БИЗНЕС-ИНФОРМАТИКА

УДК 519.7

О НЕКОТОРЫХ НАПРАВЛЕНИЯХ НАУЧНЫХ ИССЛЕДОВАНИЙ В ОБЛАСТИ КРИПТОАНАЛИЗА СИММЕТРИЧНЫХ АЛГОРИТМОВ[1]

А.И. Пестунов, А.А. Перов, Т.М. Пестунова
Новосибирский государственный университет
экономики и управления «НИНХ»
E-mail: pestunov@gmail.com

Представлен обзор некоторых направлений научных исследований в области криптоанализа симметричных алгоритмов. В частности, выделены задачи, связанные с поиском слабых ключей, со статистическим анализом криптоалгоритмов, с анализом итеративных конструкций. Рассмотрены задачи, являющиеся специфическими для поточных шифров, криптографических хеш-функций и итеративных блочных шифров. Обоснована практическая значимость ведения научных исследований в области криптоанализа симметричных алгоритмов и описаны основные принципы этих исследований.

Ключевые слова: блочный шифр, хеш-функция, поточный шифр, криптоанализ, симметричная криптография.

ON SOME SCIENTIFIC PROBLEMS IN CRYPTANALYSIS OF SYMMETRIC ALGORITHMS

A.I. Pestunov, A.A. Perov, T.M. Pestunova
Novosibirsk State University of Economics and Managemen
E-mail: pestunov@gmail.com

A survey of some important scientific directions in the sphere of symmetric cryptography is presented. We emphasize problems connected with weak keys, with statistical analysis of symmetric algorithms and with investigation of iterative constructions. Some problems, specific to stream ciphers, iterative block ciphers and cryptographic hash-functions are considered. We also advocate practical significance of scientific work in cryptanalysis and sketch its basic principles.

Keywords: block cipher, hash-function, stream cipher, cryptanalysis, symmetric cryptography.

Стратегической целью криптографии на протяжении многих веков неизменно остается создание стойкого и удобного шифра, но нельзя утверждать, что она в полной мере достигнута. Если говорить про удобство, то проблема заключается в том, что принципы создания шифров и требования

[1] Работа поддержана грантом РФФИ №14-01-31484 (мол_а).

к ним существенным образом зависят от состояния технологий на момент их разработки. С одной стороны, шифры должны обеспечивать приемлемую производительность на различных программных и аппаратных архитектурах, накладывающих свои ограничения, а с другой – противостоять угрозам со стороны злоумышленников, которые могут обладать передовыми вычислительными технологиями. Например, современным трендом в криптографии является разработка алгоритмов защиты информации для «интернета вещей» (internet of things), состоящего из легковесных (малоресурсных) устройств, таких как смартфоны, планшеты, микроконтроллеры, смарт-карты и т.д. Дополнительные сложности возникают в силу того, что в современных условиях все больше бизнес-процессов из реальной жизни переносятся в виртуальную сетевую среду, приводя к тому, что сегодня криптография призвана решать не только проблему конфиденциальности, но и создавать такие протоколы, как платежные системы, криптовалюты, системы электронного голосования, сетевые игры и пр. Создать же некий универсальный криптоалгоритм, удовлетворяющий одновременно множеству требований, пока не удается.

Основная проблема, связанная с достижением стойкости, заключается в том, что к настоящему моменту не создан применимый на практике шифр или криптоалгоритм, для которого можно было бы строго доказать невозможность его «взлома». В частности, известный шифр Вернама, для которого получено строгое математическое доказательство его абсолютной стойкости [11], использовать на практике проблематично из-за невозможности удовлетворить требования к секретному ключу в подавляющем большинстве случаев. По этой причине на практике применяют криптоалгоритмы, для которых имеются некоторые оценки стойкости, но отсутствуют строгие математические доказательства. Для них существует угроза того, что рано или поздно они окажутся успешно атакованы. Тем не менее опубликованные уязвимости довольно редко представляют собой реализуемые на практике угрозы, зачастую являясь недостатками, которые могут привести к реальной опасности лишь в будущем. Здесь можно провести аналогию с совершенствованием дверных замков: люди пользуются ими для защиты своего имущества, не имея абсолютной гарантии их надежности даже при наличии новейших моделей.

В условиях невозможности получения доказательств стойкости основным способом ее оценки является криптоанализ – разработка атак на криптоалгоритмы и поиск их уязвимостей. В настоящей статье представлен обзор основных направлений научных исследований в области криптоанализа симметричных алгоритмов, основными из которых являются поточные шифры, криптографические хеш-функции и итеративные блочные шифры. Хотя здесь следует заметить, что появление новых прорывных технологий может как открыть другие направления исследований, так и сделать неактуальными какие-то из существующих. Так, например, многие из рассматриваемых в настоящей статье задач не имели бы смысла, если бы не был изобретен персональный компьютер. В то же время возможность создания полноценного квантового компьютера привела к тому, что уже сейчас, можно сказать заблаговременно, разрабатываются новые криптосистемы в предположении его наличия.

СТОЙКОСТЬ ШИФРОВ ПРОТИВ ПОЛНОГО ПЕРЕБОРА КЛЮЧЕЙ И ВЫБОР ДЛИНЫ КЛЮЧА

Абсолютная стойкость упомянутого во введении шифра Вернама базируется на том, что его секретный ключ должен быть истинно случайным и иметь длину, равную длине сообщения. Оба требования, очевидно, трудно осуществимы на практике. Например, при передаче видеофайла высокого разрешения, скажем, размера 10–20 Гб, собеседники должны предварительно обменяться ключом такой же длины. Более того, получить истинно случайные числа невозможно (это исключительно теоретическая модель), а приборы, генерирующие подобие таких чисел (скажем, установки для определения координат частиц при хаотическом движении), дороги, медленны и труднодоступны.

Проблема длинного истинно случайного ключа в современной криптографии решается посредством использования ключа фиксированной длины (в настоящее время обычно составляющей от 64 до 256 бит, или от 8 до 32 символов), которая в условиях современного состояния вычислительной техники призвана гарантировать стойкость против полного перебора ключей. В 2005 г. считалось, что условная граница между «короткими» ключами и ключами «достаточной длины» лежит в районе 80 бит (10 символов) [5], хотя, естественно, ее можно считать лишь грубым ориентиром в силу того, что возможности злоумышленника, а также его мотивация и время действия ключа могут существенно варьироваться. Например, ключи, которые предполагается регулярно обновлять, могут быть короткими, а ключи для длительного использования должны быть длиннее. Со сводкой рекомендаций по выбору длины ключа, представленными различными организациями и специалистами, можно ознакомиться на сайте [36].

