = \mathbf{P}(\xi_k^{mn} \geqslant 1) \leqslant n\,(1 - k/n)^m \underset{k/n\ll 1}{\approx} ne^{-k\frac{m}{n}}$.

4 Distributed generation of Merkle trees

Our practical task is to generate proofs for nodes of Merkle tree. The nodes form a partially ordered set (poset) whose Hasse diagram is the tree itself.

Some basic facts about posets can be found in [5,ch.3]. Let P be a poset. A subset $I \subseteq P$ is called a *down-set* (resp. *up-set*) if for each $x \in I$ and $y \in P$ with $y \leqslant x$ (resp. $y \geqslant x$) we have $y \in I$. Note that down-sets in P are up-sets in the opposite poset P^{op}

and vice versa. And $I \subseteq P$ is a down-set iff its complement $P \smallsetminus I$ is an up-set. The set of up-sets in P form a distributive lattice ordered by inclusion (this statement is a part of Birkhoff's representation theorem). Denote $\min P$ the set of minimal elements in P.

A Merkle tree M_ℓ with $2^\ell - 1$ nodes as a poset consists of words of length $< \ell$ in alphabet of two letters, say $\{0, 1\}$; and $w \geqslant w'$ iff w' start with w. So the empty word corresponds to the greatest element, the root. The number u_ℓ of up-sets in this poset satisfies the recurrent relation $u_{\ell+1} = u_\ell^2 + 1$ (the sequence A003095).

One can generalise Makov chains from Examples 1,2 to the case of poset N. In particular, for poset-guided analog of coupon collector Markov chain: a graph (not mentioning loops) is the Hasse diagram for the lattice of down-sets in N. The further lumping like in Example 3 exists only for special posets.

Let N be a poset. We consider a Markov chain, where states are up-sets in N. Non-zero elements of transition matrix are

$$p(N', N'') = |N' \smallsetminus N''|! \cdot S(m, |N' \smallsetminus N''|) \cdot |\min N'|^{-m},$$

where $N' \smallsetminus \min N' \subseteq N'' \subseteq N'$ and $|N' \smallsetminus N''| \leqslant m$. If N is a discrete poset we obtain a Markov chain from Example 4.

Note that very similar constructions around Birkhoff's representation theorem describe shapes of cells of higher categories in [1].

Remark 2. We can extend the model from Example 5 to the case of poset N. The only modification is to define a linear ordering of N as a monotone bijections $\sigma : N \xrightarrow{\cong} \{1 < 2 < \cdots < |N|\}$.

The number of linear orderings of a Merkle tree: $|\operatorname{ord}(M_{\ell+1})| = |\operatorname{ord}(M_{\ell+1})|^2 \binom{2^\ell - 2}{2^{\ell-1}-1}$ and $|\operatorname{ord}(M_{\ell+1})| = \prod_{k=1}^{\ell-1} \binom{2^{k+1}-2}{2^k-1}^{2^{\ell-k-1}} = (2^\ell - 1)! / \prod_{k=2}^{\ell} (2^k - 1)^{2^{\ell-k}}$.

In this more general situation Proposition 2 is broken if we use equiprobability distributions. An analog of this proposition remains true if we consider a system of agreed probability distributions in general different from uniform.

Bibliographic references

[1] Bespalov, Y. *Categories: Between cubes and globes. Sketch I*, Ukrainian Journal of Physics **64** (2019), no. 12, 1125–1128.

[2] Kemeny, J.G., Snell J.L. *Finite Markov chains*, - Undergraduate Texts in Mathematics, Springer-Verlag, 1976.

[3] Levin, D.A., Peres, Y., Wilmer, E.L. *Markov chains and mixing times*, 2nd ed., AMS, 2017.

[4] O'Neill, B. *The classical occupancy distribution: Computation and approximation*, The American Statistician (2019).

[5] Stanley, R.P. *Enumerative combinatorics*, 2nd ed., - Cambridge studies in advanced mathematics, 49, vol. 1, Cambridge University Press, 2011.

STATISTICAL INFERENCES ON EMBEDDINGS IN STEGANOGRAPHY

Yu. Kharin[1,a], E. Vecherko[1,b]
[1,2]*Research Institute for Applied Problems of Mathematics and Informatics*
Minsk, BELARUS
e-mail: [a]kharin@bsu.by, [b]vecherko@bsu.by

This paper is concerned with topical problems in steganography on detection of embeddings and statistical estimation of the models parameters. Binary stationary Markov chains with known and unknown parameters are used as mathematical models of cover-sequences. ML-estimators for models parameters are constructed. Statistical tests for detecting embeddings are constructed based on run statistic, short run statistic and likelihood ratio statistic. For a family of contiguous alternatives the asymptotic power of tests based on run statistics is found. A polynomial algorithm is developed for the statistical estimation of the positions of embeddings. Two approaches for evaluating security of steganographic schemes are proposed.
Keywords: steganography; embedding; Markov chain; statistical estimators; short run; test; security

