С. С. Агафьин

LW-КРИПТОГРАФИЯ: ШИФРЫ ДЛЯ RFID-СИСТЕМ

Все чаще и чаще бытовые предметы усовершенствуются с помощью встроенных компьютеров. Это происходит настолько стремительно, что можно считать повсеместную компьютеризацию новым этапом развития информационных технологий. Стоит также отметить, что сейчас 98,8 % всех производимых микропроцессоров применяются в различных встроенных устройствах и лишь 1,2 % — в обычных компьютерах [1].

Одним из наиболее быстро развивающихся направлений в сфере компьютеризированных небольших устройств являются RFID-системы. RFID — это метод автоматической идентификации объектов, в котором посредством радиосигналов считываются или записываются данные, хранящиеся в так называемых RFID-метках.

Любая RFID-система состоит из считывающего устройства и RFID-метки (иногда также применяется термин «RFID-тег»).

Большинство RFID-меток состоит из двух частей: интегральной схемы для хранения и обработки информации и антенны для приема и передачи сигнала.

По типу источника питания RFID-метки делятся на следующие категории:

- пассивные,
- активные,
- полупассивные.

Пассивные RFID-метки не имеют встроенного источника энергии. Электрический ток, индуцированный в антенне электромагнитным сигналом от считывателя, обеспечивает достаточную мощность для функционирования кремниевого чипа, размещенного в метке, и передачи ответного сигнала.

Активные RFID-метки обладают собственным источником питания и не зависят от энергии считывателя, вследствие чего они читаются на дальнем расстоянии, имеют большие размеры и могут быть оснащены дополнительной электроникой. Однако такие метки наиболее дороги, а у батарей ограничено время работы.

Полупассивные RFID-метки, также называемые полуактивными, очень похожи на пассивные метки, но оснащены батареей, которая обеспечивает чип энергопитанием.

На текущий момент RFID-технологии используются в самых разнообразных сферах: от сельского хозяйства до транспорта.

По мнению генерального директора государственной корпорации «РОСНАНО» [2], Россия, возможно, перейдет на чипы для банковских карт с интерактивной радиосвязью RFID, с помощью которых в ближайшие годы в мире должна произойти революция в розничной торговле.

В подтверждение этого можно привести тот факт, что ГК «РОСНАНО» и ИТ-компания «Систематика» создают предприятие по разработке меток радиочастотной идентификации. Инвестиции в проект составят 690 млн руб., выручка предприятия к 2015 г. должна достигнуть 800 млн руб.

На основании вышеперечисленного можно сделать вывод, что данные технологии в скором времени станут повсеместно распространенными.

Однако не стоит забывать о проблемах безопасности. Особенно остро этот вопрос стоит при применении RFID-технологий в военной или финансовой сферах. Из-за жестких ценовых ограничений система защиты должна быть не только надежной и производительной, но и дешевой в реализации.

Добиться этого позволяет применение LW-криптографии. Данный раздел криптографии ставит своей целью разработку алгоритмов для устройств, которые не способны обеспечить большинство существующих шифров достаточными ресурсами для функционирования.

Так как наибольшее распространение получили пассивные RFID-метки, далее рассматриваются алгоритмы, применимые именно к ним.

Основой любой LW-криптосистемы, используемой в RFID-тегах, являются симметричные алгоритмы. Их использование обусловлено, прежде всего, более высокой по сравнению с асимметричными шифрами скоростью работы, что является критичным в рассматриваемых устройствах.

Каждый разработчик алгоритмов в области LW-криптографии вынужден искать баланс между надежностью, производительностью и ценой. Например, для блочных шифров размер ключа определяет соотношение надежность/стоимость, число раундов шифрования — надежность/производительность, а особенности аппаратной конструкции — производительность/цена. Как правило, любые две из трех целей разработки могут быть легко достигнуты, в то время как удовлетворение всех трех требований — крайне сложная задача. Например, можно обеспечить приемлемое соотношение между надежностью и производительностью, однако для реализации подобного алгоритма потребуется большая площадь на схеме, что приводит к повышению стоимости. С другой стороны, можно создать надежную и дешевую систему, но с ограниченной производительностью.