Длины ключей некоторых известных шифров

Название шифра	Длина ключа		Количество всех возможных ключей
	в битах	в символах (байтах)	
Шифр Цезаря (русский алфавит)	5	0,625	32
DES	56	7	10^{16}
Skipjack	80	10	10^{24}
AES (мин.), CAMELLIA (мин.)	128	16	10^{38}
3DES	168	21	10^{51}
AES (макс.), CAMELLIA (макс.), ГОСТ 28147–89, ГОСТ Р 34.12–2015	256	32	10^{77}

В таблице приведены длины ключей для шифров, качественно различающихся по уровню стойкости. Среди рассмотренных примеров слабый исторический шифр Цезаря, устаревающий из-за короткого ключа DES, обновленный и прежний российские стандарты, стандарт США шифр AES, шифр 3DES (модернизированный DES), японский шифр Camellia и шифр Skipjack. Современные шифры имеют длину ключа от 128 до 256 бит, шифр Цезаря сильно отстает, а устаревающий DES не дотягивает до условного порога стойкости в 80 бит.

Наличие у шифра ключа достаточной длины не гарантирует его стойкости. Более того, на данный момент неизвестно шифров, для которых доказано отсутствие атак быстрее полного перебора ключей. Следовательно, важной стратегической проблемой в области криптографии является разработка шифра, для которого можно было бы доказать отсутствие атак быстрее полного перебора ключей. Это даст возможность обеспечить требуемый уровень стойкости шифра одним только выбором подходящей длины ключа. Проблема создания шифра, для которого можно было бы доказать отсутствие атак быстрее полного перебора, на сегодняшний день не решена, поэтому предпринимаются попытки создания шифров, для которых можно было бы доказать отсутствие атак хотя бы одного определенного типа. В связи с этим актуальной является проблема создания методов построения атак, которые потенциально может использовать злоумышленник.

Следует также отметить, что к настоящему моменту довольно мало работ теоретического характера по криптоанализу, а подавляющее большинство атак носят частный характер и применимы только к конкретному шифру, не предоставляя возможности явного обобщения на другие шифры, даже близкие по классу [3]. Отсюда вытекает необходимость теоретических обобщений и математических обоснований тех или иных положений криптоанализа.

Задача 1. Разработка применимого на практике шифра с фиксированной длиной ключа, для которого можно строго математически доказать отсутствие атак, работающих быстрее полного перебора ключей.

Задача 2. Разработка методов построения атак на криптоалгоритмы и поиск уязвимостей этих криптоалгоритмов.

Задача 3. Создание криптоалгоритма, для которого можно строго математически доказать невозможность проведения атаки определенным методом.

Задача 4. Разработка и теоретическое обоснование отдельных положений, связанных с разработкой атак на криптоалгоритмы.

РАЗРАБОТКА АТАК НА ШИФРЫ КАК ОСНОВНОЙ ПОДХОД К ОЦЕНКЕ ИХ СТОЙКОСТИ

Как было отмечено выше, наличие ключа достаточной длины не гарантирует стойкости шифра из-за его внутренних уязвимостей, которые можно использовать для разработки атаки, опирающейся именно на них. В то же время пока не созданы применимые на практике шифры, для которых доказано отсутствие таких внутренних уязвимостей, и, следовательно, существует угроза появления атак, сложность которых ниже, чем у полного перебора ключей. В этих условиях основным подходом к оценке стойкости шифров являются попытки разработки атак на них. Упрощенно говоря, шифр считается стойким, пока против него неизвестно ни одной атаки, работающей эффективнее метода полного перебора ключей. Для шифров с большой длиной ключа, например, 256 бит, даже наличие атак, работающих быстрее полного перебора, не представляет никакой реальной угрозы, если их сложность лишь незначительно ниже, скажем 2^{250}. Тем не менее

подобные результаты называют сертификационными недостатками шифра, поскольку его стойкость ниже, чем заявленная, определяемая длиной ключа [5].

Учитывая изложенные выше соображения, перед публикацией и внедрением в практическое использование нового шифра разработчики сами применяют известные методы криптоанализа, как бы пробуя свой шифр на прочность. Если шифр оказывается уязвим к какой-либо атаке, он должен быть либо доработан, либо заменен другим. Таким образом, важным направлением исследований является разработка атак, которые работают быстрее метода полного перебора ключей. Основным показателем эффективности атаки является ее сложность (трудоемкость). В зависимости от криптоалгоритма и типа атаки сложность может определяться следующими основными показателями:

– количеством пробных расшифрований/зашифрований;

– объемом требуемой для реализации атаки памяти компьютера;

– количеством требуемых открытых/шифрованных текстов (блоков, сообщений);

– вероятностью успеха атаки;

– сценарием, в котором реализуется атака.

Сложность полного перебора определяется длиной (обозначим ее через n) секретного ключа и составляет 2^n. Причем если на некоторый шифр неизвестно атак вообще, то научный интерес представляют атаки, которые имеют сложность немногим менее сложности полного перебора. Например, на российский шифр ГОСТ 28147–89[2] со 256-битовым секретным ключом долгое время не было известно атак быстрее полного перебора, но в публикации [24] представлена атака со сложностью 2^{225}, что, конечно, не несет никакой практической угрозы его пользователям, но представляет научный интерес, и эта атака опубликована в одном из самых престижных журналов по криптографии – Journal of Cryptology.

Атаки на шифры разрабатываются по принципу соревнования: новые атаки должны быть эффективнее ранее известных по общепринятым показателям. Именно такие, более эффективные атаки представляют научный интерес. Атаки, которые не являются более эффективными ранее известных, могут представлять научный интерес только в очень редких случаях. Следует отметить, что подавляющее большинство существующих атак на шифры имеют недостижимую на практике сложность, в силу чего не угрожают пользователям этих шифров; отсюда вытекает, что дополнительной актуальной задачей является разработка атак, которые можно было бы реализовать на практике, и, если это удается сделать, то авторы как правило это особо подчеркивают, говоря об этом в названии статьи и указывая время работы атаки. Так, в статье [20] отмечается, что время работы разработанной атаки на шифр KASUMI на одноядерном персональном компьютере составляет менее двух часов. В статье [15] описывается атака на легковесный блочный шифр Keeloq, которая, по расчетам авторов, требует 7,8 дней работы 64-ядерного компьютера. Авторы также приводят рас-

[2] Действовал в качестве официального стандарта до 01.01.2016 г. Ныне заменен на ГОСТ Р 34.12–2015.

четы по созданию устройства стоимостью 10 000 евро, которое вычислит секретный ключ за два дня. Еще одна атака демонстрирует, что некоторые плохо изученные шифры могут быть «взломаны» вскоре после их публикации. Так, блочный шифр Nimbus, заявленный на конкурс NESSIE, подвергся анализу, в результате которого была разработана атака, требующая 136 выбранных открытых текстов и, в худшем случае, 1024 пробных шифрований [22], что, очевидно, займет менее секунды на современном компьютере. Примером эффективной атаки являются атаки на поточные шифры семейства F-FCSR, отрабатывающие на персональном компьютере менее, чем за секунду [23].

Помимо сложности атаки ее эффективность определяется сценарием, в котором она реализуется. Сценарий атаки – это совокупность предположений относительно возможностей злоумышленника; сценарии могут быть более сильными и более слабыми. Атаки, которые реализуются в более слабом сценарии, более ценны для криптоаналитика и говорят о большей слабости шифра. Самый слабый сценарий – это атака по известному шифрованному тексту, предполагающий, что криптоаналитик имеет доступ только к шифрованному тексту. Атака по известному открытому тексту подразумевает, что имеется доступ не только к шифрованному, но и соответствующему ему открытому тексту (или его частям). При реализации атаки по выбранному открытому/шифрованному тексту на вход/выход шифра можно подавать любые сообщения по своему усмотрению. Наконец, атака на связанные ключи подразумевает, что имеется информация о некотором соотношении между несколькими ключами, и цель – найти их.