1 Introduction

The majority papers on the problem of detection of embeddings in steganography are based on some empirical characteristics of cover-sequences and stego-sequences. Using mathematical models in steganography provides construction of new estimators for security of steganographic schemes. The problem of detection of embeddings using mathematical models are considered in [1,3,4]. For example, in [4] the most powerful statistical test was constructed in the case when the cover-sequence is a Bernoulli scheme of independent trials. In this paper we draw attention to the interesting results on detection of embeddings, estimation of positions of embeddings [3] and statistical estimation for model parameters [2] when the cover-sequence mathematical model is Markov chain of the first order.

2 Mathematical model

First, we introduce the notations: $V = \{0,1\}$ is a binary alphabet, V_T is a set of the binary T-dimensional vectors, $\mathbb{N}$ is a set of integer numbers, $I\{A\}$ is an indicator function of the event A, $u_{t_1}^{t_2} = (u_{t_1}, \ldots, u_{t_2}) \in V_{t_2-t_1+1}$ $(t_1, t_2 \in \mathbb{N},\ t_1 \le t_2)$ is a binary string of $t_2 - t_1 + 1$ bits, $w(\cdot)$ is Hamming weight, $\mathfrak{L}\{\xi\}$ is probability distribution of a random variable ξ, $\mathfrak{B}(\theta)$ is Bernoulli probability distribution with parameter $\theta = \mathbf{P}\{\xi = 1\}$, $\Phi(\cdot)$ is the distribution function for the standart normal law $\mathcal{N}(0,1)$, $\mathrm{sgn}(\cdot)$ is the sign function.

A general mathematical (q,r)-model of embedding which is described in [3] allows to embed r-bits message block into a q-bits cover-sequence block. The secret is a key which contains the information of the positions of embeddings. Here we consider a (1,1)-model of embedding with $q = r = 1$.

As it is shown in [2], an adequate model of the cover-sequence for embedding a message is a binary sequence $x_1^T = (x_1, x_2, \ldots, x_T) \in V_T,\ x_t \in V,\ t = 1, \ldots, T$, which is a homogeneous Markov chain of order 1 with a symmetric matrix of one-step transition probabilities P:

$$P = \frac{1}{2} \begin{pmatrix} 1+\varepsilon & 1-\varepsilon \\ 1-\varepsilon & 1+\varepsilon \end{pmatrix},\ |\varepsilon| < 1,\ \varepsilon \neq 0. \tag{1}$$

Here ε is the model parameter: the case $\varepsilon = 0$ corresponds to a scheme of independent trials and was examined in [4]. We note that the Markov chain (1) satisfies the ergodicity conditions and has uniform stationary probability distribution $(1/2, 1/2)$. Let us further assume that the Markov chain (1) is stationary, so its initial state probability distribution coincides with the uniform distribution.

In practical applications a message is subjected to a cryptographic transformation before being embedded in the cover-sequence, and hence we assume that a message $\xi_1^M = (\xi_1, \ldots, \xi_M) \in V_M,\ M \leq T$, is a sequence of M independent Bernoulli random variables, $\mathfrak{L}\{\xi_t\} = \mathfrak{B}(\theta_1)$, $\theta_1 \in (0,1)$.

A secret key $\gamma_1^T = (\gamma_1, \ldots, \gamma_T) \in V_T$ specifies the positions at which the message bits $\{\xi_t\}$ are embedded in the cover-sequence x_1^T. For the (1,1)-model of embedding the key is a sequence of T independent Bernoulli random variables, $\mathfrak{L}\{\gamma_t\} = \mathfrak{B}(\delta)$, where $\delta \in (0,1)$ indicates the embeddings fraction.

Under the above model the popular methods of embedding in steganography ("LSB replacement" and "± 1 embedding") are equivalent and the stego-sequence y_1^T is generated as follows:

$$y_t = x_t \oplus \gamma_t x_t \oplus \gamma_t \xi_{\tau_t},\ \tau_t = \sum_{j=1}^{t} \gamma_j \leq M. \tag{2}$$

The random sequences $\{x_t\},\ \{\xi_t\},\ \{\gamma_t\}$ are assumed to be independent.

From a practical point of view the case $\theta_1 = 1/2$ in (2) is the most useful and difficult case for the proposed model of embedding as the one-dimensional probability distribution of the cover-sequence is not changed after embedding: $\mathbf{P}\{x_t = 1\} = \mathbf{P}\{y_t = 1\} = 1/2,\ t = 1, 2, \ldots, T$.

