УДК 621.316.97

ВОЗМОЖНО ЛИ КРИПТОСТОЙКОЕ ШИФРОВАНИЕ С КЛЮЧОМ 16 БИТ?

Ю.М. Брауде-Золотарев, научный консультант СНПО «Элерон», к.т.н.; davydov@eleron.org

Ключевые слова: *генератор случайных связей, потоковый шифратор, криптостойкость, последовательность случайных чисел.*

Введение. В основополагающей работе [1] К. Шеннон показал, что идеально стойкий шифр — это последовательность случайных чисел с длиной, равной длине шифруемого сообщения или шифровальный блокнот с используемыми один раз страницами случайных чисел, меньшими «интервала единственности» (ИЕ) шифруемого сообщения. Примеры стойких шифраторов, а также нестойких, нарушивших эти принципы, даны в [2—7]. Среди нестойких — генераторы случайных чисел (ГСЧ) потоковых шифраторов стандартов США — ORIX с регистрами 32 + 32 + 32 и Европы — GSM-A5 с регистрами 19 + 22 + 23 [5].

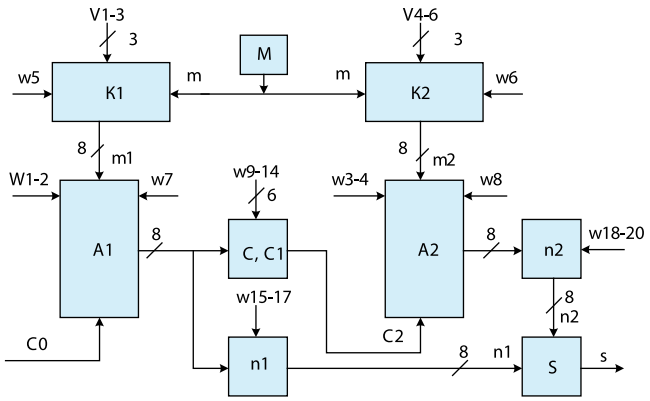
Опыт микроэлектроники показал, что интенсивность отказов регистровых микросхем при прочих равных условиях пропорциональна длине регистров и рассеиваемой кристаллом мощности. Необходимость снижения энергопотребления и длины регистров ГСЧ для технических средств охраны (ТСО) отмечена в [8, 9]. Длина регистров ГСЧ, формирующих стойкие последовательности случайных чисел (ПСЧ), была снижена с 256 (1997 г. [2]) до 39 бит (2004 г. [6, 7]). В ГСЧ-39 [7] работают четыре автомата с регистрами 8 бит и один — с регистром 7 бит. Стойкие ГСЧ можно создать из четырех, а при вводе дополнительной рандомизации — даже из трех байтовых автоматов ГСЧ-39. Но для стойкого ГСЧ с регистром 16 бит потребовался длительный поиск пар нестационарных ГП, необходимых для простой и эффективной рандомизации [10].

Алгоритм ГСЧ-16. В ГСЧ-16, как и в ГСЧ-39, использованы нелинейные и нестационарные пары ГП. В ГСЧ-39 работают 18 разрядов вектора обновления (ВО) ключа и 16 разрядов вектора управления (ВУ). В два байтовых автомата ГСЧ-16 введены всего шесть разрядов ВО. Необходимую рандомизацию в нем обеспечивают 30 разрядов ВУ благодаря найденным в [10] парам ГП. Из них 14 — выбирают рабочие пары ГП, 14 — устанавливают другие конструктивные параметры структурной схемы и 2 разряда устанавливают рабочий режим.

Программа поиска пар ГП [10] проанализировала циклы, формируемые всеми возможными парами ГП, начиная с пары (Ox00, Ox00) и заканчивая парой (OxFF, OxFF). Пары с количеством частных циклов, больших двух и с циклами короче 58 программа отбрасывала. Были найдены 164 пары ГП с частными циклами: 120 + 136 (64 пары); 77 + 179 (18 пар); 76 + 180 (18 пар) и 58 + 198 (64 пары). Эти пары ГП решили отмеченную в [4, 13] проблему хорошей рандомизации, не порождающей коротких циклов и слабых ключей. Ослабление ограничения 58 бит могло бы пополнить перечень хороших пар, но это было не нужно. Для многих задач ТСО достаточны две пары ГП в каждом автомате A1 и A2 и возможные 128 пары ГП пока нигде не потребовались.

