УДК 621.316.97

АБСОЛЮТНО КРИПТОСТОЙКИЕ И САМЫЕ ПРОСТЫЕ ШИФРАТОРЫ

Ю. М. Брауде-Золотарев, научный консультант ФГУП СНПО «Элерон», к.т.н; + 7 (495) 322-6292

Ключевые слова: *криптостойкость, имитостойкость, потоковый шифратор, генератор случайных чисел, обновление ключа, последовательность случайных чисел, шифрблокнот.*

Введение. Построение абсолютно криптостойких и простых шифраторов — важнейшая задача современной криптографии. Они необходимы для высокоскоростных каналов связи и радиосетей технических средств охраны (ТСО), от объектов которой нередко требуется, чтобы их автономные источники питания работали год до замены [1—3]. В то же время многие шифраторы, описанные в [4—8], а также в стандарте ARIA [9], для этого непригодны из-за энергоемких и медленных алгоритмов.

Сложным в программной, но самым простым и экономичным в аппаратной реализации остается (с 1997 г. и до сих пор) шифратор — генератор случайных чисел (ГСЧ) [10]. В нем «кроссинговер» изменяет содержимое (ключ) и функции обратной связи (генераторные полиномы — ГП) двух автоматов путем перестановки секций их регистров сдвига (РС) в одном такте четырьмя переключателями. Каждый переключатель занимает один условный вентиль (УВ) — четыре транзистора КМОП, а разряд РС (D-триггер) — пять УВ. Микросхема Н1515ХМ1-888 [10] (меньше 3 тыс. УВ) содержит два ГСЧ — шифратор и дешифратор, каждый с 256-разрядным РС, в который вводят ключ. Максимальная скорость таких ГСЧ на два порядка выше, чем у микросхемы шифратора, реализующего ГОСТ 28147-89 на той же элементной базе и с той же длиной ключа, но с обработкой многоразрядных слов, а энергопотребление (на равных скоростях) — почти на три порядка ниже. На скорости 10 кбит/с ГСЧ потребляет около 30 мкА от 5 В ($1{,}5 \cdot 10^{-8}$ Дж/бит).

Цель работы — рассмотреть алгоритмы известных шифраторов [4—13] и в условиях, когда разработаны микросхемы даже для атак на шифраторы [8], рекомендовать алгоритмы, стойкие к возможным атакам [7, 8, 14, 15], — самые простые и быстрые в аппаратной и программной реализации.

Так как программная реализация и процессор основаны, в конечном счете, на микроэлектронике, то сложность алгоритмов будем оценивать по критериям микроэлектроники, а не по объему вычислительных операций. Шифраторы, соответствующие ГОСТ 28147-89, AES, ARIA, уже реализованы на микросхемах (ASIC), а ряд других — на программируемых логических интегральных схемах (ПЛИС) [4—9]. В смежной области помехоустойчивого кодирования, когда нужны высокие скорости и надежность, аппаратная реализация вытесняет программную [16].

Оценка сложности. На сложность микросхемы, наряду с количеством УВ, существенно влияет площадь трасс — внутренних соединений. В трассе обычно очень высока плотность тока — это основная причина старения и отказов. Узкие участки испаряются и оседают на широких, поэтому ширину трассы и зазора выбирают из условия равной вероятности обрыва узкой трассы и замыкания широкой. Если ширина трасс увеличивается, повышается их емкость и энергопотребление, снижается быстродействие; если уменьшается — растет сопротивление и падает надежность. Ширина и протяженность пучков трасс приблизительно пропорциональны количеству УВ, а их площадь и энергопотребление — квадрату количества УВ. Поскольку сведения по топологии (трассам) анализируемых шифраторов отсутствуют, их сложность будем оценивать снизу — только количеством УВ.

Шифраторы с двоичными РС [10—13] показали скорости шифрования, близкие к скоростям РС, которые существенно выше скоростей при многоразрядных вычислениях.

ГСЧ-39 [11, 12] содержит четыре байтовых РС и один 7-разрядный РС с нелинейными обратными связями (РСНЛ). Он создает абсолютно криптостойкие последовательности случайных чисел (ПСЧ), эквивалентные шифрблокноту объемом 2^{39} бит, равным циклу ПСЧ. Коротких циклов и слабых ключей нет. Ключ 39 бит вводят в эти РС, причем возможны два варианта. В ГСЧ-39-1 [11] использованы РС (автоматы) с нестационарными (изменяемыми) функциями обратной связи, имеющие два состояния — пары генераторных полиномов (ГП) с нелинейным управлением от того же автомата. Трудности, связанные с поиском пар ГП, не создающих коротких циклов, удалось преодолеть. Диапазон неравномерного движения автоматов от 1/4 до 1/16. Сложность — около 800 УВ. В ГСЧ-39-2 [12] введены 16-разрядный вектор управления (ВУ), выбирающий рабочие пары ГП и другие цепи ГСЧ, и 18-разрядный вектор обновления (ВО) ключа. Эти ВУ и ВО увеличили цикл ПСЧ до 2^{73} и сложность до 12 тыс. УВ.