Сценарии различаются по возможности их осуществления на практике, однако все они так или иначе базируются на разумных соображениях. Сценарий по известному шифрованному тексту самый слабый: для его реализации злоумышленнику достаточно прослушивать канал передачи информации, что, например, при использовании беспроводного сетевого соединения сделать очень легко. Сценарий по известному открытому тексту может быть реализован, если для части передаваемых (или хранящихся) данных злоумышленнику удалось перехватить соответствующие им открытые данные (это может случиться, например, в случае неосторожности пользователей); и далее, если злоумышленник вычислит секретный ключ шифрования, то он сможет расшифровать и остальные зашифрованные данные.

Сценарий по выбранному открытому/шифрованному тексту был отчасти реализован во времена второй мировой войны [11]. Утверждается, что американские военные, подкупив немецкую охрану, получили возможность проведения экспериментов с немецкой шифровальной машинкой «Энигма» с целью определения секретного ключа, задающего положение шифровальных дисков внутри нее. Вскрывать машинку физически было нецелесообразно, поскольку немецкие шифровальщики впоследствии заметили бы это и обновили ключ, что сделало бы всю операцию бесполезной. В итоге американцы могли подавать на вход (шифровать) или на выход (расшифровывать) любые сообщения по своему усмотрению для получения ключа, и после возврата «Энигмы» использовать его для расшифрования дальнейшей вражеской переписки.

Сценарий атаки на связанные ключи также не является искусственной выдумкой, хотя злоумышленнику реализовать его сложнее предыдущих, а пользователям, соответственно, легче от него защититься. Атака на связанные ключи может быть проведена, если пользователи при регулярном обновлении паролей генерируют их не случайно, а используют некую закономерность, облегчающую их создание. Если злоумышленник узнает это правило, то ему станет легче найти эти пароли. Однако, выбирая случайные пароли при обновлении, пользователи легко могут защититься от этой атаки. И все-таки специалисты по криптоанализу периодически напоминают (особенно при публикации атак в более привычных сценариях), что атака на связанные ключи достаточно сложна в реализации [8, 21]. При этом научный интерес имеет задача конвертации атаки из более сильного в более слабый сценарий. Например, в статье [20] рассматривается возможность конвертации атаки по выбранному открытому тексту в атаку по известному открытому тексту и в атаку по известному шифрованному тексту.

Задача 5. Разработать атаку на криптоалгоритм и оценить ее сложность и вероятность успеха (для статистических атак).

Задача 6. Разработать атаку на криптоалгоритм, сложность которой была бы меньше (хотя бы по одному из общепринятых показателей), чем у ранее известных атак на этот криптоалгоритм.

Задача 7. Разработать атаку на криптоалгоритм, которая не просто имела бы сложность меньше, чем у ранее известных, но и допускала бы эффективную практическую реализацию.

Задача 8. Разработать атаку на криптографический алгоритм в более слабом сценарии, чем существующие атаки.

СТАТИСТИЧЕСКИЙ АНАЛИЗ КРИПТОГРАФИЧЕСКИХ АЛГОРИТМОВ

Одним из видов атак на криптоалгоритмы является атака-различитель (distinguishing attack), которая заключается в том, чтобы разработать новый или найти существующий статистический критерий, проверяющий гипотезу о равномерности распределения шифрованного текста (против ее альтернативы). Эта универсальная атака относится ко всем симметричным криптоалгоритмам. В идеале шифр должен преобразовывать информацию так, чтобы шифрованный текст выглядел, как случайный, однако современные шифры являются детерминированными алгоритмами, не способными генерировать истинно случайные последовательности, поэтому теоретически для любого шифра эту «неслучайность» можно обнаружить. Соответственно, важным требованием к шифру является неотличимость шифрованного текста от случайной последовательности никакими известными тестами, методами, критериями. Если шифрованный текст удается отличить от равномерно распределенных случайных чисел, то это является интересным научным результатом и указывает на недостаток шифра. Более того, подобный недостаток может быть использован для определения секретного ключа [9, 16].

Криптоалгоритмы в неурезанном виде (без каких-либо упрощений) обладают достаточно хорошими свойствами (как статистическими, так и в плане стойкости), и отличить шифрованный текст от случайного за реаль-

ное время на реальных выборках невозможно, если только не использовать шифры в режиме электронной кодовой книги (Electronic Code Book, ECB), который частично сохраняет избыточность открытого текста, и построить атаку-различитель становится возможным даже не за счет уязвимостей шифра, а за счет избыточности языка. Например, в статье [10] удалось найти отклонения от случайности у «серьезных» шифров RC6 и AES именно в этом режиме. Хотя бывают случаи, что «бракуются» новые криптоалгоритмы, например, поточный шифр ZK-CRYPT, заявленный на конкурс eStream [4].

Задача 9. Разработка новых и исследование существующих универсальных статистических тестов и критериев для проверки последовательностей на соответствие равномерному распределению.

Задача 10. Построение специализированных тестов для конкретных криптоалгоритмов, а также подбор параметров универсальных тестов для их применения к конкретному криптоалгоритму.

Задача 11. Построение атак-различителей для урезанных версий шифров.

РАЗРАБОТКА АТАК НА ИТЕРАТИВНЫЕ КРИПТОАЛГОРИТМЫ

Современные блочные шифры и криптографические хеш-функции являются итеративными, т.е. они представляют собой композицию простых преобразований, называемых раундами или циклами. В среднем число раундов итеративных криптоалгоритмов составляет от 10 до 30, хотя имеются и исключения, состоящие из меньшего или значительно большего числа раундов. Например, легковесные шифры KATAN и KTANTAN состоят из более чем 100 раундов. Понятие раунда довольно условно, поскольку он либо может быть разбит на несколько подраундов (например, у шифров RC5 или RC6), либо, наоборот, несколько раундов могут быть сгруппированы (у шифра CAST-256 48 раундов объединены в 12 четверок).

Большая часть современных шифров (даже тех, которые не играют важной роли в реальных приложениях) достаточно стойкие, и разработка атак на полноценные неурезанные версии этих шифров, как правило, невозможна, поэтому научный интерес представляют атаки на шифры с сокращенным числом раундов. К этому призывают, в частности, известные специалисты Б. Шнайер и Н. Фергюсон [12], и по этому пути идут современные исследования [16, 30].

Проблема статистического анализа, рассмотренная выше, применительно к итеративным алгоритмам может быть расширена. При статистическом тестировании важным показателем является размер выборки (N), на котором фиксируются отклонения от случайности, причем обычно этот размер увеличивается с увеличением числа раундов шифра (r), приводя к функциональной зависимости $N(r)$. Используя методы экстраполяции, в ряде случаев оказывается возможным спрогнозировать размер выборки на большее число раундов, когда эксперименты становятся невозможными из-за вычислительной невозможности обработать большую выборку. Пример решения задачи такого рода приведен в статьях [7, 28], где строится прогноз для шифров RC6, FROG и LOKI97, кандидатов конкурса AES.