Структурная схема ГСЧ-16. На ней (см. рис.) представлены: автоматы A1, A2; два демультиплексора K1 и K2, синхронизаторы C, C1; узлы n1 и n2 циклического сдвига, сумматор S и источник бит обновления ключей M. Рабочую пару (ГП1, ГП2) выбирают разряды ВУ w1,w2 в A1 и w3,w4 в A2. В испытательном режиме разряды ВУ w5 = w6 = 0 запрещают обновление ключа в A1 и в A2, а в рабочем режиме всегда w5 = w6 = 1. Разряды ВУ w7 = 0 и w8 = 0 разрешают слияние циклов в A1 и в A2.

Автомат A1 двигает базовая синхронизация C0 = 1. Автомат A2 двигает синхронизация C2 = 1, выбираемая в синхронизаторах C, C1 разрядами ВУ (w9—w14) из 64 вариантов. Разряды a(j) и a(j + 4) автомата A1 выбирают разряды w9—w11. Функцию C1 выбирают из четырех вариантов разряды (w12, w13): C1(01) = a(j); C1(10) = aj⊕a(j + 4); C1(11) = a(j)&a(j + 4); C1(00) = a(j)∨a(j + 4). Здесь обозначены: где ⊕ — поразрядное суммирование по модулю 2 (XOR), j + 4 — арифметическая сумма по модулю 8; & — И; ∨ — ИЛИ. Синхронизация C2 = C1⊕w14. Вероятное количество тактов синхронизации C2 относительно базовых тактов C0 у 32 вариантов — около



1/2, у 16 — около 1/4 и у 16 — около 3/4. В любом варианте C2 неравномерное замедленное движение A2 относительно A1 создает «расползание» циклов этих автоматов.

Нелинейное движение по ИЛИ в каждом автомате определяют состояния (a7, a6) двух старших разрядов. Если a7 = 1 или a6 = 1, то новое состояние автомата A = A⊕ГП1, иначе A = A⊕ГП2, а ГП1 и ГП2 — выбранная рабочая пара ГП автоматов A1 (w1, w2) и A2 (w3, w4). Новое состояние автомата A циклически сдвигаем влево на один разряд (в сторону старших разрядов) и проверяем его состояние. Если автомат достиг точки слияния (A = 00 в первом цикле или A = TC во втором) и слияние разрешено, то для A = TC выполняем TC⊕TC = 00, а для A = 00 выполняем 00⊕TC = TC, что переводит автомат в другой частный цикл и создает полный цикл. При запрете слияний (w7 = 1, w8 = 1) автомат остается в том же частном цикле. Затем в рабочем режиме (w5 = w6 = 1) мультиплексоры K1, K2 добавляют по XOR биты обновления m1 = m и m2 = m⊕1 через «полусумматоры» на выходах разрядов a(j) регистров автоматов A1 и A2. Выходы этих полусумматоров включены ко входам разрядов a(j + 1) и ко входам узлов сдвига n1, n2. Обновляемые разряды a(j) выбирают разряды v1—v6 вектора обновления (ВО). На удлиненном интервале C2 в неподвижном автомате A2 могут быть несколько обнов-

лений выдаваемых разрядов. Поэтому любой очередной бит m = 1 или m = 0 блока М на каждом такте С0 изменяет один разряд в А1 или в А2.

Испытания показали, что обновление переносит скачком состояние автомата в новую «точку» полного цикла, что величины скачков в совокупности возможных состояний автоматов и пар ГП распределены по полным циклам хаотически и что последовательности состояний А1 и А2 после обновлений эргодичны. Поэтому обновление соответствует вводу в ГСЧ нового ключа. Такая рандомизация проще и эффективнее методов, описанных в [4, 13].

Разряды ВУ w15—w17 и w18—w20 устанавливают в n1 и n2 циклический сдвиг байт (на 0—7 разрядов), выдаваемых А1 и А2 соответственно. Сумматор S суммирует поразрядно (по XOR) эти байты и выдает S-байтовую последовательность случайных чисел (ПСЧ).

