Защита информации

в беспроводных технологиях

Многие разрекламированные и широко используемые средства беспроводных технологий (БТ) подвержены риску взлома. В связи с этим разработчики и потребители должны критически относиться к сертификатам и рекламе средств защиты информации. В статье рассказывается об основных опасностях, подстерегающих при эксплуатации БТ, и о лучших алгоритмах криптозащиты, имитозащиты, помехоустойчивости и надежности. Уделено внимание малому энергопотреблению и эффективному использованию выделенной полосы частот. Затрагивается вопрос аппаратной реализации БТ на микросхемах.

Юрий Брауде-Золотарев
braude-zolotarev@mail.ru

Беспроводные технологии используются в мобильной радиосвязи, сетях технических средств охраны, войсковых радиостанциях (ВРС) и гражданских каналах с ценной научной, технологической и коммерческой информацией. Растут диапазоны частот и скорости БТ (до 300 ГГц и 100 Мбит/с). На необходимость обеспечения информационной безопасности БТ обращают внимание многие ИТ-специалисты. В [6] указаны причины незащищенности ВРС Минобороны РФ от заградительных помех, от перехвата информации и навязывания ложных приказов и рекомендованы алгоритмы защиты от средств радиоэлектронной борьбы (СРБ) и для выполнения требований [11] о разработке на микросхемах конкурентной на мировом уровне аппаратуры.

Рекомендации криптографии

Следует считать заверения о криптостойкости шифратора без указания на использованный алгоритм опасным обманом, «создающим иллюзию защищенности». Для криптозащиты рекомендуются действительно случайные последовательности чисел (True Random Number Sequence, TRNS), создаваемые простыми генераторами случайных чисел на двоичных регистрах сдвига с нелинейными и нестационарными генераторными полиномами (ГП). Однако разработку таких ГП затрудняет отсутствие их теории.

Специалистами неоднократно отмечалась абсолютная криптостойкость рекомендованного К. Шенноном (Claude Elwood Shannon) шифрблокнота с однократным использованием «страниц». Абсолютно криптостойкий шифратор (АКШ) на микросхеме БИС Н1515ХМ1-888 давно разработан по заказу Минобороны СССР в составе комплекта БИС защиты ВРС от СРБ. По требованию криптоаналитиков КГБ он опубликован [12].

Следует напомнить, что для вскрытия распространенных псевдослучайных последовательностей на базе стационарных линейных и нелинейных ГП (LFSR, NLFSR) даже при неизвестной структуре ГП достаточно принять 2n их реализаций, где n — максимальная степень ГП.

Опасность сертификатов и рекламы слабых средств защиты

Наибольшие препятствия защите БТ создают сертификаты и реклама слабых средств защиты, которым доверять нельзя. Известно, что алгоритмы WEP, а затем и WPA, рекомендованные для защиты Wi-Fi, были взломаны, и в WPA-2 (IEEE 802/11i) их заменили на AES. Стандарты криптозащиты радиосвязи США (ORIX) и Европы (GSM-A5) также подвергались взлому. Шифраторы GMR-1 и GMR-2 спутниковой мобильной радиосвязи, связанной с сетями GSM и Inmarsat, сертифицированные Европейским институтом стандартов связи (ETSI) и лицензией ФСБ, выданной в августе 2010 г., взломали в январе 2012 г. Но они еще работают в мобильной спутниковой радиосвязи, связанной с сетью GSM. Шифратор РС-4 с ключом 128 бит рекомендовали часто и использовали широко. Теперь его взламывают за 3 с. В Netscape и в стандартах IEEE его заменили на AES. Для взлома шифраторов TOYOCRYPT и LILI-128 достаточно 2^{13} операций ноутбука — меньше 1 с. Шифраторы F-FCSR ввели в 2005 г. После обнаружения слабостей их преобразовали в F-FCSR-H (аппаратный) и F-FCSR-8 (программный). В сентябре 2008 г. из-за слабостей их исключили из перечня рекомендуемых.