Чаще всего итеративные криптографические алгоритмы состоят из одинаковых раундов, повторяющихся фиксированное число раз, однако у некоторых криптоалгоритмов раунды не просто могут различаться, но и быть неравноценными по криптографическим свойствам. Например, блочный шифр MARS состоит из 32 раундов, 16 из которых не используют ключи и являются исключительно перемешивающими преобразованиями. Их криптографическая ценность значительно ниже, чем у оставшихся 16 раундов, снабжаемых ключами, поэтому при сравнении атак на MARS следует учитывать не только число раундов у атакуемой версии шифра, но и их качество. Более того, в данном шифре присутствуют так называемые отбеливания (сложения/вычитания с ключами), которые хотя и не являются полноценными раундами шифрования, но существенно затрудняют проведение некоторых атак. По этим причинам в статье [6] при сравнении результативности атак учитывается не число атакованных раундов, а число вычисленных бит расширенного ключа у соответствующих атакам версий шифра.

Задача 12. Разработать атаку на такую урезанную версию шифра, которая состоит из большего числа раундов, чем атакованные ранее.

Задача 13. Найти статистические недостатки у урезанной версии шифра и построить экстраполяцию длины выборки, при которой можно найти статистические недостатки при большем числе раундов.

Задача 14. Разработать новую атаку на некоторую урезанную версию шифра, которая была атакована ранее, но атака имела большую сложность, чем новая.

Задача 15. Разработать атаку, направленную на такую урезанную версию итеративного криптоалгоритма, которая использует больше ключевого материала, чем атакованные ранее версии.

ПОИСК СЛАБЫХ КЛЮЧЕЙ КРИПТОГРАФИЧЕСКИХ АЛГОРИТМОВ

В общем случае при разработке атак на криптографические алгоритмы предполагается, что пользователь выбирает секретный ключ произвольно и, следовательно, атаки должны работать для всех ключей. Тем не менее для некоторых шифров оказывается возможным выделить часть ключей, называемых слабыми ключами, при использовании которых стойкость шифра существенно снижается. Это дает возможность разработать атаку, эффективность которой окажется выше, чем у атак, подразумевающих использование произвольного ключа.

Рассмотрим несколько примеров подобных исследований. В статье [29] представлена дифференциальная атака в сценарии связанных ключей на шифр MISTY1 с полным числом раундов (равным 8), которая требует $2^{90.93}$ операций шифрования и работает для $2^{103.57}$ слабых ключей, что составляет $2^{-24.43}$ часть всех 128-битовых ключей. В статье [27] предложены четыре атаки (также дифференциальных в сценарии связанных ключей) на 8 из 20 раундов шифра SEED со 192-битовым ключом; размер класса слабых ключей варьируется от 2^{119} до 2^{123}, что составляет от 2^{-73} до 2^{-69} части всех ключей.

Отметим атаки на оригинальные шифры WIDEA-4 и WIDEA-8, представляющие собой соответственно комбинацию 4 и 8 шифров IDEA со

128-битовым ключом; длина ключа WIDEA-4 равна 512 бит, а WIDEA-8 – 1024 бита. В работе [33] предложен ряд атак на эти шифры, у которых размеры классов слабых ключей варьируются от 2^{242} до 2^{272} для WIDEA-4 и от 2^{754} до 2^{784} для WIDEA-8.

Размер класса слабых ключей не всегда может быть вычислен точно; так, в статье [8] дается нижняя оценка мощности класса слабых ключей шифрсистемы PRINT в виде функции от различных параметров.

После публикации атак на шифр в предположении использования слабых ключей по-прежнему актуальной остается задача разработки атак, не накладывающих никаких ограничений на используемый ключ. Так, в статье [5] опубликована атака на 24 раунда шифра CAST-256 без предположения о слабых ключах, в то время как ранее 24 раунда можно было «взломать» только для слабых ключей, количество которых составляет 2^{-36} от всех ключей.

Алгоритмы проверки ключа на принадлежность классам слабых, как и любые другие алгоритмы, имеют сложность, следовательно, научный интерес представляет разработка новых алгоритмов, которые бы снижали ее (в каком-либо общепринятом смысле). Например, в статье [25] представлены атаки на известный блочный шифр Blowfish в предположении использования слабых ключей по отношению к атаке «отражения» (reflectively weak keys) и метод проверки ключа на слабость, требующий 2^{34} известных открытых текстов с соответствующими им парами шифртекстов.

Поскольку размер класса слабых ключей является его важной характеристикой, то, с точки зрения криптоаналитика, научный интерес представляет расширение этого класса. Так, в статье [18] для блочного шифра IDEA описаны классы слабых ключей, наибольший из которых имеет размер 2^{64}, тогда как ранее были описаны классы размеров 2^{51} и 2^{63}.

Подытоживая приведенные выше рассуждения, можно выделить следующие проблемы, которые представляют научный интерес в контексте поиска слабых ключей.

Задача 16. Разработать атаку на криптоалгоритм, которая была бы эффективнее существующих, пусть и в предположении использования только некоторой части ключей (называемых слабыми), определяемых каким-либо условием.

Задача 17. Разработать алгоритм, проверяющий, является ли ключ слабым; повысить эффективность известных алгоритмов проверки слабости ключа.

Задача 18. Описать класс слабых ключей и оценить или вычислить его размер.

Задача 19. Найти класс слабых ключей, размер которого больше, чем у ранее известных.

НАПРАВЛЕНИЯ ИССЛЕДОВАНИЙ В ОБЛАСТИ ПОТОЧНЫХ ШИФРОВ

Поточные шифры – это модификация шифра Вернама, где вместо длинного истинно случайного ключа используется псевдослучайная последовательность (ключевой поток), сгенерированная детерминированным алгоритмом (называемым генератором ключевого потока), принимающим

на вход короткий секретный ключ. Обычно поточные шифры состоят из следующих трех этапов: формирование внутреннего состояния (internal state) в зависимости от секретного ключа; генерация очередного псевдослучайного числа на основе внутреннего состояния; изменение внутреннего состояния.

Секретный ключ используется только для формирования исходного вида внутреннего состояния, и далее генерируемые псевдослучайные числа уже не имеют непосредственной зависимости от него. Следовательно, определение злоумышленником внутреннего состояния поточного шифра, по большому счету, эквивалентно знанию секретного ключа, поэтому определение внутреннего состояния – это один из видов атак на поточные шифры. Например, в статье [35] предлагается атака, определяющая внутреннее состояние шифра X-FCSR-256, требуя $2^{44.3}$ предварительно сгенерированных[3] блоков псевдослучайных чисел, и атака на шифр X-FCSR-128, требующая $2^{55.2}$ блоков[4].