3 Statistical estimation for parameters of embeddings

We build the likelihood function for the observed stego-sequence $\nu_1^T \in V_T$. Following [2,3], we divide the set V_t of the binary t-dimensional vectors into $t+1$ disjoint subsets:

$V_t = \Gamma_0^{(t)} \cup \Gamma_1^{(t)} \cup \ldots \cup \Gamma_t^{(t)}$,

$$\Gamma_0^{(t)} = \{u_1^t \in V_t : \ u_t = 1\}, \ \Gamma_1^{(t)} = \{u_1^t \in V_t : \ u_{t-1} = u_t = 0\},$$
$$\Gamma_j^{(t)} = \{u_1^t \in V_t : \ u_{t-j} = 0, u_{t-j+1} = \ldots = u_{t-1} = 1, u_t = 0\}, \ 1 < j < t,$$
$$\Gamma_t^{(t)} = \{u_1^t \in V_t : \ u_1 = \ldots = u_{t-1} = 1, u_t = 0\},$$

which generates the all possible key subsequences $\gamma_1^t = u_1^t \in V_t$.

The set $\Gamma^{(q,r)}$ of all keys for (q,r)-model (every q-size block of secret key has a Hamming weight of 0 or r) is

$$\Gamma^{(q,r)} = \{u_1^T \in V_T : \ w(u_1^T) = rb_r(u_1^T)\} \subseteq V_T, \ |\Gamma^{(q,r)}| = (1 + C_q^r)^{T/q},$$
$$b_h(u_1^T) = \sum_{k=1}^{T/q} I\{w(u_{q(k-1)+1}^{qk}) = h\}, \ h \in \{0, \ldots, q\}.$$

Lemma 1. *The likelihood function for the (q,r)-model of embedding is as follows:*

$$L(\varepsilon, \delta) = \mathbf{P}\{y_1^T = \nu_1^T\} = 2^{-T} \sum_{u_1^T \in \Gamma^{(q,r)}} (1-\delta)^{b_0(u_1^T)} (\delta / C_q^r)^{b_r(u_1^T)} \prod_{t=1}^{T} \varphi_t(u_1^t, \nu_1^t),$$

$$\varphi_t(u_1^t, \nu_1^t) = \begin{cases} 1, \ u_1^t \in \Gamma_j^{(t)}, \ j \in \{0, t\} \\ 1 + (-1)^{\nu_{t-j} + \nu_t} \varepsilon^j, \ u_1^t \in \Gamma_j^{(t)}, \ 1 \le j \le t-1. \end{cases}$$

Maximum likelihood estimators (ML-estimators) $\hat{\varepsilon}, \hat{\delta}$ of the model parameters ε, δ are the solution of the following maximization problem: $L(\varepsilon, \delta) \to \max\limits_{\varepsilon \in [-1,1], \ \delta \in [0,1]}$. In [2] the polynomial algorithm is provided for calculating a value of likelihood function $L(\cdot)$ in a fixed point (ε, δ) in case $r < q$. The ML-estimators construction is based on that algorithm.

4 Statistical detection of embeddings

4.1 Run test

We define two hypotheses concerning the embeddings fraction $\delta \in [0,1]$:

$$\mathcal{H}_0 : \ \{\delta = 0\}, \ \mathcal{H}_1 : \ \{\delta > 0\}. \tag{3}$$

The hypothesis $\mathcal{H}_0$ means that there is no embeddings and the stego-sequence y_1^T is equal to the cover-sequence x_1^T. The composite alternative $\mathcal{H}_1$ means the presence of embeddings of some unknown fraction $\delta > 0$. If the parameter of the cover-sequence ε is known then the null hypothesis is simple and will be denoted by $\mathcal{H}_{0,\varepsilon}$, otherwise $\mathcal{H}_0$ is also a composite hypothesis. If the hypothesis $\mathcal{H}_0$ holds then the probability measure $\mathbf{P}$ will be denoted by $\mathbf{P}_0$, otherwise by $\mathbf{P}_\delta$.

We introduce the run statistic

$$\mathcal{B}_T = \mathcal{B}_T(y_1^T) = 1 + \sum_{t=1}^{T-1} y_t \oplus y_{t+1},$$

that is used in the "run test" [6] and means the total number of runs. By virtue (1) under the null hypothesis $\mathcal{H}_{0,\varepsilon}$ the sequence of indicators $I\{y_t \oplus y_{t+1} = 1\}$ consists of independent random variables with Bernoulli distribution $\mathfrak{B}(2^{-1}(1-\varepsilon))$. In practice it is convenient to use the asymptotic version of test as $T \to \infty$ which is given by the critical region

$$\mathcal{X}_{1\alpha}^{\mathcal{B}} = \{y_1^T : \ \mathrm{sgn}(\varepsilon)\mathcal{B}_T \geq \mathrm{sgn}(\varepsilon)(1 + \tfrac{1}{2}T(1-\varepsilon)) - \tfrac{1}{2}t_\alpha\sqrt{T(1-\varepsilon^2)}\}, \tag{4}$$

where t_α is a quantile of level $\alpha \in (0,1)$ for the standard normal distribution, $\Phi(t_\alpha) = \alpha$.

