Приложение 4

Научная программа XVIII Всероссийской конференции
«Сибирская научная школа-семинар с международным участием “Компьютерная безопасность и криптография”» – SIBECRYPT'19

10.09.2018

Теоретические основы прикладной дискретной математики

Преобразования векторных пространств, *n*-арные полугруппы, гиперэллиптические кривые, аффинные многообразия

Тип доклада	ФИО докладчика	Название доклада
Пленарный	*Черемушкин А.В.*	Свойства сильно зависимых *n*-арных полугрупп
Пленарный	*Фомичев В.М.*	Математические основы матрично-графового подхода к оценке характеристик итеративных преобразований векторного пространства
Устный	*Авезова Я.Э.*, *Фомичев В.М.*	Точная формула экспонента перемешивающего орграфа регистрового преобразования
Устный	*Бобров В.М.*	Оценка с помощью матрично-графового подхода характеристик локальной нелинейности итераций преобразований векторных пространств
Устный	*Григорьев В.С.*	О примитивности перемешивающих графов подстановок регистров сдвига с двумя обратными связями
Устный	*Колесников Н.С.*, *Новоселов С.А.*	О *j*-инвариантах гиперэллиптических кривых с заданным действием эндоморфизма Фробениуса порядка 2 на группу l-кручения
Устный	*Куликов В.Р.*, *Идрисова А.Р.*	Конфигурации конечных случайных множеств с заданной структурой зависимости
Устный	*Мельничук Е.М.*, *Новоселов С.А.*	Характеристические многочлены некоторых гиперэллиптических кривых родов 2,3 и *p*-ранга 1
Устный	*Малыгина Е.С.*	О модулярных многочленах гиперэллиптических кривых рода 2, задаваемых многочленами Диксона
Устный	*Новоселов С.А.*, *Болтнев Ю.Ф.*	Characteristic polynomials of the curve $y^2=x^7+ax^4+bx$ over finite fields
Устный	*Облаухов А.К.*	О метрической регулярности некоторых классов булевых функций
Устный	*Пудовкина М.А.*	Об ортоморфизмах неабелевых групп, имеющих циклическую подгруппу индекса 2
Устный	*Титов С.С.*, *Геут К.Л.*	О блокировке двумерных аффинных многообразий
Устный	*Шоломов Л.А.*	Минимальное представительное множество для системы частотных классов недоопределённых слов

10.09.2018

Математические основы информатики и программирования

Аппаратная реализация языков программирования, разрешимость формальных грамматик, генерическая сложность алгоритмов

Тип доклада	ФИО докладчика	Название доклада
Устный	*Висман Я.А.*	Реализация операций алгоритмического языка ЛЯПАС-Т логическими схемами
Устный	*Колбасина И.В., Сафонов К.В.*	О разрешимости формальных грамматик
Устный	*Рыбалов А.Н.*	О генерической сложности проблемы декодирования линейных кодов

11.09.2018

Математические методы криптографии

Совершенные шифры, криптоанализ, криптопротоколы, хеш-функции, разделение секрета, реализация s-блоков шифрсистем, свойства регистровых преобразований

