Безопасность RFID-систем

В. Бельский, Е. Грибоедова, К. Царегородцев, А. Чичаева

Аннотация—**Радиочастотные метки (RFID-метки) широко используются во всем мире для идентификации и аутентификации объектов. В силу архитектурных особенностей и довольно низкой стоимости реализации RFID-метки часто характеризуются жесткими ограничениями на затрачиваемые ресурсы памяти и вычислительную мощность, что в свою очередь неминуемо отражается на требованиях к используемым криптографическим механизмам и протоколам. Существующих стандартизованных протокольных решений из других областей применения становится недостаточно, и требуется разработка специализированных алгоритмов именно для технологии RFID.**

В настоящей статье приводится классификация существующих RFID-систем, описываются типичные сценарии их использования. Основное внимание уделяется сравнительному анализу существующих криптографических механизмов защиты информации с учетом особенностей применения в средствах радиочастотной идентификации. Перечисляются эксплуатационные и криптографические свойства, которые необходимо учитывать при проектировании и сравнении RFID-систем. Приводится обзор известных на данный момент моделей противника, которые используются для анализа протоколов подобного типа.

Ключевые слова—**RFID, аутентификация, ГОСТ**

I Введение

На протяжении двух десятилетий в мире активно развивается технология радиочастотной идентификации (RFID, Radio Frequency IDentification), позволяющая быстро и точно идентифицировать и/или аутентифицировать объект посредством использования радиоволн для считывания и передачи информации, хранящейся в RFID-метке.

RFID-системы успешно применяются в самых различных областях, таких как розничная торговля, логистика, платежные системы, системы контроля и управления доступом (СКУД), системы учета животных и анализа их поведения и многих других. При этом рынок RFID-меток продолжает расти с каждым годом [1]. Технология RFID имеет существенные преимущества. Так, например, некоторые классы RFID-меток не нуждаются во внутреннем источнике питания и в силу относительной простоты реализации обладают низкой стоимостью. Малые размеры меток позволяют легко прикреплять их к различным объектам и считывать с расстояния нескольких десятков метров. Указанными преимуществами обусловлен стремительный рост популярности данной технологии на протяжении последних лет [1, 2].

Однако, как это часто бывает с любыми новыми и стремительно развивающимися технологиями, процесс разработки необходимых открытых международных стандартов далек от завершения. В настоящий момент многие функционирующие RFID-системы не в полной мере отвечают необходимым требованиям безопасности, более того, в большинстве RFID-меток просто отсутствуют какие-либо криптографические механизмы, что делает эти системы уязвимыми ко множеству атак.

Российский рынок занимает незначительную долю в мировом рынке технологий RFID [2] и находится на этапе становления. Исследования безопасности протоколов аутентификации в RFID-системах недостаточно представлены в русскоязычной специальной литературе, а стандартизованные решения на базе российских криптографических алгоритмов отсутствуют. Поэтому разработка указанных протоколов является крайне актуальной задачей.

Настоящая статья посвящена первому этапу, который должен быть проведен при разработке любого криптографического протокола: классификации и сравнительному анализу существующих RFID-систем с учетом обеспечиваемых свойств безопасности, а также технических и эксплуатационных характеристик, с целью выбора наиболее релевантной модели противника, в рамках которой в дальнейшем будут проводиться исследования стойкости протоколов.

Статья построена следующим образом. В Разделе II выделены основные компоненты RFID-системы и описаны принципы работы технологии RFID. В Разделе III рассматриваются основные характеристики RFID-систем и обсуждаются различные классификации RFID-меток. Раздел IV посвящен рассмотрению основных атак и моделей угроз, наличие которых необходимо учитывать при выборе модели противника. В Разделах V , VI и VII более подробно обсуждаются свойства аутентификации, конфиденциальности и целостности данных, а также приватности (конфиденциальности источника) соответственно. В заключении в Разделе VIII приводятся ключевые требования, которые могут браться за основу при проектировании RFID-систем, удовлетворяющих различным требованиям безопасности.

Систематизированный и подробный обзор существующих механизмов, а также наличие сравнительного анализа используемых подходов позволит, с точки зрения авторов, существенно упростить процесс изучения современной научной литературы по данному вопросу, а также поможет при выборе и разработке конкретного протокольного решения.

Статья получена 12 июля 2021.

Владимир Сергеевич Бельский, Лаборатория Криптографии АО НПК «Криптонит», (email: v.belsky@kryptonite.ru).

Екатерина Сергеевна Грибоедова, Лаборатория Криптографии АО НПК «Криптонит», (email: e.griboedova@kryptonite.ru).

Кирилл Денисович Царегородцев, Лаборатория Криптографии АО НПК «Криптонит», (email: k.tsaregorodtsev@kryptonite.ru).

Анастасия Александровна Чичаева, Лаборатория Криптографии АО НПК «Криптонит», (email: a.chichaeva@kryptonite.ru).

II Основные принципы работы технологии RFID

II-A Компоненты RFID-системы

Любую RFID-систему можно разделить на две части (см. рисунок 1): **RFID-считыватель** (Interrogator, reader) и **RFID-метку** (TAG, transponder).

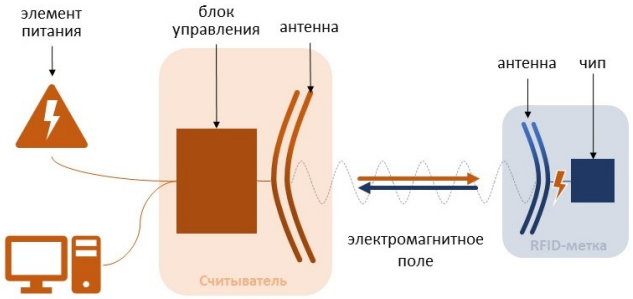

Рис. 1. Основные компоненты RFID-системы

RFID-считыватель включает в себя следующие основные компоненты:

- элемент связи (антенну), принимающую и передающую сигнал;
- блок управления, включающий передатчик и приемник (радиочастотный модуль), память и микропроцессор;
- постоянный источник питания.

Кроме того, многие считыватели оснащены дополнительным интерфейсом, который позволяет им пересылать полученные данные в другую систему (на персональный компьютер, в систему управления и т. д.).

RFID-метка обычно состоит из двух компонентов:

- элемента связи (антенны), принимающей и передающей сигнал;
- чипа, обрабатывающего информацию и включающего следующие компоненты: передатчик и приемник, память (см. подробнее III-B) и микропроцессор.

Замечание 1: В отличие от RFID-считывателя, RFID-метка чаще всего является пассивным элементом, то есть не имеет своего собственного источника питания (хотя существует т.н. активные RFID-метки, в состав конструкции которых включается автономный источник питания, см. подробнее III-A). В случае пассивной метки вся энергия, необходимая для ее работы, подается RFID-считывателем через генерируемое им электромагнитное поле. В настоящей статье основное внимание уделяется именно такому типу меток.

Замечание 2: Существуют так называемые «бесчиповые» метки, то есть метки, не содержащие интегральных микросхем. В настоящей статье данный тип меток не учитывается, так как предоставляемый ими функционал не позволяет говорить о поддержке каких-либо криптографических механизмов.

II-B Принципы взаимодействия элементов RFID-системы

В зависимости от того, на каком расстоянии от считывателя и на какой частоте работает метка, характер электромагнитного взаимодействия и способ передачи ответного сигнала может быть основан на одном из следующих двух подходов: работе в ближнем поле и работе в дальнем поле (см. подробнее III-A1).

Когда метка приближается к считывателю на определенное расстояние, между ними возникает электромагнитное взаимодействие, активирующее и передающее энергию метке. В зависимости от того, в каком поле считывателя (ближнем или дальнем) работает метка, характер данного взаимодействия (тип связи метки и считывателя) может быть разным (см. III-A1):

- емкостная или индуктивная связь (в случае работы в ближнем поле);
- связь за счет возникновения токов, наведенных падающей электромагнитной волной (в дальнем поле).

Активированная метка посылает ответный сигнал считывателю с целью идентификации. Так, в простейшем случае RFID-метка передаёт только свой уникальный идентификатор (TAG ID). В более сложных системах с поддержкой криптографических вычислений происходит двусторонний обмен информацией по принципу запрос-ответ. В процессе взаимодействия происходит идентификация и аутентификация (односторонняя или двусторонняя) сторон взаимодействия, при этом опционально между сторонами могут передаваться дополнительные данные в открытом или защищенном виде.

Информация между меткой и считывателем передается бесконтактным способом:

- считыватель обладает постоянным источником питания и активным передатчиком, поэтому сам формирует исходящий сигнал и может поддержать практически любой метод физической передачи информации (модуляции);
- поскольку метка не содержит активного передатчика, процесс передачи информации от метки к считывателю осуществляется за счет модуляции сигнала от считывателя (его специального изменения), с последующей регистрацией считывателем этих изменений, поэтому во всех протоколах инициатором взаимодействия является считватель, а RFID-метка только отвечает на сообщения. При этом метка существенно ограничена в способе осуществления модуляции, и его выбор зависит от типа взаимосвязи метки и считывателя (см. III-A1).

После обработки данных связь с RFID-меткой может быть завершена, дальше принимается решение об идентификации.

III Основные характеристики систем RFID

На текущий момент существует большое количество различных RFID-систем. Выбор конкретного варианта представляет из себя некий компромисс, учитывающий множество критериев, тесно взаимосвязанных друг с

другом. Два следующих подраздела посвящены систематизации всех этих критериев, призванной упростить выбор итоговой RFID-системы.

Условно процесс выбора системы мы разделяем на два этапа:

1) На первом этапе (см. III-A) предлагается выбрать тип RFID-меток в соответствии с международной классификацией ISO. На этом этапе мы фиксируем самые базовые параметры (дальность действия, частоту), зависящие в первую очередь от сферы использования рассматриваемой RFID-системы.
2) На втором этапе (см. III-B) предлагается определить конкретные технические характеристики чипа RFID-метки, тип которой был зафиксирован на первом этапе. При этом основными факторами, влияющими на выбор итоговых технических характеристик, являются допустимый бюджет и требования по безопасности проектируемой RFID-системы.

К примеру, малая площадь дешевого чипа не позволит разместить на нем реализацию тяжелого криптографического протокола, предоставляющего необходимые свойства безопасности, а энергозависимость бюджетной памяти наложит ограничения на применение каких-либо счетчиков, обязав использовать лишь схемы без изменяющегося внутреннего состояния.

III-A Физические характеристики RFID-меток

III-A1 Ближнее и дальнее поле

Работу RFID-метки можно организовать в ближнем или в дальнем поле считывателя (см. рисунок 2). **Ближним полем** называется область распространения сигнала, расположенная в пределах одной длины волны от антенны считывателя. К **дальнему полю** относится область, удаленная от антенны на расстояние, превышающее удвоенную длину волны.

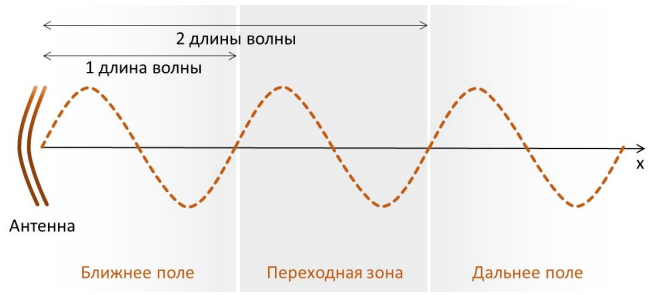

Рис. 2. Ближнее и дальнее поле антенны

Подробнее о физических принципах и особенностях работы в ближнем и дальнем поле можно прочесть в [3]. Мы же остановимся на предоставлении краткой выжимки, знакомящей читателя с основными терминами, которые могут встретиться при поиске литературы на тему работы в ближнем или дальнем поле, а также выделении принципиальных особенностей, характерных для каждого из случаев.

Работа в ближнем поле характеризуется следующими особенностями:

- **Тип антенны:** используются антенны, размер которых много меньше длины волны: элементарный диполь, малая рамка (катушка).
- **Характер поля:** можно считать, что в ближнем поле электрические поля не связаны с магнитными, и в зависимости от типа используемой антенны одно преобладает над другим: электрическое поле преобладает при использовании элементарного диполя; магнитное поле преобладает при использовании малой рамки.
- **Тип связи между меткой и считывателем:** связь может быть емкостной (при использовании электрического поля) или индуктивной (при использовании магнитного поля). Среди RFID-систем ближнего поля индуктивно связанные системы находят наиболее широкое распространение. В этом случае ток, протекающий по первичной обмотке (антенне считывателя), создает магнитное поле вокруг себя, при попадании в которое на вторичной обмотке (антенне RFID-метки) возникает индукционный ток, который можно использовать для питания чипа.
- **Характер убывания напряженности поля:** напряженность электрического поля убывает пропорционально $\frac{1}{r^3}$, а напряженность магнитного поля – пропорционально $\frac{1}{r^2}$, где r – расстояние до антенны.
  Вывод 1: указанные различия во многом обуславливают популярность использования именно индуктивной связи между считывателем и меткой.
  Вывод 2: системы, работающие в ближнем поле, имеют существенные ограничения на дальность работы (до 1 метра), так как на больших расстояниях падение мощности становится критическим.

