УДК 004.056.55 DOI: 10.30748/nitps.2017.26.23

Н.А. Полуяненко

Харьковский национальный университет имени В.Н. Каразина, Харьков

АНАЛИЗ СОВРЕМЕННЫХ ТЕНДЕНЦИЙ РАЗВИТИЯ ГЕНЕРАТОРОВ ПОТОКОВОГО ШИФРОВАНИЯ

В работе приведен большой обзор современной отечественной и зарубежной литературы, посвященный криптографической защите информации и, в частности, системам потоковой генерации псевдослучайных последовательностей. Изучены результаты международных проектов и конкурсов в области проектирования систем потокового шифрования, таких как NESSIE, CRYPTREC, eSTREAM. Показана устойчивая тенденция к применению в потоковых алгоритмах регистров сдвига с нелинейной обратной связью, проанализированы их достоинства и недостатки, рассмотрены примеры реализации.

Ключевые слова: *защита информации, криптография, потоковые шифры, псевдослучайные последовательности, алгоритмы шифрования, регистры сдвига с нелинейной обратной связью, РСНОС.*

Введение

Современные системы криптопреобразования имеют широкое применение для защиты информационно-телекоммуникационных систем и технологий, в частности, для защиты важной государственной информации, персональных данных, секретной и коммерческой тайны и т.п. [1–7].

Среди систем криптопреобразований особое место занимают симметричные потоковые алгоритмы [8–23], в которых информация подается и обрабатывается в виде бесконечного потока, то есть последовательности, которая гипотетически может быть бесконечной длины. Главным преимуществом симметричных криптографических преобразований является установление определенной зависимости между отдельными символами потока данных, что позволяет обеспечить дополнительную защиту от навязывания ложной информации, или ложных режимов работы аппаратуры защиты или конечного оборудования телекоммуникационных систем и сетей. В соответствии с этим, криптографическое потоковое преобразование обычно пользуется большим доверием у пользователя потому, что потоки данных, которые защищаются потоковыми алгоритмами, не могут быть преобразованы, а именно: в результате преднамеренных или непреднамеренных действий пользователей, злоумышленников или каких-нибудь природных сил и факторов [8–23].

Безусловным преимуществом потоковых криптоалгоритмов является также высокие показатели скорости с возможностью распараллеливания определенных процессов потокового криптопреобразования. В поточном шифровании криптопреобразование производится путем объединения *псевдослучайной последовательности* (ПСП), имеющей определенные криптографические свойства, с сообщением, как правило, с помощью побитового сложения [8–12; 24].

Расшифровывание на стороне получателя основано на вычитании от полученных данных точно такой же ПСП, то есть если ПСП сформировать заблаговременно, тогда шифрование / расшифрование можно проводить параллельно, задействовав одновременно несколько вычислительных систем. Соответственно скорость такого потокового криптопреобразования значительно увеличивается в сравнении с традиционными (блоковыми) методами [25].

Традиционно псевдослучайные двоичные последовательности используются в навигационных системах, системах связи, системах криптографической защиты информации, защите сетевой инфраструктуры и т.п. ПСП являются ядром, которое обеспечивает безопасность в применяемых технологиях. Генераторы ПСП должны быть способны генерировать близкие к случайным, непредсказуемые наборы последовательностей и иметь высокую криптографическую защищенность для применения. Если есть уязвимость в алгоритме или ПСП производит предсказуемые наборы случайных чисел, то все приложения будут склонны к криптографическим атакам.

Рассмотрим подробнее области применения ПСП, а также особенности, которым должны отвечать генераторы ПСП в тех или иных случаях.

Изложение основного материала

Анализ области применения технологий, требующих псевдослучайные числа

Сетевые технологии.

В наше время, использование сетей и их применение растет с большой скоростью. Пользователи

интернета сами часто раскрывают важную информацию, такую, как пароли от аккаунтов, пароли от банковских счетов, персональную и финансовую информацию, важную информацию по транзакциям и т.д. Кроме этого в Интернете существует множество других уязвимостей, таких как: кража паролей, вирусные атаки, подмена данных, угрозы конфиденциальности сообщений, угроза целостности данных и т.д., что создает потенциальную утечку частной информации пользователей. Защита сетевой инфраструктуры реализуются с помощью механизмов генерации ключей (публичные и секретные ключи), генерации паролей, генерации одноразовых паролей и т.п. Имплементация этих механизмов проводится путем генерации наборов случайных последовательностей, имеющих высокую степень непредсказуемости – ПСП. ПСП являются основой для обеспечения безопасности сетевых технологий, таких как: умные телефоны, беспроводные локальные сети, сетевые протоколы, различные онлайн покупки, авторизация в веб-приложениях и т.д. Таким образом, построение защищенной системы является важным элементом сетевой инфраструктуры, так как она обеспечивает конфиденциальность, целостность и доступность данных пользователей.

Мобильные устройства для Mobile-Agent связи.

С помощью мобильных агентов (приложений) на мобильных устройствах происходят атаки в процессе общения и миграции из одного устройства в другое. В связи с чем критическая информация в приложениях на мобильных устройствах, а также процесс обмена этой информацией, должен быть защищен, чтобы злоумышленник не смог изменить или воспользоваться ею. Этот процесс требует генерации секретного ключа, который является сильным, с криптографической точки зрения, набором псевдослучайных чисел [26].

Применение на смартфонах:

Смарт-карты используют псевдослучайные числа для обеспечения безопасности, но они не имеют необходимых вычислительных мощностей, в связи с чем реализация генератора ПСП на таких устройствах затруднена. Обычно псевдослучайные числа производятся физическими генераторами случайных чисел, но они уязвимы к изменениям окружающей среды. Следовательно, для обеспечения защиты от различного рода атак требуется использование легковесных, но криптографически стойких генераторов псевдослучайных чисел [27].

Применение в генерации ключей и перекодирование.

Согласно [28], распределение секретного ключа и перекодирование являются основными проблемами в любых исследованиях безопасности цифровых технологий. В беспроводной среде эти проблемы возрастают за счет малых размеров аппаратных составляющих в инфраструктуре, малой мощности и стоимости памяти. Потоковые шифры используются в безопасной связи в WEP (Wired Equivalent Privacy) и в военной сфере. В связи с чем должны быть разработаны криптографически сильные шифры, которые обеспечивают высокую случайность и устойчивость зашифрованного текста к атакам. Шифр должен быть разработан в SSL (Secure Socket Layer). Необходимо реализовать возможность использования повторного применения в групповой связи (возможно для достаточно продолжительного использования), различных ключей, применяемых для обеспечения безопасности.

