конференция РусКрипто

(/)

Конференция Программа Участникам Материалы ассоциации

ПРОГРАММА КОНФЕРЕНЦИИ

ТЕМАТИЧЕСКАЯ СЕКЦИЯ

КРИПТОГРАФИЯ И КРИПТОАНАЛИЗ

Классическая секция конференции, посвященная научным и практическим вопросам криптографии и криптоанализа.

ВЕДУЩИЕ СЕКЦИИ

МАТЮХИН Дмитрий Викторович

К.ф.-м.н., ФСБ России (http://www.fsb.ru/)

АЛЕКСЕЕВ Евгений Константинович

К.ф.-м.н., КриптоПро (https://www.cryptopro.ru/)

ЖУКОВ Алексей Евгеньевич

К.ф.-м.н., Ассоциация «РусКрипто», МГТУ им. Баумана (http://www.bmstu.ru/)

37 ЭКСПЕРТОВ

20 ДОКЛАДОВ

ЧАСТЬ I. 23 МАРТА, 17:00 — 19:30

Криптографический конкурс: разделение секрета или порча секрета. Cryptographic challenge — Secret Sharing or Secret Spoiling

Eric Filiol, профессор, ENSIBS-France (https://www-ensibs.univ-ubs.fr/fr/index.html), НИУ ВШЭ (https://www.hse.ru/)

Эрик Филиол предлагает участникам конференции принять участие в криптографическом конкурсе. Участникам конференции будет представлен код программы, реализующий протокол разделения секрета Шамира, и содержащий уязвимость (бэкдор) в системе безопасности. Цель конкурса – выявить недостаток и объяснить, как его можно использовать со значительной вероятностью успеха. Победителю будет вручен специальный приз от нашего уважаемого французского коллеги.

Свойства некоторых режимов шифрования при использовании TWIN-конструкции с блочным шифром «Магма»

Гузаирова Диана Маратовна, СФБ Лаб (https://sfblaboratory.ru/)

Двойное параллельное шифрование (TWIN-конструкция) — способ увеличения допустимой нагрузки на ключ для некоторых режимов, к примеру, CTR и GCM. С использованием теории доказуемой стойкости получены соответствующие оценки, выполнено сравнение с характеристиками стандартизированных режимов. Также показано, что использование в TWIN шифра «Магма» затрудняет применение известных методов определения секретного ключа.

О свойствах алгоритма S3G-128 при использовании усеченной хэш-функции Стрибог

Кирюхин Виталий Александрович, старший специалист, СФБ Лаб (https://sfblaboratory.ru/)

Ключевой алгоритм S3G-128 построен на основе хэш-функции Стрибог, используется в аппаратных модулях устройств мобильной связи. Рассматриваются свойства S3G-128 при усечении Стрибога до одного вызова функции сжатия: получены оценки в рамках теории доказуемой стойкости; разработан метод определения секретного ключа для 6 (из 12) раундов.

О поиске разностных соотношений для подстановки ALZETTE с максимальным или близким к нему значением разностной характеристики

Дмух Андрей Александрович, Академия криптографии Российской Федерации (https://cryptoacademy.gov.ru/)
Пасько Дмитрий Олегович, Академия криптографии Российской Федерации (https://cryptoacademy.gov.ru/)

Предлагается подход для поиска разностных соотношений ARX-подстановки ALZETTE с переменным числом итераций, позволяющий получить соотношения с максимальными или близкими к максимальным разностными характеристиками.

Использование преобразований, задаваемых умножением на элемент кольца, в качестве линейных преобразований в XSL-схемах

Давыдов Степан Андреевич, специалист-исследователь, НПК «Криптонит» (https://kryptonite.ru/)
Шишкин Василий Алексеевич, к.ф.-м.н., руководитель лаборатории криптографии, НПК «Криптонит» (https://kryptonite.ru/)

Одной из основополагающих задач, стоящих перед разработчиками современных симметричных базовых криптографических систем является задача построения линейных преобразований с заданными криптографическими характеристиками. В работе рассматривается класс линейных преобразований, задаваемых умножением на элемент кольца. Такие преобразования могут быть эффективно реализованы с

использованием современных инструкций процессора — CLMUL и XOR. Среди матриц указанного вида были найдены матрицы размера 8×8 с 8-битными блоками и показателем рассеивания 8, матрицы 16×16 с 4-битными блоками и показателем рассеивания 12.