Theorem 1. *Let the model of embedding (2) holds. Then as $T \to \infty$ the asymptotic size of the test (4) for hypotheses $\mathcal{H}_{0,\varepsilon}, \mathcal{H}_1$ that is based on the total number of runs $\mathcal{B}_T$ coincides with a preassigned significance level $\alpha \in (0,1)$. The asymptotic expression for the power of this test for the $(1,1)$-model of embedding under the family of contiguous alternatives $\mathcal{H}_{1,\delta}: \ \{\delta = \dfrac{\rho}{T^\beta}\}, \ \beta > 0$, is as follows*

$$W_1^{\mathcal{B}} \to \begin{cases} 1, & 0 < \beta < 1/2, \\ \Phi(t_\alpha + 2\rho\dfrac{|\varepsilon|}{\sqrt{1-\varepsilon^2}}), & \beta = 1/2, \\ \alpha, & \beta > 1/2. \end{cases} \tag{5}$$

Let us now construct the sequence of indicators of the states changing (a change from "1" to "0" and vice versa) for the stego-sequence $y_1, \ldots, y_T \in V_T$:

$$z_t = y_t \oplus y_{t+1} \in V, \ t = 1, \ldots, T-1. \tag{6}$$

Then we define a set of patterns in the new sequence (6):

$$\{\mathfrak{b}_1, \mathfrak{b}_2, \ldots\}, \ \mathfrak{b}_\tau = (1, \underbrace{0, \ldots, 0}_{\tau}, 1), \ \tau \in \mathbb{N} \cup \{0\},$$

where $\mathfrak{b}_\tau$ is a subsequence of τ states "0" which is bounded from the left and from the right by states "1". Such patterns specify the runs of "0" and "1" of length $\tau + 1$ in the stego-sequence $\{y_t\}$.

4.2 Short run test

Let us consider the bivariate short run statistic

$$(\mathcal{B}_{T,1}, \ \mathcal{B}_{T,2}) = (\sum_{t=1}^{T-2} z_t, \ \sum_{t=1}^{T-2} z_t z_{t+1}), \tag{7}$$

where the statistic $\mathcal{B}_{T,2}$ is the total number of runs of "0" and "1" of length 1 in the stego-sequence $\{y_t\}$.

Under the alternative $\mathcal{H}_1$ the initial first-order moments of statistic $(\mathcal{B}_{T,1}, \mathcal{B}_{T,2})$ are

$$\begin{aligned}
\mathbf{E}_\delta\{\mathcal{B}_{T,1}\} &= (T-2)\tfrac{1}{2}(1-(1-\delta)^2\varepsilon) = \\
&= \mathbf{E}_0\{\mathcal{B}_{T,1}\} + T\tfrac{1}{2}\delta(2-\delta)\varepsilon + o(T),\ T\to\infty, \\
\mathbf{E}_\delta\{\mathcal{B}_{T,2}\} &= (T-2)\tfrac{1}{4}(1-(1-\delta)^2\varepsilon(2-\varepsilon)) = \\
&= \mathbf{E}_0\{\mathcal{B}_{T,2}\} + T\tfrac{1}{4}\delta(2-\delta)\varepsilon(2-\varepsilon) + o(T),\ T\to\infty.
\end{aligned} \tag{8}$$

Lemma 2. *Under the $(1,1)$-model of embedding, if the alternative $\mathcal{H}_1$ holds, then the random variables z_t, z_s are independent with $|t-s|\geq 2$, the random variables $z_t, z_s z_{s+1}$ are independent with $|t-s|\geq 2$, and $z_t z_{t+1}, z_s z_{s+1}$ are independent with $|t-s|\geq 3$.*

In [3] it is shown that the random bivariate variable

$$\frac{1}{\sqrt{T}}\left(\mathcal{B}_{T,1} - \tfrac{1}{2}T(1-(1-\delta)^2\varepsilon), \mathcal{B}_{T,2} - \tfrac{1}{4}T(1-(1-\delta)^2\varepsilon(2-\varepsilon))\right)'$$

has an asymptotically normal probability distribution $\mathcal{N}_2((0,0)', \Sigma_1)$, with zero mean, and its covariation matrix $\Sigma_1 = (\sigma_{1,ij}),\ i,j=0,1$, is being the follows:

$$\begin{gathered}
\sigma_{1,00} = \tfrac{1}{4}(1-(1-\delta)^2\varepsilon^2(1-6\delta+3\delta^2)), \\
\sigma_{1,01} = \sigma_{1,10} = \tfrac{1}{4}(1-(1-\delta)^2\varepsilon(1-\varepsilon)^2 - (1-\delta)^4\varepsilon^2(3-2\varepsilon)), \\
\sigma_{1,11} = \tfrac{1}{16}(5-(1-\delta)^2(2(4+\delta^3)\varepsilon + 2(1-10\delta+5\delta^2)\varepsilon^2 - \\
-2(4-16\delta+8\delta^2+\delta^3)\varepsilon^3 + (3-10\delta+\delta^2)\varepsilon^4)).
\end{gathered}$$