Работа в дальнем поле характеризуется следующими особенностями:

- **Тип антенны:** чаще всего используются резонансные антенны, характерные размеры которых соизмеримы с длиной волны излучаемого сигнала (например, полуволновые диполи).
  Вывод: из этого свойства следует, что системы, взаимодействующие в дальнем поле, работают с более высокими частотами (UHF и выше), где малая длина волны позволяет использовать антенны подходящего размера. А системы с более низкой частотой (HF, LF), длина волны которых превышает десятки и сотни метров, не предназначены для работы в данном поле.
- **Характер поля:** электрические и магнитные поля взаимосвязаны, и их суперпозиция представляет собою электромагнитную волну.
- **Тип связи между меткой и считывателем:** связь осуществляется за счет возникновения токов, наведенных падающей электромагнитной волной.
- **Характер убывания напряженности поля:** напряженность поля (как электрического, так и магнитного) убывает пропорционально $\frac{1}{r}$, где r — расстояние до антенны.
  Вывод: из этого свойства следует, что системы, взаимодействующие в дальнем поле, могут работать на больших расстояниях (десятки метров). В случае, когда система работает в ближнем поле, напряженность, а следовательно и мощность, убывает значи-

тельнее быстрее, что позволяет устанавливать более точные ограничения на дальность считывания.

III-A2 Источник энергии

В части используемых источников энергии RFID-метки делятся на два типа: **пассивные** и **активные**. Пассивные RFID-метки не имеют собственного источника питания и получают всю необходимую для работы энергию через электромагнитное поле считывателя. Активные RFID-метки имеют встроенную автономную батарею, которая поставляет всю необходимую для работы чипа энергию или ее часть.

Замечание 3: Иногда выделяют еще один класс меток, называемых полуактивными. При таком типе классификации учитывается как наличие дополнительного источника питания, так и наличие активного передатчика. Так, пассивные метки не имеют ни элемента питания, ни активного передатчика; полуактивные метки содержат элемент питания, но не имеют активного передатчика; активные метки имеют оба этих компонента.

Пассивные RFID-метки имеют следующие основные особенности:

- обладают меньшей мощностью и, как следствие, имеют меньшую дальность работы, либо требуют более мощных RFID-считывателей;
- не могут хранить данные в энергозависимой памяти из-за невозможности удерживать информацию при удалении от считывателя;
- имеют практически неограниченный срок службы, так как не требуют замены автономного источника питания;
- могут быть компактными, более дешевыми в производстве.

Активные RFID-метки имеют следующие основные особенности:

- являются более мощными и, как следствие, могут работать на больших расстояниях (в частности, имеют более высокую допустимую скорость движения метки относительно считывателя), допускают использование менее мощных RFID-считывателей;
- могут хранить данные в энергозависимой памяти;
- имеют ограниченный срок службы, зависящий от количества энергии, запасенной в автономном источнике питания;
- имеют больший размер, более дорогие в производстве и обслуживании.

Как уже упоминалось ранее, в настоящей статье основное внимание уделяется пассивным меткам.

III-A3 Частота и дальность считывания

RFID-метки классифицируют по рабочей частоте, для каждого диапазона которой создан отдельный стандарт серии ISO 18000:

Таблица I
Классификация RFID-меток по рабочей частоте

Диапазон частот	Длина волны в вакууме	Стандарт ISO	Частота
125–135 кГц	≈ 2300м	ISO 18000-2 [4]	Низкая (LF)
13,56 МГц	≈ 22м	ISO 18000-3 [5]	Высокая (HF)
433 МГц, 860–960 МГц	≈ 69см, 30–35см	ISO 18000-7 [6], ISO 18000-6 [7]	Ультравысокая (UHF)
2,45 ГГц	≈ 12см	ISO 18000-4[8]	Микроволны (SHF)

Метки ультравысоких частот (UHF и SHF) чаще всего работают в дальнем поле, в этом случае они характеризуются считыванием на больших расстояниях (десятки метров для UHF меток, сотни для SHF) и допускают большую скорость перемещения относительно считывателя. Однако существуют реализации RFID-систем, поддерживающих данный диапазон частот и в ближнем поле (см. [9, 10]), вследствие малой длины волны дальность работы подобных систем обычно не превышает десятка сантиметров.

Метки LF и HF диапазонов работают только в ближнем поле, то есть имеют меньший радиус считывания (до 1 метра), и для них могут быть установлены более точные ограничения на удаленность метки от считывателя. Для меток HF диапазона существует отдельная классификация по дальности считывания (см. Таблицу II) в соответствии со стандартами ISO:

Таблица II
Классификация RFID-меток диапазона HF по дальности считывания

Дальность считывания	Стандарт ISO	Комментарий
Менее 1 см	ISO 10536 [11]	Метки с сильной связью (close-coupled)
Менее 10 см	ISO 14443 [12]	Метки близкого действия (proximity cards)
Менее 1 м	ISO 15693 [13]	Метки дальнего действия (vicinity cards)

III-A4 Итоговая классификация

В Таблице III приведена итоговая классификация меток по рабочей частоте, где для каждой частоты приводятся соответствующие стандарты ISO, а также выделяется основная сфера применения меток данного типа. Ниже даны небольшие комментарии относительно каждой из них.

Метки низкой частоты (**LF диапазон**) характеризуются самой большой длиной волны. Чем больше длина волны, тем менее она подвержена помехам среды, что позволяет использовать эти метки в более агрессивных для радиочастотного сигнала средах: вблизи воды и металла. Поэтому LF метки в основном применяются для чипирования животных.

Метки высокой частоты (**HF диапазон**) наиболее распространены на практике и чаще всего используют поддержку криптографических примитивов. Одна из причин подобной популярности заключается в том, что они работают в ближнем поле, и их радиус действия является

Таблица III
Классификация RFID меток по рабочей частоте и приложениям

Диапазон частот	Стандарты	Приложения
Метки диапазона низкой частоты LF 125 — 135 кГц ISO 18000-2 [4]	Стандарты радиочастотной идентификации животных: ISO 14223 ISO 11784 ISO 11785	Разработаны для идентификации животных (в т.ч. домашнего скота), но используются достаточно широко, например, в автомобильных иммобилайзерах.
Метки диапазона высокой частоты, HF 13,56 МГц ISO 18000-3 [5]	ISO 14443 (метки близкого действия) ISO 15693 (метки дальнего действия) ISO 10536 (метки с сильной связью)	Бесконтактные смарт-карты для широкого круга приложений. Бесконтактные метки для приложений логистики, идентификации товаров, платежных систем, СКУД и т.д.
Метки диапазона ультравысокой частоты, UHF 860 — 960 МГц ISO 18000-6 [7]	Стандарты для UHF меток с различными типами связи: ISO 18000-61 ISO 18000-62 ISO 18000-63 ISO 18000-64	Бесконтактные метки для приложений логистики, идентификации товаров со средней дальностью. Используются для идентификации медицинского, промышленного и научного оборудования.
Метки диапазона ультравысокой частоты, UHF 433 МГц ISO 18000-7 [6]	ISO 17363 — применение RFID в цепочке поставок грузовых контейнеров ISO 18185 — идентификация грузовых контейнеров и электронных пломб	Бесконтактные метки для приложений логистики, в частности применяются в цепочках поставок грузовых контейнеров.
Метки диапазона микроволн 2,45 ГГц ISO 18000-4 [8]	ISO 17363 — применение RFID в цепочке поставок грузовых контейнеров	Бесконтактные метки для приложений логистики, идентификации товаров с увеличенной дальностью.

наиболее подходящим для систем, к которым предъявляются строгие требования по безопасности.

Так, для транспортных карт (например, карт метро) важно, чтобы радиус считывания метки не превышал десятка сантиметров. В противном случае будет велико число ошибочных считываний карт других пассажиров, стоящих рядом в очереди к турникету. СКУД являются еще одним примером, в котором ложное срабатывание метки мимо проходящего сотрудника является серьезной угрозой.

Еще одним аргументом в пользу использования меток с небольшим радиусом считывания является возможность обеспечения более эффективной защиты от relay-атаки (подробнее см. раздел V-E), которая не может быть предотвращена исключительно криптографическими методами: для защиты от данной атаки используется подход ограничения времени ответа (distance bounding protocols), учитывающий скорость распространения сигнала в среде при ограниченном допустимом расстоянии считывания (чем меньше это расстояние и чем медленнее сигнал распространяется в среде, тем эффективнее будет работать подход).

Как упоминалось ранее (см. III-A3), метки **UHF диапазона** также могут работать в ближнем поле, однако, по сравнению с HF диапазоном, RFID-системы данного типа менее распространены на практике и обычно накладывают более высокие требования на бюджет производства. Однако, если объект идентификации сам по себе представляет достаточно большую ценность, использование меток подобного типа может быть оправдано (идентификация медицинского, промышленного, научного оборудования).

В случае систем идентификации грузов и приложений логистики считывание, наоборот, должно успешно проходить на расстоянии многих метров и поддерживать возможность перемещения метки относительно считывателя. С задачами данного типа справляются метки **UHF и SHF диапазона**, работающие в дальнем поле. При этом для обеспечения работы на совсем дальних расстояниях (сотни метров) RFID-метка чаще всего обладает автономным источником энергии для возможности получения необходимой мощности.

III-A5 Классификация RFID-меток: выводы

В этом разделе были рассмотрены основные типы RFID-меток и стандарты, связанные с ними. Далее основное внимание мы будем уделять рассмотрению пассивных меток, работающих в ближнем поле на расстоянии от 1 см до 1 метра, поскольку эта дистанция считывания является наиболее подходящей для систем, поддерживающих криптографические методы защиты информации. Нас будут интересовать метки с HF и UHF диапазонами частот (2 и 3 строки таблицы III).

В следующем разделе рассмотрим конкретные технические требования, предъявляемые к чипу.

III-B Технические характеристики RFID-меток

RFID-метки предназначены для аутентификации и идентификации объектов. Эти задачи решаются с помощью использования различных протокольных решений, зависящих от сферы применения метки (см. III-A) и накладываемых требований безопасности

Самыми простыми и самыми дешевыми являются метки, поддерживающие только чтение идентификационного номера (TAG ID), записанного при производстве. Как правило, такие метки вообще не содержат перезаписываемой памяти и работают под управлением простейших электронных схем. Для полной деактивации такой метки может существовать специальный пароль (Kill Password), который также записывается в метку на этапе производства. Именно так деактивируются противокражные

метки.

Дальнейшее развитие функционала включает в себя поддержку записи информации на RFID-метку. В этом случае на метке присутствует области записываемой памяти, часть из которых, как правило, защищена паролем (Access Password). Например, подобным образом может изменяться число поездок на транспортном билете, которое записано в защищенной паролем области.

Для выполнения более сложных протоколов взаимодействия (например, выполнения криптографических преобразований) необходимы более технологичные и дорогие чипы. В зависимости от требуемого функционала на метке может присутствовать отдельный процессор или криптографический сопроцессор.

Возможность реализации на RFID-метке сложных протоколов в первую очередь зависит от таких параметров микросхемы, как тип и объем доступной памяти, площадь чипа и мощность. Поговорим подробнее про каждый из них.

III-B1 Память

Память в чипе можно разделить на:

- энергонезависимую (ROM, EEPROM и др.);
- энергозависимую (RAM, SRAM, DRAM и др.).

Все «чиповые» RFID-метки обладают энергонезависимой памятью, в которой записаны TAG ID, ключи и другие данные.

Простейшие RFID-метки хранят небольшое число данных и предоставляют только возможность считывания идентифицирующей информации, поэтому не требуют наличия энергозависимой памяти. Однако, при использовании меток с более расширенным функционалом (например, поддержкой криптографических вычислений) требуется большие объёмы памяти и скорость чтения данных, что приводит к необходимости использования некоторых видов энергозависимой памяти RAM (статической и динамической).

В дальнейшем по умолчанию будем подразумевать, что RFID-метки обладают обоими типами памяти (энергонезависимой и энергозависимой), так как криптографические механизмы могут быть эффективно реализованы только на метках такого типа.

Далее рассмотрим подробнее особенности энергонезависимой памяти RFID-меток.

Чтение и запись

RFID-метки по типу энергонезависимой памяти можно разделить на три класса:

- только для считывания (read only, RO): RFID-метка, в памяти которой данные хранятся без возможности их изменения и доступны только для считывания;
- с однократной записью и многократным считыванием (write once/read many, WORM): RFID-метка, информация на которую может быть частично или полностью записана пользователем только один раз, а считана многократно;
- с многократной записью и многократным считыванием (Read and Write, RW): RFID-метка, в памяти которой данные хранятся с возможностью их изменения и считывания, при этом число циклов перезаписи блоков памяти обычно варьируется от 100 тысяч до 1 млн ([14, 15, 16]).