Тип доклада	ФИО докладчика	Название доклада
Пленарный	*Романьков В.А.*	Эффективные методы алгебраического криптоанализа и защита от них
Устный	*Авезова Я.Э.*	О перемешивающих свойствах нестационарного регистра сдвига
Устный	*Агибалов Г.П.*	О криптографической обратимости конечных автоматов
Устный	*Агиевич С.В., Маслов А.С., Ярошеня Ю.С.*	Lower bounds on probabilities of differential trails in Bash-f
Устный	*Алексеевский И.А.*	Пороговая реализация S-блока государственного стандарта симметричного шифрования РФ
Устный	*Антонов К.В., Семенов А.А.*	Поиск линеаризационных множеств в алгебраическом криптоанализе как задача псевдобулевой оптимизации
Устный	*Бобровский Д.А.*	О свойствах некоторых схем разделения секрета на основе хеш-функций
Устный	*Боровкова И.В.*	Криптоанализ шифрсистем с функциональными ключами
Устный	*Ведунова М.В., Игнатова А.О.*	Блокировка многообразий в конечных полях
Устный	*Высоцкая В.В.*	О некоторых свойствах криптосистем, построенных на основе квазициклических кодов
Устный	*Гребнев С.В.*	Постквантовая версия протокола "Лимонник-3"
Устный	*Гребнев С.В.*	Криптографические свойства отечественных протоколов выработки общего ключа
Устный	*Гребнев С.В.*	О трудоемкости одного метода дискретного логарифмирования
Устный	*Грибанова И.А., Семенов А.А.*	Об аргументации отсутствия свойств случайного оракула у некоторых криптографических хеш-функций
Устный	*Давлетшина А.М.*	Поиск эквивалентных ключей криптосистемы Мак-Элиса – Сидельникова, построенной на двоичных кодах Рида – Маллера
Устный	*Киршанова Е.*	Введение в криптоанализ систем на евклидовых решетках
Устный	*Комиссаров С.М.*	Об алгоритмической реализации s-боксов 16x16 со структурами ARX и «Бабочка»
Устный	*Коренева А.М.*	Оценка характеристик перемешивания и нелинейности хэш-функций семейства MD5
Устный	*Коренева А.М., Тулебаев А.И., Фомичев В.М.*	О параметрах генератора раундовых ключей алгоритма 2-ГОСТ

Устный	*Лисовский К.А.*	Разделение секрета на плоскостях Холла
Устный	*Максимов К.В.*	Об оптимизации характеристик низкоресурсного алгоритма шифрования PRESENT с помощью модификации некоторых функциональных элементов
Устный	*Матвеев Н.А.*	О перемешивающих свойствах регистровых преобразований, реализуемых при некоторых модификациях аддитивных генераторов
Устный	*Медведев Н.В., Титов С.С.*	Однородные матроиды, блок-схемы и схемы разделения секрета
Устный	*Медведева Н.В., Титов С.С.*	Геометрическая модель совершенных шифров
Устный	*Олефиренко Д.О.*	Задача нахождения короткого вектора решетки в бесконечной норме
Устный	*Перов А.А.*	Об использовании технологий машинного обучения для проверки статистических свойств симметричных криптографических алгоритмов
Устный	*Сапегина М.Д.*	Оценка характеристик нелинейности итераций преобразований векторных пространств с помощью матрично-графового подхода
Устный	*Сорокин М.А.*	APN-преобразования и разделяющее свойство мультимножеств
Устный	*Токарева Н.Н.*	О построении S-блоков
Устный	*Толмачев Н.С., Хегай А.А., Черникова А.П.*	Многообразие в некоторых подмножествах бинарных полей Галуа
Устный	*Хайруллин И.И.*	О свойствах многомерных генераторов на основе линейных регистров сдвига и нелинейной комбинирующей функции

12.09.2018

Математические основы компьютерной безопасности

Контроль целостности и управление доступом, обфускация вычислений, анализ интернет-трафика, программно-аппаратные закладки

Тип доклада	ФИО докладчика	Название доклада
Пленарный	*Колегов Д.Н.*	Обзор современных тенденций в области разработки и реализации криптографических протоколов защиты транспортного уровня
Устный	*Девянин П.Н.*	О моделировании в рамках МРОСЛ ДП-модели мандатных контроля целостности и управления доступом в СУБД PostgreSQL
Устный	*Елисеев В.Л.*	Искусственные нейронные сети как механизм обфускации вычислений
Устный	*Кабанов И.М.*	Разработка средств обнаружения и предотвращения вторжений и управление инцидентами безопасности на основе анализа сетевого трафика
Устный	*Семибратов И.В.*	Оценка вероятности успеха некоторых атак нарушителя в блокчейн-сети «Биткоин»
Устный	*Фескович А.О.*	Кластеризация интернет-трафика
Устный	*Галайчук Г.*	Проблема программно-аппаратных закладок в устройствах хранения информации

12.09.2018

Вычислительные методы в дискретной математике

Алгоритмы псевдобулевой оптимизации, эксперименты над алгоритмами, интеллектуальный анализ данных, алгоритмы маршрутизации, деревья хеширования