Аутентификация, противостояние DOS атакам в стандарте 802.11.

WLANs (беспроводные локальные сети), которые основаны на стандартах 802.11, уязвимы для DOS атак (отказ в обслуживании) из-за незащищенных и непрошедших проверку подлинности пакетов управления и контроля. DOS атаки, основанные на управлении и контроле пакетов, могут быть отфильтрованы при использовании аутентификации с использованием генератора псевдослучайных чисел. Предусматривается механизм аутентификации для защиты от несанкционированного доступа, но при этом требуется криптографически сильная и весьма непредсказуемая случайная последовательность, механизм которой можно создать на основе программной реализации генератора ПСП [29].

RFID технологии.

В настоящее время не существует криптографически безопасного метода для генерации ПСП для технологий с крайне ограниченными ресурсами, таких как RFID (Radio Frequency IDentification – радиочастотная идентификация). Данная технология представляет собой способ автоматической идентификации объектов, в котором посредством радиосигналов считываются или записываются данные, хранящиеся в так называемых транспондерах или RFID-метках. Недорогие RFID-метки не могут выделить больше, чем несколько сотен вентилей для функциональных возможностей безопасности [30]. Даже самая компактная из современных систем шифрования содержит более 1000 вентилей [31]. Отсутствие адекватных механизмов защиты приводит к возникновению многих проблем в области безопасности и блокирует потенциальное применение различных RFID технологий.

Беспроводная связь.

В области беспроводной связи ПСП используются для скремблирования и передачи сигнала. Скремблирование (англ. Scramble – перемешивать; разновидность кодирования информации, для передачи по каналам связи и хранения информации, улучшающая спектральные и статистические характеристики) позволяет придать передаваемому сиг-

налу некоторые полезные инженерно-технические свойства, например, уменьшает вероятность помех со смежными каналами, или применяется для упрощения восстановления синхронизации [32]. Применение ПСП в передаче увеличивает пропускную способность исходного сигнала, делает возможным сохранить или даже увеличить производительность связи при мощности сигнала ниже минимального уровня шума [33]. Как для скремблирования, так и для передачи, важен тщательный подбор ПСП, так как ее длина, скорость передачи, корреляция и другие свойства определяют возможности результирующих систем.

Построение кодовых шкал.

В работах [34] предложено использовать ПСП максимального периода при построении кодовых шкал преобразователей угловых и линейных перемещений. Кодовые шкалы, получившие название «псевдослучайные кодовые шкалы» (ПСКШ), имеют одну информационную дорожку, выполненную в соответствии с символами ПСП и n считывающих элементов, размещенных вдоль дорожки. Считывающие элементы дают возможность получить при полном перемещении шкалы 2^n–1 различных n-разрядных кодовых комбинаций. Особенностью ПСКШ является то, что n-разрядная шкала может быть построена с использованием различных кодовых масок информационной дорожки. Многообразие масок шкалы определяется числом различных ПСП последовательностей максимального периода для определенного n. Основой метода для построения всего спектра таких последовательностей является алгоритм вычисления нормальных (собственных) децимаций ПСП максимального периода.

Проектирование алгоритмов потокового шифрования

Разработка, исследование и обоснование условий использования современных потоковых криптоалгоритмов является чрезвычайно сложной и трудоемкой задачей. Современный потоковый симметричный шифр должен обеспечивать высокий уровень стойкости, иметь необходимый уровень быстродействия и эффективности функционирования на разных вычислительных платформах. Эти требования обеспечиваются эффективностью разных составляющих: выбранной базовой структурой алгоритма, линейными и нелинейными преобразованиями и т.д.

При проектировании систем поточных шифров сформулирован ряд требований [35], которые включают в себя теоретические критерии Р. Рюппеля (R. Rueppel) [36]. В соответствии с этими требованиями схемы генераторов ПСП должны обладать:

– большим периодом выходной последовательности;

– хорошими статистическими свойствами выходной ПСП;

– нелинейностью или, точнее говоря, высокой линейной сложностью выходной ПСП.

Хотя, на сегодняшний момент не существует теоретического доказательства [37] необходимости и достаточности этих требований, но для создания криптографически стойких систем потокового шифрования они должны выполняться. Основная часть существующих потоковых схем шифрования состоит из отдельных блоков, основными из которых являются [35]:

– регистры сдвига с обратной связью (как правило, линейной);

– дискретные функции усложнения;

– запоминающие устройства;

– узлы, реализующие неравномерное движение.

Основным базовым элементов практически любого современного генератора поточного шифрования являются регистры сдвига с обратной связью. На практике чаще всего применяют регистры сдвига с линейной обратной связью (РСЛОС) [38]. Такие криптографические примитивы хорошо себя зарекомендовали в использовании уже на протяжении многих лет. Основные преимущества РСЛОС:

– высокое быстродействие криптографических алгоритмов;

– применение только простейших операций сложения и умножения, аппаратно реализованных практически во всех вычислительных устройствах;

– хорошие криптографические свойства (генерируемые последовательности имеют большой период и хорошие статистические характеристики);

– хорошо подходят для систем с низким энергопотреблением;

– легкость анализа с использованием алгебраических методов за счет линейной структуры.

Распространенными криптографическими алгоритмами, которые построены с использованием РСЛОС, являются: поточный шифр A5/1, используемый для обеспечения конфиденциальности в телефонной сотовой связи стандарта GSM [39]; поточный шифр E0, используемый в протоколе Bluetooth [40] и т.д. РСЛОС являются одним из самых популярных устройств для генерации псевдослучайных двоичных последовательностей.

Одним из первых, кто обсуждал генерацию ПСП с помощью регистров сдвиг, является Голомб (Golomb) в своей книге [41]. Современная трактовка предмета содержится в Голомб и Гонг (Gong) [42].