Несомненно, использование RFID-меток, обладающих более продвинутой памятью, позволяет реализовать более сложные криптографические механизмы и обеспечить более высокий уровень защиты, но при этом стоимость метки значительно возрастает. Поэтому выбор конкретного типа памяти RFID-метки всегда является компромиссом между ценой и свойствами безопасности, выполнение которых обеспечивает метка.

Следует отметить, что на RFID-метках только для считывания не могут быть реализованы криптографические протоколы, так как нет возможности записать на них ключи, поэтому мы останавливаемся на рассмотрении меток, предоставляющих возможность однократной или многократной записи. При этом необходимо понимать, что RFID-метки с энергонезависимой памятью с однократной записью позволяют реализовать только криптографические протоколы без внутреннего состояния (stateless схемы), а многократная запись уже допускает сохранение и обновление внутреннего состояния (stateful схемы), например, появляется возможность хранить значение счетчика для режима работы блочного шифра CTR (см. [17]).

Примерами меток, содержащих конфигурационную перезаписываемую память, являются:

- чипы компании Shanghai fudan microelectronics FM13HF02N [18], в которых в перезаписываемой конфигурационной памяти хранится счетчик;
- метки компании NXP Semiconductors NTAG213, NTAG215, NTAG216, а также метки семейства Mifare Plus [19], которые являются популярными в России, хранят счетчики обращений к памяти;
- метки компании STMicroelectronics (ST25TA512, ST25TA02K-P) и др.

Защищенная область памяти

При расширении функционала меток возникает необходимость использования защищенной области памяти (доступ к которой невозможен извне), в которой хранятся секретные параметры протокола (криптографические ключи, счетчики и др.). Обычно память данного типа защищается с помощью некриптографических методов [20, 21], например, счетчиков доступа, паролей или защиты от физического вскрытия. Ниже приведём несколько более подробных примеров таких механизмов.

Как уже упоминалось выше, некоторые RFID-метки оснащены конфигурационной памятью, которая может использоваться для хранения секретных ключей, прав доступа к секторам пользовательской памяти, а также другой важной информации. Программируется конфигурационная память в процессе персонализации RFID-метки. Процесс программирования конфигурационной памяти завершается последовательным пережиганием предохранителей, блокирующих определенные части памяти, делая её однократно программируемой (OTP – Once programmed memory). Чтобы получить доступ к такой памяти, как правило используется специальный пароль.

У меток, обладающих перезаписываемой конфигурационной памятью, есть дополнительная возможность

хранить значения различных счетчиков доступа. Например, чтобы предотвратить атаки методом перебора пароля, с помощью специальной команды можно установить максимально допустимое количество отрицательных попыток проверки пароля, превышение которого приведет к постоянной блокировке защищенной части памяти.

Помимо возможности блокировки памяти некоторые RFID-метки (например, серии серии NTAG2**TT) защищены от физического вскрытия («Tag Tamper Resistant»), с помощью специальной петли, контакт которой разрывается при вскрытии, что свидетельствует об отсутствие целостности метки. В это случае метка может продолжать отвечать ложными данными, блокируя доступ к реальным, что может являться дополнительным механизмом защиты.

Исследование механизмов зашиты памяти выходит за рамки нашей работы, поэтому далее будем считать, что доступ к защищенной памяти может получить только процессор и криптографический модуль метки ((1) на Рисунке 3), а нарушитель может только подавать команды на вход процессору.

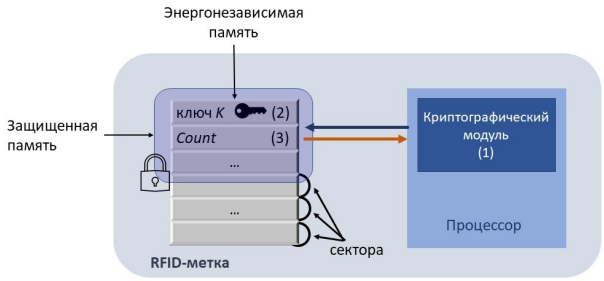

Рис. 3. Схема взаимодействия с памятью RFID-метки

Права доступа

В RFID-метках могут быть реализованы многопользовательские протоколы (см. например, протокол аутентификации, описанный в стандарте ISO 29167–10 [22]). В этом случае на метке может храниться не один ключ, а несколько, соответствующих разным правам доступа.

При этом на метке помимо конфигурационных данных могут храниться пользовательские данные, разделенные на сектора, для работы с которыми должны быть реализованы механизмы настройки прав доступа, определяющие возможность считывания, записи, передачи и других действий с секторами.

Вопрос настройки прав доступа является обширной задачей, требует проведения отдельных исследований и остаётся за рамками нашей работы.

III-B2 Площадь

RFID-метки обычно имеют жесткие ограничения по стоимости, а стоимость прямо пропорциональна площади чипа. Поэтому при реализации криптографических протоколов важно, чтобы они занимали сравнительно небольшую площадь. Для возможности сравнения площадей независимо от устройства принято указывать площадь в эквивалентах логического вентиля (gate equivalent, GE). Одна единица GE соответствует площади логического вентиля NAND (штрих Шеффера) с двумя входами. Площадь, выделяемая для криптографических протоколов, может варьироваться, но авторы [23, 24] считают, что из 1000-10000GE, обычно доступных в RFID-метках, только 250-4000GE могут использоваться для задач, связанных с безопасностью. Некоторые дорогие смарт-карты с повышенным уровнем безопасности, предназначенные для СКУД, могут предоставить площадь 3000GE и больше (например на метках семейства Mifare plus [19] есть дополнительный сопроцессор AES, компактная реализация которого занимает ≈2500GE [25, 20]), но для более маленьких устройств, таких как недорогие RFID-метки, площадь не должна превосходить 1000-2000GE.

III-B3 Мощность и энергия

Реализация криптографических примитивов на RFID-метках ограничена не только доступной площадью микросхемы, но и доступной мощностью для вычисления криптографических преобразований. Вопрос потребляемой энергии особенно важен для пассивных меток, получающих энергию через электромагнитное поле от считывателя.

Как уже упоминалось ранее (Раздел III-A1), мощность в метке убывает при удалении от считывателя, при этом характер этого убывания зависит от того, в каком поле (ближнем или дальнем) работает метка.

Необходимые параметры мощности и энергопотребления во многом зависят от конкретной реализации алгоритма, поэтому их невозможно зафиксировать на текущем этапе исследований.

IV Модели противника для RFID-системы

Стойкость любой криптосистемы можно оценить только в рамках определенной модели противника, которая согласно [26, 27] состоит из трех компонент:

1) **тип атаки (см. IV-A):** возможности противника по взаимодействию с системой;
2) **модель угрозы (см. IV-B):** задача противника по нарушению свойства безопасности;
3) **Предположение о ресурсах противника (см. IV-C):** как вычислительные, так и информационные.

Ниже рассмотрим каждый из перечисленных пунктов более подробно.

IV-A Тип атаки

При анализе стойкости системы важно определить, каким образом противник может вмешиваться в её работу. Качественные возможности противника по взаимодействию с криптосистемой определяются типом атаки. По уровню осуществления операций все типы атак можно разделить на два класса:

1) атаки протокольного уровня (см. IV-A1);
2) атаки физического уровня (см. IV-A2): физическое воздействие на компоненты системы.

Более подробную информацию об атаках для каждого из уровней, а также о возможностях их практической реализации можно получить в [28, 29, 30, 31]. Также дополнительную информацию можно получить в работах [32, 33], посвященных обзору технологии Интернета вещей (IoT devices), одной из составляющих которого являются RFID-метки.

IV-A1 Атаки протокольного уровня

Стандартным предположением о возможностях противника при рассмотрении интерактивных протоколов является модель Долева-Яо [34, 35]. Согласно этой модели, противник может подслушивать (и хранить) данные сеансов связи считывателя и RFID-меток, навязывать сообщения метке и считывателю (например, заставить считыватель начать протокол аутентификации метки либо заставить метку ответить на запрос на аутентификацию), посылать сообщения от своего или чужого имени, пытаться модифицировать передаваемые сообщения. Иногда противнику даются дополнительные (к упомянутым выше) возможности: взлом меток (данная возможность играет роль, если есть некоторая общая информация для нескольких RFID-меток в системе), регистрация (создание) своих легитимных RFID-меток, доступ к информации по побочному каналу.

IV-A2 Атаки физического уровня

В рамках атак физического уровня можно рассматривать противников со следующими возможностями:

- считывание, копирование и модификация информации из области памяти RFID-метки путем несанкционированного физического воздействия;
- вывод метки из строя (после физического вскрытия или воздействия сильным электромагнитным полем);
- получение информации о ключах и обрабатываемых данных из побочных каналов (например, путём замера времени ответа и энергопотребление метки с целью восстановить конфиденциальную информацию);
- блокирование канала связи между меткой и считывателем (например, путём внесения помех).

Атаки физического уровня можно лишь частично предотвратить с помощью криптографических методов (например, для защиты от атак по побочным каналам могут использоваться механизмы внешнего или внутреннего преобразования ключа из RFC 8645 [36]).

При формировании модели противника для RFID-систем могут учитываться и задействоваться дополнительные организационные меры, позволяющие ограничить возможности противника по проведению атак на физическом уровне (например, установление особых требований к безопасному хранению RFID-метки).

Противодействие указанным выше атакам требует технических мер защиты и является темой отдельного исследования.

IV-B Модели угроз

Анализ конкретной криптосистемы невозможен без понимания того, что является нарушением безопасности её работы. Для этого необходимо выделить основные свойства безопасности системы и определить цели противника по их нарушению. Формализовать задачи противника можно с помощью модели угроз.

Для RFID-систем выделяют следующие модели угроз [30], [31].

1) **Нарушение аутентификации источника (см. V).** Выполнение передачи сообщений нелегитимной стороной, выдаваемых за сообщения легитимного источника (как RFID-метки, так и считывающего устройства).
   Примером реализации данной угрозы является клонирование метки или реализация relay-атак V-E.
2) **Нарушение конфиденциальности передаваемых данных (см. VI).** Получение неправомерного доступа к передаваемым данным.
3) **Нарушение целостности передаваемых данных (см. VI).** Изменение или навязывание сообщений с передаваемыми данными между меткой и считывающим устройством (как в одну, так и в другую стороны).
4) **Нарушение конфиденциальности источника (приватности) (см. VII).** Неправомерное чтение идентификатора метки либо другой информации, позволяющей противнику однозначно восстановить источник сообщения, либо отслеживать источник.
   Метка взаимодействует со считывающими устройствами без каких-либо признаков активности со стороны метки. Эта особенность может быть использована для скрытого сбора информации. Полученная информация может быть достаточно личной, например медицинские данные, а в некоторых случаях противник может даже отследить местонахождение пользователей. Эта угроза является очень серьёзной и достаточно распространённой.
5) **Нарушение режима работы системы (доступности).** Выполнение действий, влияющих на корректную и устойчивую работу системы.
   Типичным примером реализации данной угрозы является проведения DoS-атак, приводящих к сбою системы.

На практике криптографические методы позволяют защититься не от всех угроз. Например, свойство конфиденциальности источника не выполняется во многих протоколах RFID-систем, поскольку для аутентификации требуется согласовать используемый ключ. Согласование достигается путем трансляции карточкой своего $TAG\ \ ID$ в канал незащищенным образом, что дает противнику возможность отслеживать карточку. Известно, что невозможно построить RFID-систему, которая удовлетворяла бы сразу трем условиям: эффективная, безопасная, неотслеживаемая (см. например [37], [38]).

В последующих разделах V, VI, VII мы обсудим основные методы и подходы к их обеспечению основных свойств безопасности, а также рассмотрим различные модели противников, формализующие типы атак и модели угроз для каждого из свойств.

IV-C Предположение о ресурсах противника

Под противником обычно понимается вероятностный интерактивный алгоритм (например можно формализовать его с помощью машины Тьюринга с оракулом [39, 40]). В свою очередь, вычислительные ресурсы противника определяются как величина, ограничивающая сумму времени работы противника и размера его программы [26]. Вычислительные ресурсы противника определяются непосредственно при оценке стойкости конкретных криптосистем, поэтому этот аспект остается за рамками нашей статьи.

V Аутентификация сторон

Обеспечение свойства аутентификации стороны (метки или считывателя) означает, что только легитимный участник сможет пройти проверку второй стороны (честного проверяющего). Взаимная аутентификация подразумевает одновременную аутентификацию обеих сторон [30].

Далее в Разделах V-A и V-B рассматриваются два основных подхода к обеспечению свойства аутентификации: на основе симметричной и асимметричной криптографии соответственно. В Разделе V-C приводится сравнительный анализ подходов, а в Разделе V-D рассматриваются основные модели противника для анализа свойства аутентификации.