ГСЧ-16 [13] содержит два байтовых автомата с РСНЛ, формирующих абсолютно криптостойкие байтовые ПСЧ. Ключ 16 бит. Исследованы два варианта с разным количеством пар нестационарных ГП n в каждом автомате. Количество переключателей, выбирающих пары, равно $(n - 1)$. В ГСЧ-16-1 $n = 4$. Цикл его ПСЧ (объем шифрблокнота) — 2^{41} байт. Сложность — около 600 УВ. В ГСЧ-16-2 $n = 128$ и объем цикла шифрблокнота — 2^{51} байт. У этого ГСЧ количество УВ в цепях выбора пар в автоматах возросло с 0,2 до 8 тыс. УВ, а общая сложность — до 9 тыс. УВ. Поэтому в сети пакетной имитостойкой радиосвязи ТСО [3] был реализован только первый вариант ГСЧ.

A5/2 [7] — стандарт GSM. Использует три РС длиной 64 (19 + 22 + 23) разряда с линейной обратной связью (РСЛ) и неравномерным движением. Ключ — 64 бит. Алгоритм нестойкий. Объем перебора для вскрытия ключа — 2^{40}. Сложность — около 800 УВ.

ORIX [7] — стандарт радиосвязи США. Использует три РСЛ (32 + 32 + 32) с неравномерным движением, таблицу замен 8×56 (4096 разрядов) и 8-разрядный блок фиксированных замен. Алгоритм нестойкий. Для вскрытия нужны 24 байт открытого текста и перебор 2^{16} состояний ключа. Сложность — более 20 тыс. УВ.

Шифраторы с многоразрядными вычислениями отличаются наибольшей сложностью и энергоемкостью. Они значительно уступают шифраторам

с двоичными вычислениями, так как используют пересылки многоразрядных слов [4—9], которые часто не обеспечивают криптостойкость. О скоростях их работы можно судить только косвенно — по назначению. У самых быстрых шифраторов (CHAMELEON и PANAMA — для платного телевидения) скорости существенно ниже, чем скорости ГСЧ [10—13].

AES [5, 7] — стандарт США. Реализован на микросхеме и программно. Использует 32-разрядные слова с байтовыми подстановками в таблицы замен 8×256 и в блоки замен с четырьмя таблицами. Выборка — 4-байтовое слово из 256 возможных. Выполняет в каждом из 14 раундов умножение и перемешивание столбцов состояний и поразрядное сложение по модулю 2 фрагмента текущего ключа с раундовым ключом. Алгоритм стойкий. Сложность — около 100 тыс. УВ.

ARIA [9] — стандарт Южной Кореи. Реализован на микросхеме и программно. В каждом из 14 раундов реализуется наложение ключа по модулю 2. Табличные замены для преобразований в поле Галуа 2^8 осуществляются с использованием четырех таблиц (из которых две заимствованы у AES) и с расширением ключа наложением по модулю 2 трех псевдослучайных констант размером 8×256. Алгоритм стойкий. Сложность — около 100 тыс. УВ.

CHAMELEON [7] реализован программно. Использует 64-разрядный РСЛ, чей выход поступает в таблицу замены объемом 2^{16} 64-разрядных слов. Алгоритм стойкий. Сложность — более 4 млн. УВ.

COS [7] использует РСНЛ с внутренним секретным ключом 256 бит. Несекретные ключи: внешний — 128, 192 или 256 и сеансовый — 32 бит. Вспомогательный РСЛ ввода ключа — 256 разрядов. Таблица расширения ключа — 2048 разрядов (256 байт). Две таблицы обратной связи, каждая 256 разрядов. В алгоритме обнаружены слабости. Сложность с 256-разрядным ключом — более 25 тыс. УВ.