Фирма IDC указала в Интернете, что более 70% российского рынка заняли фирмы Cisco, «Аладдин Р.Д.», Check Point, JuniperNetworks и «Код безопасности». Все они в заверяют о наилучшей криптостойкости, простоте и надежности предлагаемых программ и аппаратуры. Но ни одна фирма не сообщает о выбранных алгоритмах криптозащиты, о затрате энергии на шифруемый бит и не дает оценок их сложности, подтверждающих эти преимущества. Это указывает на слабость, сложность и низкую надежность рекламируемых средств.

Алексей Синцов (Digital Security) указал на слабости защиты в Google, «Яндексе» и программах дистанционного банковского обслуживания. Их быстро устранили Google и Яндекс. Но слабости программ телебанкинга, позволяющие хакерам подделывать электронные

цифровые подписи и готовить мошеннические платежные поручения, создатели этих сервисов не устраняют уже более двух лет.

Итак, получается, что многие разработчики, изготовители и потребители шифраторов не понимают, что только АКШ гарантируют защиту информации, а реклама и сертификаты других шифраторов, более сложных, чем АКШ, защиту не гарантируют.

Абсолютно криптостойкие шифраторы

Определенные теоретически преимущества двоичных регистров сдвига с нелинейными и изменяемыми случайно нестационарными ГП на практике впервые показал АКШ [12]. Заказчик указал на непригодность БИС ГОСТ-28147-89 для защиты ВРС от СРБ из-за ее большого энергопотребления и частых отказов этих БИС в непрерывно работающих ВРС и потребовал снизить энергопотребление не менее чем в 10 раз, так как мерой старения является потребленная энергия. Фактически энергопотребление БИС АКШ около 0,01 относительно БИС ГОСТ того же изготовителя при равных ключах и скоростях шифрования, и его надежность в 100 раз выше БИС ГОСТ.

Реализуют АКШ 1,4 тыс. условных вентилей (УВ) и короткие трассы. Один УВ — четыре транзистора. Все цепи рандомизации используют меньше 70 УВ. Особенностями АКШ являются «кроссинговер» (обмен секциями регистров сдвига автоматов) и «реверс» («зеркальное» изменение ГП автомата). Эти простые средства изменяют содержимое («ключ») и аппаратную структуру автоматов. Преимущества АКШ [12] относительно ГОСТ отметили криптоаналитики НИИ Минобороны, КГБ и ФАПСИ. Для замены ГОСТ они рекомендовали создать АКШ, простые также программно, ввиду сложности программной реализации кроссинговера и реверса на средствах, использующих ГОСТ. Такие АКШ созданы и описаны в [6, 13].

Испытания вариантов нестационарных ГП на двоичных регистрах сдвига разной длины показали преимущества ГП на регистрах сдвига длиной 8 бит с нелинейностью на простейших двухвходовых элементах «И», «ИЛИ». Из-за отсутствия теории «хорошие» пары нестационарных ГП с двумя циклами (не короче 50) сначала искали вручную. Затем полным перебором группой ПЭВМ были получены и опубликованы 164 пары хороших нестационарных и нелинейных ГП для байтовых регистров сдвига и восемь пар для семиразрядных без коротких циклов.

Первый простой программно АКШ с ключом 39 на пяти РС (8×4+7) содержит меньше 800 УВ и эквивалентен шифрблокноту объемом 2^{39} бита [14]. Этот объем можно увеличить до 2^{73}, усложнив АКШ до 1,2 тыс. УВ введением дополнительных цепей рандомизации. У АКШ с наименьшим ключом 16 бит сложность меньше 800 УВ, а объем шифрблокнота 2^{41} байт. Этого достаточно для непрерывной работы со скоростью 16 кбит/с в течение 30 лет. Для АКШ с ключом 256 бит нужно около 3 тыс. УВ. Он сложнее АКШ [12] вдвое, но проще и надежнее БИС ГОСТ в 50 раз и быстрее более чем в 100 раз [13].