V-A Аутентификация, использующая методы симметричной криптографии

Подход на основе симметричной криптографии подразумевает, что перед началом взаимодействия между сторонами был распределен общий секретный ключ (например, на этапе производства). Аутентификация сторон в этом случае происходит за счет (неявного) подтверждения факта обладания этим ключом. Для этого аутентифицирующаяся сторона отправляет значение, сформированное с помощью некоторой функции PRF и общего секретного ключа.

Замечание 4: В настоящей статье под PRF подразумевается некоторая функция, результат которой на случайном входе трудно предсказать. В частности, для построения протокола может быть использована любая псевдослучайная функция, однако в общем случае требование псевдослучайности (неотличимости значений функций от случайных бит) является избыточным [41].

Можно выделить два основных подхода к построению протоколов аутентификации в RFID-системе, использующих методы симметричной криптографии:

1) Построение схем без внутреннего состояния (stateless-схем, см. рисунок 4). Как правило, в этом случае для обеспечения защиты от атак повторной пересылки сообщений (replay-атак) проверяющая сторона генерирует некоторое случайное значение, призванное гарантировать свежесть ответной пересылки.
2) Построение схем с внутренним состоянием (stateful-схем, см. рисунок 5). В этом случае у сторон появляется возможность гарантировать защиту от повторов путем хранения некоторого внутреннего состояния $State$ (это состояние может содержать информацию об обновляемом симметричном ключе, счетчике соединений и т.д.).

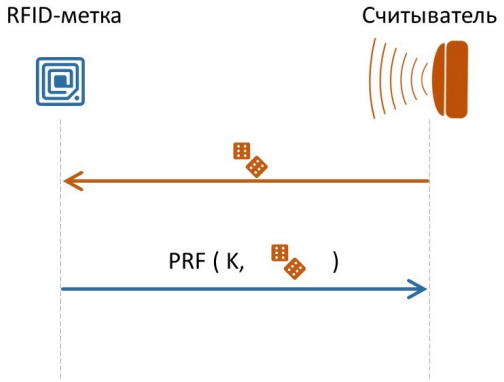

Рис. 4. Схема простейшего stateless-протокола аутентификации RFID-метки, использующего методы симметричной криптографии

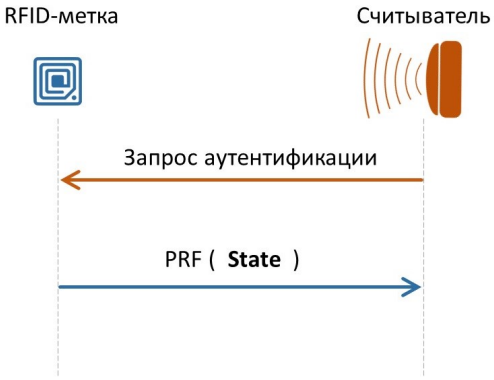

Рис. 5. Схема простейшего stateful-протокола аутентификации RFID-метки, использующего методы симметричной криптографии

Преимуществом использования симметричных алгоритмов является их быстродействие и сравнительно небольшая площадь реализации, что позволяет использовать протоколы такого типа на метках с сильно ограниченными вычислительными ресурсами.

Одним из недостатков использования симметричных подходов при аутентификации является сложность в обеспечении свойства конфиденциальности источника (свойства приватности, см. раздел VII), так как для решения задачи идентификации RFID-метка может действовать в рамках одного из двух вариантов:

1) переслать свой TAG ID в открытом виде (см. рисунок 6), что предполагает полное отсутствие приватности;

2) не передавать TAG ID, заставив считыватель выполнить перебор (полный или частичный) ключей, хранящихся в базе данных (см. рисунок 7);

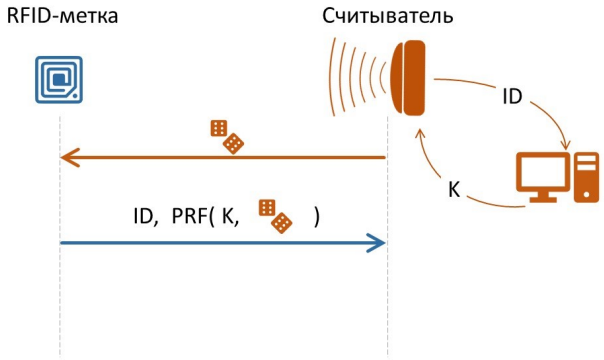

Рис. 6. Простейшая схема идентификации RFID-метки без обеспечения свойства приватности

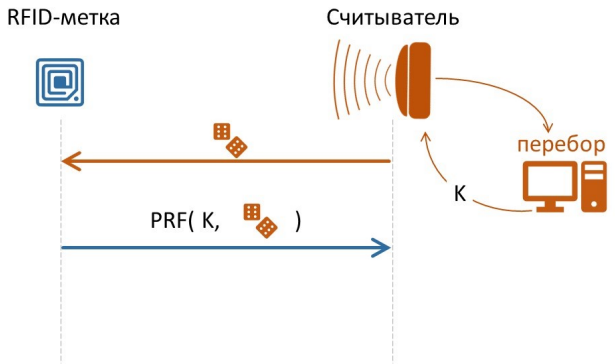

Рис. 7. Простейшая схема идентификации RFID-метки без передачи TAG ID

Далее рассмотрим самые популярные подходы к реализации протоколов аутентификации, основанных на методах симметричной криптографии:

1) аутентификация на основе блочного шифра (см. V-A1);
2) аутентификация на основе хэш-функций (см. V-A2);
3) аутентификация на основе низкоресурсной (lightweight) криптографии (см. V-A3).

V-A1 Аутентификация на основе блочного шифра

В протоколах данного вида в качестве функции PRF может использоваться блочный шифр. Примеры таких решений можно посмотреть в [42], [43]. Следует отметить, что большая часть проколов аутентификации для RFID-систем, стандартизованных в ISO, используют блочные шифры (см. [22, 44, 45, 46]).

V-A2 Аутентификация на основе хэш-функций

Одни из первых протоколов аутентификации, основанных на вычислении хэш-функций, были предложены в статьях [24, 47, 48]. В указанных статьях предлагается использовать хэш-функцию для вычисления кода аутентификации $HMAC(K, \cdot)$, при этом ключ K предлагается менять на производный. Таким образом, функция $HMAC$ в этом подходе играет роль псевдослучайной функции PRF. Данные протоколы имеют различные недостатки (например, для протокола из [48] характерны проблемы, связанные с рассинхронизацией), и все они предполагают полный перебор вариантов на стороне сервера. В дальнейшем были предложены модификации, использующие деревья (tree-based search) и табличные методы (см. [30]). Реализация указанных протоколов занимает площадь, недоступную в простейших RFID-метках (за счет более «тяжеловесной» хэш-фунции).

V-A3 Аутентификация на основе низкоресурсной криптографии

Подходы на основе низкоресурсной криптографии либо предполагают замену блочного шифра на более низкоресурсную версию (например, PRESENT [49], SIMON, SPECK [50] и другие), либо используют совершенно отличные от стандартных подходы (см. например [51], [52], [53], [54], [55]). Низкоресурсные протоколы часто становятся объектами атак криптоаналитиков (см. [56], [57]), и хотя они имеют свои плюсы для применения в RFID-системах, вопрос их безопасности остаётся открытым.

V-B Аутентификация, использующая методы асимметричной криптографии

Второй подход предполагает, что на метке может быть реализованы криптографические механизмы, основанные на сложных теоретико-числовых задачах (например, задаче дискретного логарифмирования в группе точек эллиптической кривой, задаче решения зашумленной системы линейный двоичных уравнений или других задачах), что позволяет применять стандартные методы аутентификации, используемые в современных протоколах (см. например схемы идентификации в [58] и [59]). Главным препятствием для использования аутентификации на основе систем с открытым ключом является значительная ограниченность вычислительных ресурсов метки при заданном энергопотреблении и низкой стоимости производства.

Можно выделить следующие основные подходы к реализации протоколов аутентификации в RFID-системах, основанные на методах асимметричной криптографии:

1) аутентификация на основе эллиптической криптографии (см. V-B1);
2) аутентификация на основе задачи обучения с ошибками (см. V-B2).

V-B1 Аутентификация на основе эллиптических кривых

Как было отмечено выше, основным препятствием для использования асимметричной криптографии в RFID-метках является ее относительная «тяжеловесность». Основной работой в данном направлении является все более и более эффективная реализация арифметики эллиптических кривых (см. [60, 61, 62]). Эффективно реализо-

ванные вычисления в группе точек эллиптической кривой позволяют использовать аутентификацию на основе электронной цифровой подписи [63] или схем идентификации [64].

Дополнительно рассматриваются возможности использования ограниченного класса кривых (специального вида), специальных полей (над которыми определяется кривая) или специальных простых чисел (см. например [31]). В среднем площадь реализации арифметики эллиптических кривых занимает не менее 10000 GE [60, 31], хотя обычно на RFID-метках для криптографии выделяется не более 3000 GE.

V-B2 Аутентификация на основе задачи обучения с ошибками

Существует ещё один нестандартный подход к аутентификации в протоколах RFID, основанный на задаче обучения с ошибками. В основе данного подхода лежит сложная задача решения зашумленной системы линейных уравнений над полем из двух элементов. Первый простейший протокол HB на основе указанной задачи был предложен в [65]. Протокол HB является нестойким в модели противника, который может навязывать метке сообщения для обработки (что является стандартным предположением при анализе).

Было предложено множество вариантов модификации исходной схемы: HB^{+} [66], $HB^{\#}$ [67], HB^{++} [68], $HB-MP$ [69], протокол из [70], которые пытались исправить недостатки схемы, описанной в [65].

К сожалению, многие из предложенных схем являются нестойкими в реалистичных моделях противника [71], [72].

Обучение с ошибками является перспективным направлением аутентификации, основанной на асимметричных криптопримитивах, но пока что не представлено среди стандартов ISO. Также следует отметить, что хотя операции, используемые в алгоритмах, основанных на задаче обучения с ошибками, являются более низкоресурсными, чем эллиптические, размер ключа для таких криптосистем должен быть больше, чем в эллиптических, чтобы предоставлять сравнимые уровни безопасности.

V-C Сравнение подходов

В Таблице IV собраны основные подходы к обеспечению свойства аутентификации источника. Для каждого из них приводится средняя площадь, необходимая для его реализации (измеряется в gate equivalent (GE)) и пример соответствующих стандартов в ISO.

Оценки на площадь реализации взяты из работ [73], [74], [75].

Таблица IV
Сравнение подходов к обеспечению свойства аутентификации источника

Подход	GE	ISO
Блочный шифр	$800-3000$	ISO 29167-10 [22] ISO 29167-14 [76]
Хэш-функции	$5000-10000$	—
Низкоресурсная криптография	$700-1200$	ISO 29167-11 [44] ISO 29167-21 [45] ISO 29167-22 [46]
Эллиптическая криптография	≥ 10000	ISO 29167-12 [63]
Обучение с ошибками	оценки не найдены	—

V-D Модель противника для свойства аутентификации

Модели противника для взаимной и односторонней аутентификации можно найти в [77] и [42] соответственно, а также частично в [41, 78].

Модели различаются по возможностям, предоставляемым противнику на каждом из этапов взаимодействия с оракулами, и целями, которых должен добиться противник.

V-E Relay-атаки и свойство distance-bounding

Отметим, что ни одна из вышеперечисленных моделей не учитывает следующую простую атаку как угрозу для безопасности: противник перехватывает все ответы легитимного участника протокола и отсылает их от своего имени (relay-атака). Другими словами, любой протокол аутентификации на основе любого криптографического механизма подвержен следующей атаке: перехват сообщений от легитимного участника с последующей передачей противником от своего имени. Такой тип атак упоминается в книгах [79, 80] под названиями “проблема гроссмейстера” (grand chessmaster problem) или нарушитель-посередине (intruder in the middle) соответственно.

Указанная выше проблема действительно является серьезной практически осуществимой угрозой для протоколов аутентификации в RFID-системе [29] и не может быть решена исключительно криптографическими методами. Кратко рассмотрим возможные варианты атак и их практические последствия для аутентификации RFID-меток.

V-E1 Классический способ нарушения свойства аутентификации

В этой ситуации противнику удается успешно пройти аутентификацию, не взаимодействуя никак с легитимной RFID-меткой. Пример угрозы: противник подслушивает некоторое количество сеансов взаимодействия в СКУД, а затем сам успешно проходит аутентификацию и получает доступ в запретную зону.

Рис. 8. Противник в легитимной зоне выдает себя за легитимную метку

V-E2 Подделка расстояния

В такой ситуации RFID-метка, имеющая секретный ключ, убеждает считыватель, что она находится в некотором близком радиусе от считывателя, при этом находясь в более дальней зоне.