Unfortunately, using the bivariate statistic (7) does not allow to obtain an analytic expression of the test power because the covariance matrix depends on δ (see [3]). The following important property of the asymptotically normal distribution of the random variable (7) under the alternative $\mathcal{H}_{1,\delta}$ is that with δ changing from 0 to 1 the center of distribution of $(\mathcal{B}_{T,1}, \mathcal{B}_{T,2})$ always lies on the line

$$\begin{cases} b_1 = \tfrac{1}{2}T\varepsilon\Delta + \tfrac{1}{2}T(1-\varepsilon), \\ b_2 = \tfrac{1}{4}T\varepsilon(2-\varepsilon)\Delta + \tfrac{1}{4}T(1-\varepsilon)^2, \end{cases} \quad \Delta = \delta(2-\delta). \tag{9}$$

Taking into account the above property (9) we construct a statistical test for hypotheses $\mathcal{H}_{0,\varepsilon}, \mathcal{H}_1$ based on the statistic obtained as the orthogonal projection of $(\mathcal{B}_{T,1}, \mathcal{B}_{T,2})$ on the line (9). With $\varepsilon > 0$ the test is given by the critical region $\mathcal{X}^{\mathfrak{h}+}_{1\alpha}$:

$$\{y_1^T:\ \mathcal{B}_{T,1} + \tfrac{1}{2}(2-\varepsilon)\mathcal{B}_{T,2} \geq \tfrac{1}{2}T(1-\varepsilon) + \tfrac{1}{8}T(1-\varepsilon)^2(2-\varepsilon) - t_\alpha\sqrt{Td_{\mathfrak{h}}}\}, \tag{10}$$

$$d_{\mathfrak{h}} = 2^{-6}(1-\varepsilon^2)(68-100\varepsilon+65\varepsilon^2-20\varepsilon^3+3\varepsilon^4).$$

Theorem 2. *Let the model of embedding (2) holds and let $\varepsilon > 0$. Then as $T\to\infty$ the asymptotic size of the test (10) for the hypotheses $\mathcal{H}_{0,\varepsilon}, \mathcal{H}_1$ based on the projection of short run statistic*

$$\mathfrak{h} = \mathcal{B}_{T,1} - \tfrac{1}{2}T(1-\varepsilon) + \tfrac{1}{2}(2-\varepsilon)(\mathcal{B}_{T,2} - \tfrac{1}{4}T(1-\varepsilon)^2) \tag{11}$$

coincides with the significance level $\alpha \in (0,1)$. *The asymptotic power of this test for the* $(1,1)$*-model of embedding under the family of contiguous alternatives* $\mathcal{H}_{1,\delta}:\ \{\delta = \frac{\rho}{\sqrt{T}}\}$ *is as follows:*

$$W_1^{\mathfrak{h}+} \to \Phi\left(t_\alpha + \frac{\rho\varepsilon(1+\frac{1}{4}(2-\varepsilon)^2)}{\sqrt{d_{\mathfrak{h}}}}\right),\ T\to\infty. \tag{12}$$

The proves of Lemma 2, Theorem 1 and Theorem 2 we give in [3].

4.3 Likelihood ratio test

Let us now consider the case when the parameter ε in (1) is unknown and separeted from zero: $\varepsilon_0 \le |\varepsilon| < 1$, where $\varepsilon_0 > 0$ is a known boundary value.

To test the hypotheses $\mathcal{H}_0, \mathcal{H}_1$ we now construct the statistical likelihood ratio test. The statistic λ_T of this test for the hypotheses $\mathcal{H}_0,\ \mathcal{H}_1$ is

$$\lambda_T = \lambda_T(y_1^T) = -2\ln\frac{L(\hat{\varepsilon},0)}{\max\{L(\hat{\varepsilon}_1,\hat{\delta}_1), L(\hat{\varepsilon},0)\}} \ge 0, \tag{13}$$

where $\hat{\varepsilon}, (\hat{\varepsilon}_1,\hat{\delta}_1)$ are the ML-estimators under the hypotheses $\mathcal{H}_0$ and $\mathcal{H}_1$ respectively. The statistic (13) is equivalent to the likelihood ratio statistic $\dfrac{\max\limits_{|\varepsilon|<1,\delta>0}\mathbf{P}_\delta\{y_1,\dots,y_T\}}{\max\limits_{|\varepsilon|<1}\mathbf{P}_0\{y_1,\dots,y_T\}}$.

