Министерство образования и науки Российской Федерации

Федеральное учебно-методическое объединение в системе высшего образования
по укрупненной группе специальностей и направлений подготовки
10.00.00 «Информационная безопасность»

Региональное отделение ФУМО ВО ИБ
по Сибирскому и Дальневосточному федеральным округам

Томский государственный университет
систем управления и радиоэлектроники

VII ПЛЕНУМ СибРОУМО
регионального отделения ФУМО ВО ИБ
по Сибирскому и Дальневосточному федеральным округам

XVI МЕЖДУНАРОДНАЯ НАУЧНО-ПРАКТИЧЕСКАЯ КОНФЕРЕНЦИЯ
«Проблемы информационной безопасности государства, общества и личности»

Доклады VII Пленума СибРОУМО
и материалы XVI конференции

6–10 июня 2018 г.
г. Томск

В-Спектр
Томск–2018

УДК 004.056
Д 63

Д 63 **Доклады VII Пленума СибРОУМО и материалы XVI конференции «Проблемы информационной безопасности государства, общества и личности»**, Томск, 6–10 июня 2018 г. – Томск: В-Спектр, 2018. – 110 с.
ISBN 978-5-91191-393-9

Настоящий сборник содержит научно-методические и учебно-методические материалы VII Пленума Сибирского регионального учебно-методического объединения вузов России по образованию в области информационной безопасности и конференции, проведенных 6–10 июня 2018 г. на базе ТУСУРа.

УДК 004.056

Оргкомитет выражает признательность всем научно-педагогическим и научным коллективам, которые приняли непосредственное участие в организации и проведении Пленума СибРОУМО и конференции.

Особую благодарность выражаем Томскому государственному университету систем управления и радиоэлектроники.

Составители: ***Е.Б. Белов (председатель), А.А. Шелупанов, Р.В. Мещеряков, А.А. Конев, Е.М. Давыдова***

Ответственный за выпуск: ***А.А. Шелупанов***

Генеральный спонсор конференции:
ГК «ИнфоТеКС»
Спонсоры конференции:
ООО «Удостоверяющий центр Сибири»
ЗАО «Аладдин Р.Д.»
АО «ПКК Миландр»

ISBN 978-5-91191-393-9

СОДЕРЖАНИЕ

Раздел 1. Информационные материалы

Раздел 2. Доклады VII Пленума СибРОУМО

Раздел 3. Материалы XVI Международной научно-практической конференции «Проблемы информационной безопасности государства, общества и личности»

УДК 519.7

Г.П. Агибалов

О криптографии в информационной безопасности (на примере ТГУ)

Сообщается о результатах научных исследований кафедры защиты информации и криптографии Томского государственного университета за последние 10 лет по анализу и синтезу криптосистем с функциональными ключами и по созданию доверенного программно-аппаратного обеспечения криптографии, а также о планах кафедры по подготовке специалистов в области компьютерной криптографии.

Ключевые слова: криптография, криптоанализ, функциональные ключи, доверенное программно-аппаратное обеспечение, компьютерная криптография, профессиональный цикл дисциплин.

В 2009 г. отмечалось 50-летие научной школы криптографии в Томском государственном университете (ТГУ) и сообщалось о её важнейших достижениях к тому времени [1]. Сейчас, накануне 60-летия этой школы, мы хотим продолжить данное сообщение научными достижениями школы в последнее время и поделиться ближайшими планами развития криптографии в ТГУ как в сфере науки, так и, в особенности, в образовательной сфере. Это наше желание продиктовано, главным образом, печальным выводом, к которому мы приходим, сравнивая уровни развития криптографии в США и в России по открытым американским источникам четвертьвековой давности [2–6] и современным отечественным открытым источникам в лице лучших российских научных журналов по криптографии (Прикладная дискретная математика и математические вопросы криптографии), а также по трудам ежегодной Всероссийской научной конференции Sibecrypt. Это сравнение убедительно говорит за то, что «наша криптография» отстаёт от «их криптографии» как минимум на 30 лет – и по научным результатам, и по их востребованности государством, обществом, личностью, и по широте и глубине охвата криптографии в образовательных целях высшими учебными заведениями страны. И это всё при том, что 3/4 выпускников кафедры защиты информации и криптографии ТГУ работают за «бугром», а 2/3 – в США.