Применительно к внутреннему состоянию поточного шифра существует особый тип слабых ключей, называемых, *конфликтующими*, которые приводят к одинаковым или в значительной степени совпадающим внутренним состояниям. Поскольку длина внутреннего состояния обычно выше, чем длина ключа, то такой ситуации быть не должно, хотя наличие конфликтующих ключей не обязательно означает возможность вычисления секретного ключа или внутреннего состояния. С подобными исследованиями шифра RC4 можно ознакомиться в статье [32].

Говоря непосредственно о качестве ключевого потока, следует отметить, что он должен удовлетворять естественным требованиям, которым удовлетворяют случайные числа:

– последовательность должна проходить известные статистические тесты и критерии;

– знание начала последовательности не должно влиять на вероятность предсказания (угадывания) последующих чисел;

– последовательность не должна иметь регулярно повторяющихся (с вероятностью большей, чем для случайных чисел) сочетаний.

Нарушение этих требований считается атакой на поточный шифр. Например, в статье [31] описаны пары символов, которые повторяются в последовательности, сгенерированной поточным шифром RC4, чаще, чем это должно происходить в истинно случайной последовательности. В этой же статье предложен алгоритм, позволяющий предсказать очередной бит последовательности с вероятностью 0,85 при наличии последовательности длины 2^{45}, в то время как для случайной последовательности предсказание бита имеет вероятность 0,5. Другой алгоритм позволяет предсказать очередной байт с вероятностью 0,82 (для случайных чисел предсказать байт можно с вероятностью менее 0,004) при наличии начала последовательности длины 2^{50}.

Существует возможность описания зависимостей между символами открытого и шифрованного текста в виде систем алгебраических уравнений

[3] В терминах злоумышленника – перехваченных блоков.

[4] Данные поточные шифры генерируют псевдослучайные числа блоками.

[1]. Символы ключа являются неизвестными, подлежащими вычислению криптоаналитиком. Примеры атак такого типа предлагаются в статьях [1, 2].

Таким образом, при исследовании поточных шифров актуальными являются следующие задачи.

Задача 20. Разработать алгоритм, который по заданной псевдослучайной последовательности сможет восстановить его внутреннее состояние или его часть.

Задача 21. По началу псевдослучайной последовательности, полученной с помощью поточного шифра, предсказать следующие элементы с вероятностью большей, чем в случае случайного угадывания.

Задача 22. Найти в генерируемом ключевом потоке сочетания символов, которые повторяются чаще, чем должны при использовании истинно случайных чисел.

Задача 23. Представление зависимостей между символами открытого и шифрованного текста в виде систем уравнений, где неизвестными являются символы ключа, и их решение.

ЗАДАЧИ В РАМКАХ ИССЛЕДОВАНИЯ КРИПТОГРАФИЧЕСКИХ ХЕШ-ФУНКЦИЙ

Традиционно криптографические хеш-функции относятся к классу симметричных алгоритмов, хотя здесь необходимо понимать, что данная классификация в полной мере относится только к ключевым хеш-функциям. Эти хеш-функции предполагают наличие общего секретного ключа у взаимодействующих сторон и предназначены для обеспечения целостности и аутентификации в доверенной среде. Бесключевые хеш-функции, строго говоря, не являются симметричными криптоалгоритмами, поскольку они не требуют секретного ключа вообще. Однако отнесение бесключевых хеш-функций к симметричным криптоалгоритмам вполне оправдано. Например, ключевые хеш-функции строятся на базе блочных шифров (CBC-MAC) [5, 13], которые являются симметричными алгоритмами, и на базе бесключевых хеш-функций (HMAC); тематика одной из ведущих конференций по симметричной криптографии Fast Software Encryption (http://fse.rub.de/) постоянно включает секции по криптографическим хеш-функциям. Более того, ключевые хеш-функции, крайне редко разрабатываются как независимые алгоритмы: обычно используются либо HMAC, либо CBC-MAC, поэтому разработка и исследование криптографических хеш-функций подразумевает главным образом работу с бесключевыми.

Практически все задачи, связанные с криптоанализом хеш-функций, вытекают из требований, предъявляемых к ним. При этом необходимо либо обеспечить удовлетворение этим требованиям, либо выявить обратное, т.е. построить атаку. Криптографическая хеш-функция, обозначим ее через $h(x)$, должна удовлетворять следующим требованиям [5, 12, 13]:

1) для любого x вычисление $h(x)$ должно осуществляться относительно быстро;

2) при известном y должно быть практически невозможно найти x, для которого $y = h(x)$;

3) при известном x должно быть практически невозможно найти $x' \neq x$ такое, что $h(x) = h(x')$;

4) должно быть практически невозможно найти пару x и x' ($x' \neq x$) такую, что $h(x) = h(x')$.

Функции, удовлетворяющие первым двум требованиям, принято называть однонаправленными или односторонними. Третье требование называют устойчивостью к коллизиям первого рода, а четвертое – к коллизиям второго рода. Коллизия – это пара аргументов хеш-функции, которые приводят к одинаковому значению функции. При проведении исследований, связанных с криптографическими хеш-функциями, следует учитывать, что в основном это итеративные алгоритмы, поэтому задачи, связанные с итеративными алгоритмами, актуальны и для хеш-функций.

Задача 24. Разработка криптографических хеш-функций, для которых можно было бы строго доказать удовлетворение всем требованиям (хотя бы некоторым).

Задача 25. Разработать алгоритм, который по значению хеш-функции находит соответствующий ему аргумент (задача обращения хеш-функции).

Задача 26. Разработать алгоритм, который по значению хеш-функции находит часть соответствующего ему аргумента (задача частичного обращения хеш-функции).

Задача 27. Разработать алгоритм нахождения коллизий или частичных коллизий (совпадения не во всех битах).

НАУЧНЫЕ ИССЛЕДОВАНИЯ В ОБЛАСТИ КРИПТОАНАЛИЗА БЛОЧНЫХ ШИФРОВ

В принципе блочные шифры могут быть различных типов, но сейчас подвергаются исследованию и используются на практике в основном итеративные блочные шифры. Кроме того, блочные шифры могут использоваться и для генерации псевдослучайных чисел, и для построения криптографических хеш-функций (как ключевых, так и нет). По этим причинам все задачи, которые рассмотрены выше применительно к итеративным алгоритмам, поточным шифрам и хеш-функциям, так или иначе актуальны для блочных шифров.

Если говорить про специфические задачи, то выделим разработку и анализ режимов функционирования блочных шифров. В настоящее время имеются режимы для генерации псевдослучайных чисел (CTR), для выработки кода аутентичности сообщения (CBC-MAC), режим поточного шифра (OFB), несколько режимов шифрования (например, ECB, CBC) и др. Поскольку все режимы имеют достоинства и недостатки, то в настоящее время продолжаются их исследование и разработка.

Не так давно предложен метод виртуальных изоморфизмов как вариант разработки атак на блочные шифры. Идея метода заключается в том, чтобы для шифра, который требуется «взломать», построить класс изоморфных шифров, найти в нем слабый шифр и атаковать его. Затем, согласно имеющемуся изоморфизму, перенести атаку на исходный шифр. Однако пока метод не получил интенсивного развития из-за отсутствия понятных

техник построения таких изоморфизмов, хотя автор и утверждает, что AES уязвим к этому методу [34].