Рис. 9. Легитимная метка в нелегитимной зоне успешно проходит аутентификацию

Пример угрозы: пациенту с положительным тестом на заболевание предписано сидеть дома, его личность и местоположение контролируется с помощью запрос-ответной аутентификации. При реализации данной угрозы больной может убедить систему, что находится дома, при этом физически находясь в другом месте.

V-E3 Атака мафиози (mafia fraud)

В такой ситуации противник, не имеющий секретный ключ, путем «обмана» легитимной RFID-метки со знанием секретного ключа, убеждает считыватель, что он знает секрет.

Пример угрозы: противник на платной дороге подъезжает к транспондеру, пересылает запрос на оплату автомобилисту позади или впереди себя, происходит оплата, противник проезжает через шлагбаум.

Пример №2: противник взламывает автомобильную сигнализацию машины. Для этого он подходит к автомобилю, получает запрос на аутентификацию, пересылает запрос на другое свое устройство, находящееся близко к легитимному владельцу автомобиля с ключом, получает ответ от ключа, пересылает ответ на свое устройство, находящееся поблизости от автомобиля и открывает дверь путем пересылки (правильного) ответа на запрос (см. [81]).

Рис. 10. Противник в нелегитимной зоне путем обмана легитимной метки успешно проходит аутентификацию

V-E4 Атака террориста (terrorist fraud)

В такой ситуации противник, не имеющий секретный ключ, путем сговора с легитимной RFID-меткой со знанием секретного ключа, убеждает считыватель, что он знает секрет и находится в некотором близком радиусе от считывателя, при этом находясь в более дальней зоне.

Рис. 11. Противник в нелегитимной зоне в сотрудничестве с легитимной меткой успешно проходит аутентификацию

В отличие от предыдущей ситуации, в рассматриваемом случае RFID-метка “добровольно” взаимодействует с противником, при этом предполагается, что она выдает лишь некоторое ограниченное количество информации, не выдавая долговременный секретный ключ (т.е. помогает противнику пройти только одну конкретную аутентификацию).

V-E5 Противодействие атакам

Для устранения атак рассмотренных выше типов могут быть использованы специальные протоколы [82, 83, 84], учитывающие скорость распространения сигналов в среде (т.н. distance-bounding protocols). При этом критически важным становится минимизация временных задержек при обработке сообщений (задержка в одну наносекунду дает погрешность в 30 сантиметров в определении местоположении метки). Таким образом, протоколы distance-bounding должны учитывать не только математические, но и прикладные, физические характеристики метки и используемого протокола пересылки сообщений. Разработка подобных протоколов является темой отдельного

исследования.

VI Конфиденциальность и целостность передаваемой информации

Задача передачи информации от метки к считывателю и в обратном направлении ничем (помимо сильно ограниченных вычислительных ресурсов метки и возможных ограничений, накладываемых типом и объёмом используемой памяти) не отличается от стандартной задачи передачи информации между участниками протокола, которая является основополагающей в криптографии. Рассматриваемая задача хорошо изучена, и для нее предложено как множество моделей противника, так и множество протоколов для ее решения.

VI-A Модель противника для свойств конфиденциальности и целостности

Для задачи обеспечения конфиденциальности передаваемых данных разработано множество общепринятых моделей, таких как LOR-CPA, ROR-CPA, ROZ-CPA, IND-CPA и других (см. [78], [85], [86]).

Задача обеспечения целостности передаваемых данных также является базовой в криптографии. Стандартной моделью для целостности данных является модель UF-CMA (см. например [78]).

Задача одновременного обеспечения конфиденциальности и целостности являлась объектом пристального внимания криптографического сообщества на протяжении продолжительного времени. К настоящему моменту общепринятыми являются модели LOR-CCA + INT-PTXT, LOR-CPA + INT-CTXT (см. [87]), либо комбинированная модель IND-CCA3 ([88]).

VII Конфиденциальность источника

В зависимости от условий функционирования системы под конфиденциальностью источника могут подразумеваться следующие свойства:

- Конфиденциальность идентификатора метки: постоянный идентификатор метки должен быть защищен от перехвата/подслушивания в радиоэфире.
- Конфиденциальность местоположения метки: присутствие или прибытие метки в определенную местность не может быть определено путем прослушивания радиоэфира.
- Невозможность сопоставления проведенных операций (untraceability, неотслеживаемость): прослушивая радиоэфир, противник не должен иметь возможность узнать, взаимодействовал ли считыватель с одной и той же меткой.

Иногда требуются более сильные условия, например, forward privacy, которое подразумевает, что даже при условии записи противником всех сеансов взаимодействия в RFID-системе, после взлома конкретной метки нельзя по записанным протоколам взаимодействия понять, в каких из них участвовала данная метка.

Заметим также, что задачи, поставленные в рамках свойства конфиденциальности источника, аналогичны задачам в других прикладных протоколах. Так, в документе [89], посвященном требованиям безопасности в сетях мобильной связи, в разделе 5.1.1 сформулировано свойство конфиденциальности идентификатора абонента с аналогичными требованиями.

VII-A Модель противника для свойства конфиденциальности источника

В соответствии с тем, что для различных RFID-систем требуется выполнение различных по силе свойств безопасности, а также в связи с тем, что противник может иметь разные возможности по нарушению работы системы, выделяют несколько моделей противников.

IND-модель

В такой модели противник не может различить, с какой из двух различных меток он взаимодействует (см. [90]). Модель является развитием идей, предложенных в [91].

UNP^*-модель

Противник не может различить, взаимодействует ли он с реальной меткой (на которой записана секретная информация, например, секретный ключ) или с симулятором метки, который отвечает случайно на запросы (см. [92]). В той же статье [92] показано, что стойкость в UNP^*-модели влечет стойкость в IND-модели, но не наоборот. Также показано, что минимальные необходимые и достаточные условия для стойкости в UNP^*-модели — реализация на метке псевдослучайной функции. То есть, если RFID-система является безопасной в UNP^*-модели, то каждая из меток в этой системе может вычислять некоторую псевдослучайную функцию (PRF, см. [78]), и наоборот, если на каждой из меток реализована псевдослучайная функция (например, блочный шифр [78]) плюс имеется дополнительная память для хранения счетчика, то можно построить такой протокол аутентификации, который бы являлся стойким в UNP^*-модели.

ZK-модель

Предыдущие две модели подходят для двух- и трехэтапных протоколов аутентификации. Для того, чтобы рассмотреть более общие ситуации, необходимо вводить другие модели. Так, в [93] предложена модель, основанная на идее доказательств с нулевым разглашением, формализующая следующую идею: протокол не дает никакой дополнительной информации противнику, если вся информация, которая может быть получена противником при взаимодействии с честной меткой, может быть сгенерирована самим противником без взаимодействия с меткой (т.е. взаимодействие с меткой не дает никакой информации противнику). Данная модель является более сильной, чем упомянутая выше IND-модель, но менее требовательной, чем UNP^*-модель. Авторы статьи [93]

утверждают, что их модель более реалистична, чем модель, предложенная в [92].

В статье [94] предложен протокол взаимной аутентификации, являющийся стойким в ZK-модели. Для протокола необходимо, чтобы на метке была реализована псевдослучайная функция, а также имелась бы энергонезависимая перезаписываемая память для хранения счетчика. Также в данном протоколе происходит перебор ключей на стороне БД.

Модель Vaudeney

Модель была предложена в [95] и получила дальнейшее развитие в работе [96]. В статье вводится несколько типов противников согласно их возможностям в отношении RFID-системы:

- Weak-противник не имеет возможности взлома выбранной RFID-метки;
- Forward-противник имеет возможность взламывать выбранные RFID-метки, но только на последнем этапе атаки;
- Destructive-противник также может взламывать выбранные RFID-метки, но считается, что после взлома метка выводится из строя;
- Strong-противник усиляет Destructive-противника, поскольку считается, что взломанная им метка не выводится из строя, и ее отслеживание после взлома также считается угрозой;

Дополнительно мы можем рассматривать по две версии каждого из упомянутых противников (обычный или narrow-противник) согласно тому, имеет ли противник доступ к частичному выходу протокола аутентификации или нет соответственно (например, может ли он знать, успешно или неуспешно аутентифицировалась метка; эта информация может быть получена в том числе из побочных каналов).

RFID-система является стойкой в соответствующей модели противника, если противник не может различить, происходит ли взаимодействие с настоящей системой или с симулятором, не имеющим доступа к секретным ключам.

В статье [95] были получены следующие результаты:

1) Невозможно достичь конфиденциальности источника в strong-модели противника.
2) Протокол, обладающий свойством конфиденциальности источника в narrow-strong модели противника, может быть преобразован в схему выработки общего ключа, и наоборот, любая криптосистема с открытым ключом, являющаяся IND-CCA стойкой, может быть использована для построения вышеупомянутого протокола. Другими словами, конфиденциальность в указанной модели требует реализации асимметричных механизмов на метке.
3) Все 8 предложенных моделей противника попарно различны, каждый обычный противник сильнее чем narrow-вариант того же противника, strong-противник сильнее destructive, destructive-противник сильнее forward, forward-противник сильнее weak-противника.

В той же статье [95] были проанализированы несколько протоколов.

- Возможно построить протокол, стойкий в модели weak-противника на основе псевдослучайной функции. Однако необходим перебор ключей на стороне БД.
- Возможно построить протокол, стойкий в модели narrow-destructive противника на основе двух псевдослучайных функций (аналогично протоколу OKS [48]). Однако необходим перебор ключей на стороне БД, дополнительно требуется хранить на метке изменяемое секретное состояние (необходима энергонезависимая перезаписываемая память), к тому же протокол имеет уязвимость, связанную с рассинхронизацией.
- Возможно построить протокол, стойкий в модели narrow-strong противника. Однако необходимо, чтобы на метке были реализованы алгоритмы асимметричной криптографии.

VII-B Конфиденциальность источника: выводы

В литературе было предложено множество моделей противников для свойства конфиденциальности источника (приватности).

Были исследованы взаимосвязи между различными моделями, хотя некоторые модели и не могут быть сравнимы напрямую.

- Самой слабой из предложенных моделей является IND-модель.
- UNP^*-модель является усилением IND-модели. Было показано, что UNP^*-модель фактически эквивалентна тому, что на метке реализована псевдослучайная функция (протокол, стойкий в данной модели можно преобразовать в псевдослучайную функцию, и наоборот, если на метке реализована псевдослучайная функция и имеется дополнительная энергонезависимая перезаписываемая память для хранения счетчика, то на их основе возможно реализовать протокол аутентификации, стойкий в UNP^*-модели).
- ZK-модель расширяет UNP^*-модель с трехшаговых протоколов аутентификации на более общие. Данная модель также является более сильной, чем IND-модель. Протокол, стойкий в ZK-модели можно также реализовать на базе псевдослучайной функции и энергонезависимой перезаписываемой памяти.
- Модели Vaudeney, введенные в [95], также не предполагают какую-либо структуру протокола аутентификации. Стойкость протокола в narrow-strong-модели эквивалентна тому, что на метке реализована асимметричная криптография. Предложены протоколы, стойкие в weak-модели (на основе псевдослучайной функции), в narrow-destructive-модели (две псевдослучайные функции и память), в narrow-strong-модели (асимметричная криптография).

Заметим, что многие из предложенных протоколов предлагают большой перебор на стороне сервера для выполнения свойства неотслеживаемости метки. Взаимосвязь между конфиденциальностью источника и количеством ресурсов, которые необходимо затратить для проверки ответа метки, отдельно изучалась в [37] в самой

слабой IND-модели противника (см. [90]).

Перечислим некоторые из полученных результатов.

1) Если метки имеют независимые ключи и используют лишь симметричные криптомеханизмы, то подтверждение правильности прохождения аутентификации в протоколе, стойком в IND-модели, требует $O(n)$ вычислений, где n — общее число меток в системе.
2) Если мы позволяем меткам иметь зависимые ключи, то возможно построить систему, в которой перебор можно сократить до $O(\log(n))$, однако система не будет даже IND-стойкой, если противник может взломать хотя бы одну метку [97].
3) Общим выводом статьи [37] является тот факт, что возможно построить систему, в которой считыватель производит $O(v)$ вычислений, и при этом вероятность противника нарушить свойство безопасности в IND-модели есть $O(\frac{1}{v})$.

К сожалению из-за особенности работы RFID-системы даже при условии, что протокол аутентификации сохраняет конфиденциальность источника, существуют возможности отслеживать метку, узнавать принадлежность метки некоторому классу меток и другие последствия, не учитываемые моделями (См. [38]).

VIII Вывод

Особенности работы RFID-систем накладывают ряд ограничений на возможность реализации криптографических механизмов. Проведенный анализ основных физических и технических характеристик RFID-систем позволил выделить ключевые требования, которые нужно учитывать при создании криптографических протоколов для рассматриваемых систем.