LEVIATHAN [7] реализован программно на 32-разрядных процессорах. Использует 24 сумматора по модулю 2, 16 сумматоров по модулю 2^{32} и 32 таблицы замены с 256 элементами в каждой. Самым сложным является «дерево» блоков выбора с 15 узлами, в каждом $3 \times n$ бит ($n = 32$ для ключа 128 и $n = 64$ для ключа 256). Использует нелинейную рандомизацию с байтовыми блоками подстановок, сумматорами по модулю 2 и по модулю 256 с функциями, которые зависят от ключа. Цикл шифра — 2^{48} 32-разрядных слов (2^{53} бит). Алгоритм стойкий. Для ключа 256 бит сложность — более 60 тыс. УВ.

LILI-128 [7] содержит два РСЛ, имеющих общую длину 128 слов (39 + 89). Реализован программно. Ключ 128 бит. Циклы РСЛ ($2^{39} - 1$) и ($2^{89} - 1$). Слабых ключей (кроме 00…00) нет. Цикл шифра — около 2^{128}. Первый РСЛ управляет неравномерным движением второго (интервалы от одного до четырех тактов). На выходе второго РСЛ работает нелинейный фильтр с таблицей истинности 16×64. Обнаруженные слабости разработчики надеются устранить вводом изменяемых ГП. Сложность — около 6 тыс. УВ.

PANAMA [7] реализован программно. Содержит два РСНЛ с 32-разрядными словами. Первый — длиной 17 слов (544 разряда) и второй — с 8192 разрядами, состоящий из 32 секций, в каждой восемь групп 32-разрядных слов. Входные блоки — 256 бит. Ключ 256 бит. Использует четыре итерации — нелинейную, перестановки, диффузию и модификацию предыдущего состояния при помощи трех 256-разрядных сумматоров по модулю 2. Алгоритм стойкий. Сложность — около 50 тыс. УВ.

PIKE [7] реализован программно. Использует три РСНЛ с 32-разрядными словами общей длиной 170 слов (55 + 57 + 58) (и в каждом — нелинейную аддитивную обратную связь на сумматоре по модулю 2^{32}). Вариант неравномерного движения выбирают из четырех возможных выходов первого РСНЛ. Выход — сумма по модулю 2 выходов трех РСНЛ. Обнаружены слабости. Сложность — около 27 тыс. УВ.

RC4 [7] использует два 8-разрядных счетчика, три сумматора по модулю 2^8 и 8-разрядный блок замены с изменяемой таблицей замены 8×256. Обнаружены слабости. Сложность — более 40 тыс. УВ.

SEAL [7] реализован программно. Использует восемь РСЛ с 32-разрядными словами, память, блоки замены с общей памятью 3000 байт (24000 разрядов), четыре таблицы замены (16, 512, 256 и 1024 слов) с 32-разрядными словами общим объемом 58 тыс. разрядов и таблицу 2 Кбайта (16 тыс. разрядов), зависящую от ключа. Длина секретного ключа 160 бит плюс 32-разрядный параметр. Формирует 32-разрядные ПСЧ. Алгоритм стойкий. Сложность — более 400 тыс. УВ.

SNOW [7] содержит три РСЛ с 32-разрядными словами, каждый длиной 16 слов (всего 3×512 разрядов). Первый РСЛ управляет автоматом, который содержит два РСЛ, два сумматора по модулю 32, два 32-разрядных сумматора по модулю 2 и блок замены размером 32×32, обрабатывающий выход первого РСЛ и содержащий четыре одинаковые секции (8×32). Кроме обычного режима, возможна переменная инициализация (Initialization Variable — IV), реализуемая двумя 32-разрядными словами. Длина ключа — 256 или 128 бит. Алгоритм стойкий. Сложность — около 20 тыс. УВ.

SOBER [7] программно реализован на 8-разрядном РСЛ длиной 17 слов (136 разрядов) в режиме кольцевого буфера со скользящим индексом. Для ускорения вычислений используется двойной размер буфера РСЛ. Введены два 256-разрядных сумматора по модулю 2 и два умножения в поле 256. Возможны четыре варианта формирования байтов выхода. Ключ — 128 бит. Предназначен для мобильной радиосвязи. Алгоритм стойкий. Сложность — около 18 тыс. УВ.

SQ1-R [7] программно реализован: N-разрядный квазисчетчик, N-разрядный РСНЛ, 18 счетчиков по модулю 2^N, таблица замен S, таблица вариаций V — каждая с 2^N элементами от 0 до ($2^N - 1$) и третья таблица замен с $N2^N$ элементами. Счетчик динамически переставляет элементы таблицы и изменяет функции выхода, устраняя слабости фиксированных таблиц. Ключ 2^N — начальное заполнение таблицы замен S. Алгоритм стойкий. При $N = 8$ сложность более 30 тыс. УВ.