О квази-адамаровых преобразованиях на конечных группах

Пудовкина Марина Александровна, д.ф-м.н., профессор, НИЯУ МИФИ (https://mephi.ru/)

Для произвольной конченой группы введены обобщенные квази-адамаровы преобразования, частным случаем которых являются псевдо-адамаровы преобразования алгоритмов блочного шифрования семейства Safer, Twofish, а также квази-адамаровы преобразования, заданные на декартовом произведении Z^2_{2^m}. Доказан критерий биективности, а также выявлена связь биективности с принадлежностью к преобразованиям, которые можно считать обобщением ортоморфизмов и полных преобразований, применяемых в дискретной математике и криптографии.

Построение множества невозможных разностей алгоритмов шифрования Фейстеля с небиективной функцией усложнения для произвольного числа раундов

Дмитрий Захаров, НИЯУ МИФИ (https://mephi.ru/)

Доклад победителя конкурса студенческих докладов.

Задача скрытой подгруппы в методах квантового крипотанализа

Поляков Михаил Вадимович, МГТУ им. Н.Э.Баумана (http://bmstu.ru/)

Задача скрытой подгруппы возникает как подзадача в квантовом алгоритме Шора, который эффективно решает задачу факторизации и дискретного логарифмирования. В тоже время, поиск скрытой подгруппы (или еще говорят, скрытого сдвига) является составной частью ряда методов криптоанализа симметричных шифрсистем. В данной работе рассматривается вопрос решения задачи скрытой подгруппы на квантовом компьютере для поиска линейных структур в симметричных криптоалгоритмах.

О реализации хэш-функции ГОСТ 34.11-2018 в виде квантовой схемы

Денисенко Денис Витальевич, МГТУ им. Н.Э. Баумана (https://www.bmstu.ru/)
Рудской Владимир Игоревич, ТК 26 (https://tc26.ru/)

В докладе представлена реализация уменьшенной модели хэш-функции ГОСТ 34.11-2018 в виде квантовой схемы. Показано, что минимальное необходимое количество логических кубит зависит от длины хэшируемого сообщения. Представлены оценки минимального необходимого количества логических кубит для реализации ГОСТ 34.11-2018.

ЧАСТЬ II. 24 МАРТА, 10:00 — 12:00

О статистических свойствах последовательностей, формируемых физически неклонируемыми функциями для использования в механизмах идентификации и аутентификации

Романенков Роман Александрович, ТК 26 (https://tc26.ru/)
Уривский Алексей Викторович, Инфотекс (https://infotecs.ru/)
Щербакова Анна Олеговна, Инфотекс (https://infotecs.ru/)
Бондаренко Александр Иванович, Академия криптографии Российской Федерации (https://cryptoacademy.gov.ru/)
Маршалко Григорий Борисович, ФСБ России (http://www.fsb.ru/)

Работа посвящена исследованию характеристик двоичных последовательностей, вырабатываемых с использованием физически неклонируемых функций (ФНФ). Предложен набор статистических экспериментов, позволяющий сделать вывод о свойствах ФНФ на основе анализа характеристик вырабатываемых ими двоичных последовательностей. Приведены результаты экспериментальных исследований ФНФ, основанных на использовании статической памяти с произвольным доступом (ФНФ типа SRAM).

Псевдослучайные функции «с забыванием» в механизмах защиты на основе паролей

Никифорова Лидия Олеговна, инженер-аналитик, КриптоПро (https://www.cryptopro.ru/)
Ахметзянова Лилия Руслановна, заместитель начальника отдела криптографических исследований, КриптоПро (https://www.cryptopro.ru/)

В работе рассматриваются псевдослучайные функции «с забыванием» (oblivious PRF, OPRF). Данный механизм позволяет клиенту получать результат вычисления псевдослучайной функции, использующей в качестве ключа секрет сервера, от своих данных. Вычисление выполняется с помощью интерактивного протокола таким образом, что клиент не узнает секрет сервера, а сервер не получает никакой информации о данных клиента и результате вычисления. Основное внимание в работе уделено рассмотрению OPRF в качестве составной части механизмов защиты на основе малоэнтропийных секретов (паролей). Рассмотрены механизм распределенного хранения секрета с доступом по паролю, менеджер паролей. Для рассмотренных механизмов обозначены свойства безопасности, которые ими обеспечиваются, описаны принципы построения.