The statistical test of size $\alpha \in (0,1)$ based on the statistic λ_T is defined by the critical region

$$\mathcal{X}_{1\alpha}^{\lambda} = \{y_1^T \in V_T:\ \lambda_T \ge \lambda_\alpha\}, \tag{14}$$

where $\lambda_\alpha > 0$ is the solution of the equation

$$\sup_{\varepsilon_0\le|\varepsilon|<1}\mathbf{P}_0\{\lambda_T \ge \lambda\} = \sup_{\varepsilon_0\le|\varepsilon|<1}(1-F_0(\varepsilon,T,\lambda_T)) = \alpha. \tag{15}$$

Here $F_0(\varepsilon,T,\lambda_T)$ is the probability distribution function of the statistic (13) under the null hypothesis $\mathcal{H}_0$.

To estimate the value of λ_α, satisfying (15), we use the Monte-Carlo procedure: we model M_0 samples of Markov chain of length T with the parameter ε_0. For each sample we calculate the value of the statistic by (13). Let $\lambda^{(1)},\dots,\lambda^{(M_0)}$ be the calculated values. Then λ_α can be estimated by the sample quantile of level $1-\alpha$: $\hat{\lambda}_\alpha = \lambda_{([(1-\alpha)M_0])}$; the accuracy of this procedure increases as $M_0 \to \infty$. So, the test (14) for hypotheses $\mathcal{H}_0, \mathcal{H}_1$: the hypothesis $\mathcal{H}_0$ (respectively $\mathcal{H}_1$) is adopted if $p \ge \alpha$ ($p < \alpha$), where

$$p = \frac{1}{M_0+1}(1+\sum_{i=1}^{M_0} I\{\lambda^{(i)} > \lambda_T\}).$$

5 Statistical estimation of embeddings positions

If the alternative $\mathcal{H}_1$ is adopted, then there is one more problem: estimate positions of embeddings – the indexes $t \in \{1, \ldots, T\}$ at which in accordance with (2) a bit of the cover-sequence $\{x_t\}$ is replaced by a bit of the hidden message $\{\xi_t\}$.

The estimator by the maximum a posteriori probability criterion admits the following equivalent representation:

$$\begin{aligned} \hat{\gamma}_1^{T*} &= \arg \max_{u_1^T \in \Gamma^{(q,r)}} \mathbf{P}_\delta\{\gamma_1^T = u_1^T | y_1^T = \nu_1^T\} = \\ &= \arg \max_{u_1^T \in \Gamma^{(q,r)}} \mathbf{P}_\delta\{\gamma_1^T = u_1^T, y_1^T = \nu_1^T\}. \end{aligned} \tag{16}$$

The solution of the maximization problem (16) for the (q, r)-model [3] of embeddings by the brute force has a computational complexity $O(T(1 + C_q^r)^{T/q})$. So, we develop a polynomial algorithm for solving this problem based on the classical Viterbi algorithm [5].

We denote:

$$\begin{gathered} \mathfrak{s}_t(u_{t-c}, \ldots, u_t) = \max_{u_1, \ldots, u_{t-c-1} \in V} \log \mathbf{P}_\delta\{y_1^t = \nu_1^t, \gamma_1 = u_1, \ldots, \gamma_t = u_t\}, \\ c = \max\{2r + 1, q - 1\}. \end{gathered}$$

The initial values of $\mathfrak{s}_t(u_1, \ldots, u_t)$ при $t = 1, \ldots, c$ are as follows:

$$\begin{aligned} \mathfrak{s}_1(u_1) &= \log \varphi_1(u_1, \nu_1) + \log \mathbf{P}_\delta\{\gamma_1 = u_1\}, \\ \mathfrak{s}_t(u_1, \ldots, u_t) &= \mathfrak{s}_{t-1}(u_1, \ldots, u_{t-1}) + \log \varphi_t(u_1^t, \nu_1^t) + \\ &\quad + \log \mathbf{P}_\delta\{\gamma_t = u_t | \gamma_{t-1} = u_{t-1}, \ldots, \gamma_1 = u_1\}, \ 2 \le t \le c, \end{aligned} \tag{17}$$

where $\varphi_t(\cdot)$ is found in Lemma 1.