- Криптографические механизмы защиты целесообразно реализовывать на RFID-метках, которые работают в ближнем поле; данное условие накладывает физические ограничения на дальность считывания и делает менее критичными возможность relay-атак.
- Криптографические протоколы должны быть доступными для реализации на пассивных RFID-метках без собственных автономных источников питания (на активных метках могут могут быть реализованы и более сложные механизмы).
- Реализация криптографии возможна только на RFID-метках, обладающих WORM- или RW-памятью.
- Реализация криптографии на RFID-метке должна занимать сравнимо небольшую площадь (не более 3000-4000GE); в частности, это ограничение приводит к необходимости использовать механизмы симметричной криптографии;

В работе помимо физических ограничений проанализированы также существующие модели противника, характерные для RFID-систем. Эти сведения могут быть использованы в дальнейшем при оценке стойкости криптографических протоколов, предназначенных для RFID-систем.

С помощью криптографических методов защиты информации можно реализовать широкий класс защищенных RFID-систем в зависимости от целевых физических и технологических характеристик системы, а также требований по безопасности. При конструировании простейших систем целесообразно использовать stateless-схемы на основе симметричных криптографических механизмов. Это позволит обеспечить определенный уровень безопасности при небольшой стоимости метки. В случае повышения требований к безопасности можно реализовать stateful-схемы на метках, обладающих перезаписываемой памятью, и обеспечить неотслеживаемость метки, а также реализовать дополнительные средства защиты от relay-атак с использованием физических параметров соединения метки с считывателем.

Библиография

[1] Das Raghu. RFID Forecasts, Players and Opportunities 2019-2029. The complete analysis of the global RFID industry. — URL: https://www.idtechex.com/en/research-report/rfid-forecasts-players-and-opportunities-2019-2029/700. access date: 22.06.2021.

[2] Григорьева Анастасия. Rfid в 2015 и в 2020 году // Компоненты и технологии. — 2021. — Vol. 3.

[3] Scharfeld Tom Ahlkvist. An analysis of the fundamental constraints on low cost passive radio-frequency identification system design : Ph. D. thesis / Tom Ahlkvist Scharfeld ; Massachusetts Institute of Technology. — 2001.

[4] ISO/IEC 18000-2 Information technology - Radio frequency identification for item management - Part 2: Parameters for air interface communications below 135 kHz. — 2009.

[5] ISO/IEC 18000-3 Information technology — Radio frequency identification for item management — Part 3: Parameters for air interface communications at 13,56 MHz. — 2010.

[6] ISO/IEC 18000-7 Information technology — Radio frequency identification for item management — Part 7: Parameters for active air interface communications at 433 MHz. — 2014.

[7] ISO/IEC 18000-6 Information technology — Radio frequency identification for item management — Part 6: Parameters for air interface communications at 860 MHz to 960 MHz General. — 2013.

[8] ISO/IEC 18000-4 Information technology — Radio frequency identification for item management — Part 4: Parameters for air interface communications at 2,45 GHz. — 2018.

[9] Xing Zijian. Near-Field Antenna of RFID System // Radio Frequency Identification. — 2017. — P. 5.

[10] Nikitin Pavel V, Rao KVS, Lazar Steve. An overview of near field UHF RFID // 2007 IEEE international conference on RFID / IEEE. — 2007. — P. 167–174.

[11] ISO/IEC 10536 Identification cards — Contactless integrated circuit(s) cards — Close-coupled cards.

[12] ISO/IEC 14443 Cards and security devices for personal identification — Contactless proximity objects.

[13] ISO/IEC 15693 Cards and security devices for personal identification — Contactless vicinity objects.

[14] STMicroelectronics. — ST25TA512B, ST25TA02KB ST25TA02KB□D, ST25TA02KB□P Datasheet. NFC Forum Type 4 Tag IC with up to 2-Kbit EEPROM, 2018.

[15] NXP Semiconductors. — NTAG213/215/216 NFC Forum Type 2 Tag compliant IC with 144/504/888 bytes user memory, 2015.

[16] STMicroelectronics. — AN5085 Application note. Cycling endurance and data retention of EEPROMs in ST25DVxxx products based on CMOS F8H process, 2018.

[17] Межгосударственный стандарт ГОСТ 34.13-2018 Информационная технология (ИТ). Криптографическая защита информации. Режимы работы блочных шифров.

[18] Shanghai Fudan Microelectronics Group Company Limited. — FM13HF02N HF RFID IC based on ISO/IEC 15693 Datasheet, 2014.

[19] NXP Semiconductors. — MF1P(H)x2 MIFARE Plus EV2 Product short data sheet, 2020.

[20] Fan Junfeng. Cryptographic hardware: how to make it cool, fast and secure // CHES. — 2012.

[21] RFID security: cryptography and physics perspectives / Jorge Guajardo, Pim Tuyls, Neil Bird et al. // RFID Security. — Springer, 2008. — P. 103–130.

[22] ISO/IEC 29167-10 Information technology — Automatic identification and data capture techniques — Part 10: Crypto suite AES-128 security services for air interface communications. — 2017.

[23] Towards the five-cent tag : Rep. / Technical Report MIT-AUTOID-WH-006, MIT Auto ID Center, 2001. Available from ; Executor: Sanjay E Sarma et al. : 2001.

[24] Weis Stephen August. Security and privacy in radio-frequency identification devices : Ph. D. thesis / Stephen August Weis ; Massachusetts Institute of Technology. — 2003.

[25] Pushing the limits: A very compact and a threshold implementation of AES / Amir Moradi, Axel Poschmann, San Ling et al. // Annual International Conference on the Theory and Applications of Cryptographic Techniques / Springer. — 2011. — P. 69–88.

[26] Об одном подходе к формализации задач криптографического анализа (готовится к печати) / Е.К. Алексеев, Л.Р. Ахметзянова, А.М. Зубков et al. // Матем. вопр. криптогр. — 2020.

[27] Ященко В.В. Введение в криптографию. Издание 4, дополненное. — 2012.

[28] RFID systems: A survey on security threats and proposed solutions / Pedro Peris-Lopez, Julio Cesar Hernandez-Castro, Juan M Estevez-Tapiador, Arturo Ribagorda // IFIP international conference on personal wireless communications / Springer. — 2006. — P. 159–170.

[29] Mitrokotsa Aikaterini, Beye Michael, Peris-Lopez Pedro. Classification of RFID Threats based on Security Principles // Security Lab, Faculty of Electrical Engineering, Mathematics and Computer Science, Delft University of Technology. — 2011.

[30] Li Yingjiu, Deng Robert H, Bertino Elisa. RFID security and privacy // Synthesis Lectures on Information Security, Privacy, & Trust. — 2013. — Vol. 4, no. 3. — P. 1–157.

[31] RFID security: a lightweight paradigm / Ahmed Khattab, Zahra Jeddi, Esmaeil Amini, Magdy Bayoumi. — Springer, 2016.

[32] Zhao Kai, Ge Lina. A survey on the internet of things security // 2013 Ninth international conference on computational intelligence and security / IEEE. — 2013. — P. 663–667.

[33] Ali Inayat, Sabir Sonia, Ullah Zahid. Internet of things security, device authentication and access control: a review // arXiv preprint arXiv:1901.07309. — 2019.

[34] Dolev Danny, Yao Andrew. On the security of public key protocols // IEEE Transactions on information theory. — 1983. — Vol. 29, no. 2. — P. 198–208.

[35] Mao Wenbo. Modern cryptography: theory and practice. — Pearson Education India, 2003.

[36] Rfc 8645 re-keying mechanisms for symmetric keys. — 2019.

[37] Damgård Ivan, Pedersen Michael Østergaard. RFID security: Tradeoffs between security and efficiency // Cryptographers' Track at the RSA Conference / Springer. — 2008. — P. 318–332.

[38] van Deursen Ton. 50 ways to break RFID privacy // IFIP PrimeLife International Summer School on Privacy and Identity Management for Life / Springer. — 2010. — P. 192–205.

[39] Goldreich Oded. Foundations of cryptography: volume 1, basic tools. — Cambridge university press, 2007.

[40] Savage John E. Models of computation // Early Years. — 2014. — Vol. 4, no. 1.1. — P. 2.

[41] Message authentication, revisited / Yevgeniy Dodis, Eike Kiltz, Krzysztof Pietrzak, Daniel Wichs // Annual International Conference on the Theory and Applications of Cryptographic Techniques / Springer. — 2012. — P. 355–374.

[42] Mol Petros, Tessaro Stefano. Secret-Key Authentication Beyond the Challenge-Response Paradigm: Definitional Issues and New Protocols // Manuscript, December. — 2012.

[43] Park Namje, Kim Marie, Bang Hyo-Chan. Symmetric key-based authentication and the session key agreement scheme in IoT environment // Computer Science and its Applications. — Springer, 2015. — P. 379–384.

[44] ISO/IEC 29167-11 Information technology — Automatic identification and data capture techniques — Part 11: Crypto suite PRESENT-80 security services for air interface communications. — 2014.

[45] ISO/IEC 29167-21 Information technology — Automatic identification and data capture techniques — Part 21: Crypto suite SIMON security services for air interface communications. — 2018.

[46] ISO/IEC 29167-22 Information technology — Automatic identification and data capture techniques — Part 22: Crypto suite SPECK security services for air interface communications. — 2018.

[47] Security and privacy aspects of low-cost radio frequency identification systems / Stephen A Weis, Sanjay E Sarma, Ronald L Rivest, Daniel W Engels // Security in pervasive computing. — Springer, 2004. — P. 201–212.

[48] Cryptographic approach to "privacy-friendly" tags / Miyako Ohkubo, Koutarou Suzuki, Shingo Kinoshita et al. // RFID privacy workshop / Cambridge, USA. — Vol. 82. — 2003.

[49] PRESENT: An ultra-lightweight block cipher / Andrey Bogdanov, Lars R Knudsen, Gregor Leander et al. // International workshop on cryptographic hardware and embedded systems / Springer. — 2007. — P. 450–466.

[50] The SIMON and SPECK lightweight block ciphers / Ray Beaulieu, Douglas Shors, Jason Smith et al. // Proceedings of the 52nd Annual Design Automation Conference. — 2015. — P. 1–6.

[51] Lee Jun-Ya, Lin Wei-Cheng, Huang Yu-Hung. A lightweight authentication protocol for internet of things // 2014 International Symposium on Next-Generation Electronics (ISNE) / IEEE. — 2014. — P. 1–2.

[52] Li Ming, Dai Zhao Peng, Xi Fang. A new scheme on XOR Operation for Low-cost RFID // Applied Mechanics and Materials / Trans Tech Publ. — Vol. 303. — 2013. — P. 2207–2210.

[53] Ren X., Xu X., Tang Hong-jun. A new mutual authentication scheme for low-cost RFID // 2007 IET Conference on Wireless, Mobile and Sensor Networks (CCWMSN07). — 2007. — P. 170–173.

[54] LMAP: A real lightweight mutual authentication protocol for low-cost RFID tags / Pedro Peris-Lopez, Julio Cesar Hernandez-Castro, Juan M Estévez-Tapiador, Arturo Ribagorda // Proc. of 2nd Workshop on RFID Security. — Vol. 6. — 2006.

[55] M^2AP: a minimalist mutual-authentication protocol for low-cost RFID tags / Pedro Peris-Lopez, Julio Cesar Hernandez-Castro, Juan M Estevez-Tapiador, Arturo Ribagorda // International conference on ubiquitous intelligence and computing / Springer. — 2006. — P. 912–923.

[56] Li Ticyan, Wang Guilin. Security analysis of two ultra-lightweight RFID authentication protocols // IFIP international information security conference / Springer. — 2007. — P. 109–120.

[57] Avoine Gildas, Carpent Xavier, Martin Benjamin. Strong authentication and strong integrity (SASI) is not that strong // International workshop on radio frequency identification: security and privacy issues / Springer. — 2010. — P. 50–64.

[58] Schnorr Claus-Peter. Efficient identification and signatures for smart cards // Conference on the Theory and Application of Cryptology / Springer. — 1989. — P. 239–252.

[59] Menezes Alfred J, Van Oorschot Paul C, Vanstone Scott A. Handbook of applied cryptography. — CRC press, 2018.

[60] Kumar Sandeep, Paar Christof. Are standards compliant elliptic curve cryptosystems feasible on RFID // Workshop on RFID security / Citeseer. — 2006. — P. 12–14.

[61] Elliptic-curve-based security processor for RFID / Yong Ki Lee, Kazuo Sakiyama, Lejla Batina, Ingrid Verbauwhede // IEEE Transactions on Computers. — 2008. — Vol. 57, no. 11. — P. 1514–1527.

[62] A milestone towards RFID products offering asymmetric authentication based on elliptic curve cryptography / Holger Bock, Michael Braun, Markus Dichtl et al. // Invited talk at RFIDsec. — 2008.

[63] ISO/IEC 29167-16 Information technology — Automatic identification and data capture techniques — Part 16: Crypto suite ECDSA"=ECDH security services for air interface communications. — 2015.

