О применении шифрования при разработке энергоэффективных УКВ приемопередатчиков

Н. С. Соколов, А. Б. Степанов*

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

*sabarticle@yandex.ru

Аннотация. **Статья посвящена применению шифрования при разработке энергоэффективных УКВ приемопередатчиков на основе технологии LoRa. Рассматриваются наиболее перспективные методы шифрования, предназначенные для IoT. Приводится обоснование выбора микроконтроллера STM32F051R8T6 для реализации энергоэффективных УКВ приемопередатчиков, позволяющего выполнять шифрование. В качестве метода шифрования для данного микроконтроллера предлагается использовать Grain-128a.**

Ключевые слова: энергоэффективные приемопередатчики; технология LoRa; УКВ; Advanced Encryption Standart; Elliptic Curve Cryptography; Grain-128a; ChaCha20; PRESENT.

I. Введение

При создании любого устройства связи перед проектировщиком неминуемо возникает проблема несанкционированного доступа к передаваемым данным. Основным же методом борьбы со злоумышленниками при передаче данных является их шифрование. Актуальной задачей является разработка энергоэффективных УКВ приемопередатчиков, в которых обеспечивается защита передаваемых данных за счет применения передовых методов шифрования.

На первый взгляд, выбор метода шифрования может представляться тривиальной задачей, сводящейся к применению наиболее защищенного алгоритма. Действительно, существует возможность использования криптографических методов, обеспечивающих практически абсолютную безопасность сегмента сети. Однако в большинстве практических случаев при проектировании телекоммуникационного оборудования, такого как передатчики и приемники, возникают существенные ограничения, связанные с габаритами устройств, вычислительными ресурсами применяемой элементной базы и ее энергопотреблением.

В настоящей работе анализируются методы криптографической защиты данных, после чего на основе теоретического исследования предлагается наиболее подходящий шифр для внедрения в перспективное устройство связи, реализуемое на базе технологии LoRa.

Для реализации вычислительных задач устройства при выполнении шифрования необходимо выбрать энергоэффективный микроконтроллер с высокой тактовой частотой, развитой периферией и невысокой стоимостью. Из представленных на рынке вариантов можно выделить устройства компаний Texas Instruments, STMicroelectronics, Microchip Technology Inc., Espressif Systems, АО «ПКК Миландр» и др.

Проведенный анализ публикаций показал, что при шифровании данных с использованием низкопроизводительной элементной базы наибольшее распространение получили методы: Advanced Encryption Standart, Elliptic Curve Cryptography, Grain-128a, ChaCha20, PRESENT [1–6].

1. Advanced Encryption Standart (AES) – симметричный блочный шифр. Алгоритм преобразует блок данных фиксированного размера (128 бит) с использованием ключа длиной 128 бит, 192 бит или 256 бит. Основан на методе шифрования Rijndael. Преимуществами данного шифра являются широкое распространение и стандартизация, энергоэффективность, высокая скорость шифрования. К недостаткам метода можно отнести сложность безопасного распределения ключей и уязвимость к атакам по сторонним каналам [1].

2. Elliptic Curve Cryptography (ECC) – криптография на эллиптических кривых. Метод ассиметричного шифрования с помощью использования теории множеств, геометрии и модулярной арифметики. Может использоваться для безопасного обмена AES-ключами между устройствами. Основным преимуществом шифра можно назвать очень высокую криптографическую устойчивость. Данный метод имеет существенный недостаток – высокую вычислительную сложность [2].

3. Grain-128a – метод шифрования, сочетающий потоковое шифрование и аутентификацию. Шифр был специально разработан для маломощных устройств, позволяя не тратить дополнительные ресурсы устройства на систему проверки подлинности сообщений. К преимуществам метода можно отнести крайне высокую скорость шифрования, реализация занимает менее 1 Кб памяти. Данный метод менее изучен по сравнению с другими шифрами [3-4].

4. ChaCha20 – симметричный потоковый метод шифрования. Современный способ шифрования данных, который позволяет получить значительное ускорение шифрования на малопроизводительной элементной базе без аппаратного ускорения. К преимуществам метода можно отнести высокую скорость шифрования по сравнению с другими методами на элементной базе без аппаратного ускорения, используется в современных IoT-протоколах и достаточно устойчив. Данный метод менее распространен и протестирован по сравнению с другими аналогами. К существенным недостаткам можно отнести то, что повторное использование одноразового числа (nonce) приводит к полной утере безопасности системы и достаточно большой размер кода (занимает примерно 3–5 Кб памяти) [5].