Испытания показали, что замена пар ГП и обновление разрядов регистров сдвига переносят состояние АКШ скачком в новую «точку» полного цикла (что соответствует вводу нового ключа) и что величины скачков в полных циклах автоматов распределены хаотически и последовательности состояний байтовых регистров сдвига эргодичны. В [13] показаны преимущества этих простых программно и аппаратно АКШ в сравнении с другими шифраторами, включая стандарты AES и ARIA. Очевидно, что АКШ [13] могут обеспечить информационную безопасность всех БТ. Минобороны РФ и ВНИИС (ныне концерн «Созвездие») знают об АКШ [12] более 22 лет и об АКШ [14] более семи лет и могли бы этими АКШ защитить ВРС наиболее просто, но выбирали нестойкие и сложные зарубежные алгоритмы. В [15] отмечено, что алгоритмы не защищенных от СРБ новых ВРС выбраны для «карманных интересов больших начальников» и завышения стоимости разработок.

Предпочтительные структуры сигналов для БТ

Выбор структур сигналов в БТ — модуляции, помехоустойчивого кодирования и криптостойкой расстановки пакетов — имеет важное значение [3–6, 13, 16]. Даже на малых расстояниях (несколько метров) многие фирмы используют сверхширокополосные сигналы с частотно-временными позициями пакетов (Frequency Hopping и Time Hopping, FH и TH), устанавливаемыми случайно AES [10]. Для многих БТ, включая ВРС, возможна частая смена ключей, источников питания и редкая передача сигналов, но для технических средств охраны периметров необходим год работы передатчика с регулярной передачей сигналов контроля без замены питания и ключей. В технических средствах охраны [16] использованы случайные частотно-временные позиции пакетов, управляемые АКШ. Количество TH — 32 при среднем интервале 3 мин. и около 1000 FH в полосе частот 48 кГц. Защита от заградительных помех (ЗП) при этом около 90 дБ. Случайные частотно-временные позиции лучше других защищают от СРБ и имеют наивысшую помехоустойчивость при наименьшей энергии бита. В [16] рекомендована офсетная фазовая модуляция (ОФМ-4) с модулирующими квадратурными компонентами, сдвинутыми на половину такта. Она значительно улучшает условия обнаружения и синхронизации. Рекомендовано использовать наиболее короткие широкополосные пакеты с наибольшим количеством позиций во времени, допускаемым ограничениями разрешенной мощности передачи [16].

Теория и техника помехоустойчивого кодирования

Для надежной защиты информации в БТ необходимо помехоустойчивое кодирование [6, 16]. Преимущества кодеров и декодеров (кодеков) на двоичных регистрах сдвига с малой плотностью проверок на четность (Low Density Parity Check, LDPC) известны давно. В [17] описан кодек на микросхеме 5503ХМ7-158 с ПН 1,5 мкм (Зеленоград, ТЦ МИЭТ), разработанный по заказу Минобороны РФ для спутникового канала беспилотника. Он реализован на базе LDSR — совершенного разностного множества СРМ-133, укороченного до 99, с кодовой скоростью R = 1/2. Кодек не уступает по помехоустойчивости кодеку СРМ-553 челнока «Буран» благодаря нестационарным ГП с двумя ветвями кодирования. Его сложность — около 5 тыс. УВ, энергопотребление — около 20 мкДж/бит и энергетический выигрыш кодирования более 4 дБ. Кодек устойчив к большим помехам, а его синхронизация устойчива при действии плотного (до 50%) пакета ошибок длиной до 25 бит. Эти преимущества ценны для всех БТ, а особо — для защиты технических средств охраны и ВРС, от заградительных помех (ЗП) и помех от наложений пакетов со случайными частотно-временными позициями ЧВП. Недостатки — работа с длинными пакетами (не менее 99 бит) и использование жесткого решения.

Для БТ с низкоскоростной речью предпочтителен блоковый кодек (16, 8) [18] с байтовыми информационными блоками и с оптимальным синдромным декодированием (ОСД). Он хорошо работает с ЧМ и ФМ, при негауссовских помехах и при ЗП. Он проще кодеков БЧХ при лучшей помехоустойчивости.