В макете простейшего ГСЧ-16 его состояние устанавливают 43 разряда: 20 разрядов ВУ, 16 разрядов регистров А1 и А2, 6 разрядов ВО и один разряд М. В рабочем режиме всегда w5 = w6 = 1 и поэтому количество работающих состояний — не 2^{43}, а 2^{41}. Можно увеличить их количество до 2^{51}, увеличив количество рабочих пар в каждом автомате с четырех до 128, но это пока не потребовалось.

Циклы ГСЧ-16 и эргодичность ПСЧ. При запрете обновления и слияний длина общего цикла ГСЧ-16 благодаря неравномерному движению автомата А2 относительно А1 равна произведению длин выбранных частных циклов пар А1, А2. Коротких циклов нет. Длина минимального цикла равна 58×58 = 3364 бит. При разрешенных слияниях цикл ГСЧ-16 равен 256×256 = 2^{16}.

При обновлении ключей в ГСЧ-16 статистические характеристики участков ПСЧ разной длины не отличаются от характеристик идеальных ПСЧ той же длины, полученных от физических источников по всем критериям, включая энтропию. Предпочтение, как и в [7], отдано энтропии, которая, в отличие от другого распространенного критерия «Хи-квадрат», не требует произвольного выбора порога — критерия случайности и сразу дает численную оценку. Исследования подтвердили эргодичность ПСЧ. При увеличении длины интервала анализа ПСЧ ее энтропия приближается к 8 — энтропии идеальной ПСЧ неограниченной длины. Любой бит байта S можно использовать как эргодичную битовую ПСЧ.

Криптостойкость и имитостойкость ГСЧ-16. В [5] показано, что для коротких ключей (32—64 бит) «интервалы единственности» (ИЕ) осмысленных (не сжатых) сообщений лежат в пределах 40—75 бит. Более длинный шифр, полученный на одном ключе, профессионал, имеющий комплект специализированных микросхем, вскроет силовой атакой перебором за 2 с при ключе 40 бит и за 8 мс — при ключе 32 бита. Наиболее уязвимы для атаки повторяющиеся высокоизбыточные цифровые сообщения в ТСО. Поэтому была взята оценка ИЕ снизу — длина ключа 16 бит. В первой модели ГСЧ-16 выбран «с запасом»: интервал обновления (ИО) 8 бит существенно меньше ИЕ. Эти байты ПСЧ подобны сменным страницам шифроблокнота, заполненным шифром от идеального источника ПСЧ, что обеспечивает [1, 3—5] идеальную криптостойкость.

В ТСО передаваемые сообщения о состоянии объектов охраны считают известными аналитику, атакующему ГСЧ, и несекретными, а основная задача ГСЧ — обеспечение имитостойкости радиосети, т. е. обнаружение ложных пакетов. В ТСО структурная схема ГСЧ-16 и частотно-временные позиции (ЧВП) переданных пакетов (байты ПСЧ с выхода сумматора S) известны аналитику. Ему неизвестны выбранные состояния А1, А2, ВУ, ВО и биты *m* обновления ключа. Хаотичное распределение скачков обновления по всем точкам полных циклов не позволяет ему по наблюдениям байт ПСЧ и ЧВП на выходе ГСЧ-16 предсказать следующий байт. Эргодичная ПСЧ неотличима от случайной ПСЧ. Знание любого байта уменьшает неопределенность состояния ГСЧ в 256 раз — с 2^{41} до $2^{41-8} = 2^{33}$. Аналитик получит перебором 2^{33} равновероятных вариантов состояний ГСЧ-16, соответствующих этому байту. При накоплении последовательности *k* шифрованных байт ее неопределенность — 2^{33k} быстро растет с *k*, что не позволит ему предсказать ПСЧ и расшифровать шифр.

Бесполезно и угадывание. Для двух байт, задающих ЧВП (10 разрядов — позицию по частоте и 5 разрядов — смещение во времени), вероятность успешно угадать следующую ЧВП — 2^{-15} (около $0{,}3 \cdot 10^{-4}$). Первый же пакет на ложной ЧВП вызовет тревогу. Итак, ГСЧ-16 не позволяет предсказывать ожидаемые ЧВП и передавать на них ложные пакеты [11], что гарантирует имитостойкость сети. Отсутствие информации, необходимой для предсказаний ЧВП, обеспечивает и криптостойкость и имитостойкость ГСЧ-16.