Очевидно, что данная проблема имеет три варианта решения:

1. Использование проверенных стандартных алгоритмов;

2. Модификация известных алгоритмов с целью повышения производительности и снижения логической сложности;

3. Разработка новых алгоритмов.

Проблема первого подхода в том, что большинство современных шифров первоначально разработано для применения в программном обеспечении, без оглядки на аппаратные приложения. Конечно, этот подход оправдан, потому что, во-первых, большая часть алгоритмов используется на компьютерах, а во-вторых, благодаря дешевизне современных процессоров создание высокопроизводительных дешевых аппаратных реализаций не представляет собой проблемы. Однако для RFID-систем данные допущения не работают, а значит, применение в них стандартных криптографических алгоритмов невозможно.

Второй подход заключается в модификации шифра с богатой историей исследований, который был изначально разработан для применения в аппаратном обеспечении. Неоспоримым преимуществом данного решения является то, что надежности рассматриваемого шифра уже посвящено множество исследований и, значит, работа по устранению слабостей создаваемого алгоритма упрощается. Однако не стоит забывать, что неосторожная модификация системы может привести к серьезным нежелательным последствиям. Следовательно, при изменении некоторых элементов алгоритма необходимо тщательно оценивать вероятность появления дополнительных слабостей.

Большинство же решений в области LW-криптографии основывается на третьем подходе. Ясно, что создание нового шифра без определенных изъянов стойкости представляет собой довольно сложную задачу, однако существующие алгоритмы показывают неплохие результаты и, возможно, в будущем найдут применение в криптосистемах, обеспечивающих безопасность RFID-устройств.

LW-алгоритмы бывают как блочными, так и поточными. На данный момент известны только три описанных поточных LW-шифра, имеющих относительно приемлемые характеристики. Это алгоритмы MICKEY, Trivium и GRAIN. Однако данные шифры не применимы в пассивных RFID-системах в силу индивидуальных особенностей каждого из них. Так, например, Trivium требует площадь на чипе, превышающую допустимую более чем в полтора раза (3488 GE[1] при ограничении в 2000 GE [1]). На текущую версию шифра GRAIN может быть успешно проведена атака на связанных ключах [3]. Что касается MICKEY, то разработчиками проверена его стойкость лишь к некоторым атакам, однако этого недостаточно для обеспечения уверенности в его надежности.

[1] GE (gate equivalent) — единица измерения площади, требуемой интегральной схеме. Определяется как минимальная площадь, необходимая для логического вентиля И-НЕ.

Таким образом, можно заключить, что на данный момент среди поточных шифров нет алгоритма, удовлетворяющего основным требованиям RFID-систем.

В разделе блочных шифров ситуация обстоит несколько лучше. Рассмотрим подробнее некоторые блочные LW-алгоритмы.

Прежде всего, стоит отметить шифр DESL. Он разработан на основе алгоритма DES (Data Encryption Standart), описанного в начале 70-х годов прошлого века. Выбор данного шифра в качестве основы для новой криптосистемы не случаен. Преимущество DES перед остальными известными алгоритмами заключается, в первую очередь, в том, что он был изначально разработан для применения в аппаратных устройствах. Также в силу того, что данный шифр имеет более чем тридцатилетнюю историю исследований, можно полагать, что его основные уязвимости найдены и устранены.

Для оптимизации использования DES в RFID-системах была проведена его модификация. Прежде всего, были исключены перестановки IP и IP^{-1}, которые не влияют на стойкость [4], однако занимают место на схеме. Затем восемь оригинальных S-блоков были заменены одним, повторенным восемь раз. Авторами доказано, что данное изменение не влияет на стойкость алгоритма к основным атакам, таким как линейный и разностный криптоанализы. Полученный шифр получил название DESL. Его основным недостатком является малый размер ключа — 56 бит. Хотя для его раскрытия полным перебором требуются месяцы работы кластера из нескольких десятков компьютеров, на суперкомпьютере данная задача решается всего за три дня. Следовательно, подобный алгоритм стоит применять только там, где требуется краткосрочная защита или где важность защищаемых данных относительно невелика. Для реализации алгоритма необходимо 1848 GE, что приемлемо для LW-шифра.