Однако, несмотря на многочисленные достоинства применения РСЛОС в поточных шифрах они имеют ряд существенных недостатков в силу своей линейности [43]. Последние исследования показы-

вают, что генераторы ПСП на основе РСЛОС склонны к различным угрозам, таким как перехват передаваемой информации, слежка, подмена информации. Особо актуальна данная проблема в технологиях беспроводной передачи данных, где используемые криптографические механизмы безопасности являются недостаточно надежными [44]. Было обнаружено, что поточные шифры могут быть подвержены различным сетевым атакам [45].

Для построения наименьшего РСЛОС, генерирующего заданную двоичную последовательность, может быть использован Алгоритм Берлекемпа-Месси (Berlekamp-Massey). Первоначально он был изобретен Берлекемпом для декодирования БЧХ (Bose-Chaudhuri-Hocquenghem) кодов [46]. Месси связал алгоритм Берлекемпа с синтезом РСЛОС и упростил его [47]. Впоследствии было много модификаций и усовершенствований алгоритма. Кроме того, было показано, что похожие на результаты алгоритма Берлекемпа-Месси могут быть получены с помощью алгоритма Евклида [48].

Существуют несколько методов проектирования генераторов псевдослучайной последовательности, которые разрушают линейные свойства и тем самым делают такие системы криптографически более стойкими [38]:

– использование нелинейной функции, объединяющей выходы нескольких РСЛОС (такие как генератор Геффе);

– использование нелинейной фильтрующей функции для содержимого каждой ячейки единственного РСЛОС;

– использование выхода РСЛОС для управления синхросигналом одного или нескольких РСЛОС (алгоритм А5);

– динамическое изменение параметров рекурренты (длины регистра и коэффициентов обратной связи) и т.д.

Применение РСНОС в генераторах ПСП

Одним из перспективных подходов является применение конструкции на основе *регистров сдвига с нелинейной обратной связью* (РСНОС) [35; 37; 50–52]. РСНОС представляют из себя обобщенный случай РСЛОС, но в отличии от последних, в РСНОС текущее состояние является нелинейной функцией предыдущих состояний [53]. Как показано в [37], в настоящее время, РСНОС отводиться важная роль в системах генерации случайных чисел.

Преимуществами систем, в которые внедрены криптографические примитивы на основе РСНОС, по сравнению с РСЛОС, являются:

– более высокая стойкость (в частности линейная сложность);

– выходная последовательность имеет статистические характеристики не хуже, чем хорошо изученные РСЛОС (прохождение тестов на случайность генерируемой последовательности);

– более сложный, по сравнению с РСЛОС, криптоанализ, отсутствие хорошо разработанного математического аппарата;

– структура (объем памяти, количество операций на один выходной бит, архитектура производства) практически идентична РСЛОС;

– нелинейность уже введена в регистр, что не требует дополнительного усложнения (а как следствия, дополнительного объема оперативной памяти и дополнительных вычислительных операций), то есть соотношения время/память аналогично РСЛОС;

– значительно большее количество комбинаций обратных связей (в том числе и тех, которые генерируют последовательность с максимально возможным периодом). Это позволяет реализовать схемы, основанные на одной базовой модели (фиксированном количестве ячеек регистра сдвига) и различных долговременных ключах, или же, когда требуется выполнить большое количество шифраторов (например, при серийном производстве), но необходимо обеспечить несовместимость различных партий;

– отсутствие простых алгоритмов для восстановления структуры РСНОС по генерируемой ими последовательности, таких как алгоритм Берлекемпа-Месси для РСЛОС;

– простота в программной и аппаратной реализации.

Есть много теоретических результатов, демонстрирующих преимущества использования нелинейных последовательностей в области беспроводной связи. Например, комплементарные последовательности могут решить известную проблему управления мощностью в системах с ортогональным частотным разделением каналов (OFDM), поддерживая плотно ограниченное отношение пиковой мощности к средней [54]. В [55] показано, что применение систем с использованием нескольких несущих в спектре дополняют друг друга и расширяют последовательности Лежандра, опережая системы с кодовым разделением каналов (CDMA). Тем не менее, из-за отсутствия эффективных методов аппаратных средств для генерирования нелинейных последовательностей, их теоретические преимущества в настоящее время не могут быть использованы.

Исследования стандартизированных алгоритмов потокового криптографического преобразования показывают, что имеет место устойчивая тенденция построения схеме генераторов ПСП, построенных с применением регистров сдвига [25], в том числе и с нелинейной обратной связью. Поточные шифры на основе РСНОС включаются в Achterbahn [56], Dragon [57], Grain [58], Trivium [59], VEST [60]. В работах [61–64] показано, что РСНОС более ус-

тойчивы к криптоаналитическим атакам, чем РСЛОС.

Однако, несмотря на перспективность применения РСНОС как одного из основных элементов генератора ПСП, многие фундаментальные проблемы, связанные с РСНОС, остаются недостаточно изученными [65]. На сегодняшний день даже такую простую характеристику, как период последовательности, формируемый регистрами сдвига, в обратную связь которых введена нелинейность, трудно определить [35].

Стандартизованные алгоритмы потокового криптопреобразования

На сегодняшний день вопрос разработки и стандартизации потоковых криптопреобразований решается во многих технологично развитых странах мира [25]. Однако, наибольшее распространение имеют всемирно известные криптоалгоритмы, которые стандартизованы на международном или национальном уровне. Среди таких алгоритмов можно выделить алгоритм SNOW 2.0, определенный стандартам международной организации по стандартизации ISO/IEC 18033-4 «Information technology – Security techniques – Encryption algorithms – Part 4: Stream ciphers» [66]. В рамках относительно недавно проведенного (2004 – 2008 г.г.) международного проекта по выявлению новых систем потокового шифрования, пригодных для широкого применения, организованного Европейским Союзом – eSTREAM можно выделить несколько победителей, которые удовлетворяют установленным требованиям:

– программно-ориентированные: HC-128; Rabbit; Salsa 20/12; SOSEMANUK;

– аппаратно-ориентированные: Grain; MICKEY; Trivium.

Следует отметить также международный стандарт ISO/IEC 29192 «Information technology – Security techniques – Lightweight cryptography» [22], который посвящен алгоритмам «легковесной криптографии» (англ. Lightweight cryptography). Это криптоалгоритмы, реализация которых ориентирована на дешевые и нетребовательные к скорости и объему памяти оборудования, то есть соответствующие алгоритмы криптографического преобразования не требуют сложных вычислений или больших размеров памяти. Часть третья стандарта посвящена потоковым шифрам, а именно алгоритмам Enocoro [67].