Theorem 3. *Under the (q, r)-model of embeddings [3] with $q > r$, the recurrence relation*

$$\begin{gathered} \mathfrak{s}_t(u_{t-c}, \ldots, u_t) = \log \mathbf{P}_\delta\{\gamma_t = u_t | \gamma_{t-1} = u_{t-1}, \ldots, \gamma_{t-c} = u_{t-c}\} + \\ + \max_{u_{t-c-1} \in V} \mathfrak{s}_{t-1}(u_{t-c-1}, u_{t-c}, \ldots, u_{t-1}) + \log \mathfrak{f}_t(u_{t-2r-1}^t, \nu_{t-2r-1}^t) - \log 2, \end{gathered} \tag{18}$$

holds for $\mathfrak{s}_t(\cdot)$ with $t > c$, where

$$\mathfrak{f}_t(u_{t-2r-1}^t, \nu_{t-2r-1}^t) = \begin{cases} 1, \ u_1^t \in \Gamma_0^{(t)}, \\ 1 + (-1)^{\nu_{t-j} + \nu_t} \varepsilon^j, \ u_1^t \in \Gamma_j^{(t)}, \ 1 \le j \le 2r + 1. \end{cases}$$

Under Theorem 3 conditions the estimator $\hat{\gamma}_1^T = (\hat{\gamma}_1, \ldots, \hat{\gamma}_T)$ of the key γ_1^T by the maximum a posteriori probability criterion is

$$\begin{aligned} &(\hat{\gamma}_{T-c}, \ldots, \hat{\gamma}_T) = \arg \max_{u_{T-c}, \ldots, u_T \in V} \mathfrak{s}_T(u_{T-c}, \ldots, u_T), \\ &\hat{\gamma}_t = \arg \max_{v \in V} \mathfrak{s}_{t+c}(v, \hat{\gamma}_{t+1}, \ldots, \hat{\gamma}_{t+c}), \ t = T - c - 1, \ldots, 1. \end{aligned} \tag{19}$$

The estimator $\hat{\gamma}_1^T = (\hat{\gamma}_1, \ldots, \hat{\gamma}_T)$ of the key is obtained as a backward step of the algorithm for finding $\max\limits_{u_{T-c},\ldots,u_T \in V} \mathfrak{s}_T$ by (17),(18).

The algorithm of estimating the positions of embeddings (forward step by (17),(18) and backward step (19)) has a computational complexity $O(2^c + (T-c)2^{2c+2})$.

Computer experiments for estimating the models parameters and detecting the embeddings based on the run test, the short run test and the likelihood ratio test are done with simulated data [2,3]. The experiments agree with the presented here theoretical results.

6 Security of a steganographic scheme

Here we propose an approach for evaluating security of a steganographic scheme based on statistical tests developed in Section 4.

Security of a steganographic scheme with respect to some statistical test with significance level $\alpha \in (0,1)$, determined by the critical region $\mathfrak{X}_\alpha$, – is a property of the steganographic scheme that indicates its ability to resist some steganalytic attack when the goal of such attack is to prove the fact of embeddings presence using the test $\mathfrak{X}_\alpha$. To evaluate security of a steganographic scheme with respect to the test $\mathfrak{X}_\alpha$ we use the probability of type II error:

$$\mathfrak{S}_\alpha^{\mathfrak{X}_\alpha} = \mathbf{P}_\delta\{y_1^T \in \overline{\mathfrak{X}}_\alpha\} \in [0, 1-\alpha], \delta > 0. \tag{20}$$

The security of a steganographic scheme is the greater, the greater the value of $\mathfrak{S}_\alpha^{\mathfrak{X}_\alpha}$. The security $\mathfrak{S}_\alpha^{\mathfrak{X}_\alpha}$ is connected with the power W_1 of the test: $\mathfrak{S}_\alpha^{\mathfrak{X}_\alpha} = 1 - W_1$. We define a steganographic scheme to be κ-secured ($\kappa \in [0, 1-\alpha]$) w.r.t. the test $\mathfrak{X}_\alpha$ with the fixed significance level α if the following inequality holds:

$$\mathfrak{S}_\alpha^{\mathfrak{X}_\alpha} = \mathbf{P}_\delta\{y_1^T \in \overline{\mathfrak{X}}_\alpha\} \geq \kappa. \tag{21}$$

The dependence of the security $\mathfrak{S}_\alpha^{\mathfrak{X}_\alpha}$ on the embeddings fraction $\delta \in [0,1]$ we call the security profile of the considered steganographic scheme. The maximum value of fraction δ_+ which satisfies the inequality (21):

$$\delta_+ = \sup\{\delta : \mathfrak{S}_\alpha^{\mathfrak{X}_\alpha} \geq \kappa\},$$

is called the critical fraction of embeddings.

To construct the steganographic scheme the developer needs to analyze the security of it for some fixed set of values of the significance level: $\alpha \in [\alpha_-, \alpha_+]$. In this situation the averaged security of the steganographic scheme can be used:

$$\mathfrak{S}^{\mathfrak{X}} = \tfrac{1}{\alpha_+ - \alpha_-} \int_{\alpha_-}^{\alpha_+} \mathfrak{S}_\alpha^{\mathfrak{X}_\alpha} d\alpha.$$

For illustration on the simulated data, Figure 1 represents the plots of the averaged ($\alpha_- = 0, \alpha_+ = \frac{1}{2}$) security profiles $\mathfrak{S}^{\mathfrak{X}_1^{\mathfrak{h}+}} \in [0, \frac{3}{4}]$ of the $(1,1)$-steganographic scheme (1),(2) w.r.t. the test $\mathfrak{X}_1^{\mathfrak{h}+}$ for three situations: $(\varepsilon, T) \in$