TWOPRIME [7] реализован программно на 32-разрядных процессорах. Содержит два 32-разрядных циклических счетчика с циклами — простыми числами, меньшими 2^{32} (на 5 и на 17), выдающими запросы в восемь байтовых блоков замен, чьи выходы преобразуют восемь сумматоров по модулю 256 и затем восемь блоков замен с байтовыми входами и 32-разрядными выходами. Их обрабатывают последовательно таблица с 256 входами и выходом 8 байт, блоки замены, поразрядные сумматоры по модулю 2, 10 сумматоров по модулю 255 и 256 и два сумматора, добавляющие две 32-разрядные константы. Ключ 128. Стойкость обеспечивают обновления счетчиков. За такт выдает 8 байт шифра. Сложность — более 25 тыс. УВ.

В обзор не включены *LUCIPHER, FEAL, IDEA, стохастические* [6, 7] и многие другие шифраторы с алгоритмами, подобными представленным в этом разделе. Интересны, но очень сложны обновления ключа. В Panama обновляют по модулю 2 три 256-разрядных сумматора. В SQ1-R, AES, стохастических шифраторах и ARIA вве-

дено перемешивание в таблицах замен. В SNOW возможен ввод переменной инициализации. В TWOPRIME обновляют 64 разряда в двух счетчиках. Одноразрядные обновления в ГСЧ [11—13] намного проще.

Итак, рекомендовать для новых разработок алгоритмы с многоразрядными вычислениями нельзя из-за большого количества УВ и сложных трассировок, пересылающих такие числа. Простейший из них — SOBER (на PC с байтовыми словами) — в 20 раз сложнее ГСЧ-39-1 [12] или ГСЧ-16-1 [13], у которых скорости выше почти в 1000 раз.

Рекомендации по разработке шифраторов. Из [17] видно, что идеи построения абсолютно криптостойких потоковых (бит на бит) аппаратных шифраторов первыми (в 1948—1951 гг.) предложили криптологи Марфинской лаборатории, преобразованной позже в НИИА. Но тогда не было технических средств для их реализации. Сегодня для создания самых простых, абсолютно криптостойких, надежных, экономичных по энергопотреблению и высокоскоростных шифраторов следует использовать:

- байтовые автоматы (от двух до шести) на двоичных регистрах сдвига длиной от 16 до 48 разрядов, подобные ГСЧ [12, 13];
- обновление ключа в автоматах путем одноразрядного сложения по модулю 2 бита с разрядом PC, которое создает случайные скачки по полному циклу состояний автомата; оно эквивалентно полной замене ключа;
- малоразрядные векторы управления и векторы обновления, выбирающие не более восьми пар нестационарных ГП и восьми адресов обновления ключа;
- интервалы обновления, много меньшие интервалов единственности;
- неравномерное движение автоматов в комплексе с упомянутыми средствами рандомизации.

Чрезмерное увеличение в ГСЧ количества выбираемых пар n нецелесообразно. Это видно на примере ГСЧ-16-2 с $n = 128$, сложность которого в 15 раз выше, чем у ГСЧ-16-1 с $n = 4$. Выбор n ограничивает условие: длина ГСЧ должна быть менее 56 бит, чтобы избежать сложного лицензирования [18].

Потоковые шифраторы с рекомендуемыми алгоритмами можно использовать в качестве блоковых, что удобно для пакетной радиосвязи в технических средствах охраны [3]. Их преимущества видны на примере ГСЧ-48 с шестью автоматами, каждый с $n = 4$. Его сложность — около 1,8 тыс. УВ. Объем цикла шифрблокнота — 2^{132}.

Разработку ГСЧ целесообразно начать с программной реализации, которую можно перенести на ПЛИС и на этом остановиться, если тираж не превышает 200—300 шт. В случае большого тиража предпочтительнее матричная БИС (МБИС). Для ее функционально-логического проекта можно использовать ПЛИС. В давно освоенной серии МБИС 5503ХМ (Зеленоград, МИЭТ) задержки у D-триггера < 5,5 нс, у XOR < 3 нс. С учетом задержек нестационарных ГП и обновлений возможна скорость шифрования на этой серии до 50 Мбайт/с, а на МБИС новой серии 5508БЦ2У — до 100 Мбайт/с и выше. Параметры МБИС: 5503ХМ1—680 УВ, 28 контактов; 5503ХМ2—1400 УВ, 42 контакта; 5503ХМ5—3000 УВ, 64 контакта. Видно, что в МБИС можно ввести цепи малоразрядных векторов обновления и управления. Скорости ГСЧ на ПЛИС и МБИС многократно превысят скорости известных шифраторов AES и ARIA, изготовленных на более быстрых микросхемах (ASIC). Цена ГСЧ-16—1 на МБИС 5503ХМ1 при малосерийных поставках — около 1 тыс. руб., а стоимость разработки — около 200 тыс. руб. Структурные схемы шифраторов на МБИС заслуживают отдельного рассмотрения.