Современные модели потокового шифрования на основе РСНОС

В данном разделе приведены современные алгоритмы потокового шифрования, которые были признаны победителями или получили высокую оценку на международных конкурсах или являются стандартизированными, а также приведено их краткое описание.

Потоковый шифр Snow 2.0.

Потоковый симметричный шифр Snow 2.0 является генератором ключевых потоков [69], шифр слово-ориентированный. Авторы алгоритма – Томас Йохансон и Патрик Екдаль. Snow 2.0, в настоящее время обозначается как Snow, является генератором ПСП, который использует в качестве входных данных 128 или 256-битный секретный ключ и 128-битный вектор инициализации.

Потоковый шифр Sosemanuk.

Sosemanuk [70] является новым синхронным программно-ориентированным потоковым шифром и соответствует профилю 1 международного конкурса eECRYPT. Его длина ключа может быть выбрана между 128 и 256 битами. Шифр работает с 128 битовым начальным заполнением, при этом, как утверждает разработчик алгоритма, любая длина ключа достигает 128-битной защиты.

Алгоритм Sosemanuk использует некоторые основные принципы потокового шифра Snow 2.0 и некоторые преобразования, полученные с блочного шифра Serpent [71]. Sosemanuk направленный на улучшения Snow 2.0 как в смысле безопасности, так и в смысле эффективности реализации. В шифре Sosemanuk применяется РСЛОС, который содержит 10 элементов поля $GF(2^{32})$, то есть конечного поля из 2^{32} элементами.

Потоковый шифр Grain.

Потоковый шифр Grain [72] представлен Мартыном Хеллом (Martin Hell), Томасом Юханссоном (Thomas Johansson) и Вилли Мэйером (Willi Meier). Шифр, нацеленный на аппаратную среду с очень ограниченным количеством вентилей, потребляемой мощности и памяти, он является аппаратно ориентированным. Алгоритм шифрования Grain, основанный на двух регистрах сдвига и нелинейной функции вывода. На сегодняшний день не известно атаки быстрей, чем полный перебор ключа. Сложность аппаратной реализации и скорость выгодно отличает этот алгоритм от других аппаратно ориентированных потоковых шифров, например, таких как E0 и A5/1.

Алгоритм Grain является синхронным потоковым шифром, в котором ПСП генерируется независимо от текста. Конструкция основана на двух регистрах сдвига, один с линейной обратной связью и один регистр сдвига с нелинейной обратной связью. Использование РСЛОС гарантирует минимальный период для гаммы, а также обеспечивает сбалансированность на выходе. Применения РСНОС вместе с нелинейной функцией выхода вводит нелинейность в шифр. Вход РСНОС маскируется с выходом РСЛОС таким образом, что состояние РСНОС становиться сбалансированным.

Разработчики не утверждают, что используемый PCHOC может генерировать последовательность с максимальным периодом.

Интересным моментом является то, что конструкция потокового шифра Grain позволяет увеличить скорость генерации за счет более мощных аппаратных средств. Это может быть сделано через увеличение количества реализаций функций обратной связи, вследствие чего скорость генерации также будет увеличена в несколько раз. С этой целью, последние 15 бит регистров сдвига не используются в функциях обратных связей или на выходе в функции фильтра. Это позволяет легко умножить скорость до 16 раз, если, конечно, доступна необходимое количество аппаратных ресурсов.

Потоковый шифр MICKEY.

В работе [73] представлена усовершенствованная версия 2.0 потокового шифра MICKEY (расшифровывается как Mutual Irregular Clocking KEY stream generator – генератор ключевого потока с взаимно неравномерным движением), который предназначен для аппаратных платформ с ограниченными ресурсами.

Алгоритм шифра MICKEY имеет простую аппаратную реализацию и при этом обеспечивает высокий уровень безопасности. В нем используется нерегулярное движение регистров сдвига, а также новые методы, которые обеспечивают достаточно большой период ПСП и стойкость к определенным криптоаналитическим атакам.

Генератор состоит из двух регистров R и S. Длина каждого регистра равна 100 разрядам, каждый разряд содержит 1 бит. В спецификации алгоритма сказано, что R – это линейный регистр с примитивным характеристическим полиномом, а S – нелинейный регистр. Регистр R выполняет роль «двигателя», гарантируя, что состояние генератора не повторяется при генерации одной ключевой последовательности и гарантируя то, что обеспечены хорошие локальные статистические свойства. Влияние R на движение S также предохраняет S от зацикливания в коротком цикле.

Потоковый шифр MICKEY 2.0. не предназначен для использования в особенно высокоскоростном программном обеспечении, хотя его очень просто реализовать, и он достаточно эффективен с вычислительной точки зрения. Собственная реализация разработчиком алгоритма достаточно эффективна (но без оптимизации), она генерирует 10^8 бит ключевого потока за 3,81 секунду, используя процессор Pentium 4 с частотой 3,4 ГГц [73].Существует возможность для более эффективных программных реализаций, которые генерируют несколько битов ПСП за один раз, используя таблицу реализаций управляющего регистра и создания выходной ПСП.

Потоковый шифр Trivium.

Алгоритм Trivium является аппаратно-ориентированным параллельным потоковым шифром [68]. Он был сконструирован как пример для исследования зависимостей упрощения потокового шифра без вреда безопасности, быстродействия и гибкости. Учитывая то, что шифр уже долгое время изучается и не найдено серьезных уязвимостей, то, несмотря на свою упрощенность, к данному шифру больше доверия, чем к сложным схемам [25].

Схема шифрования содержит 288 бит внутреннего состояния. Процесс генерации ПСП является итеративным и берет значения 15-ти специальных состояний бит и использует их все для обновления 3-х бит состояния и вычисления 1 бита ПСП. Далее процесс повторяется снова, пока не будет сгенерировано 2^{64} битов ПСП.

Целью шифра Trivium является компактность в среде с ограниченными входными параметрами, энергоэффективность на платформах с малыми источниками энергии, а также быстрота в приложениях, которые требуют высокоскоростного шифрования.