Тип доклада	ФИО докладчика	Название доклада
Пленарный	*Грибанова И.А., Отпущенников И. В., Павленко А.Л., Семенов А.А.*	Применение алгоритмов псевдобулевой оптимизации к построению алгебраических атак на некоторые легковесные блочные шифры
Устный	*Белый И.Д.*	Построение латинских квадратов
Устный	*Быкова В.В., Монгуш Ч.М.*	Алгоритм декомпозиции бинарного контекста с сохранением формальных понятий
Устный	*Дали Ф.А.*	Экспериментальные исследования некоторых структурных свойств локальных нелинейных биективных преобразований
Устный	*Женевский С.В., Мельников С.Л., Шурупов А.Н.*	О проблеме распознавания алгебраических пороговых функций
Устный	*Заикин О.С.*	Криптоанализ некоторых поточных шифров при помощи алгоритма решения проблемы булевой выполнимости, базирующегося на методе опорных векторов
Устный	*Кузнецов А.А.*	Эффективные алгоритмы маршрутизации на графах Кэли групп подстановок
Устный	*Малыгин Е.А.*	Блок-схемы Киркмана на основе примитивных многочленов и алгоритма Зеха – Якоби
Устный	*Маняев Г.О., Шурупов А.Н.*	Сравнительный анализ эффективности решения систем псевдобулевых неравенств алгоритмами имитации отжига, Балаша и внутренней точки
Устный	*Миронкин В.О.*	О вероятностных свойствах деревьев хэширования, построенных на основе равновероятного случайного отображения
Устный	*Руменко Н.Ю., Костюк А.В.*	Способ решения недоопределенных систем линейных уравнений над F_sup_2 с искаженными правыми частями и ограничением на малый вес решения

13.09.2018

Дискретные функции

APN-функции, бент-функции, векторные булевы функции, корреляционно-иммунные отображения

Тип доклада	ФИО докладчика	Название доклада
Устный	*Городилова А.А., Останина А.Ю.*	Свойства ассоциированных булевых функций APN-функций
Устный	*Карпова Л.А., Панкратова И.А.*	Синтез биективных векторных булевых функций
Устный	*Киселева Н.М., Липатова Е.С., Трифонова Е.Е.*	О свойствах подстановок на $\{0,1\}^n$
Устный	*Коломеец Н.А.*	О свойствах бент-функций, построенных по некоторой бент-функции с помощью подпространств
Устный	*Кузьмина Т.А.*	О свойствах алгебраической нормальной формы бент-функций
Устный	*Куценко А.В.*	Об изометрических отображениях множества самодуальных бент-функций

Устный	*Метальникова А.И.*, *Панкратова И.А.*	О классах булевых функций ограниченной сложности
Устный	*Милосердов А.В.*	О связи нелинейных и дифференциальных свойств векторных булевых функций
Устный	*Панков К.Н.*	Рекуррентные формулы для числа корреляционно-иммунных отображений
Устный	*Шапоренко А.С.*	О кватернарных и булевых бент-функциях

13.09.2018

Прикладная теория кодирования, автоматов и графов

Вершинные и реберные расширения графов, задача о кратчайшем пути в сети, динамические системы двоичных векторов, гомоморфизмы регистров сдвига, построение матроидов

Тип доклада	ФИО докладчика	Название доклада
Устный	*Абросимов М.Б.*, *Лобов А.А.*	О вершинных 1-расширениях 4-слойных графов
Устный	*Абросимов М.Б.*, *Рыбалко А.А.*	О минимальных рёберных 1-расширениях орграфов
Устный	*Абросимов М.Б.*, *Камил И.*, *Судани Х.*	О построении минимальных вершинных и рёберных 1-расширений методом МакКея
Устный	*Быкова В.В.*, *Солдатенко А.А.*	Приближенный алгоритм для задачи о ресурсоограниченном кратчайшем пути в сети и его расширения
Устный	*Жаркова А.В.*	О некоторых свойствах динамических систем двоичных векторов, ассоциированных с графами
Устный	*Чередник И.В.*	Гомоморфизмы регистров сдвига в обобщенные линейные автоматы
Устный	*Шаршина С.В.*	Построение матроидов, непредставимых над конечными полями

Председатель программного комитета  Г.П. Агибалов