Подобная ситуация складывается и с алгебраическим криптоанализом, предлагающим построить систему уравнений, решение которой будет эквивалентно вычислению секретного ключа шифра [19]. И, действительно, для некоторых шифров такие системы построены, например, для AES, но их решение для неурезанных версий шифров пока является задачей будущего.

Задача 28. Разработка и анализ режимов функционирования блочных шифров для решения различных задач.

Задача 29. Построение класса шифров, изоморфных данному; поиск в этом классе шифра, у которого можно найти уязвимости; и перенос этих уязвимостей на исходный шифр согласно изоморфизму.

О ЗНАЧИМОСТИ ИССЛЕДОВАНИЙ В ОБЛАСТИ КРИПТОАНАЛИЗА И ВОЗНИКНОВЕНИИ ДОВЕРИЯ К СИММЕТРИЧНЫМ КРИПТОАЛГОРИТМАМ

Несмотря на то, что пока еще не создан доказуемо стойкий и применимый на практике криптографический алгоритм, итеративные блочные шифры, криптографические хеш-функции и поточные шифры широко используются и, по большому счету, являются одними из наиболее надежных компонентов в системах защиты информации. Случаи, когда утечка критически важной информации или потеря крупных финансов происходили вследствие атаки непосредственно на криптографический алгоритм, крайне редки. По статистике наиболее результативные атаки используют ошибки в программных реализациях или человеческий фактор.

На сегодняшний день наибольшим доверием пользуются блочные шифры и криптографические хеш-функции, что проявляется в наличии государственных стандартов на них. Здесь можно упомянуть «свежие» российские стандарты ГОСТ Р.34.12–2015 (на блочный шифр) и ГОСТ Р.34.11–2012 (на хеш-функцию); их предшественников ГОСТ 28147–89 и ГОСТ Р.34.11–1994, доставшихся нам еще с советских времен; Advanced Encryption Standard (AES) – принятый в 2002 г. новый стандарт блочного шифрования США и его предшественника Data Encryption Standard (DES), активно использовавшегося с 1977 г.; нельзя оставить без внимания и новый стандарт США на криптографическую хеш-функцию SHA-3, официально принятый в 2015 г.; отметим также китайский стандарт беспроводной связи SMS4 и рекомендованный для государственного и промышленного использования в Японии блочный шифр Camellia.

Доверие к блочным шифрам и криптографическим хеш-функциям объясняется, на наш взгляд, их итеративной структурой, создающей многослойный барьер против потенциальных атак; большой запас длины ключа также добавляет уверенности в их стойкости. Дело в том, что применяемые на практике шифры находятся под пристальным вниманием ученых со всего мира, поскольку выявление новых (пусть даже незначительных) уязвимостей этих шифров считается значимым результатом, достойным публикации в ведущих научных журналах. При этом скрывать их «в столе» и не публиковать в надежде выявить существенные уязвимости, которые

можно будет использовать на практике в своих интересах, не имеет особого смысла – слишком уж низка вероятность их обнаружения. Это означает, что для ученого польза от публикации нового результата в журнале более притягательна, чем маловероятные серьезные уязвимости, за использование которых вообще можно получить уголовное наказание. Таким образом, атаки, опубликованные в последних выпусках ведущих научных журналов, можно с большой долей уверенности считать наиболее опасными уязвимостями этих шифров.

В итоге стандартизуются или рекомендуются к использованию только те шифры, которые выдержали интенсивные атаки ученых. Итеративная же структура этих криптоалгоритмов позволяет создать определенный запас прочности, что не дает возможности быстро разработать прорывную атаку на такие активно исследуемые алгоритмы. Однако с течением времени постепенно будут появляться атаки, представляющие в перспективе все большую опасность, но в силу большой длины ключа и запаса в количестве раундов этот процесс достаточно медленный. Дополнительный запас создается и благодаря тому, что передовые атаки обычно реализуются в относительно нереальных сценариях, прежде всего – это атаки на связанные ключи.

Нечто подобное произошло с российским стандартом блочного шифрования ГОСТ 28147–89, который хотя и разрабатывался за стенами спецслужб, вскоре после его публикации в книге Б. Шнайера «Прикладная криптография» в 1994 г. подвергся довольно интенсивному анализу (главным образом иностранными учеными), который тем не менее долгое время не подвергал сомнению стойкость данного шифра (сводку публикаций по этой теме можно посмотреть в статье [7]). Лишь в 2011 г. в докладе японского специалиста Т. Исобе была представлена атака на полную 32-раундовую версию этого шифра [7], причем эта атака была чисто теоретической в силу ее высокой сложности – 2^{225} операций шифрования, что лишь незначительно меньше сложности полного перебора ключей. Имеется также атака в предположении использования слабых ключей со значительно меньшей сложностью $2^{125.5}$ операций шифрования, но вероятность случайного выбора такого ключа ничтожно мала и составляет 2^{-128} [26]. Тем не менее в 2015 г. был обновлен стандарт блочного шифрования России ГОСТ Р.34.12–2015. Наверняка, причиной смены стандарта стали не только эти публикации, но в любом случае итеративная структура, запас числа раундов и длины ключа предоставили специалистам и пользователям шифра ГОСТ 28147–89 достаточное время для разработки и принятия нового стандарта без особой тревоги за стойкость старого варианта.

Эволюция американского стандарта AES, видимо, происходит по схожему сценарию, за исключением того, что он выбирался в открытом соревновании. Первые оценки стойкости данного шифра и результаты его криптоанализа были представлены в исходной статье, где предлагался этот шифр, но после принятия его в качестве стандарта интенсивность публикаций, предлагающих его всевозможные уязвимости, только возросла. И хотя реальной угрозы реализации какой-либо из опубликованных атак на практике пока нет, не исключена вероятность, что в обозримом будущем будет запущен проект по разработке нового стандарта.

ЗАКЛЮЧЕНИЕ

В настоящей статье рассмотрены направления исследований, которые условно можно отнести к теоретическим, не затрагивающим и не учитывающим особенности реализации криптоалгоритмов на конкретных устройствах. В частности, за пределами обзора остались так называемые атаки по побочным каналам, нацеленные на вычисление пользовательского ключа и получение прочей секретной информации с использованием данных о физических процессах, протекающих при работе алгоритма (side channel attack). При этом могут сниматься показания времени выполнения атомарных операций, энергопотребления, температуры и т.д. Некоторые «активные» атаки подразумевают еще и внедрение каких-либо особенностей или ошибок, влияющих на эти показатели (fault injection attack).

Некоторые из открытых проблем, рассмотренных в данной статье (прежде всего те, которые касаются создания доказуемо стойких криптоалгоримов), тесно связаны с открытыми проблемами теории чисел, теории алгоритмов, теории графов, математической статистики и многих других наук. Тем самым их решение может оказать влияние на другие науки и наоборот. Для некоторых задач даже неизвестно, могут ли они быть решены в принципе, поэтому доказав, например, принципиальную невозможность создания шифра, стойкого против полного перебора ключей, можно внести существенный вклад не только в криптографию, но и в другие науки.