Необходимость в компактности реализации предусматривает бит-ориентированный подход. Это также обуславливает использование нелинейного внутреннего состояния, чтобы не расходовать всю построенную нелинейность на выходе генератора. Для того, чтобы обеспечить мощную и быструю реализацию, конструкция должна обеспечивать распараллеливания операций. В случае Trivium это сделано за счет обеспечения того, что любое значение бита не используется минимум в 64-х итерациях, после того как он был изменен. Таким образом, до этих 64-х итераций значение может быть вычислено один раз, при условии, что 3 входа элемента сложения (AND), и 11 входов элемента XOR в оригинальной схеме дублируются соответствующее количество раз. Это позволяет делить тактовую частоту на коэффициент 64 без вреда для пропускной способности.

Несмотря на то, что Trivium разработан не для программной реализации, он эффективен и на стандартных персональных компьютерах.

Так как внутреннее состояние Trivium нелинейно разворачивается, его период трудно определить. Если пропустить AND-входы (в результате получить полностью линейные схемы), можно установить, что любая пара ключ / вектор инициализации, которая будет сгенерирована, имеет период $2^{96-3}–1$.

Потоковый шифр Achterbahn-128/80.

Шифр Achterbahn [74] был представлен на конкурсе eSTREAM как аппаратно-ориентированный алгоритм. В окончательной версии спецификации шифра он называется Achterbahn-128/80, поскольку он поддерживает ключи длиной 128 бит и 80 бит соответственно. Внутреннее состояние шифра со-

ставляет 351 бит для Achterbahn-128 и 297 бит для Achterbahn-80.

Achterbahn-128 представляет потоковый генератор, состоящий из 13 двоичных РСНОС с примитивными образующими полиномами и длиною регистров от 21 до 33. Последовательности от РСНОС используются в качестве входных данных для нелинейной булевой функции выхода. Выходное значение является булевой нелинейной функцией объединения соответствующих выходных последовательностей от всех РСНОС.

Achterbahn-80 состоит из 11 примитивных РСНОС, которые являются такими же, как и в предыдущем случае, за исключением первого и последнего регистра. Как мы можем видеть, Achterbahn-128 содержит Achterbahn-80 в качестве несущей конструкции.

Потоковый шифр Dragon.

Потоковый шифр Dragon [57], построенный на основе 1024-битного РСНОС и нелинейной функции фильтра с 64-битной памятью. Dragon может использоваться со 128-битными или с 256-битными ключом и вектором инициализации. Данные версии называются Dragon-128 и Dragon-256, соответственно. Обе версии работают практически идентично, за исключением процесса инициализации ключа.

Dragon разрабатывался с учётом требований как к производительности, так и к безопасности. Он использует два высоко оптимизированных 8×32 S-бокса и простые операции из 32-битовых слов. Как утверждают разработчики, компоненты шифра Dragon разработаны с учетом защиты от всех известных атак.

Dragon имеет хорошую производительность. Эффективная реализация алгоритма Dragon на программируемых логических интегральных схемах фирмы Altera достигает производительности 1.06 Гб/с. Алгоритм требует около 4 килобайт памяти, поэтому подходит для использования в системах с ограниченными аппаратными ресурсами, что делает его весьма конкурентоспособным по сравнению с другими слово-ориентированными потоковыми шифрами.

Потоковый шифр VEST.

VEST (англ. Very Efficient Substitution Transposition – очень эффективная перестановка) это серия аппаратно-ориентированных поточных шифров общего назначения, которые обеспечивают однопроходное шифрование с аутентификацией и могут работать как хэш-функция, стойкая к коллизиям второго рода. Шифры VEST разработаны в Synaptic Laboratories. Все шифры этой серии поддерживают режим работы с ключами переменной длины.

Шифры VEST [75] были разработаны Шоном О'Нейлом (Sean O'Neil). Впервые были представлены на турнире eSTREAM в 2005 году, прошли во второй отборочный тур, но не попали в третий и не прошли в финал.

VEST-4 генерирует 4 бита выхода за один такт и предлагает 80-битное шифрование, имеет минимальный гарантированный период не меньше 2^{128}, ориентирован на недорогие средства, такие как RFID и смарт-карты. VEST-16 генерирует 16 бит за один такт, предлагает 160-битное шифрование, подходит для высокоскоростных приложений, низкую стоимость, низкой аппаратные затраты. VEST-32 генерирует 32 бита за такт, предлагает 256-битное шифрование, подходит для высокоскоростных приложений с высокой степенью защиты. VEST-16 и VEST-32 имеют минимальный гарантированный период не меньше 2^{138}.

Разработчиками заявлено, что на программируемой логической микросхеме Stratix-II фирмы Altera скорость генерации реализации VEST-32 составляет порядка 13 Гб/с, а VEST-16 – 7 Гб/с.

Выводы

Современные потоковые системы криптопреобразований представляют собой мощный механизм, который обеспечивает быструю обработку больших массивов информационных данных с обеспечением основных криптографических требований безопасности и конфиденциальности. Сложность и масштабность научно-исследовательских робот по обоснованию структуры современных поточных шифров, исследования их криптографических и эксплуатационных свойств, подтверждаются большим количеством международных и национальных проектов, программ и конкурсов. В частности, международные проекты NESSIE, CRYPTREC, eSTREAM и другие были ориентированы на разработку эффективных криптоалгоритмов, удовлетворяющих высоким требованиям криптографической стойкости, а также эффективности программной и аппаратной реализации. Одним из приоритетов вышеуказанных программ была разработка и исследование современных потоковых симметричных шифров.

Современные системы поточного шифрования применяются для защиты информации практически во всех криптографических приложениях и на всех этапах их жизненного цикла; шифрование применяется в информационно-телекоммуникационных системах для решения различных задач в зависимости от предъявляемых требований; криптографические протоколы на основе поточного криптопреобразования используются для аутентификации, установки секретов и ключей, согласования секретов и ключей, разделение секретов, когда предъявляются высокие требования к сложности и скорости, и так далее. Можно утверждать, что криптографическая защита информации является важной составной частью в обеспечении безопасности современных информа-

ционно-телекоммуникационных систем и технологий. Потоковые криптопреобразования используются в таких системах, где поставлены достаточно жесткие требования безопасности и скорости, потому что именно потоковый способ криптографического преобразования является наиболее надежным, а соответствующие средства криптографической защиты информации являются более быстродействующими и нетребовательными к вычислительным ресурсам.