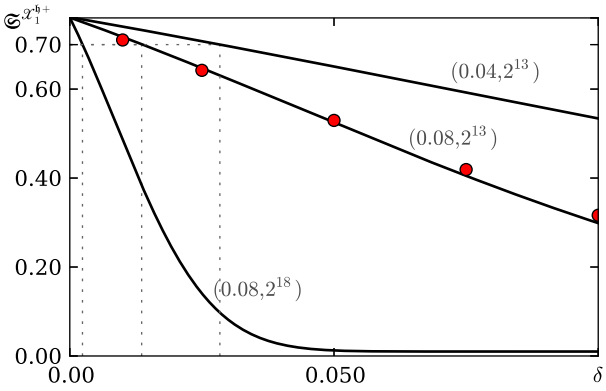


Figure 1. Averaged security profiles w.r.t. $\mathfrak{X}_1^{\mathfrak{h}+}$ when $\alpha_- = 0, \alpha_+ = \frac{1}{2}$

$\{(0.08, 2^{18}), (0.08, 2^{13}), (0.04, 2^{13})\}$. The curves of the theoretical averaged security w.r.t. the test $\mathfrak{X}_1^{\mathfrak{h}+}$ are marked by the solid lines; these theoretical values are calculated using the asymptotic expression (12) for the power W_1 of the test. The experimental values of the averaged security in situation $(0.08, 2^{13})$ are marked by the circles; these experimental values are calculated using $K = 2^9$ simulated stego-sequences (2) for each value of α from the lattice $\{0.00, 0.01, 0.02, \ldots, 0.5\}$. It is seen from Figure 1, for example, that the steganographic scheme (1),(2) is 0.70-secured ($\mathfrak{S}^{\mathfrak{X}_1^{\mathfrak{h}+}} \geq 0.70$), if the embeddings fraction δ is not more than the critical embeddings fraction $\delta_+ = 0.0024, 0.0136, 0.0284$ for situations $(0.08, 2^{18})$, $(0.08, 2^{13})$ и $(0.04, 2^{13})$ respectively.

Note that the similar approach for evaluating security of a steganographic scheme is based on statistical estimators $\hat{\delta}$ for the embeddings fraction presented in Section 3 of this paper. In this approach the security of a steganographic scheme is defined by the relative mean square error:

$$\mathfrak{S}^{\hat{\delta}} = \mathbf{E}\{(\frac{\hat{\delta} - \delta}{\delta})^2\}.$$

7 Conclusion

Under the proposed (q, r)-model of embeddings into a binary stationary Markov chain (as a model of cover-sequence) we constructed the following statistical inferences on the model: ML-estimators for model parameters; statistical tests for detection of embeddings based on run statistic, short run statistic and likelihood ratio statistic; statistical estimator for positions of embeddings. Performance of statistical inferences is evaluated. Two approaches for evaluating security of steganographic schemes are proposed using performance characteristics of constructed statistical inferences.

Bibliographic references

[1] Filler, T. The Square Root Law of Steganographic Capacity for Markov Covers / T. Filler, A.D. Ker, J. Fridrich // Media Forensics and Security XI. Proc. SPIE, San Jose. — 2009. — Vol. 7254. — P. 801–811.

[2] Kharin Yu., Vecherko E. Statistical estimation of parameters for binary Markov chain models with embeddings // Discrete Mathematics and Applications. — 2013. — V. 23, I. 2. — P. 153–169.

[3] Kharin Yu., Vecherko E. Detection of embeddings in binary Markov chains // Discrete Mathematics and Applications. — 2016. — V. 26. I. 1. — P. 13–29.

[4] Ponomarev K. A parametric model of embedding and its statistical analysis // Discrete Mathematics and Applications. —2009. — V. 19, I. 6. — P. 587–596.

[5] Rabiner L.R. A tutorial on hidden Markov models and selected applications in speech recognition // Proc. of the IEEE. — 1989. — V. 77, I. 2. — P. 257–286.

[6] A statistical test suite for random and pseudorandom number generators for cryptographic applicatiions: NIST Special Publication 800-22 Rev. 1a. // National Institute of Standards and Technology. — 2010.

Index

Научное издание

ТЕОРЕТИЧЕСКАЯ И ПРИКЛАДНАЯ КРИПТОГРАФИЯ

Материалы международной научной конференции

Минск, 20–21 октября 2020 г.

В авторской редакции

Ответственный за выпуск *В. А. Волошко*

Подписано в печать 17.11.2020. Формат 60×84/8. Бумага офсетная.
Печать цифровая. Усл. печ. л. 15,34. Уч.-изд. л. 9,72.
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