В [19] показано, что у кодеков Рида-Соломона вычисления в многоразрядных полях Галуа очень сложны, и также сложны турбо-кодеки. У них энергопотребление и надежность хуже, чем у кодеков [17, 18], более чем в 50 раз, а помехозащита слабее. В [20] приведен пример микросхемы AHA4541, показывающий сложность итеративных турбо-кодеков.

О необходимости цифрового кодирования речи

В беспроводных технологиях часто используют передачу речи. Надежно защитить речь и значительно увеличить количество каналов БТ могут только цифровые кодеки. Аналоговую речь быстро вскрывают средства, основанные на ее статистической избыточности. Для лучшей защиты от помех и лучшего использования ресурсов канала связи предпочтительнее низкие скорости речи S, но у них баллы качества b обычно ниже. В [21] дан анализ кодеков речи, включающий:

- MELP (IEEE MILCOM 2001) с S = 0,6, 1,2 и 2,4 кбит/с, b = 2,7, 3,1 и 3,45;
- ADPCM (G.728) с S = 32 кбит/с, b = 3,6;
- LD CELP с S = 3.8 кбит/с, b = 3,8;
- CS CELP с S = 8 кбит/с, b = 3,9;
- LPC-10 с S = 2,4 кбит/с, b = 2,9;
- MP MLQ (Multi Pulse Maximum Likehood Quantization) G.723.1 с S = 6,3 кбит/с, b = 3,9 и др.

У лучшего из них — кодека MP MLQ — скорость в пять раз меньше, чем у ADPCM при лучшем качестве. Он реализован на СБИС.

Анализ показывает, что возможно создание алгоритмов цифровой речи, лучших, чем MP MLQ. На разработку низкоскоростных кодеков речи ФСБ утвердило ТЗ [22], в п. 3.2.1 которого заданы скорости 300, 600, 1000, 1200, 2400, 4800 и 9600 бит/с. Срок завершения ОКР — сентябрь 2012 г.

Принципиальные недостатки войсковых радиостанций (ВРС)

В [6] показана незащищенность ВРС от СРБ и для надежной защиты предложены алгоритмы, описанные в [13, 14, 17, 18]. Войсковые испытания ВРС шестого поколения (ВРС-6), изготовленных «Созвездием» по НИОКР «Единая система управления тактического звена» (ЕСУ ТЗ), показали,

что они не защищены от СРБ [15]. В этих ВРС-6 использована архитектура программно определяемого радио (Software-Defined Radio, SDR), которая сочетает АЦП и процессор. Возник SDR в программе Speak Easy (США), но из-за высокого энергопотребления и низкой надежности его в Америке не используют. Однако и «Ангстрем» использовал алгоритм SDR в ВРС-6 «Азарт». О сложности использованных в ВРС-6 алгоритмов сведений нет. Ясно только, что доступная «Ангстрему» информация по АКШ [12–14] и кодекам [16–18] не использована. Вместо АКШ применен неназванный криптоалгоритм, несмотря на риск его взлома. Не защищен от СРБ и рекламируемый УНКВ [23].

Выбрали SDR в ЕСУ ТЗ из-за рекламы многих выполняемых функций, эффектных для некомпетентных чиновников Минобороны, но ненужных для ВРС тактического звена, которые существенно усложнили ВРС-6: связь с сетями Wi-Fi, WiMAX, Mech и связь с сотовыми телефонами. Из-за очень сложных демодуляторов сигналов QAM-16, QAM-64 и турбо-кодеков сложность этих ВРС-6 выше по меньшей мере в 200 раз, чем при использовании рекомендованных в [6] алгоритмов. Из [10] видно, что ни одна фирма для сверхширокополосных сигналов SDR не использовала.