[64] A low-cost PKC-based RFID authentication protocol and its implementation / Lili Wei, Zhaotong Luo, Qiang Qu et al. // 2014 Tenth International Conference on Computational Intelligence and Security / IEEE. — 2014. — P. 415–419.

[65] Hopper Nicholas J, Blum Manuel. Secure human identification protocols // International conference on the theory and application of cryptology and information security / Springer. — 2001. — P. 52–66.

[66] Juels Ari, Weis Stephen A. Authenticating pervasive devices with human protocols // Annual international cryptology conference / Springer. — 2005. — P. 293–308.

[67] Gilbert Henri, Robshaw Matthew JB, Seurin Yannick. $hb^{\#}$: Increasing the Security and Efficiency of HB+ // Annual International Conference on the Theory and Applications of Cryptographic Techniques / Springer. — 2008. — P. 361–378.

[68] Bringer Julien, Chabanne Hervé, Dottax Emmanuelle. hb^{++}: a Lightweight Authentication Protocol Secure against Some Attacks // Second international workshop on security, privacy and trust in pervasive and ubiquitous computing (SecPerU'06) / IEEE. — 2006. — P. 28–33.

[69] Munilla Jorge, Peinado Alberto. HB-MP: A further step in the HB-family of lightweight authentication protocols // Computer Networks. — 2007. — Vol. 51, no. 9. — P. 2262–2267.

[70] Efficient authentication from hard learning problems / Eike Kiltz, Krzysztof Pietrzak, Daniele Venturi et al. // Journal of Cryptology. — 2017. — Vol. 30, no. 4. — P. 1238–1275.

[71] Ouafi Khaled, Overbeck Raphael, Vaudenay Serge. On the security of $HB^{\#}$ against a man-in-the-middle attack // International Conference on the Theory and Application of Cryptology and Information Security / Springer. — 2008. — P. 108–124.

[72] Gilbert Henri, Robshaw Matthew JB, Seurin Yannick. Good variants of HB+ are hard to find // International Conference on Financial Cryptography and Data Security / Springer. — 2008. — P. 156–170.

[73] O'Neill Maire et al. Low-cost SHA-1 hash function architecture for RFID tags // RFIDSec. — 2008. — Vol. 8. — P. 41–51.

[74] Feldhofer Martin, Rechberger Christian. A case against currently used hash functions in RFID protocols // OTM Confederated International Conferences" On the Move to Meaningful Internet Systems" / Springer. — 2006. — P. 372–381.

[75] Hash functions and RFID tags: Mind the gap / Andrey Bogdanov, Gregor Leander, Christof Paar et al. // International workshop on cryptographic hardware and embedded systems / Springer. — 2008. — P. 283–299.
[76] ISO/IEC 29167-14 Information technology — Automatic identification and data capture techniques — Part 14: Crypto suite AES OFB security services for air interface communications. — 2015.
[77] Bellare Mihir, Rogaway Phillip. Entity authentication and key distribution // Annual international cryptology conference / Springer. — 1993. — P. 232–249.
[78] Bellare Mihir, Rogaway Phillip. Introduction to modern cryptography // UCSD CSE. — 2005. — Vol. 207. — P. 207.
[79] Schneier Bruce. Applied cryptography: protocols, algorithms, and source code in C. — John Wiley & sons, 2007.
[80] Stinson Douglas Robert, Paterson Maura. Cryptography: theory and practice. — CRC press, 2018.
[81] Wetzels Jos. Broken keys to the kingdom: Security and privacy aspects of RFID-based car keys // arXiv preprint arXiv:1405.7424. — 2014.
[82] Brands Stefan, Chaum David. Distance-bounding protocols // Workshop on the Theory and Application of of Cryptographic Techniques / Springer. — 1993. — P. 344–359.
[83] A framework for analyzing RFID distance bounding protocols / Gildas Avoine, Muhammed Ali Bingöl, Süleyman Kardaş et al. // Journal of Computer Security. — 2011. — Vol. 19, no. 2. — P. 289–317.
[84] A formal approach to distance-bounding RFID protocols / Ulrich Dürholz, Marc Fischlin, Michael Kasper, Cristina Onete // International Conference on Information Security / Springer. — 2011. — P. 47–62.
[85] Katz Jonathan, Lindell Yehuda. Introduction to modern cryptography. — Chapman and Hall/CRC, 2014.
[86] Rosulek Mike. The joy of cryptography // Oregon State University EOR. — 2018. — P. 1.
[87] Bellare Mihir, Namprempre Chanathip. Authenticated encryption: Relations among notions and analysis of the generic composition paradigm // International Conference on the Theory and Application of Cryptology and Information Security / Springer. — 2000. — P. 531–545.
[88] Shrimpton Tom. A characterization of authenticated-encryption as a form of chosen-ciphertext security. // IACR Cryptol. ePrint Arch. — 2004. — Vol. 2004. — P. 272.
[89] 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; Security architecture (Release 16). — 2020.
[90] Juels Ari, Weis Stephen A. Defining Strong Privacy for RFID // Proceedings of the Fifth IEEE International Conference on Pervasive Computing and Communications Workshops. — 2007. — P. 342–347.
[91] Avoine Gildas. Adversarial Model for Radio Frequency Identification. // IACR Cryptol. ePrint Arch. — 2005. — Vol. 2005, no. 7. — P. 49–62.
[92] On two RFID privacy notions and their relations / Yingjiu Li, Robert H Deng, Junzuo Lai, Changshe Ma // ACM Transactions on Information and System Security (TISSEC). — 2008. — Vol. 14, no. 4. — P. 1–23.
[93] A new framework for RFID privacy / Robert H Deng, Yingjiu Li, Moti Yung, Yunlei Zhao // European Symposium on Research in Computer Security / Springer. — 2010. — P. 1–18.
[94] A zero-knowledge based framework for RFID privacy / Robert H Deng, Yingjiu Li, Moti Yung, Yunlei Zhao // Journal of Computer Security. — 2011. — Vol. 19, no. 6. — P. 1109–1146.
[95] Vaudenay Serge. On privacy models for RFID // International conference on the theory and application of cryptology and information security / Springer. — 2007. — P. 68–87.
[96] Paise Radu-Ioan, Vaudenay Serge. Mutual authentication in RFID: security and privacy // Proceedings of the 2008 ACM symposium on Information, computer and communications security. — 2008. — P. 292–299.
[97] Molnar David, Soppera Andrea, Wagner David. A scalable, delegatable pseudonym protocol enabling ownership transfer of RFID tags // International workshop on selected areas in cryptography / Springer. — 2005. — P. 276–290.

Security of RFID systems

V. Belsky, E. Griboedova, K. Tsaregorodtsev, A. Chichaeva

***Abstract*—Radio-frequency tags (RFID tags) are widely used throughout the world to identify and authenticate objects.**

Due to the architectural features and in order to minimize implementation cost RFID tags are often subject to considerable restrictions (memory resources, computing power, chip area, etc), which, in turn, has a significant impact on the used cryptographic mechanisms and protocols. Existing cryptographic standards from other fields are not suitable for RFID systems, that is why the development of new RFID-specific algorithms is necessary.

In this article, we give a classification of RFID systems and describe typical scenarios for their use. We focus on the comparative analysis of the existing cryptographic mechanisms, considering the particularities of radio-frequency identification systems. We list important operational and cryptographic features that must be taken into account during RFID system development. We conclude with an overview of currently known security models that are used to analyze cryptographic protocols for RFID systems.

***Keywords*—cryptographic protocols / RFID, authentication protocol, Security and privacy**

References

[1] Das Raghu. RFID Forecasts, Players and Opportunities 2019-2029. The complete analysis of the global RFID industry. — URL: https://www.idtechex.com/en/research-report/rfid-forecasts-players-and-opportunities-2019-2029/700. access date: 22.06.2021.

[2] Grigor'eva Anastasiya. RFID v 2015 i v 2020 godu // Komponenty i tekhnologii. — 2021. — Vol. 3. — In Russian.

[3] Scharfeld Tom Ahlkvist. An analysis of the fundamental constraints on low cost passive radio-frequency identification system design : Ph. D. thesis / Tom Ahlkvist Scharfeld ; Massachusetts Institute of Technology. — 2001.

[4] ISO/IEC 18000-2 Information technology - Radio frequency identification for item management - Part 2: Parameters for air interface communications below 135 kHz. — 2009.

[5] ISO/IEC 18000-3 Information technology — Radio frequency identification for item management — Part 3: Parameters for air interface communications at 13,56 MHz. — 2010.

[6] ISO/IEC 18000-7 Information technology — Radio frequency identification for item management — Part 7: Parameters for active air interface communications at 433 MHz. — 2014.

[7] ISO/IEC 18000-6 Information technology — Radio frequency identification for item management — Part 6: Parameters for air interface communications at 860 MHz to 960 MHz General. — 2013.

[8] ISO/IEC 18000-4 Information technology — Radio frequency identification for item management — Part 4: Parameters for air interface communications at 2,45 GHz. — 2018.

[9] Xing Zijian. Near-Field Antenna of RFID System // Radio Frequency Identification. — 2017. — P. 5.

[10] Nikitin Pavel V, Rao KVS, Lazar Steve. An overview of near field UHF RFID // 2007 IEEE international conference on RFID / IEEE. — 2007. — P. 167–174.

[11] ISO/IEC 10536 Identification cards — Contactless integrated circuit(s) cards — Close-coupled cards.

[12] ISO/IEC 14443 Cards and security devices for personal identification — Contactless proximity objects.

[13] ISO/IEC 15693 Cards and security devices for personal identification — Contactless vicinity objects.

[14] STMicroelectronics. — ST25TA512B, ST25TA02KB ST25TA02KB□D, ST25TA02KB□P Datasheet. NFC Forum Type 4 Tag IC with up to 2-Kbit EEPROM, 2018.

[15] NXP Semiconductors. — NTAG213/215/216 NFC Forum Type 2 Tag compliant IC with 144/504/888 bytes user memory, 2015.

[16] STMicroelectronics. — AN5085 Application note. Cycling endurance and data retention of EEPROMs in ST25DVxxx products based on CMOS F8H process, 2018.

[17] Mezhgosudarstvennyj standart GOST 34.13-2018 Informacionnaya tekhnologiya (IT). Kriptograficheskaya zashchita informacii. Rezhimy raboty blochnyh shifrov. — In Russian.

[18] Shanghai Fudan Microelectronics Group Company Limited. — FM13HF02N HF RFID IC based on ISO/IEC 15693 Datasheet, 2014.

[19] NXP Semiconductors. — MF1P(H)x2 MIFARE Plus EV2 Product short data sheet, 2020.

[20] Fan Junfeng. Cryptographic hardware: how to make it cool, fast and secure // CHES. — 2012.

[21] RFID security: cryptography and physics perspectives / Jorge Guajardo, Pim Tuyls, Neil Bird et al. // RFID Security. — Springer, 2008. — P. 103–130.

[22] ISO/IEC 29167-10 Information technology — Automatic identification and data capture techniques — Part 10: Crypto suite AES-128 security services for air interface communications. — 2017.

[23] Towards the five-cent tag : Rep. / Technical Report MIT-AUTOID-WH-006, MIT Auto ID Center, 2001. Available from ; Executor: Sanjay E Sarma et al. : 2001.

[24] Weis Stephen August. Security and privacy in radio-frequency identification devices : Ph. D. thesis / Stephen August Weis ; Massachusetts Institute of Technology. — 2003.

[25] Pushing the limits: A very compact and a threshold implementation of AES / Amir Moradi, Axel Poschmann, San Ling et al. // Annual International Conference on the Theory and Applications of Cryptographic Techniques / Springer. — 2011. — P. 69–88.

[26] Ob odnom podhode k formalizacii zadach kriptograficheskogo analiza / E.K. Alekseev, L.R. Ahmetzyanova, A.M. Zubkov et al. // Matematicheskie Voprosy Kriptografii (Mathematical Aspects of Cryptography). — 2020. — In Russian.

[27] Yashchenko V.V. Vvedenie v kriptografiyu.-izdanie 4 dopolnennoe-mcnmo: Moskva, 2012 g. — 2012. — In Russian.

[28] RFID systems: A survey on security threats and proposed solutions / Pedro Peris-Lopez, Julio Cesar Hernandez-Castro, Juan M Estevez-Tapiador, Arturo Ribagorda // IFIP international conference on personal wireless communications / Springer. — 2006. — P. 159–170.

[29] Mitrokotsa Aikaterini, Beye Michael, Peris-Lopez Pedro. Classification of RFID Threats based on Security Principles // Security Lab, Faculty of Electrical Engineering, Mathematics and Computer Science, Delft University of Technology. — 2011.

[30] Li Yingjiu, Deng Robert H, Bertino Elisa. RFID security and privacy // Synthesis Lectures on Information Security, Privacy, & Trust. — 2013. — Vol. 4, no. 3. — P. 1–157.