В последние десять лет криптографическая школа ТГУ занималась в основном исследованиями криптосистем с функциональными ключами [7–14], разработкой доверенного программно-аппаратного обеспечения криптографии [15, 16] и переориентацией образовательного процесса в ТГУ в области информационной безопасности на криптографию. Об этом и будет идти речь далее.

Криптография с функциональными ключами

Разработаны общая схема построения итеративных блочных шифров с функциональными ключами и два её частных случая – специальные схемы для построения таких шифров некоторых двух классов. Общая схема оригинальная, прототипами специальных схем послужили известные схемы Фейстеля и Lucifer. Все схемы шифров с аддитивными раундовыми ключами являются также частными случаями данной общей схемы шифров с функциональными ключами.

Введено понятие шифра с водяными знаками, защищающего одновременно конфиденциальность и легитимность использования информации. Построен ряд примеров таких шифров на базе поточных шифров с функциональными ключами.

Определено понятие криптоавтомата как некоторого класса C автоматных сетей с фиксированной структурой N, построенных с помощью операций последовательного, параллельного и с обратной связью соединений инициальных конечных автоматов с функциями переходов и выходов, принадлежащих произвольным функциональным классам. Ключ криптоавтомата может содержать в себе начальные состояния и функции переходов и выходов некоторых компонент в N так, что задание любого конкретного ключа k влечёт за собой выбор вполне определённой автоматной сети N_k в C в качестве конкретного криптографического алгоритма. Криптоанализ криптоавтомата осуществляется путём решения системы уравнений, сопоставляемой сети N_k и доопределения возникающих при этом частичных функций её компонент в заданных классах. Для её решения предложен метод DSS, который в применении к некоторой системе уравнений E является итерацией следующей тройки действий: 1) E разделяется (Divided) на две подсистемы E' и E'', где E' легко решаема; 2) E' решается (Solved); 3) решение E' подставляется (Substituted) в E''. Определение и криптоанализ иллюстрируются на примерах автономных криптоавтоматов, обобщающих известные в поточных шифрах схемы криптографических генераторов на регистрах сдвига с линейной обратной связью (LFSR) – генератора дельта-, тау-шагов и генератора с альтернативным управлением (с перемежающимся шагом). Представлен ряд атак на эти криптоавтоматы с ключами различных типов, сочетающих в себе и начальные состояния, и функции переходов и выходов компонент в сети криптоавтомата. Возникающие в них доопределения частичных функций в соответствующих классах продемонстрированы на классе, состоящем из всех булевых функций от

большого числа переменных с малым количеством существенных аргументов из них.

Определён новый симметричный блочный шифр подстановки на множестве булевых векторов произвольной длины n, в котором ключом служит векторная булева функция $f(x_1, \ldots, x_n)$ размерности n, получаемая операциями перестановки и отрицания над переменными и координатными функциями некоторой биективной (обратимой) векторной булевой функции $g = (g_1, \ldots, g_n)$, в которой для каждого $i = 1, \ldots, n$ координатная функция g_i существенно зависит от небольшого числа s_i переменных из ряда $x_1, \ldots, x_n$. Функции $g_1, \ldots, g_n$, их существенные переменные и числа $s_1, \ldots, s_n$ являются открытыми параметрами шифра. По данному определению ключ f является, как и функция g, биекцией, и число существенных переменных каждой координатной функции в нём находится среди $s_1, \ldots, s_n$. Зашифрование блока P открытого текста в блок C шифртекста выполняется по правилу $C = f(P)$, а его расшифрование – по правилу $P = f^{-1}(C)$. Криптоанализ шифра атакой с известным открытым текстом с угрозой раскрытия ключа сводится к нахождению по части функции f существенных переменных для её координатных функций и доопределению частей последних на всех наборах значений этих их переменных с сохранением свойства биективности f. Предложен алгоритм решения этой задачи в общем случае, а также при некоторых ограничениях на операции перестановки и отрицания в формуле искомого ключа.

Для построения обратимых векторных булевых функций $g(x_1, \ldots, x_n)$ от большого числа n переменных из координатных функций с малым числом s существенных переменных предложены два метода. В первом методе, предполагающем $s|n$ и $n = st$, функция g строится как набор из t биективных векторных функций размерности s от непересекающихся подмножеств переменных. Существование обратимых векторных функций размерности s с координатными функциями, существенно зависящими от s переменных, доказано конструктивно. Представлены количественные оценки эффективности этой конструкции, полученные в компьютерном эксперименте. Во втором методе функция g определяется индукцией по числу n её переменных, в которой при $n = s$ она берётся из первого метода, а при $n = s + i$ для $i > 0$ её первые $s + i - 1$ координатные функции совпадают с координатными функциями в фунции g от $s + i - 1$ переменных, а $(s + i)$-я координатная функция получается как сумма $x_{(s+i)}$ и функции от переменных $x_1, \ldots, x_{(s+i-1)}$, существенно зависящей от $s - 1$ переменных.