5. PRESENT – облегченный симметричный блочный шифр, разработанный специально для ресурсоограниченных устройств. Метод оперирует 64-битными блоками данных и поддерживает ключи длиной 80 бит или 128 бит, выполняя шифрование за 31 этап преобразований. Преимуществами данного метода являются минимальное использование ресурсов микроконтроллера и высокая скорость шифрования. Также благодаря оптимизированной структуре шифр потребляет минимальное количество энергии, что критически важно при проектировании устройств связи. Метод специально разрабатывался как один из самых компактных и простых в реализации криптоалгоритмов, что привело к малой длине ключа, а следовательно, и относительно низкой криптографической стойкости метода. PRESENT – современный метод шифрования, поэтому несмотря на формальное подтверждение стойкости, шифр не прошел многолетнего тестирования в реальных системах [6].

Целью данной работы является выбор и обоснование метода шифрования наиболее пригодного для применения при разработке энергоэффективных УКВ приемопередатчиков на базе технологии LoRa.

II. Выбор микроконтроллера для разработки энергоэффективных приемопередатчиков

Минимальный набор элементов для реализации энергоэффективного приемопередатчика включает в себя микроконтроллер, модуль LoRa, антенну, элементы, позволяющие осуществлять ввод и вывод данных.

При разработке приемопередатчиков могут применяться различные микроконтроллеры [7-8]. Приведенный обзор позволил определить микроконтроллеры, обладающие требуемыми характеристиками и низкой стоимостью:

- MSP430F149IPMR – 16 разрядный микроконтроллер, разработанный компанией Texas Instruments. Обладает тактовой частотой 8 МГц, ПЗУ – 60 Кб, ОЗУ – 2 Кб и сверхнизким энергопотреблением ~0,1 мА в активном режиме.
- STM32F051R8T6 – 32 разрядный микроконтроллер компании STMicroelectronics на базе Cortex-M0. Имеет тактовую частоту 48 МГц, ПЗУ – 64 Кб, ОЗУ – 8 Кб и низким энергопотреблением ~0,5 мА в активном режиме.
- ATmega328P-AU – 8 разрядный микроконтроллер, выпускаемый компанией Microchip Technology Inc. Обладает тактовой частотой 20 МГц, ПЗУ – 32 Кб, ОЗУ – 2 Кб, энергопотреблением ~5 мА.
- K1986BE92F1I – 32 разрядный микроконтроллер, разработанный российской компанией АО «ПКК Миландр» на базе Cortex-M3. Имеет тактовую частоту 80 МГц и внушительную ПЗУ – 128 Кб, ОЗУ – 32 Кб. А также энергопотребление ~10 мА. Стоимость данного микроконтроллера значительно выше ранее рассмотренных.

Анализируя приведенные характеристики в данной работе, предлагается использовать при разработке энергоэффективных приемопередатчиков на базе технологии LoRa микроконтроллер STM32F051R8T6. Данный микроконтроллер обеспечивает баланс между производительностью, энергоэффективностью и экономической целесообразностью.

III. Выбор метода шифрования

Рассмотрим возможность применения описанных ранее методов при использовании микроконтроллера STM32F051R8T6.

1. Advanced Encryption Standart (AES) – при использовании ключа длиной 128 бит на ядре Cortex-M0 скорость обработки данных составляет примерно 40–60 cpb (cycles per byte).

2. Elliptic Curve Cryptography (ECC) – применение данного метода с использованием микроконтроллера STM32F051R8T6 потребует значительных вычислительных ресурсов, что может привести к работе алгоритма не в реальном времени.

3. Grain-128a – при использовании метода на ядре Cortex-M0 скорость обработки данных составляет примерно 5–10 cpb.

4. ChaCha20 – при использовании шифра на ядре Cortex-M0 скорость обработки данных составляет примерно 20 cpb.

5. PRESENT – скорость обработки данных при использовании ядра Cortex-M0 в среднем составляет 15 cpb.

Оптимальный криптографический алгоритм должен обеспечивать баланс между вычислительной сложностью, уровнем безопасности и скоростью шифрования (рис. 1).

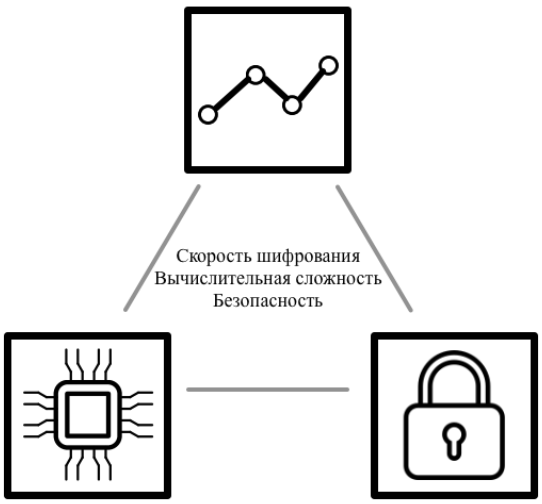

Рис. 1. Основные принципы выбора метода шифрования

Выбор оптимального соотношения этих параметров определяется спецификой конкретной системы. В ряде случаев необходимо уделить особое внимание безопасности, даже если это повлечет значительное повышение требований к производительности. В некоторых устройствах, наоборот, допустимо ограничиться элементарными алгоритмами защиты для максимального увеличения скорости шифрования.

