Международная научная конференция «Теоретическая и прикладная криптография»

Белорусский государственный университет
Минск, 20–21 октября 2020 года

Информация: http://conf.bsu.by/theoreticalandappliedcrypto
Обратная связь: apmi@bsu.by
Онлайн: https://meet.bsu.by/bsu_skype/HGFDLJSG

20 октября (вторник)

10:00 **10:10**	Открытие конференции: **Ю.С. Харин**
	СИММЕТРИЧНАЯ КРИПТОГРАФИЯ
10:10 **10:40**	Групповые свойства SH-обобщения алгоритма блочного шифрования Фейстеля **М.А. Пудовкина**
10:40 **11:10**	Линейный анализ ARX-шифров в зависимости от функции смешивания с раундовым ключом **А.Н.Лебедев, А.А.Козлов**
11:10 **11:40**	Выпуск промежуточных имитовставок при аутентифицированном шифровании **С.В. Агиевич**
11:40 **12:10**	Разработка методики статистического тестирования псевдослучайных последовательностей с применением закона повторного логарифма **А.И. Трубей, М.В. Мальцев, В.Ю. Палуха, И.К. Пирштук**
12:10 **12:40**	Анализ алгоритма шифрования Калина 128/256 с уменьшенным числом раундов интегральным методом **Д.А. Федченко**
	КРИПТОГРАФИЯ С ОТКРЫТЫМ КЛЮЧОМ И РАЗДЕЛЕНИЕ СЕКРЕТА
12:40 **13:10**	Агрегированная подпись на эллиптических кривых **Г.Л.Козина**
13:10 **13:40**	Непороговое модулярное разделение секрета **Г.В. Матвеев, В.В. Матулис**
13:40 **14:00**	**Кофе-пауза**
	БЛОКЧЕЙН-СИСТЕМЫ
14:00 **14:30**	Models of distributed proof generation for ZK-SNARK-based blockchains **Yu. Bespalov, A. Garoffolo, L. Kovalchuk, H. Nelasa, R. Oliynykov**
14:30 **15:00**	Криптографические протоколы на основе блокчейна, стойкого в теоретико-информационном смысле: идеи, реализация, оценки стойкости и надежности **А.М. Кудин**
	ЭФФЕКТИВНАЯ РЕАЛИЗАЦИЯ
15:00 **15:30**	Метод деления на двоичную экспоненту для выполнения декодирующей операции в пороговом МИМА-криптомодуле разделения секрета с маскирующим преобразованием **А.Ф. Чернявский, А.А. Коляда, С.Ю. Протасеня**
15:30 **16:00**	Эффективная многоразрядная арифметика для параллельной модели вычислений **А.Н. Терещенко, В.К. Задирака**

21 октября (среда)

ТЕОРЕТИЧЕСКИЕ ОСНОВЫ

10:00 **10:30**	Компонентная примитивность орграфов **В.М. Фомичев**
10:30 **11:00**	Дискретные временные ряды в криптологии **Ю.С. Харин**
11:00 **11:20**	Об аппроксимации случайных булевых функций пороговыми функциями **В.А. Волошко**

СТЕГАНОГРАФИЯ

11:20 **11:40**	Клептография vs криптография & стеганография **М.Е. Шелест, Б.А. Коваленко, А.И. Трубей**
11:40 **12:00**	Использование системных свойств и параметров текстовых файлов в стеганографических приложениях **П.П. Урбанович, Д.Э. Юрашевич**
12:00 **12:20**	**Кофе-пауза**

ПРИЛОЖЕНИЯ

12:20 **12:40**	О разработке профессионального стандарта "Специалист по криптографической защите информации" **В.П. Лось, Е.Б. Белов**
12:40 **13:00**	Стойкость парольных систем аутентификации в социальных сетях **М.Н. Бобов**
13:00 **13:20**	Сравнительный анализ криптографических архитектур распространенных систем мгновенного обмена сообщениями **М.А. Казловский**
13:20 **13:40**	Защита информации в сетях беспроводного доступа, на основе стандарта безопасности IEEE 802.11ac **А.Н. Ковалевич, Т.Н. Ковалевич**
13:40 **14:00**	Bel VPN продукты. Что нового? **А.М. Сапрыкин, В.М. Саверченко, В.Г. Каревич**

ЗАКРЫТИЕ КОНФЕРЕНЦИИ