Доверенное программно-аппаратное обеспечение криптографии

Так мы называем проприетарное программно-аппаратное обеспечение, свободное от недокументированных закладок, уязвимостей программного обеспечения, скрытых информационных каналов, шпионского софта и критических ошибок исполняемого кода. Его мы создаём на базе собственного языка программирования ЛЯПАС, предназначенного для представления алгоритмов дискретной математики.

Разработано криптографическое расширение ЛЯПАС-Т этого языка [15], вобравшее в себя элементарные операции из современных криптографических алгоритмов, в том числе над длинными целыми числами и длинными булевыми векторами. Создан и запущен в опытную эксплуатацию компилятор с ЛЯПАСа-Т в язык Ассемблера под ОС Linux. С его помощью ведётся отладка, исполнение, экспериментальное исследование алгоритмов на ЛЯПАСе-Т и их доработка по результатам исследования. Разработаны проекты процессора, аппаратно реализующего ЛЯПАС-Т, его исполняемого кода и препроцессора, транслирующего программы на ЛЯПАСе-Т в исполняемый код процессора. Создан ряд прикладных программ на ЛЯПАСе-Т для криптографической защиты управляющей информации (ГОСТ, AES, ElGamal, KASUMI, WHT и др.). Создаётся многоуровневый транслятор с ЛЯПАСа-Т в машинный код для разработки методом раскрутки собственной ОС, гарантирующей запуск и исполнение программ на ЛЯПАСе-Т без привлечения чужеродных ОС. Предложена и реализована в трансляторе новая семантика операций над комплексами в ЛЯПАСе-Т, обеспечивающая более безопасную работу с ними исполняемым программам и более удобную работу с ними программистам [16].

Криптографическое образование

Ниже перечислен ряд криптографических дисциплин вместе с их краткими аннотациями, предлагаемых в качестве основы профессионального цикла ООП «Компьютерная криптография». Большинство из них уже апробировано в учебном процессе ТГУ по программе компьютерной безопасности.

Правовое обеспечение криптографии: актуальные вопросы правового регулирования криптографии в России и других странах, включая организацию лицензирования и оценки соответствия в области использования криптографии, применение цифровой подписи в России при организации документооборота, нормативные акты органов исполнительной власти, уполномоченных в области использования криптографии в России.

История криптографии: исторические шифры от древнего мира до компьютерной эры, криптография российских царей, шифры Второй мировой войны, советская криптография.

Теория вычислительной сложности в криптографии: сложность алгоритмов, асимптотические оценки сложности, основные сложностные классы алгоритмов, неразрешимые задачи, труднорешаемые задачи, машины Тьюринга, классы P и NP, NP-полные задачи, NP-полнота задачи выполнимости, генерическая сложность, генерическая разрешимость, генерическая разрешимость задачи останова МТ, абсолютно неразрешимые задачи, генерическая сложность дискретного логарифмирования.

Криптографические методы защиты информации: дискретная информация, проблемы и методы

её защиты, шифры, симметричные и асимметричные шифры, схемы цифровой подписи, хэш-функции, криптографические стандарты, теория секретности Шеннона, шифры, не распространяющие искажений, стойкость шифров с открытым ключом, стойкость хэш-функций, общие схемы разделения секрета.

Криптографические методы аутентификации: основные понятия теории аутентификации, аутентификация на основе криптографических хэш-функций, коды аутентификации на основе шифров, криптосистемы, сочетающие аутентификацию и шифрование, теория имитостойкости Симмонса, характеризация кодов аутентификации ортогональными массивами, криптоанализ кодов аутентификации, оценки стойкости кодов аутентификации.

Криптографические протоколы: протоколы идентификации, распределения ключей, SSH, SSL, атаки на протоколы, доказательства с нулевым разглашением.

Алгебраическая криптография: представления и характеры представлений групп, их приложения в криптографии, метод линейного разложения в алгебре, его применение в криптоанализе алгебраических протоколов распределения криптографических ключей, применение метода линейного разложения в криптоанализе алгебраических шифров с открытым ключом.