Об оценках длины ключа ГСЧ-16. Согласно [1, 4, 5], оценкой длины ключа потокового шифратора является длина его регистров — 16 бит. Эта оценка отражена в названии статьи. Она основана на том, что внешние блоки ВУ, ВО выбирают вариант структуры шифратора, а бит обновления *m* аналогичен вводу ключа в регистры и что эти установки не увеличивают общее ключевое пространство. Такая же оценка приведена в ГОСТ 28147—89 [4], где секретная таблица замены с объемом 512 бит, используемая для взаимодействия с ключом и «расширяющая» ключ, не отнесена к ключу.

Однако некоторые криптографы считают оценки [1, 4, 5] и ГОСТ устаревшими и неприменимыми для ГСЧ-16 — шифратора нового типа, в котором секретны не только вводимые в регистры 16 бит ключа, но и 25 разрядов ВО, ВУ и М при четырех парах ГП. По их оценкам, общая длина «расширенного» ключа этого ГСЧ — 41 бит, а при 128 парах ГП в А1 и А2 — 51 бит.

Но эти разногласия не влияют на выбор областей применения ГСЧ-16, так как шифровальные криптографические средства с длиной ключа менее 56 бит, согласно [12], лицензирования не требуют. Преимущества рандомизации рассмотренного ГСЧ-16 видны при их сравнении с рандомизацией в генераторах потоковых шифраторов, описанных в [4, 5, 13].

Объем шифрблокнота (цикла) ГСЧ-16. Эргодичная ПСЧ, формируемая в макете ГСЧ-16, завершит цикл после перебора всех 2^{16} состояний регистров А1 и А2 и 2^{25} состояний ВО, ВУ и М. Объем шифрблокнота равен 2^{41} байт (2^{44} бит). После этого для гарантии непредсказуемости страниц нового шифрблокнота необходимо установить новые начальные состояния А1, А2, ВО, ВУ и М.

Работа макетов ГСЧ-16 в широкополосном (24 кГц) радиоканале ТСО [11] обеспечивает передачу на случайных ЧВП от объектов охраны (ОО) в центр охраны (ЦО) узкополосных (50 Гц) пакетов с интервалами 3 мин, а также редкую передачу пакетов от ЦО к ОО. Их прием благодаря узкой шумовой полосе (около 100 Гц) при мощности 1 мВт и скорости 50 бит/с возможен на расстоянии более 20 км. Объем 2^{41} байт не будет исчерпан за несколько тысячелетий.

Для криптозащиты радиоканалов со скоростями 1,2—9,6 кбит/с этот объем достаточен для работы в течение нескольких лет непрерывной работы. Так как ГСЧ в ЦО и во всех ОО доступны службе охраны для обновления состояния после года работы в стационарных ОО и после суток — в мобильных

ОО, то для ТСО нет необходимости увеличивать количество пар ГП и разрядность ВУ.

При реализации ГСЧ-16 на недорогом (до 30 евро за 1 шт.) отечественном кристалле МБИС 5503ХМ7 (МИЭТ, Зеленоград) возможна скорость работы около 50 Мбайт/с (400 Мбит/с). Для криптозащиты таких высокоскоростных каналов в течение года будет необходим максимальный объем шифрблокнота 2^{51} байт и 30 разрядов ВУ (28 разрядов рабочего режима). Многоразрядный корпус для такой микросхемы не потребуется, так как можно использовать последовательный ввод состояний в А1, А2, М, ВО и ВУ и даже поместить генераторы ВО и ВУ внутрь микросхемы. Приемлемым, хотя и не лучшим вариантом ВО и ВУ, может быть генератор де Брейна [4, 13] с примитивным ГП (39, 4, 0) и периодом 2^{39}, используемый в макете ГСЧ-16 для ТСО [11]. Лучшие варианты заслуживают отдельного анализа.

Заключение. В алгоритме ГСЧ-16 использованы нелинейные и нестационарные генераторные полиномы (ГП), автомат с неравномерным движением и обновление ключа с интервалами 1 байт, существенно меньшими «интервала единственности». Рабочие пары ГП и другие конструктивные параметры структурной схемы ГСЧ также изменяем на каждом байте. Все это обеспечивает идеальную криптостойкость и имитостойкость ГСЧ.