Высокопроизводительная псевдослучайная функция pCollapserARX256-32x2

Поликарпов Сергей Витальевич, Южный федеральный университет (https://sfedu.ru/)
Румянцев Константин Евгеньевич, Южный федеральный университет (https://sfedu.ru/)
Прудников Вадим Александрович, Южный федеральный университет (https://sfedu.ru/)

Определяется возможность использования ARX-функций в качестве основного элемента псевдо-динамической подстановки. Осуществляется интегрирование

псевдо-динамических подстановок на основе ARX-функций в структуру псевдо-случайной функции pCollapser. Создаётся и оценивается производительность последовательной и параллельной программной реализации.

Об одном классе алгоритмов контроля целостности больших блоков данных

Бобровский Дмитрий Александрович, Финансовый университет при Правительстве РФ (http://www.fa.ru/), Код Безопасности (https://www.securitycode.ru/)
Фомичев Владимир Михайлович, д.ф.-м.н., профессор, Финансовый университет при Правительстве РФ (http://www.fa.ru/), Код Безопасности (https://www.securitycode.ru/), ФИЦ ИУ РАН (https://www.frccsc.ru/)
Задорожный Дмитрий Игоревич, Код Безопасности (https://www.securitycode.ru/)
Коренева Алиса Михайловна, к.ф.-м.н., Код Безопасности (https://www.securitycode.ru/)
Курочкин Алексей Вячеславович, Код Безопасности (https://www.securitycode.ru/), МФТИ (https://mipt.ru/)

В докладе представлен класс алгоритмов контроля целостности больших блоков данных. Алгоритмы класса превосходят по производительности до 73 раз известные алгоритмы, что показывает высокий потенциал данного класса в части приложений. Вместе с тем, для некоторых алгоритмов из класса показана недостаточность уровня защиты от коллизий, что инициирует задачу тщательного выбора в заданном классе параметров алгоритмов.

Атака на шифры гаммирования, использующие q-слабые ключи

Бабаш Александр Владимирович, д.ф.-м.н., профессор, НИУ ВШЭ (https://www.hse.ru/), РЭУ им. Г.В. Плеханова (https://rea.ru/)

Под информацией о «читаемом» тексте понимается собственное подмножество всех читаемых текстов содержащее текст. Дешифрование шифра по шифрованному тексту трактуется как определение информации о зашифрованном читаемом тексте. Для шифртекста шифра гаммирования вводится понятие q-слабого ключа, учитывающее корреляцию между зашифрованным текстом и используемым ключом. Указываются методы дешифрования шифров гаммирования на основе q-слабых ключей с расчетом параметров их сложности.

О возможностях противника при атаках на некоторый класс протоколов аутентифицированной выработки общего ключа

Алексеев Евгений Константинович, начальник отдела криптографических исследований, КриптоПро (https://www.cryptopro.ru/)
Ахметзянова Лилия Руслановна, заместитель начальника отдела криптографических исследований, КриптоПро (https://www.cryptopro.ru/)
Куценок Кирилл Олегович, инженер-аналитик, КриптоПро (https://www.cryptopro.ru/)
Кяжин Сергей Николаевич, ведущий инженер-аналитик, КриптоПро (https://www.cryptopro.ru/)

В настоящей работе приводится систематизированный обзор качественных возможностей противника, атакующего протоколы аутентифицированной выработки общего ключа (AKE-протоколы, Authenticated Key Exchange), которые рассматриваются в современных криптографических исследованиях по данному направлению. Внимание в работе концентрируется на наиболее базовом типе таких протоколов, который предполагает взаимодействие двух участников (в частности, не рассматриваются протоколы с участием третьей доверенной стороны). Для каждой из возможностей, перечисленных в настоящей работе, приводится мотивация ее рассмотрения. Также приводятся примеры их применения при построении атак на известные протоколы.

ЧАСТЬ III. 24 МАРТА, 12:30 — 14:15

Новый механизм матричного гибридного асимметричного шифрования. A new matrix hybrid asymmetric ciphering mechanism

François Dupont, CNRS (https://www.cnrs.fr/en)

Предлагается новый гибридный механизм асимметричного шифрования, использующий трехпроходный протокол с ключами шифрования, которые являются коммутирующими матрицами. Такой трехпроходный протокол также позволяет проводить аутентификацию участников.