[31] RFID security: a lightweight paradigm / Ahmed Khattab, Zahra Jeddi, Esmaeil Amini, Magdy Bayoumi. — Springer, 2016.

[32] Zhao Kai, Ge Lina. A survey on the internet of things security // 2013 Ninth international conference on computational intelligence and security / IEEE. — 2013. — P. 663–667.

[33] Ali Inayat, Sabir Sonia, Ullah Zahid. Internet of things security, device authentication and access control: a review // arXiv preprint arXiv:1901.07309. — 2019.

[34] Dolev Danny, Yao Andrew. On the security of public key protocols // IEEE Transactions on information theory. — 1983. — Vol. 29, no. 2. — P. 198–208.

[35] Mao Wenbo. Modern cryptography: theory and practice. — Pearson Education India, 2003.

[36] Rfc 8645 re-keying mechanisms for symmetric keys. — 2019.

[37] Damgård Ivan, Pedersen Michael Østergaard. RFID security: Tradeoffs between security and efficiency // Cryptographers' Track at the RSA Conference / Springer. — 2008. — P. 318–332.

[38] van Deursen Ton. 50 ways to break RFID privacy // IFIP PrimeLife International Summer School on Privacy and Identity Management for Life / Springer. — 2010. — P. 192–205.

[39] Goldreich Oded. Foundations of cryptography: volume 1, basic tools. — Cambridge university press, 2007.

[40] Savage John E. Models of computation // Early Years. — 2014. — Vol. 4, no. 1.1. — P. 2.

[41] Message authentication, revisited / Yevgeniy Dodis, Eike Kiltz, Krzysztof Pietrzak, Daniel Wichs // Annual International Conference on the Theory and Applications of Cryptographic Techniques / Springer. — 2012. — P. 355–374.

[42] Mol Petros, Tessaro Stefano. Secret-Key Authentication Beyond the Challenge-Response Paradigm: Definitional Issues and New Protocols // Manuscript, December. — 2012.

[43] Park Namje, Kim Marie, Bang Hyo-Chan. Symmetric key-based authentication and the session key agreement scheme in IoT environment // Computer Science and its Applications. — Springer, 2015. — P. 379–384.

[44] ISO/IEC 29167-11 Information technology — Automatic identification and data capture techniques — Part 11: Crypto suite PRESENT-80 security services for air interface communications. — 2014.

[45] ISO/IEC 29167-21 Information technology — Automatic identification and data capture techniques — Part 21: Crypto suite SIMON security services for air interface communications. — 2018.

[46] ISO/IEC 29167-22 Information technology — Automatic identification and data capture techniques — Part 22: Crypto suite SPECK security services for air interface communications. — 2018.

[47] Security and privacy aspects of low-cost radio frequency identification systems / Stephen A Weis, Sanjay E Sarma, Ronald L Rivest, Daniel W Engels // Security in pervasive computing. — Springer, 2004. — P. 201–212.

[48] Cryptographic approach to "privacy-friendly" tags / Miyako Ohkubo, Koutarou Suzuki, Shingo Kinoshita et al. // RFID privacy workshop / Cambridge, USA. — Vol. 82. — 2003.

[49] PRESENT: An ultra-lightweight block cipher / Andrey Bogdanov, Lars R Knudsen, Gregor Leander et al. // International workshop on cryptographic hardware and embedded systems / Springer. — 2007. — P. 450–466.

[50] The SIMON and SPECK lightweight block ciphers / Ray Beaulieu, Douglas Shors, Jason Smith et al. // Proceedings of the 52nd Annual Design Automation Conference. — 2015. — P. 1–6.

[51] Lee Jun-Ya, Lin Wei-Cheng, Huang Yu-Hung. A lightweight authentication protocol for internet of things // 2014 International Symposium on Next-Generation Electronics (ISNE) / IEEE. — 2014. — P. 1–2.

[52] Li Ming, Dai Zhao Peng, Xi Fang. A new scheme on XOR Operation for Low-cost RFID // Applied Mechanics and Materials / Trans Tech Publ. — Vol. 303. — 2013. — P. 2207–2210.

[53] Ren X., Xu X., Tang Hong-jun. A new mutual authentication scheme for low-cost RFID // 2007 IET Conference on Wireless, Mobile and Sensor Networks (CCWMSN07). — 2007. — P. 170–173.

[54] LMAP: A real lightweight mutual authentication protocol for low-cost RFID tags / Pedro Peris-Lopez, Julio Cesar Hernandez-Castro, Juan M Estévez-Tapiador, Arturo Ribagorda // Proc. of 2nd Workshop on RFID Security. — Vol. 6. — 2006.

[55] M^2AP: a minimalist mutual-authentication protocol for low-cost RFID tags / Pedro Peris-Lopez, Julio Cesar Hernandez-Castro, Juan M Estevez-Tapiador, Arturo Ribagorda // International conference on ubiquitous intelligence and computing / Springer. — 2006. — P. 912–923.

[56] Li Ticyan, Wang Guilin. Security analysis of two ultra-lightweight RFID authentication protocols // IFIP international information security conference / Springer. — 2007. — P. 109–120.

[57] Avoine Gildas, Carpent Xavier, Martin Benjamin. Strong authentication and strong integrity (SASI) is not that strong // International workshop on radio frequency identification: security and privacy issues / Springer. — 2010. — P. 50–64.

[58] Schnorr Claus-Peter. Efficient identification and signatures for smart cards // Conference on the Theory and Application of Cryptology / Springer. — 1989. — P. 239–252.

[59] Menezes Alfred J, Van Oorschot Paul C, Vanstone Scott A. Handbook of applied cryptography. — CRC press, 2018.

[60] Kumar Sandeep, Paar Christof. Are standards compliant elliptic curve cryptosystems feasible on RFID // Workshop on RFID security / Citeseer. — 2006. — P. 12–14.

[61] Elliptic-curve-based security processor for RFID / Yong Ki Lee, Kazuo Sakiyama, Lejla Batina, Ingrid Verbauwhede // IEEE Transactions on Computers. — 2008. — Vol. 57, no. 11. — P. 1514–1527.

[62] A milestone towards RFID products offering asymmetric authentication based on elliptic curve cryptography / Holger Bock, Michael Braun, Markus Dichtl et al. // Invited talk at RFIDsec. — 2008.

[63] ISO/IEC 29167-16 Information technology — Automatic identification and data capture techniques — Part 16: Crypto suite ECDSA"=ECDH security services for air interface communications. — 2015.

[64] A low-cost PKC-based RFID authentication protocol and its implementation / Lili Wei, Zhaotong Luo, Qiang Qu et al. // 2014 Tenth International Conference on Computational Intelligence and Security / IEEE. — 2014. — P. 415–419.

[65] Hopper Nicholas J, Blum Manuel. Secure human identification protocols // International conference on the theory and application of cryptology and information security / Springer. — 2001. — P. 52–66.

[66] Juels Ari, Weis Stephen A. Authenticating pervasive devices with human protocols // Annual international cryptology conference / Springer. — 2005. — P. 293–308.

[67] Gilbert Henri, Robshaw Matthew JB, Seurin Yannick. $hb^{\#}$: Increasing the Security and Efficiency of HB+ // Annual International Conference on the Theory and Applications of Cryptographic Techniques / Springer. — 2008. — P. 361–378.

[68] Bringer Julien, Chabanne Hervé, Dottax Emmanuelle. hb^{++}: a Lightweight Authentication Protocol Secure against Some Attacks // Second international workshop on security, privacy and trust in pervasive and ubiquitous computing (SecPerU'06) / IEEE. — 2006. — P. 28–33.

[69] Munilla Jorge, Peinado Alberto. HB-MP: A further step in the HB-family of lightweight authentication protocols // Computer Networks. — 2007. — Vol. 51, no. 9. — P. 2262–2267.

[70] Efficient authentication from hard learning problems / Eike Kiltz, Krzysztof Pietrzak, Daniele Venturi et al. // Journal of Cryptology. — 2017. — Vol. 30, no. 4. — P. 1238–1275.

[71] Ouafi Khaled, Overbeck Raphael, Vaudenay Serge. On the security of $HB^{\#}$ against a man-in-the-middle attack // International Conference on the Theory and Application of Cryptology and Information Security / Springer. — 2008. — P. 108–124.

[72] Gilbert Henri, Robshaw Matthew JB, Seurin Yannick. Good variants of HB+ are hard to find // International Conference on Financial Cryptography and Data Security / Springer. — 2008. — P. 156–170.

[73] O'Neill Maire et al. Low-cost SHA-1 hash function architecture for RFID tags // RFIDSec. — 2008. — Vol. 8. — P. 41–51.

[74] Feldhofer Martin, Rechberger Christian. A case against currently used hash functions in RFID protocols // OTM Confederated International Conferences" On the Move to Meaningful Internet Systems" / Springer. — 2006. — P. 372–381.

[75] Hash functions and RFID tags: Mind the gap / Andrey Bogdanov, Gregor Leander, Christof Paar et al. // International workshop on cryptographic hardware and embedded systems / Springer. — 2008. — P. 283–299.

[76] ISO/IEC 29167-14 Information technology — Automatic identification and data capture techniques — Part 14: Crypto suite AES OFB security services for air interface communications. — 2015.

[77] Bellare Mihir, Rogaway Phillip. Entity authentication and key distribution // Annual international cryptology conference / Springer. — 1993. — P. 232–249.

[78] Bellare Mihir, Rogaway Phillip. Introduction to modern cryptography // UCSD CSE. — 2005. — Vol. 207. — P. 207.

[79] Schneier Bruce. Applied cryptography: protocols, algorithms, and source code in C. — John Wiley & sons, 2007.

[80] Stinson Douglas Robert, Paterson Maura. Cryptography: theory and practice. — CRC press, 2018.

[81] Wetzels Jos. Broken keys to the kingdom: Security and privacy aspects of RFID-based car keys // arXiv preprint arXiv:1405.7424. — 2014.

[82] Brands Stefan, Chaum David. Distance-bounding protocols // Workshop on the Theory and Application of of Cryptographic Techniques / Springer. — 1993. — P. 344–359.

[83] A framework for analyzing RFID distance bounding protocols / Gildas Avoine, Muhammed Ali Bingöl, Süleyman Kardaş et al. // Journal of Computer Security. — 2011. — Vol. 19, no. 2. — P. 289–317.

[84] A formal approach to distance-bounding RFID protocols / Ulrich Dürholz, Marc Fischlin, Michael Kasper, Cristina Onete // International Conference on Information Security / Springer. — 2011. — P. 47–62.

[85] Katz Jonathan, Lindell Yehuda. Introduction to modern cryptography. — Chapman and Hall/CRC, 2014.

[86] Rosulek Mike. The joy of cryptography // Oregon State University EOR. — 2018. — P. 1.

[87] Bellare Mihir, Namprempre Chanathip. Authenticated encryption: Relations among notions and analysis of the generic composition paradigm // International Conference on the Theory and Application of Cryptology and Information Security / Springer. — 2000. — P. 531–545.

[88] Shrimpton Tom. A characterization of authenticated-encryption as a form of chosen-ciphertext security. // IACR Cryptol. ePrint Arch. — 2004. — Vol. 2004. — P. 272.

[89] 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; Security architecture (Release 16). — 2020.

[90] Juels Ari, Weis Stephen A. Defining Strong Privacy for RFID // Proceedings of the Fifth IEEE International Conference on Pervasive Computing and Communications Workshops. — 2007. — P. 342–347.

[91] Avoine Gildas. Adversarial Model for Radio Frequency Identification. // IACR Cryptol. ePrint Arch. — 2005. — Vol. 2005, no. 7. — P. 49–62.
[92] On two RFID privacy notions and their relations / Yingjiu Li, Robert H Deng, Junzuo Lai, Changshe Ma // ACM Transactions on Information and System Security (TISSEC). — 2008. — Vol. 14, no. 4. — P. 1–23.
[93] A new framework for RFID privacy / Robert H Deng, Yingjiu Li, Moti Yung, Yunlei Zhao // European Symposium on Research in Computer Security / Springer. — 2010. — P. 1–18.
[94] A zero-knowledge based framework for RFID privacy / Robert H Deng, Yingjiu Li, Moti Yung, Yunlei Zhao // Journal of Computer Security. — 2011. — Vol. 19, no. 6. — P. 1109–1146.
[95] Vaudenay Serge. On privacy models for RFID // International conference on the theory and application of cryptology and information security / Springer. — 2007. — P. 68–87.
[96] Paise Radu-Ioan, Vaudenay Serge. Mutual authentication in RFID: security and privacy // Proceedings of the 2008 ACM symposium on Information, computer and communications security. — 2008. — P. 292–299.
[97] Molnar David, Soppera Andrea, Wagner David. A scalable, delegatable pseudonym protocol enabling ownership transfer of RFID tags // International workshop on selected areas in cryptography / Springer. — 2005. — P. 276–290.