Длина цикла ГСЧ — объем шифрблокнота — 2^{41} байт. Статистические характеристики формируемых ПСЧ неотличимы от характеристик идеальных ПСЧ с той же длиной, создаваемых при помощи физических источников. ГСЧ-16 прост и при программной, и при аппаратной реализации. Его можно поместить вместе с цепями взаимодействия с каналами данных и узлами управления на недорогом отечественном кристалле и получить скорость шифрования и дешифрования до 50 Мбайт/с. Длину цикла ГСЧ-16 можно увеличить до 2^{51} байт. Возможности дальнейшего улучшения ГСЧ-16 не исчерпаны.

ЛИТЕРАТУРА

1. **Шеннон К.** Теория связи в секретных системах. Работы по теории информации и кибернетике. — М.: ИЛ, 1963.
2. **Брауде-Золотарев Ю.М. и др.** Генератор случайных чисел с высокой степенью рандомизации // Труды НИИ Радио, 1997.
3. Введение в криптографию. Под общ. ред. **В.В. Ященко**. — М.: МЦНМО, ЧеРо, 1998.
4. **Иванов М.А.** Криптографические методы защиты информации в компьютерных системах и сетях. — М.: изд-во Кудиц-образ, 2001.
5. **Шнайер Б.** Прикладная криптография. — М.: Триумф, 2002.
6. **Брауде-Золотарев Ю.М.** Перспективные пути построения шифраторов // Электросвязь, 2004. № 4.
7. **Брауде-Золотарев Ю.М.** Потоковый шифратор с ключом 39 бит // Электросвязь, 2004. № 12.
8. **Мишин Е.Т. и др.** Как защитить каналы связи // Connect, 1998. № 10.
9. **Шемигон Н.Н. и др.** Использование средств криптографической защиты информации в сетях связи систем физической защиты ядерно-опасных объектов // Связь и автоматизация МВД России. Материалы юбилейного сборника. — М.: Информационный мост, 2004.
10. **Давыдов Ю.Л., Брауде-Золотарев Ю.М., Качер И.Л.** Программы, генерирующие случайные числа. Сборник научных трудов. — М.: Федеральный центр науки и высоких технологий ФГУП СНПО «Элерон ». 2008.
11. **Брауде-Золотарев Ю.М., Давыдов Ю.Л., Косарев С.А., Шептовецкий А.Ю.** Помехоустойчивость радиосетей технических средств охраны. Материалы четвертой научно-технической конференции «Фундаментальные проблемы радиоэлектронного приборостроения» (INTERMATIC-2005).. — М.: МИРЭА, МТУСИ. 2005.
12. Положение о лицензировании деятельности по распространению шифровальных (криптографических) средств. Утверждено постановлением правительства РФ от 29 декабря 2007 г. № 957.
13. **Иванов М.А., Чугунков И.В.** Теория, применение и оценки качества генераторов псевдослучайных последовательностей. — М.: изд-во Кудиц-образ, 2003.

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

Получено 3.03.08

ПАМЯТИ ВЕРЫ ФЕДОРОВНЫ ГОРЯННИКОВОЙ

Редакция журнала понесла тяжелую утрату: 7 апреля на 62-м году жизни скоропостижно скончалась наша коллега, талантливый журналист, опытный редактор, член Союза журналистов Москвы Вера Федоровна Горянникова.

Вера Федоровна проработала с нами всего шесть лет, но кажется, что мы ее знали всегда. Интервью Веры Федоровны со специалистами отрасли отличались интересными вопросами, живым языком. Она умела слушать, расположить к откровенности, добраться до сути проблемы.

До «Электросвязи» профессиональная и творческая деятельность Веры Федоровны была связана с «Профиздатом» и «КоминфоКонсалтинг». Выпускница филологического факультета МГУ им. М.В. Ломоносова, она обладала исключительной грамотностью, чувством стиля, прекрасно справлялась с текстами, требующими литературной обработки.

В течение нескольких лет Вера Федоровна была ведущим редактором и организатором журнала «Электросвязь: история и современность». Во многом благодаря ее усилиям журнал приобрел большую популярность у наших читателей.

Общительный, деликатный, высокоэрудированный человек, Вера Федоровна снискала любовь и уважение не только сотрудников редакции и авторов, но и всех, кому посчастливилось с ней общаться.

Светлая память о Вере Федоровне — жизнерадостном, отзывчивом и доброжелательном человеке навсегда сохранится в наших сердцах.

Редколлегия и редакция журнала «Электросвязь»