Квантовая криптография: квантовые вычисления, квантовое распределение криптографических ключей, квантовое бросание монеты, квантовые битовые обязательства, квантовая рассеянная передача, квантовая факторизация целых чисел, квантовое дискретное логарифмирование, квантовое безопасное совместное вычисление и т.п.

Постквантовая криптография: криптография, основанная на хэш-функциях, криптография на кодах, исправляющих ошибки, криптография, основанная на решётках, криптография на основе многопеременных систем квадратных уравнений, криптография на основе обратимых векторных булевых функций.

Криптография с функциональными ключами: обратимые системы булевых функций ограниченной сложности, симметричные блочные шифры с функциональными ключами, криптогенераторы с функциональными ключами, поточные шифры с функциональными ключами и водяными знаками, криптосистемы с открытыми функциональными ключами, криптоанализ шифров с функциональными ключами.

Методы криптоанализа: криптосистемы, угрозы, атаки, частотные методы криптоанализа симметричных шифров, алгебраические методы криптоанализа симметричных шифров, дифференциальный криптоанализ, криптоанализ на основе статистических аналогов, атаки на кратные блочные симметричные шифры, атаки на шифры с открытым ключом.

Специальные криптоалгоритмы: неотрицаемая цифровая подпись, цифровая подпись с назначенным подтверждающим, вычисление с шифрованными данными, честное бросание монеты по сети, сетевой покер, одностороннее аккумулирование, раскрытие секретов по правилу «всё-или-ничего», честные и надёжные криптоалгоритмы, доказательства с нулевым разглашением, рассеянная передача, безопасное коллективное вычисление, сублиминальный канал, битовые обязательства, криптоалгоритм с множественным ключом, разделение секрета.

Современные криптопротоколы: фрэймворк Noise, фрэймворк Strobe, протокол Wireguard, протокол X3DH, механизмы защищённой групповой передачи (DHT, ART, TESLA), протоколы аттестации.

Методы доказательства стойкости криптосистем: понятие формально доказуемой стойкости и её свойства, доказуемая стойкость криптосистем с открытым ключом, доказуемая стойкость схем цифровой подписи, доказуемая стойкость криптографических протоколов аутентификации.

Криптографическая защита компьютерных систем: криптографические методы защиты баз данных, СУБД, операционных систем, компьютерных сетей, веб-приложений, почтовых систем, их программные средства (PEM, S/MIME, PGP, Ipsec, криптопровайдеры).

Теория псевдослучайных криптографических генераторов: тесты случайности, генераторы ПСП, псевдослучайность и непредсказуемость, автоматные и регистровые генераторы ПСП, линейные рекуррентные последовательности, нормальные рекуррентные последовательности, логические уравнения генераторов ПСП, криптанализ генераторов ПСП.

Теоретико-числовые методы в криптографии: алгоритмы над большими числами, алгоритмы над полиномами, тесты на простоту и способы генерации простых чисел, алгоритмы факторизации чисел, алгоритмы дискретного логарифмирования.

Булевы функции в криптографии: корреляционная иммунность, нелинейность, бент-функции, функции с линейной структурой, совершенная нелинейность, лавинные характеристики, алгебраическая иммунность, запреты булевых функций..

Конечные автоматы в криптографии: криптоавтоматы, конечно-автоматные симметричные шифрсистемы, обратимость конечных автоматов, конечно-автоматные криптосистемы с открытым ключом.

Эллиптические кривые в криптографии: группа точек эллиптической кривой, вычисления в ней, криптографические системы (шифры, ЦП, протоколы) на эллиптических кривых.

Криптографическое обеспечение компьютерных систем ИБ: угрозы информационной безопасности, архитектура компьютерной системы информационной безопасности (КСИБ), криптографическая защита в КСИБ электронного документооборота, электронного голосования, электронной коммерции, электронной почты, облачных вычислений, криптографическое расширение системы безопасности Java.

Криптографическое обеспечение цифровой экономики: анонимные цифровые деньги, электронное голосование, одновременное подписание контракта, цифровая сертифицированная почта, групповые подписи, слепая подпись.

Аппаратная реализация криптоалгоритмов: схемы из функциональных элементов, схемы из программируемых логических матриц, языки аппаратного представления алгоритмов, системы автоматизированного проектирования, моделирование аппаратных реализаций криптоалгоритмов.