Еще раз о важности построения модели противника на примере

протокола аутентификации 5G-AKA

Царегородцев Кирилл Денисович, специалист-исследователь, НПК «Криптонит» (https://kryptonite.ru/)
Грибоедова Екатерина Сергеевна, руководитель направления стандартизации, НПК «Криптонит» (https://kryptonite.ru/)

Довольно часто вопросы «доказуемой стойкости» вызывают дискуссии; так, многими ставится под сомнение сама необходимость подобного подхода, а ошибки в доказательствах и моделях стали «притчей во языцех». В докладе на примере угрозы нарушения приватности пользователей для протокола 5G-AKA будут затронуты некоторые аспекты моделирования и теоретико-сложностных сведений: зачем нужна формализация/модель и можно ли обойтись без этого этапа? каковы гарантии, если сведение все-таки удалось построить? и наконец: отличается ли кардинально ситуация с моделями внутри криптографии от других наук?

Использование атрибутной подписи в двухуровневой распределенной информационной системе с динамической структурой

Беззатеев Сергей Валентинович, Санкт-Петербургский университет аэрокосмического приборостроения (https://guap.ru/)
Жиданов Константин Александрович, Санкт-Петербургский университет аэрокосмического приборостроения (https://guap.ru/)
Афанасьева Александра Валентиновна, Санкт-Петербургский университет аэрокосмического приборостроения (https://guap.ru/)

Рассматривается информационная система с динамической структурой, состоящая из узлов (устройств, элементов) двух типов, образующих два уровня. Узлы первого уровня получают, собирают и обрабатывают информацию. Устройства второго уровня образуют распределенную систему, использующую криптографические протоколы на базе атрибутов и обеспечивающую верификацию передаваемой информации. При этом для предотвращения сговора узлов второго уровня для каждого сеанса верификации выполняется протокол голосования, использующий атрибуты текущего сеанса.

Методика автоматизированного тестирования реализаций криптографических протоколов

Прокопьев Сергей Евгеньевич, Институт системного программирования им. В.П.

Иванникова РАН (https://www.ispras.ru/), НПК «Криптонит» (https://kryptonite.ru/)

В докладе представляется подход к тестированию реализаций криптопротоколов, основанный на использовании выразительных формальных моделей. Рассматриваются преимущества предлагаемого подхода в части измерения качества тестирования, применимости тестового инструментария для разных криптопротоколов и др.

Сеанс черной магии с разоблачениями

Eric Filiol, профессор, ENSIBS-France (https://www-ensibs.univ-ubs.fr/fr/index.html), НИУ ВШЭ (https://www.hse.ru/)

Подробное объяснение механизма работы лазейки из первого доклада в секции и вручение приза от Эрика Филиола победителю.

СЕКЦИИ И КРУГЛЫЕ СТОЛЫ (/PROGRAM/SECTIONS/)

ПАРТНЕРЫ И СПОНСОРЫ

ПРЕМИУМ-ПАРТНЕРЫ

(https://infotecs.ru/)

Золотой партнер

(https://www.cryptopro.ru/)

Золотой партнер

(https://www.rutoken.ru/)

Бронзовый партнер

(https://www.s-terra.ru/)

Бронзовый партнер

(https://kryptonite.ru/)

Бронзовый партнер

(https://goqrate.com/)

Бронзовый партнер

(https://quanttelecom.ru/)

Бронзовый партнер

(https://neobit.ru/)

Научный партнер

(https://factor-ts.ru/)

Партнер выставки

(https://answerpro.ru/)

Партнер выставки

(https://roseu.org/)

Партнер выставки

(https://systempb.ru/)

Партнер выставки

(https://www.crosstech.su/)

Партнер выставки

(https://www.stc-spb.ru/)

Партнер выставки

(https://spacebit.ru/)

Партнер выставки

(https://apkit.ru/)

Партнер конференции

(https://www.securitycode.ru/)

Партнер конференции

(https://rqc.ru/)

Партнер конференции

(https://rt-solar.ru/)

Партнер конференции

(https://ib-bank.ru/bisjournal/)

Информационный партнер

(https://cisoclub.ru/)

Информационный партнер

(http://nbj.ru/)

Информационный партнер

ОРГАНИЗАТОРЫ КОНФЕРЕНЦИИ

(http://infosystems.ru/)

(/accociation/about/)

ПРИ ПОДДЕРЖКЕ И УЧАСТИИ

ФСБ РОССИИ (HTTP://FSB.RU/), ТК26 (HTTPS://TC26.RU/), РФФИ (HTTP://WWW.RFBR.RU/RFFI/RU/), УМО ИБ (HTTP://WWW.ISEDU.RU/), МОО «АЗИ» (HTTP://AZI.RU/), ВШЭ (HTTPS://WWW.HSE.RU/)

(https://www.facebook.com/groups/ruscrypto/)