Проектирование криптографически стойких систем генерации ПСП на основе регистров сдвига, устойчивых к различного рода атакам и имеющих хорошие технические характеристики, является на сегодняшний день актуальной и необходимой задачей. Отдельное и с каждым годом возрастающее внимание уделяется проектированию систем с использованием РСНОС, которые обладают практически всеми достоинствами РСЛОС, и лишены их главного недостатка – предсказуемости. Остро ощущается отсутствие хорошо разработанного математического аппарата для анализа и синтеза алгоритмов поточного шифрования на основе РСНОС, что значительно тормозит потенциальное их развитие.

Список литературы

1. Закон України "Про державну таємницю" // Відомості Верховної Ради. – 1994. – № 16, ст. 93.

2. Закон України "Про захист інформації в інформаційно-телекомунікаційних системах" // Відомості Верховної Ради України. – 1994. – № 31, ст. 286.

3. Закон України "Про захист персональних даних" // Відомості Верховної Ради України. – 2010. – № 34, ст. 481.

4. Закон України "Про телекомунікації" // Відомості Верховної Ради України (ВВР). – 2004. –№ 12, ст. 155.

5. Закон України "Про інформацію" // Відомості Верховної Ради України (ВВР). –1992. – № 48, ст. 650.

6. Закон України "Про Національну систему конфіденційного зв'язку" // Відомості Верховної Ради України (ВВР). – 2002. – № 15, ст. 103.

7. Закон України "Про електронні документи та електронний документообіг" // Відомості Верховної Ради України (ВВР). – 2003. – № 36, ст. 275.

8. Алферов А.П. Основы криптографии / А.П. Алферов, А.Ю. Зубов, А.С. Кузьмин, А.В. Черемушкин. – М.: Гелиос АРВ, 2005. – 480 с.

9. Вембо Мао. Современная криптография. Теория и практика: пер. с англ. / Вембо Мао. – М.: Изд. дом «Вильямс», 2005. – 768 с.

10. Горбенко І.Д. Прикладна криптологія: монографія / І.Д. Горбенко, Ю.І. Горбенко. – Харків: ХНУРЕ, Форт, 2012. – 1 та 2 видання. – 868 с.

11. Горбенко І.Д. Прикладна криптологія: підручник / І.Д. Горбенко, Ю.І. Горбенко. – Харків, ХНУРЕ, Форт, 2012. – 1 та 2 видання. – 878 с.

12. Есин В.І. Безпека інформаційних систем і технологій / В.І. Есин, О.О. Кузнецов, Л.С. Сорока. – Х.: ХНУ ім. В.Н. Каразіна, 2013. – 632 с.

13. Панасенко С.П. Алгоритмы шифрования. Специальный справочник / С.П. Панасенко. – СПб.: БХВ-Петербург, 2009. – 576 с.

14. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке СИ / Б. Шнайер. – М.: «Триумф», 2002. – 797 с.

15. Alfred J. Menezes. Handbook of Applied Cryptography / Alfred J. Menezes, Paul C. van Oorschot, Scott A. Vanstone. – CRC Press, 1997. – 794 p.

16. Al-Shehri K.N. Encryption Primitives and their Application to Stream Ciphers Design: Master's Degree Thesis / K.N. Al-Shehri. – King Saud University, 2007. – 121 p.

17. Encyclopedia of cryptography and security / [Editor-in-chief Henk C.A. van Tilborg]. – Springer-Verlag, 2005. – 697 p.

18. Golic J.D. Embedding and probabilistic correlation attack on clockcontrolled shift registers / J.D. Golic, O'Connor // Advances in Cryptology – Eurocrypt '94. – Berlin: Springer-Verlag, 1994. – P. 90-100.

19. Golic J.D. On the Security of shift register based keystream generators / J.D. Golic // Fast software Encryption, Cambridge Security Workshop, December 1993. Berlin: Springer-Verlag, 1994. – P. 90-100.

20. Golic J.D. On the security of nonlinear filter generators / J.D. Golic // Proceedings of Fast Software Encryption'96, Lecture Notes in Computer Science, vol. 1039, Springer-Verlag, 1996. – P. 173-188.

21. Hell M., Johansson T. Security Evaluation of Stream Cipher Enocoro-128v2. [Электронный ресурс]. – Режим доступа к ресурсу: https://www.cryptrec.go.jp/estimation/techrep_ id2008.pdf.

22. ISO/IEC 29192-3:2012. Information technology – Security techniques – Lightweight cryptography – Part 3: Stream ciphers. [Электронный ресурс]. – Режим доступа к ресурсу: https://www.iso.org/standard/56426.html.

23. Schafheutle M. A First Report on the Stream Cipher SNOW. [Электронный ресурс]. – Режим доступа к ресурсу: http://www.cryptonessie.org.

24. Robshaw M. "Stream ciphers" Tech. Rep. TR - 701, July 1994.

25. Дослідження потокових симетричних шифрів та потокових режимів блокових симетричних шифрів: звіт про НДР (проміжний). – Аналіз та порівняльні дослідження сучасних алгоритмів потокового криптоперетворення / ХНУ ім. В.Н. Каразіна; кер. Кузнецов О.О.; вик.: Малахов С.В. [та інш., всього 11 осіб]. – Х.: ХНУ ім. В.Н. Каразіна. – 2015. – 233 с.

26. Topaloglu U. A pseudo random number generator in mobile agent interactions / U. Topaloglu, C. Bayrak, K. Iqbal // In Engineering of Intelligent Systems, 2006 IEEE International Conference on, pages 1–5, 2006.

27. Jian-Wei Fan. A random increasing sequence hash chain and smart card-based remote user authentication scheme / Jian-Wei Fan, Chao-Wen Chan, Ya-Fen Chang // In Information, Communications and Signal Processing (ICICS) 2013 9th International Conference on, pages 1-5. IEEE, 2013.

28. Tara Chand Singhal. Systems and methods for complex encryption keys, January 29 2013. US Patent 8,363,834.

29. Mansoor A., Aamir H. Pseudo random number based authentication to counter denial of service attacks on 802.11. In Wireless and Optical Communications Networks, 2008. WOCN'08. 5th IFIP International Conference on, pages 1-5. IEEE, 2008.