Как видно из проведенного обзора, большинство актуальных конкретных задач в симметричной криптографии связаны не с защитой информации, а, наоборот, со «взломом»: определение секретного ключа, поиск коллизий, определение отклонений от случайности.

Литература

1. *Агибалов Г.П.* Логические уравнения в криптоанализе генераторов ключевого потока // Вестник Томского университета. Приложение. 2003. № 6. С. 42–49.
2. *Агибалов Г.П.* Методы решения систем полиномиальных уравнений над конечным полем // Вестник Томского университета. Приложение. 2006. № 17. С. 47–52.
3. *Агибалов Г.П.* Элементы теории дифференциального криптоанализа итеративных блочных шифров с аддитивным раундовым ключом // Прикладная дискретная математика. 2008. № 1. С. 34–42.
4. *Дорошенко С.А., Лубкин А.М., Монарев В.А. и др.* Атака на потоковые шифры RC4 и ZK-CRYPT с использованием теста «Стопка книг» // Вестник СибГУТИ. 2007. № 1. С. 31–34.
5. *Пестунов А.И.* Дифференциальный криптоанализ блочного шифра CAST-256 // Безопасность информационных технологий. 2009. № 4. С. 57–62.
6. *Пестунов А.И.* Дифференциальный криптоанализ блочного шифра MARS // Прикладная дискретная математика. 2009. № 4. С. 56–63.
7. *Пестунов А.И.* Статистический анализ современных блочных шифров // Вычислительные технологии. 2007. Т. 12. № 2. С. 122–129.
8. *Пудовкина М.А., Хоруженко Г.И.* О классах слабых ключей обобщенной шифр-системы PRINT // Математические вопросы криптографии. 2013. Т. 4. № 2. С. 113–125.
9. *Рябко Б.Я., Монарев В.А., Шокин Ю.В.* Новый тип атак на блоковые шифры // Проблемы передачи информации. 2005. Т. 41. № 4. С. 97–107.
10. *Рябко Б.Я., Стогниенко В.С., Шокин Ю.И.* Адаптивный критерий хи-квадрат для различения близких гипотез при большом числе классов и его применение к не-

которым задачам криптографии // Проблемы передачи информации. 2003. Т. 39. № 2. С. 207–215.
11. *Рябко Б.Я., Фионов А.Н.* Основы современной криптографии и стеганографии // М.: Горячая линия-Телеком, 2010. 232 с.
12. *Фергюсон Н., Шнайер Б.* Практическая криптография. М.: Издательский дом «Вильямс», 2005. 424 с.
13. *Черемушкин А.В.* Криптографические протоколы. Основные свойства и уязвимости: учеб. пособие для студ. учреждений высш. проф. образования. М.: Издательский центр «Академия», 2009. 272 с.
14. *Шеннон К.* Работы по теории информации и кибернетике. М.: Издательство иностранной литературы, 1963. 830 с.
15. *Aerts W., Biham E., Dunkelman O. et al.* A practical attack on KeeLoq // Journal of Cryptology. 2012. Vol. 25. P. 136–157.
16. *Biham E., Dunkelman O., Keller N., Shamir A.* New attacks on IDEA with at least 6 rounds // Journal of Cryptology. 2015. Vol. 28. P. 209–239.
17. *Birykov A., Kushilevitz E.* From dierential cryptanalysis to ciphertext-only attacks // Proc. CRYPTO-1998. Lecture Notes in Computer Science. Vol. 1462. P. 72–88.
18. *Biryukov A., Nakahara J., Prenel B., Vandewalle J.* New weak-key classes of IDEA // Proc. ICICS-2002. Lecture Notes in Computer Science. Vol. 2513. P. 315–326.
19. *Courtois N., Pieprzyk J.* Cryptanalysis of block ciphers with overdened systems of equations // Proc. ASIACRYPT-2002. Lecture Notes in Computer Science. Vol. 2501. P. 267–287.
20. *Dunkelman O., Keller N., Shamir A.* A practical-time related-key attack on the KASUMI cryptosystem used in GSM and 3G telephony // Journal of Cryptology. 2014. Vol. 27. P. 824–849.
21. *Dunkelman O., Keller N., Shamir A.* Improved single-key attacks on 8-round AES-192 and AES-256 // Journal of Cryptology. 2015. Vol. 28. P. 397–422.
22. *Furman V.* Dierential cryptanalysis of Nimbus // Proc. Fast Software Encryption – 2001. Lecture Notes in Computer Science. Vol. 2355. P. 187–195.
23. *Hell M., Johansson T.* Breaking the stream ciphers F-FCSR-H and F-FCSR-16 in real time // Journal of Cryptology. 2011. Vol. 24. P. 427–445.
24. *Isobe T.* A single-key attack on the full GOST block cipher // Journal of Cryptology. 2013. Vol. 26. P. 172–189.
25. *Kara O., Manap C.* A new class of weak keys for Blowfish // Proc. Fast Software Encryption-2007. Lecture Notes in Computer Science. Vol. 4593. P. 167–180.
26. *Kim J.* On the security of the block cipher GOST suitable for the protection in U-business services // Personal and ubiquitous computing. 2013. Vol. 17. P. 1429–1435.
27. *Kim J., Park J., Kim Y.-G.* Weak keys of the block cipher SEED-192 for related-key differential attacks // Proc. STA-2011. P. 167–180.
28. *Knudsen L., Meier W.* Correlations in RC6 // Proc. Fast Software Encryption-2001. Lecture Notes in Computer Science. Vol. 1978. P. 94–108.
29. *Lu J., Yap W.-S., Wei Y.* Weak keys of the full MISTY1 block cipher for related-key differential cryptanalysis // Proc. RSA-2013. Lecture Notes in Computer Science. Vol. 7779. P. 389–404.
30. *Mala H., Dakhilalian M., Rijmen V., Modarres-Hashemi M.* Improved impossible differential cryptanalysis of 7-round AES-128 // Proc. INDOCRYPT-2010. Lecture Notes in Computer Science. Vol. 6498. P. 282–291.
31. *Mantin I.* Predicting and distinguishing attacks on RC4 keystream generator // Proc. EUROCRYPT-2005. Lecture Notes in Computer Science. Vol. 3494. P. 491–506.
32. *Matsui M.* Key collisions of the RC4 stream cipher // Proc. Fast Software Encryption-2009. Vol. 5665. P. 38–50.
33. *Nakahara J.* Differential and linear attacks on the full WIDEA-n block ciphers (under weak keys) // Proc. CANS-2012. Lecture Notes in Computer Science. Vol. 7712. P. 56–71.

34. *Rostovtsev A*. AES-like ciphers: are special S-boxes better then random ones? (virtual isomorphisms again) // Cryptology ePrint Archive. Report 2013/148.
35. *Stankovski P., Hell M., Johansson T*. An efficient state recovery attack on the X-FCSR family of stream ciphers // Journal of Cryptology. 2014. Vol. 27. P. 1–22.
36. www.keylength.com – BlueKrypt. Cryptographic Key Length Recommendation. 2016.