По криптозащите, имитозащите, энергопотреблению, помехоустойчивости и надежности алгоритмы ВРС-6 с SDR непригодны ни для тактического звена, ни для гражданских БТ с передачей ценной научной, технологической и коммерческой информации. Рекомендовать эти алгоритмы для БТ нельзя. Чтобы скрыть эту непригодность ВРС-6, сведения о сложности выбранных в SDR криптозащите, цифровом кодеке речи и других конкретных узлах скрывают. О таком умолчании академик АН СССР А. И. Берг говорил: «…для иных структур главным охраняемым секретом является их некомпетентность». Несмотря на незащищенность ВРС-6 с SDR [15], Минобороны заказал «Ангстрему» поставку в 2012 г. 2500 шт. ВРС-6 «Азарт».

Разработка беспроводных технологий на микросхемах

Постановление Правительства РФ № 809 от 26.11.07 [11] требует разработок на микросхемах аппаратуры, конкурентной на мировом уровне. В нем п. 66 предусматривает освоение проектных норм микросхем: к 2011 г. — 0,18 мкм, после 2011 г. — 0,090 мкм, а в 2015 г. — 0,045 мкм. В п. 137 поставлена задача на базе проектных норм 0,045 мкм увеличить скорости обмена и передачи информации, включая шифрование/дешифрование до 30 Гбит/с. Такая скорость доступна только для алгоритмов АКШ. Разработка на микросхемах продукции, конкурентной на мировом уровне, поручена многим предприятиям, и среди них — концерну «Созвездие» (п. 195 и п. 196). Выбранные для ВРС-6 алгоритмы SDR не позволят это выполнить.

Несколько российских фирм уже перешли к специализированным микросхемам [10], они смогут создать ВРС и другие средства БТ, конкурентные на мировом уровне, на базе алгоритмов [6] или лучших. «НИИ полупроводниковых приборов» (Томск) разработал комплект интегральных микросхем для сверхширокополосных сигналов со случайными частотно-временными позициями диапазона 3,1–5,1 ГГц с частотами выше 30 ГГц, реализующий преобразователи, УПЧ, векторные модуляторы, демодуляторы, частотные и фазовые детекторы и др. со скоростью до 100 Мбит/с в диапазоне до 15 ГГЦ. Случайные сигналы управления этих частотно-временных позиций не описаны. Омский НИИ приборостроения разработал для ВРС и радиоцентра микросхемы типа «система-на-кристалле» (SoC) и реализовал на них более сложные алгоритмы, чем рекомендованные в [6].

НПК «Технологический Центр МИЭТ» (ТЦ МИЭТ) разработал библиотеки элементов микросхем, содержащие цифровые и аналоговые узлы тракта приема и передачи, необходимые для защиты БТ. На одном кристалле можно поместить все узлы БТ и ВРС, защищенных от СРБ и конкурентных на мировом уровне. С новыми проектными нормами, предусмотренными в [11], эти библиотеки уже в 2012 г. обеспечат диапазон до 1 ГГц, а в 2015 — до 6 ГГц и выше. Будет доступна емкость БИС до 10 млн УВ. На таких БИС можно поместить все узлы БТ, реализующие алгоритмы, рекомендованные в [6, 10], вместе с кодеками цифровой передачи речи и с передачей высокоскоростных пакетов со случайными ЧВП.

Заключение

Алгоритмы, реализующие с малым энергопотреблением и высокой надежностью абсолютно криптостойкие шифраторы, случайную расстановку позиций сигналов по частоте и времени, фазовую модуляцию ФМ-4, помехоустойчивое кодирование и цифровую речь, например MP MLQ, известны давно. Главная причина разработок очень сложных БТ и ВРС, не защищенных от СРБ и непригодных для тактического звена, — некомпетентность заказчиков и разработчиков, выбирающих неэффективные алгоритмы. Следствием их отказов от сравнения алгоритмов стала разработка дорогих и ненадежных ВРС 6-го поколения, не защищенных от СРБ. Возможно, что эта статья поможет остановить выпуск не защищенных от СРБ, ненадежных и дорогих БТ на процессорах и разработать на отечественных микросхемах БТ и ВРС, защищенные от СРБ и конкурентные на мировом уровне. Ожидаемая сложность, энергопотребление и цена у них будут на порядок ниже, а надежность — на порядок выше, чем у новых ВРС-6.