В рамках данного исследования жесткие ограничения по указанным параметрам отсутствуют, что позволяет реализовать компромиссное решение: обеспечение

достаточного уровня защиты данных без критического ухудшения производительности устройства.

На основании приведенных преимуществ и недостатков криптографических алгоритмов с учетом заданных ограничений и требований системы, можно определить оптимальный метод защиты данных. Для проектируемого энергоэффективного приемопередатчика на базе технологии LoRa и микроконтроллера STM32F051R8T6 наиболее предпочтительным представляется шифр Grain-128a, который обеспечивает:

- достаточный уровень криптографической стойкости;
- минимальное влияние на производительность конечного устройства;
- расширенную функциональность, сочетающую шифрование данных и аутентификацию сообщений в рамках единого криптографического механизма.

Ключевым же преимуществом данного метода является его высокая производительность на маломощных микроконтроллерах, что особенно значимо для энергоэффективных устройств с длительным автономным режимом работы.

Рассмотрим алгоритм шифрования Grain-128a более подробно.

В рамках статьи алгоритм представлен в упрощенном виде, для лучшего понимания основных принципов и преимуществ данного метода шифрования. На рис. 2 приведена структурная схема алгоритма шифрования Grain-128a.

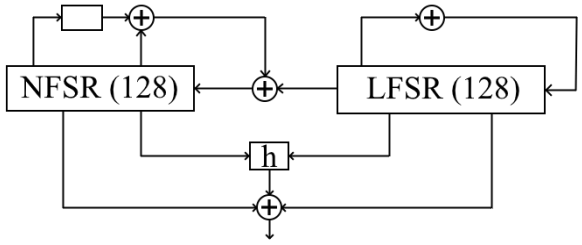

Рис. 2. Структурная схема алгоритма шифрования Grain-128a

Структурная схема алгоритма шифрования Grain-128a включает в себя:

- 128-битный LFSR (Linear Feedback Shift Register) – линейный регистр сдвига;
- 128-битный NFSR (Nonlinear Feedback Shift Register) – нелинейный регистр сдвига;
- выходную функцию;
- механизм аутентификации.

На рис. 3 приведена структурная схема механизма аутентификации рассматриваемого алгоритма.

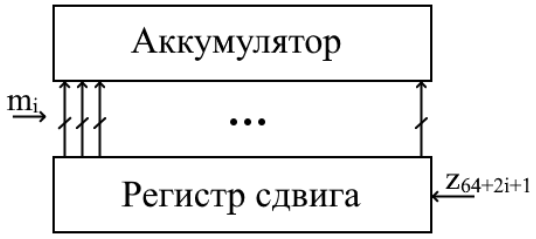

Рис. 3. Структурная схема механизма аутентификации Grain-128a

В качестве первого шага алгоритма шифрования происходит инициализация ключей (Key Loading). NFSR заполняется ключом: NFSR = (k_0, k_1, …, k_{127}). LFSR же заполняется специальным вектором инициализации IV – уникальным 96-битным номером, который создается перед каждым новым сообщением, обеспечивая уникальность шифрования каждого пакета данных, 31 битом единиц (0xFF, 0xFF, 0xFF) и последним битом (128-ым) всегда равным 0. Таким образом, LSFR приобретает следующий вид:

[IV (12 байт), 0xFF, 0xFF, 0xFF, 0x7F].

После чего алгоритм выполняет 256 тактов без вывода ключевого потока (Warm-up). Этот этап необходим для того, чтобы злоумышленник не мог узнать ключ исходя из ключевого потока. Фаза Warm-up позволяет устранить предсказуемость начального состояния шифрования.

Затем осуществляется генерация ключевого потока – последовательности псевдослучайных битов, по формуле:

$$Z_t = h(x) + y + \sum_{i \in A} l_{t+i},$$

где: $h(x)$ – нелинейная комбинация из регистра NFSR с фиксированными позициями:

$$h(x) = x_{t+12} + x_{t+95} + x_{t+12}x_{t+8} + x_{t+13}x_{t+20} + x_{t+95}x_{t+42} + x_{t+12}x_{t+95}x_{t+14};$$

y – линейная компонента LFSR с фиксированной позицией l_{t+93}; A – фиксированный набор позиций (A = {2, 15, 36, 45, 64}); t – номер текущего такта.