Bibliography

1. *Agibalov G.P*. Logicheskie uravnenija v kriptoanalize generatorov kljuchevogo potoka // Vestnik Tomskogo universiteta. Prilozhenie. 2003. № 6. P. 42–49.
2. *Agibalov G.P*. Metody reshenija sistem polinomial'nyh uravnenij nad konechnym polem // Vestnik Tomskogo universiteta. Prilozhenie. 2006. № 17. P. 47–52.
3. *Agibalov G.P*. Jelementy teorii differencial'nogo kriptoanaliza iterativnyh blochnyh shifrov s additivnym raundovym kljuchom // Prikladnaja diskretnaja matematika. 2008. № 1. P. 34–42.
4. *Doroshenko S.A., Lubkin A.M., Monarev V.A. i dr*. Ataka na potokovye shifry RC4 i ZK-CRYPT s ispol'zovaniem testa «Stopka knig» // Vestnik SibGUTI. 2007. № 1. P. 31–34.
5. *Pestunov A.I*. Differencial'nyj kriptoanaliz blochnogo shifra CAST-256 // Bezopasnost' informacionnyh tehnologij. 2009. № 4. P. 57–62.
6. *Pestunov A.I*. Differencial'nyj kriptoanaliz blochnogo shifra MARS // Prikladnaja diskretnaja matematika. 2009. № 4. P. 56–63.
7. *Pestunov A.I*. Statisticheskij analiz sovremennyh blochnyh shifrov // Vychislitel'nye tehnologii. 2007. T. 12. № 2. P. 122–129.
8. *Pudovkina M.A., Horuzhenko G.I*. O klassah slabyh kljuchej obobshhennoj shifr-sistemy PRINT // Matematicheskie voprosy kriptografii. 2013. T. 4. № 2. P. 113–125.
9. *Rjabko B.Ja., Monarev V.A., Shokin Ju.V*. Novyj tip atak na blokovye shifry // Problemy peredachi informacii. 2005. T. 41. № 4. P. 97–107.
10. *Rjabko B.Ja., Stognienko V.S., Shokin Ju.I*. Adaptivnyj kriterij hi-kvadrat dlja razlichenija blizkih gipotez pri bol'shom chisle klassov i ego primenenie k nekotorym zadacham kriptografii // Problemy peredachi informacii. 2003. T. 39. № 2. P. 207–215.
11. *Rjabko B.Ja., Fionov A.N*. Osnovy sovremennoj kriptografii i steganografii // M.: Gorjachaja linija-Telekom, 2010. 232 p.
12. *Fergjuson N., Shnajer B*. Prakticheskaja kriptografija. M.: Izdatel'skij dom «Vil'jams», 2005. 424 p.
13. *Cheremushkin A.V*. Kriptograficheskie protokoly. Osnovnye svojstva i ujazvimosti: ucheb. posobie dlja stud. uchrezhdenij vyssh. prof. obrazovanija. M.: Izdatel'skij centr «Akademija», 2009. 272 p.
14. *Shennon K*. Raboty po teorii informacii i kibernetike. M.: Izdatel'stvo inostrannoj literatury, 1963. 830 p.
15. *Aerts W., Biham E., Dunkelman O. et al*. A practical attack on KeeLoq // Journal of Cryptology. 2012. Vol. 25. P. 136–157.
16. *Biham E., Dunkelman O., Keller N., Shamir A*. New attacks on IDEA with at least 6 rounds // Journal of Cryptology. 2015. Vol. 28. P. 209–239.
17. *Birykov A., Kushilevitz E*. From dierential cryptanalysis to ciphertext-only attacks // Proc. CRYPTO-1998. Lecture Notes in Computer Science. Vol. 1462. P. 72–88.
18. *Biryukov A., Nakahara J., Prenel B., Vandewalle J*. New weak-key classes of IDEA // Proc. ICICS-2002. Lecture Notes in Computer Science. Vol. 2513. P. 315–326.
19. *Courtois N., Pieprzyk J.* Cryptanalysis of block ciphers with overdened systems of equations // Proc. ASIACRYPT-2002. Lecture Notes in Computer Science. Vol. 2501. P. 267–287.
20. *Dunkelman O., Keller N., Shamir A*. A practical-time related-key attack on the KASUMI cryptosystem used in GSM and 3G telephony // Journal of Cryptology. 2014. Vol. 27. P. 824–849.

21. *Dunkelman O., Keller N., Shamir A*. Improved single-key attacks on 8-round AES-192 and AES-256 // Journal of Cryptology. 2015. Vol. 28. P. 397–422.
22. *Furman V*. Dierential cryptanalysis of Nimbus // Proc. Fast Software Encryption – 2001. Lecture Notes in Computer Science. Vol. 2355. P. 187–195.
23. *Hell M., Johansson T*. Breaking the stream ciphers F-FCSR-H and F-FCSR-16 in real time // Journal of Cryptology. 2011. Vol. 24. P. 427–445.
24. *Isobe T*. A single-key attack on the full GOST block cipher // Journal of Cryptology. 2013. Vol. 26. P. 172–189.
25. *Kara O., Manap C*. A new class of weak keys for Blowfish // Proc. Fast Software Encryption-2007. Lecture Notes in Computer Science. Vol. 4593. P. 167–180.
26. *Kim J*. On the security of the block cipher GOST suitable for the protection in U-business services // Personal and ubiquitous computing. 2013. Vol. 17. P. 1429–1435.
27. *Kim J., Park J., Kim Y.-G*. Weak keys of the block cipher SEED-192 for related-key differential attacks // Proc. STA-2011. P. 167–180.
28. *Knudsen L., Meier W*. Correlations in RC6 // Proc. Fast Software Encryption-2001. Lecture Notes in Computer Science. Vol. 1978. P. 94–108.
29. *Lu J., Yap W.-S., Wei Y*. Weak keys of the full MISTY1 block cipher for related-key differential cryptanalysis // Proc. RSA-2013. Lecture Notes in Computer Science. Vol. 7779. P. 389–404.
30. *Mala H., Dakhilalian M., Rijmen V., Modarres-Hashemi M*. Improved impossible differential cryptanalysis of 7-round AES-128 // Proc. INDOCRYPT-2010. Lecture Notes in Computer Science. Vol. 6498. P. 282–291.
31. *Mantin I*. Predicting and distinguishing attacks on RC4 keystream generator // Proc. EUROCRYPT-2005. Lecture Notes in Computer Science. Vol. 3494. P. 491–506.
32. *Matsui M*. Key collisions of the RC4 stream cipher // Proc. Fast Software Encryption-2009. Vol. 5665. P. 38–50.
33. *Nakahara J*. Differential and linear attacks on the full WIDEA-n block ciphers (under weak keys) // Proc. CANS-2012. Lecture Notes in Computer Science. Vol. 7712. P. 56–71.
34. *Rostovtsev A*. AES-like ciphers: are special S-boxes better then random ones? (virtual isomorphisms again) // Cryptology ePrint Archive. Report 2013/148.
35. *Stankovski P., Hell M., Johansson T*. An efficient state recovery attack on the X-FCSR family of stream ciphers // Journal of Cryptology. 2014. Vol. 27. P. 1–22.
36. www.keylength.com – BlueKrypt. Cryptographic Key Length Recommendation. 2016.