Заключение. Рекомендованы алгоритмы самых простых, надежных, абсолютно криптостойких шифраторов с малым энергопотреблением для каналов ТСО и высокоскоростных каналов. Эти преимущества обеспечивают: байтовые автоматы на двоичных PC; нестационарные функции обратной связи; одноразрядное обновление ключа в автоматах с интервалами, меньшими интервала единственности; малоразрядные векторы обновления и управления и неравномерное движение. Рекомендованы длины ключей ГСЧ — от двух до шести байт, причем с ростом длины ключа их сложность растет линейно (от 0,6 до 1,8 тыс. УВ), а объем шифрблокнота — экспоненциально (от 2^{22} до 2^{132} байт). На отечественных МБИС возможны скорости ГСЧ около 100 Мбайт/с, для известных шифраторов недоступные.

ЛИТЕРАТУРА

1. **Мишин Е.Т.** и др. Как защитить каналы связи//Мир связи. — 1998. — № 10.
2. **Шемигон Н.Н.** и др. Использование средств криптографической защиты информации в сетях связи систем физической защиты ядерно-опасных объектов // Связь и автоматизация МВД России: сб. ст. «Информационный мост». — М., 2004.
3. **Брауде-Золотарев Ю.М.** и др. Система радиосвязи технических средств охраны / Матер. 6-й Междунар. науч.-техн. конф. «Перспективные технологии в средствах передачи информации», 2005.
4. **Иванов М.А.** Криптографические методы защиты информации в компьютерных системах и сетях. — М.: Кудиц-образ, 2001.
5. **Зензин О.С., Иванов М.А.** Стандарт криптографической защиты AES. Конечные поля. — М.: Кудиц-образ, 2002.
6. **Асосков М.А., Иванов М.А., Мирский А.А.** и др. Поточные шифры. — М.: Кудиц-образ, 2003.
7. **Иванов М.А., Чугунков И.В.** Теория, применение и оценки качества генераторов псевдослучайных последовательностей. — М.: Кудиц-образ, 2003.
8. **Шнайер Б.** Прикладная криптография. — М.: Триумф, 2002.
9. **Панасенко С.П.** Алгоритм ARIA — стандарт шифрования Южной Кореи // Мир и безопасность — 2008. — № 5.
10. **Брауде-Золотарев Ю.М.** и др. Генератор случайных чисел с высокой степенью рандомизации: тр. НИИ радио, 1997.
11. **Брауде-Золотарев Ю.М.** Перспективные пути построения шифраторов//Электросвязь. — 2004. — № 3.
12. **Брауде-Золотарев Ю.М.** Потоковый шифратор с ключом 39 бит // Электросвязь. — 2004. — № 12.
13. **Брауде-Золотарев Ю.М.** Возможно ли криптостойкое шифрование с ключом 16 бит?//Электросвязь. — 2009 г. — № 4.
14. **Алексейчук Ф.Н., Проскуровский Р.В., Скрыпник Л.В.** Статистическая атака на комбинированный генератор гаммы с неравномерным движением в режиме реинициализации начального состояния. Проблемы безопасности и противодействия терроризму: матер. конф. в МГУ 25—26 октября 2006 г. — М. МЦНМО, 2007.
15. **Панасенко С.П.** Современные методы вскрытия алгоритмов шифрования. URL: http://www.cio-world.ru/cioclubs/coding2.doc.
16. **Брауде-Золотарев Ю.М., Брауде-Золотарев М.Ю., Каблучкова А.А.** и др. Микросхема помехоустойчивого кодирования // Электросвязь. — 2002. — № 10.
17. **Калачев К.Ф.** В круге третьем. URL: http://anmal.narod.ru/kniga/soder.html.
18. Положение о лицензировании деятельности по распространению шифровальных (криптографических) средств: утверждено постановлением Правительства РФ от 29.12.2007 г. № 957.

Получено 12.12.08

Редакция приглашает читателей к дискуссии по теме «Защита информации».