Следующим блочным LW-алгоритмом, удовлетворяющим всем требованиям RFID-систем, является PRESENT.

В отличие от DESL данный шифр использует ключ длиной 80 бит, что значительно повышает его надежность. Разработчиками проведено исследование уязвимости данного алгоритма к линейному и разностному анализу, алгебраической атаке и некоторым другим видам атак. Показанная PRESENT стойкость является прекрасным результатом для шифра, созданного «с нуля». На данный момент не известно ни одной успешной атаки на полнораундовую версию алгоритма.

Существуют различные реализации PRESENT. Самая компактная из них требует всего 1000 GE, что является одним из лучших результатов для LW-шифров.

Помимо обеспечения безопасности передаваемых данных в RFID-системах, некоторые модификации PRESENT нашли применение и в других ресурсозависимых устройствах. Так, например, H-PRESENT-128 является самой компактной из известных хэш-функций. Кроме того, возможно применение алгоритма в качестве генератора псевдослучайных чисел для схемы crypto-GPS.

Также среди LW-шифров можно выделить семейства алгоритмов KATAN и KTANTAN [11].

Каждое из семейств состоит из трех шифров, отличающихся количеством раундов шифрования: 32, 48 или 64. Все шифры имеют 80-битный ключ. Отличие KTANTAN от KATAN состоит в том, что первые требуют меньшего количества ресурсов благодаря тому, что ключ шифрования «вшит» в устройство и не может быть изменен. В описании шифров разработчиками показана стойкость к таким атакам, как разностный и линейный анализы, атаке на связанных ключах и алгебраической атаке.

Аппаратные реализации представителей KTANTAN показывают лучшие результаты в данной области криптографии. Так, например, алгоритм KTANTAN48 может быть реализован с использованием всего 588 GE, что почти вдвое меньше, чем самая компактная реализация PRESENT.

Однако, на ряду со всеми достоинствами описанных выше блочных шифров, и для них существуют определенные угрозы, не позволяющие использовать их повсеместно. Как уже упоминалось, алгоритм DESL использует относительно короткий ключ, что делает его применение в устройствах, которые должны обеспечивать безопасность на высоком уровне, невозможным. Алгоритмы PRESENT

и KTANTAN, несмотря на множество исследований, проведенных за последние несколько лет, могут нести в себе критические уязвимости, которые сведут на нет все имеющиеся достоинства.

Существует еще множество блочных LW-алгоритмов. Однако они имеют определенные недостатки. Например, MIBS и TWIS показывают неплохие результаты как в плане быстродействия, так и в плане экономичности, однако проведено недостаточно их исследований, что, как и в случае с поточными алгоритмами, не позволяет с должной уверенностью судить об их надежности. Другие же шифры, такие как HIGHT или mCrypton, требуют для аппаратной реализации слишком много места на чипе.

Таким образом, обобщая все вышесказанное, можно заключить, что задача создания как поточного, так и блочного алгоритма шифрования для пассивных RFID-меток до сих пор актуальна и требует решения.

СПИСОК ЛИТЕРАТУРЫ:

1. *Poschmann A. Y.* Lightweight Cryptography: Cryptographic Engineering for a Pervasive World // Cryptology ePrint Archive. Report 2009/516. 2009.
2. РОСНАНО и ОАО «Группа Систематика» инвестируют в создание отечественного производителя RFID-меток // Пресс-релиз ГК РОСНАНО. URL: www.rosnano.ru.
3. *Кисик О.* Slide Resynchronization Attack on the Initialization of Grain 1.0 // Официальный сайт Ecrypt. URL: http://www.ecrypt.eu.org.
4. *Шнайер Б.* Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. М.: Триумф, 2002.