Криптография блокчейнов и криптовалют: функции хэширования блокчейнов, схемы цифровой подписи блокчейнов, протоколы битовых обязательств, протоколы с нулевым разглашением знания, криптографические генераторы блокчейнов, криптоанализ блокчейнов, криптовалюта на блокчейнах.

Доверенное программно-аппаратное обеспечение криптографии: понятие доверенного программно-аппаратного обеспечения компьютерных систем (ПАО КС), ЛЯПАС-Т как язык для представления криптоалгоритмов и протоколов в доверенных ПАО КС, доверенный компилятор ЛЯПАСа-Т, доверенная ОС ЛЯПАСа-Т, доверенный процессор ЛЯПАСа-Т, доверенные библиотеки прикладных программ на ЛЯПАСе-Т, криптографические методы обеспечения доверенности вычислений в ОС ЛЯПАС-Т.

Работа выполнена при финансовой поддержке РФФИ, проект № 17-01-000354.

Литература

1. Агибалов Г.П. 50 лет криптографии в Томском государственном университете // Прикладная дискретная математика. – 2009. – № 2 (4). – С. 104–126.

2. Яворски Д. Система безопасности Java: Руководство разработчика / Д. Яворски, П.Дж. Перроун. – М.: Вильямс, 2001. – 528 с.

3. Stinson D.R. Cryptography: Theory and Practice. – CRC Press, 1995. – 434 p.

4. Schneier B. Applied cryptography: Protocols, Algorithms, and Source Code in C. – John Wiley and Sons, 1996. – 758 p.

5. Мао В. Современная криптография: Теория и практика. – М.: Вильямс, 2005. – 768 с.

6. Смарт М. Криптография. – М.: Техносфера, 2005. – 528 с.

7. Агибалов Г.П. SIBCiphers – симметричные итеративные блочные шифры из булевых функций с ключевыми аргументами // Прикладная дискретная математика. Приложение. – 2014. – № 7. – С. 43–48.

8. Agibalov G.P. Watermarking ciphers // Прикладная дискретная математика. – 2016. – № 1(31). – С. 62–66.

9. Агибалов Г.П. О двухкаскадных конечно-автоматных криптографических генераторах и методах их криптоанализа / Г.П. Агибалов, И.А. Панкратова // Прикладная дискретная математика. – 2017. – № 35. – С. 38–47.

10. Агибалов Г.П. Криптоавтоматы с функциональными ключами // Прикладная дискретная математика. – 2017. – № 36. – С. 59–72.

11. Agibalov G.P. Substitution block ciphers with functional keys // Прикладная дискретная математика. – 2017. – № 38. – С. 57–65.

12. Панкратова И.А. Об обратимости векторных булевых функций // Прикладная дискретная математика. Приложение. – 2015. – № 8. – С. 35–37.

13. Pankratova I.A. Construction of invertible vectorial Boolean functions with coordinates depending on given number of variables // Матер. Междунар. науч. конгресса по информатике: Информационные системы и технологии. Республика Беларусь, Минск, 24–27 окт. 2016. – Минск: БГУ, 2016. – С. 519–521.

14. Карпова Л.А. Свойства координатных функций одного класса подстановок на F_2^n / Л.А. Карпова, И.А. Панкратова // Прикладная дискретная математика. Приложение. – 2017. – № 10. – С. 38–40.

15. Агибалов Г.П. О криптографическом расширении и его реализации для русского языка программирования / Г.П. Агибалов, И.А. Панкратова, В.Б. Липский // Прикладная дискретная математика. – 2013. – № 3 (21). – С. 93–104.

16. Сафонов В.О. Комплексы в ЛЯПАСе / В.О. Сафонов, Д.А. Стефанцов // Прикладная дискретная математика. – 2017. – № 38. – С. 101–109.

Агибалов Геннадий Петрович
Д-р техн. наук, профессор каф. защиты информации и криптографии Томского государственного ун-та (ТГУ)
Ленина пр., д. 36, г. Томск, Россия, 634050
Тел.: +7 (382-2) 41-28-93
Эл. почта: agibalov@isc.tsu.ru

Agibalov G.P.

About cryptography in information security (on the example of TSU)

Here is an information about some attainments of Tomsk State University information security and cryptography department for the last ten years in the synthesis and analysis of cryptosystems with the functional keys, in creating the trusted hard- and software for cryptography, and in teaching computer cryptography to students.

Keywords: cryptography, cryptanalysis, functional keys, trusted hard- and software for cryptography, computer cryptography, teaching cryptography.