30. Juels A. "RFID security and privacy: a research survey" / A. Juels // IEEE Journal on Selected Areas in Communications, Feb. 2006. vol. 24. – P. 381-394.

31. T. Good, M. Benaissa. "ASIC hardware performance," New Stream Cipher Designs: The eSTREAM Finalists, LNCS 4986, 2008. – P. 267-293.

32. Lee B.G. Scrambling Techniques for CDMA Communications / B.G. Lee, B.H. Kim. – Berlin, Springer, 2001.

33. Theory of spread spectrum communications - a tutorial / R.L. Pickholtz and et. al. // IEEE Trans. on Communications, 1982. vol. 30, no. 5. – P. 855-883.

34. Ожиганов А.А. Использование псевдослучайных последовательностей при построении кодовых шкал для преобразователей линейных перемещений / А.А. Ожиганов, Жуань Чжипэн // Изв. вузов. Приборостроение. 2008. – Т. 51, № 7. – С. 28-33.

35. Основные тенденции развития открытой криптографии (обзор по заказу cryptography.ru) // Опубликовано: geo.com.ru. [Электронный ресурс]. – Режим доступа к ресурсу: http://images.geo.web.ru/pubd/2001/10/10/0001161293/tend.pdf.

36. Rueppel R.A. Analysis and Design of Stream Ciphers / R.A. Rueppel // Springer communications and control engineering series. – 1986. – 244 p.

37. Поточные шифры / А.В. Асосков, М.А. Иванов, А.А. Мирский, А.В. Рузин, А.В. Сланин, А.Н. Тютвин. – М.: КУДИЦ-ОБРАЗ, 2003. – 336 с.

38. Торба А.А. Детерминированные генераторы псевдослучайных последовательностей для потокового шифрования на основе ДЛРР / А.А. Торба, В.А. Бобух, М.О. Торба, А.О. Тобра // Прикладная радиоэлектроника. – 2016. – Том 15, № 3. – С. 191-194.

39. Biham E. Cryptanalysis of the A5/1 GSM stream cipher / E. Biham, O. Dunkelman // in INDOCRYPT '00: Proceedings of the First International Conference on Progress in Cryptology, (London, UK), 2000. – P. 43-51, Springer-Verlag.

40. Shaked O., Wool A. Cryptanalysis of the Bluetooth E0 cipher using OBDD's. 2006. [Электронный ресурс]. – Режим доступа к ресурсу: http://citeseer.ist.psu.edu/viewdoc/download?doi=10.1.1.60.6279&rep=rep1&type=pdf.

41. Golomb S.W. Shift Register Sequences / S.W. Golomb San Francisco, Holden-Day, 1967, revised edition, Laguna Hills, CA, Aegean Park Press, 1982.

42. Golomb S.W., Gong G. Signal Design for Good Correlation. For Wireless Communication, Cryptography, and Radar. Cambridge University Press, 2005.

43. Schneier B. A self-study course in block-cipher cryptanalysis / B. Schneier // Cryptologia. – 2000. – Vol. XXIV, no. 1. – P. 18-33.

44. Parallel Computing Experiences with CUDA / M. Garland, S. Le Grand, J. Nickolls, J. Anderson, J. Hardwick, S. Morton, E. Phillips, Y. Zhang, V. Volkov // IEEE Micro, July 2008. – Vol. 28. – P. 13-27.

45. Preneel B. Understanding cryptography: a textbook for students and practitioners / B. Preneel, C. Paar, J. Pelzl. – Springer, 2009.

46. Berlekamp E.R. Nonbinary BCH decoding / E.R. Berlekamp // in International Symposium on Information Theory, (San Remo, Italy), 1967.

47. Massey J. Shift-register synthesis and BCH decoding / J. Massey // IEEE Transactions on Information Theory, 1969. – Vol. 15. – P. 122-127.

48. Dornstetter J. On the equivalence between Berlekamp's and Euclid's algorithms / J. Dornstetter // IEEE Transactions on Information Theory. – 1987. – Vol. 33, no. 3. – P. 428-431.

49. Welch L. Continued fractions and Berlekamp's algorithm / L. Welch, R. Sholtz // IEEE Transactions on Information Theory. – 1979. – Vol. 25, no. 1. – P. 19-27.

50. Gammel B.M., G¨ottfert R., Kniffler O. An NLFSR-Based Stream Cipher. Infineon Technologies AG, Munich, Germany. [Электронный ресурс]. – Режим доступа к ресурсу: https://www.researchgate.net/publication/224647778.

51. Hell M., Johansson T., Meier W., Grain – A Stream Cipher for Constrained Environments, eSTREAM submission, [Электронный ресурс]. – Режим доступа к ресурсу: http://www.ecrypt.eu.org/stream/p3ciphers/grain/Grain_p3.pdf.

52. Дослідження потокових симетричних шифрів та потокових режимів блокових симетричних шифрів: звіт про НДР (заключний). / ХНУ ім. В.Н. Каразіна; кер. Кузнецов О.О.; вик.: Малахов С.В. [та інш., всього 13 осіб]. – Х.: ХНУ ім. В.Н. Каразіна. – 2015. – 73 с.

53. Golomb S. Shift Register Sequences / S. Golomb. – Aegean Park Press, 1982.

54. Davis J. Peak-to-mean power control in OFDM, Golay complementary sequences, and Reed-Muller codes / J. Davis, J. Jedwab // IEEE Trans. on Inf. Theory. – 1999. – Vol. 45, no. 7. – P. 2397-2417.

55. Popovic B. Spreading sequences for multicarrier CDMA systems / B. Popovic // IEEE Transactions on Communications, June 1999. – Vol. 47. – P. 918-926.

56. Gammel B. Achterbahn-128/80: Design and analysis / B. Gammel, R. Gottfert, O. Kniffler // in SASC'2007: Workshop Record of The State of the Art of Stream Ciphers, 2007. – P. 152-165.

57. Chen K., Henricken M., Millan W., Fuller J., Simpson L., Dawson E., Lee H., Moon S. Dragon: A fast word based stream cipher. in eSTREM, ECRYPT Stream Cipher Project. Report 2005/006.