Литература

1. Алексеев В. Высокоскоростные сети мобильной связи поколения 3G // Беспроводные технологии. 2011. № 1–2.
2. Радько Н. М., Козленко Н. И., Мокроусов А. Н. Обеспечение безопасности информационного обмена в мобильной радиосвязи // Радиотехника. 2011. № 9.
3. Шемигон Н. Н. и др. Использование средств криптографической защиты информации в сетях связи систем физической защиты ядерно-опасных объектов. Сб. «Связь и автоматизация МВД России». М.: Информационный мост. 2004.
4. Брауде-Золотарев Ю. М., Максимов С. А., Руднев А. Н., Соколов Е. Е. Защита каналов технических средств охраны // Системы безопасности. 2002. № 5.
5. Давыдов Ю. Л. и др. Имитостойкие радиоканалы технических средств охраны // Транспортная безопасность и технологии. 2007. № 4 (33).
6. Брауде-Золотарев Ю. М. Алгоритмы надежной защиты радиостанций от средств радиоборьбы // Электросвязь. 2010. № 11.
7. Красоткин А. Секреты в воздухе витают // Беспроводные технологии. 2011. № 2.
8. Красоткин А. Радиомираж // Беспроводные технологии. 2011. № 4.
9. Маргарян С. Технологическая сеть обмена данными УКВ-диапазона // Беспроводные технологии. 2011. № 4.
10. Брауде-Золотарев Ю. М. Алгоритмы и технологии сверхширокополосных сигналов // Радиотехника. 2011. № 9.
11. Постановление Правительства РФ №809 от 26.11.07 «Развитие электронной компонентной базы и радиоэлектроники на 2008–2015 гг.».
12. Брауде-Золотарев Ю. М. и др. Генератор случайных чисел с высокой степенью рандомизации // Науч. труды НИИ радио. 1997.
13. Брауде-Золотарев Ю. М. Абсолютно криптостойкие и самые простые шифраторы // Электросвязь. 2010. № 3.
14. Брауде-Золотарев Ю. М. Потоковый шифратор с ключом 39 бит // Электросвязь. 2004. № 12.
15. Кандауров Д. Комплекс ЕСУ ТЗ: желаемое и действительное //Армейский вестник. 23.11.2011.
16. Брауде-Золотарев Ю. М., Давыдов Ю. Л., Косарев С. А., Шептовецкий А. Ю. Помехоустойчивость радиосетей технических средств охраны // Мат. IV НТК «Фундаментальные проблемы радиоэлектронного приборостроения» Intermatic-2005. Москва. МИРЭА, МТУСИ.
17. Брауде-Золотарев Ю. М., Брауде-Золотарев М. Ю., Каблучкова А. А. и др. Микросхема помехоустойчивого кодирования канала // Электросвязь. 2002. № 10.
18. Брауде-Золотарев Ю. М., Лаврентьев М. А. Помехоустойчивое кодирование радиоканалов // Радиотехника. 2004. № 6.
19. Марселос-Сарагоса Р. Искусство помехоустойчивого кодирования. Методы, алгоритмы, применение. М. Техносфера. 2006.
20. Архипкин А. Турбо-коды — мощные алгоритмы для современных систем связи // Беспроводные технологии. 2006. № 1.
21. Рихтер С. Г. Кодирование и передача речи в цифровых системах подвижной радиосвязи. М.: Радио и связь. 2011.
22. Техническое задание на ОКР «Разработка перспективного радиомодема, обеспечивающего помехоустойчивое кодирование и передачу речевых сигналов по каналам связи с ограниченной пропускной способностью». Шифр «Ц-2010-08-7.3», в/ч 35533, в/ч 43753-Р, в/ч 68240.
23. Осицкая Т. В. УНКВ — направление будущего // Связист (концерн «Созвездие»). 2011. № 22.