Таким образом обеспечивается устойчивость алгоритма: $h(x)$ вносит нелинейную компоненту, защищая поток от линейного криптоанализа, y вносит линейную компоненту, защищая поток от нелинейного криптоанализа, а использование суммы из фиксированных позиций обеспечивает дополнительную защиту, делая итоговый ключевой поток полностью непредсказуемым.

Сразу после генерации Z_t происходит сдвиг регистров LFSR и NFSR, чтобы исключить возможность предсказания алгоритма вычисления Z_t.

Для LFSR: $l_{t+128} = l_{t+96} + l_{t+81} + l_{t+70} + l_{t+38} + l_{t+7} + l_t$;

Для NFSR: $x_{t+128} = z_t + l_t + \sum_{j \in B} x_{t+j} + h(x_t)$,

где B – фиксированный набор позиций (B = {0, 26, 56, 91, 96}).

После процесса генерации псевдослучайных битов происходит смешивание бита данных с ключевым битом с помощью операции «исключающее ИЛИ».

Аутентификация сообщений в Grain-128a реализована параллельно операции шифрования. Биты незашифрованного сообщения (m_i) сравниваются с битами ключевого потока (z_i). В случае если m_i = 1 данные находящиеся в z_i заносятся в аккумулятор. Математически эту операцию можно представить следующим образом:

$$Acc = \sum_{i=0}^{n-1} m_i z_{64+2i+1},$$

где n – длина сообщения в битах.

Анализ метода шифрования позволяет выделить два ключевых преимущества с точки зрения его реализации:

- концептуальная простота рассматриваемого метода;
- вычислительная простота – низкие вычислительные затраты микроконтроллера на реализацию шифра.

IV. Заключение

Метод шифрования Grain-128a наилучшим образом подходит для обеспечения высокого уровня защиты при использовании 128-битного ключа и предъявляет минимальные требования к производительности микроконтроллера STM32F051R8T6. Это делает его наиболее пригодным для реализации в разрабатываемом энергоэффективном приемопередатчике на базе технологии LoRa.

Список литературы

[1] Joan Daemen, Vincent Rijmen. The Design of Rijndael: AES – The Advanced Encryption Standart. Springer, 2002, 253 с.

[2] An Liu, Peng Ning. TinyECC: A Configurable Library for Elliptic Curve Cryptography in Wireless Sensor Networks. Department of Computer Science. North Carolina State University: IEEE, 2010, 17 с.

[3] Martin Ågren, Martin Hell, Thomas Johansson, Willi Meier. A New Version of Grain-128 with Autentication. Symmetric Key Encryption Workshop 2011: Department of Electrical and Information TechnologyELLIIT: the Linköping-Lund initiative on IT and mobile communication, 2011, 19 с.

[4] Yosuke Todo, Takanori Isobe, Willi Meier, Kazumaro Aoki, Bin Zhang. Fast Correlation Attack Revisited - Cryptanalysis on Full Grain-128a, Grain-128, and Grain-v1. CRYPTO 2018: IACR, 2018, 29 с.

[5] Daniel J. Bernstein. ChaCha, a variant of Salsa20. Department of Mathematics, Statistics, and Computer Science (M/C 249): The University of Illinois at Chicago, 2008, 6 с.

[6] A. Bogdanov, L.R. Knudsen, G. Leander, C. Paar, A. Poschmann, M.J.B. Robshaw, Y. Seurin, C. Vikkelsoe. PRESENT: An Ultra-Lightweight Block Cipher. Cryptographic Hardware and Embedded Systems - CHES 2007, 9th International Workshop, Vienna, Austria, September 10-13, 2007, Proceedings: Springer, 2007, 18 с.

[7] Vladimirov S.S., Karavaev D.A., Stepanov A.B., Yurchenko M.A., Vladyko A.G. An Application of LoRa Technology for SD-IOV Network. В сборнике: International Congress on Ultra Modern Telecommunications and Control Systems and Workshops. 11. Сер. "11th International Congress on Ultra Modern Telecommunications and Control Systems and Workshops, ICUMT 2019" 2019. С. 8970938.

[8] Козлов Д.В., Степанов А.Б., Владыко А.Г. Разработка и тестирование макета узла SD-IOV на основе приемопередатчика LoRa и микроконтроллера STM32F103. // Научно-техническая конференция Санкт-Петербургского НТО РЭС им. А.С. Попова, посвященная Дню радио. 2020. № 1 (75). С. 83-84.