58. Hell M., Johansson T., Meier W. (2005). Grain – a stream cipher for constrained environments. [Электронный ресурс]. – Режим доступа к ресурсу: http://citeseer.ist.psu.edu/viedoc/summary?doi=10.1.1.107.9707.

59. Canniere C., Preneel B. TRIVIUM specifications. [Электронный ресурс]. – Режим доступу: http://citseer.ist.psu.edu/viewdoc/summary?doi=10.1.1.59.9030.

60. Gittins, B., Landman, H., O'Neil, S., Kelson, R. A presentation on VEST hardware performance, chip area measurements, power consumption estimates and benchmarking in relation to the AES, SHA-256 and SHA-512. Cryptology ePrint Archive, Report 2005/415. [Электронный ресурс]. – Режим доступа к ресурсу: http://eprint.iacr.org/2005/415.

61. Canteaut A. Open problems related to algebraic attacks on stream ciphers / A. Canteaut // in WCC, 2005. P. 120-134.

62. Preneel B. A survey of recent developments in cryptographic algorithms for smart cards / B. Preneel // Comput. Networks. – 2007. – Vol. 51, no. 9. – P. 2223-2233.

63. Дербунович Л.В. Генераторы ключевых последовательностей в потоковых криптографических шифрах / Л.В. Дербунович, Д.Г. Караман, А.Н. Осипенко // Тезисы докладов на 3-й Международной научно-практической конференции "Інформаційні технології та комп'ютерна інженерія". – ВНТУ, Винница, 2012. – С. 138-139.

64. Zeng K. Pseudo-random bit generators in stream-cipher cryptography / K. Zeng, C. Yang, D. Wei, T.R.N. Rao. – Computer, 1991.

65. Коробейников А.Г. Математические основы криптологии: учебное пособие / А.Г. Коробейников, Ю.А. Гатчин. – Санкт-Петербург 2004. [Электронный ресурс]. – Режим доступа к ресурсу: http://books.ifmo.ru/file/pdf/56.pdf.

66. ISO/IEC 18033-4:2011. Information technology – Security techniques – Encryption algorithms – Part 4: Stream ciphers. [Электронный ресурс]. – Режим доступа к ресурсу: https://www.iso.org/standard/54532.html.

67. Pseudorandom Number Generator Enocoro. [Электронный ресурс]. – Режим доступа к ресурсу: http://www.cryptrec.go.jp/english/cryptrec_13_spec_cypherlist_files/PDF/23_00espec.pdf.

68. The eSTREAM Project - eSTREAM Phase 3. Trivium (Portfolio Profile 2). [Электронный ресурс]. – Режим доступа к ресурсу: http://www.ecrypt.eu.org/stream/triviumpf.html.

69. Schafheutle M. A First Report on the Stream Cipher SNOW. [Электронный ресурс]. – Режим доступа к ресурсу: http://www.cryptonessie.org/.

70. The eSTREAM Project - eSTREAM Phase 3. SOSEMANUK (Portfolio Profile 1). [Электронный ресурс]. – Режим доступа к ресурсу: http://www.ecrypt.eu.org/stream/sosemanukpf.html.

71. Anderson R.J. Serpent: A Candidate Block Cipher for the Advanced Encryption Standard. University of Cambridge Computer Laboratory. Retrieved 2013-01-14. [Электронный ресурс]. – Режим доступа к ресурсу: http://www.cl.cam.ac.uk/~rja14/serpent.html.

72. The eSTREAM Project - eSTREAM Phase 3. Grain (Portfolio Profile 2). [Электронный ресурс]. – Режим доступа к ресурсу: http://www.ecrypt.eu.org/stream/grainpf.html.

73. The eSTREAM Project - eSTREAM Phase 3. MICKEY (Portfolio Profile 2). [Электронный ресурс]. – Режим доступа к ресурсу: http://www.ecrypt.eu.org/stream/miceypf.html.

74. Gammel B.M., Goetffert R., Kniffler O. Achterbahn 128/80. The eSTREAM project. [Электронный ресурс]. – Режим доступа к ресурсу: http://www.ecrypt.eu.org/stream/achtebahnp2.html.

75. O'Neil S., Gittins B., Landman H. VEST Hardware-Dedicated Stream Ciphers, eSTREAM, June 2005. [Электронный ресурс]. – Режим доступа к ресурсу: https://cr.yp.to/streamciphers/vest-16/desc.pdf.

Поступила в редколлегию 19.01.2017

Рецензент: д-р техн. наук проф. А.В. Потий, Харьковский национальный университет имени В.Н. Каразина, Харьков.

АНАЛІЗ СУЧАСНИХ ТЕНДЕНЦІЙ РОЗВИТКУ ГЕНЕРАТОРІВ ПОТОКОВОГО ШИФРУВАННЯ

М.О. Полуяненко

Анотація: у роботі приведено великий огляд сучасної вітчизняної та закордонної літератури, присвяченої криптографічному захисту інформації, зокрема, системам потокового генерування псевдовипадкової послідовності. Вивчені результати міжнародних проектів та конкурсів в області проектування систем потокового шифрування, таких як NESSIE, CRYPTREC, eSTREAM. Показана стійка тенденція до застосування в потокових алгоритмах регістрів зсуву з нелінійним зворотнім зв'язком, проаналізовані їх переваги та недоліки, розглянуто приклади реалізації.

Ключові слова: *захист інформації, криптографія, потокові шифри, псевдовипадкова послідовність, алгоритми шифрування, регістри зсуву з нелінійнім зворотним зв'язком, РЗНЗЗ.*

THE ANALYSIS OF MODERN TENDENCIES OF DEVELOPMENT OF THE STREAM CIPHER GENERATOR

N.A. Poluyanenko

Abstract: in this paper, the great overview of modern foreign and domestic literature are shown; this overview describes cryptographic protection of information and in particular systems of stream generation of pseudorandom sequences. The results of international projects and competitions in the sphere of design of stream encryption systems such as NESSIE, CRYPTREC, eSTREAM are studied. The steady trend to applying of nonlinear feedback shift registers in stream algorithms are shown. Their dignities and disadvantages are analyzed, the examples of their implementations are shown.

Keywords: *information protection, cryptography, stream cipher, pseudorandom sequences, encryption algorithm, nonlinear feedback shift registers, NLFSR.*