127106 Россия, Москва
Алтуфьевское шоссе, 5/2
Тел.: +7 (095) 9671451
Факс: +7 (095) 9671452
e-mail: director@random-art.com

Random Art Labs LTD
Annis Komninis Street 29A, Nicosia, Cyprus

В рамках доклада на конференции РусКрипто 2006

Минималистская криптография и ее применение в системах RFID

Оглавление

RA-технологии. Обеспечение безопасности систем RFID

Презентация

«Инструментальные средства обеспечения безопасности RFID технологий»

Литература

1. Способ придания реальному объекту рандомизационных свойств и рандомизационная система.
Международная заявка PCT/RU03/00141, 7 апреля 2003.
2. Система контроля сертификационных меток промышленных товаров.
НИОКР, Московский комитет по науке и технологиям, Москва 2005.
3. The EPC Global
website (www.epcglobalinc.org).
4. RFID and Sensing in the Supply Chain: Challenges and Opportunities
Salil Pradhan, Geoff Lyon, Ian Robertson and others
HP Laboratories Palo Alto HPL-2005-16, February 9, 2005
www.hpl.hp.com/ techreports/2005/HPL-2005-16.pdf
5. Security and Privacy Aspects of Low-Cost Radio Frequency Identification Systems.
Stephen A. Weis, Sanjay E. Sarma, Ronald L. Rivest and Daniel W. Engels,
In Security in Pervasive Computing, 2003.
6. Hitachi. The Word's Smallest RFID ID, μ-chip.
website (www.hitachi.co.jp/Prod/mu-chip).
7. Siemens AG – PolyIC.
website (www.simens.com).

RA-технологии. Обеспечение безопасности систем RFID

В рамках доклада на конференции РусКрипто 2006 «Минималистская криптография и ее применение в системах RFID»

С системных позиций излагаются основы стохастической криптографии и ***R**andom **A**rt* технологий. Особое внимание уделяется минималисткой криптографии и симметричным криптографическим примитивам, с регулируемой в необходимых пределах стойкостью и рассчитанным на реализацию в условиях крайнего дефицита ресурсов (печатные, пластиковые и кремниевые метки RFID). Представленные криптографические примитивы просты в исполнении, допускают масштабирование и распространение на любые платформы и качественно отличаются от существующих аналогов. Типичные варианты реализации вынесены на общее обсуждение и прошли предварительную криптографическую экспертизу.

1. Основы стохастической криптографии

Стохастическая криптография с единых теоретических позиций охватывает все основные разделы симметричной криптографии и представляет собой новое научно-практическое направление развития линейных и нелинейных стохастических систем с дискретным временем. Одним из решающих факторов развития этого направления явилось введение ***неполной арифметики*** и открытие присущих стохастическим системам ***дихотомических свойств***.

Основу стохастической криптографии составляют *дихотомические* и *полихотомические* операторы. ***Дихотомические*** *D*-операторы линейны по архитектуре и выступают в качестве строительных блоков линейных рандомизационных систем и предопределяют направления развития нелинейных систем. ***Полихотомические*** *Ð*-операторы представляются *нелинейным аналогом D*-операторов *нелинейных систем*.

Полихотомические *Ð*-операторы позволяют устранить существенные недостатки присущие дихотомическим операторам, существенно превосходят их в криптографическом отношении и более просты в исполнении.

В свою очередь, особая роль в стохастической криптографии отводится развитию ***минималисткой криптографии***, рассчитанной на супермалые блоки, длиной от 8 до 48 бит, предполагающей реализацию устойчивых к “взлому” криптографических средств и устройств в условиях крайнего дефицита ресурсов, допускающей масштабирование и распространение на традиционные и новые, сверхскоростные и высокопроизводительные криптографические приложения.

Минималисткая криптография и ее продолжения, ***моноблочны*** по архитектуре. Путем комплексирования блоков, моноблочная криптография переходит в ***мультиблочную***, допускающую использование принципов наращиваемой модульной архитектуры, особенно эффективную для программной и аппаратной реализации криптографических решений очень высокой стойкости и производительности.

2. *RA*-технологии и их преимущества

Техническая реализация стохастических систем и стохастической криптографии может быть осуществимо на основе разработанных Компанией, так называемых ***R**andom **A**rt* (***RA***) технологий

RA-технологии в техническом отношении, а также заложенным в них потенциальным возможностям заметно отличается от своих предшественниц, по следующим показателям:

1. **Простота реализации**, обусловленная простейшей линейной архитектурой и топологией, предусматривающей использование однородных линеек, построенных на основе одного из двух элементов - логической операции сложения XOR или конъюнкции И.

2. **Высокая производительность**, представленная возможностью организации всюду параллельной криптографической обработки каждого отдельного бита из блока, со скоростью соизмеримой с выполнением одной логической операции XOR.

3. **Функциональность**, обеспечиваемая нестационарным, многомерным и параметрическим характером схем реализаций, построенных на основе управляемых операций, позволяющая успешно противостоять известным криптографическим атакам.

4. **Устойчивость к сторонним атакам**, за счет элементарного набора задействуемых операций, параметризации, недетерминизма и параллелизма.

5. **Низкое энергопотребление и себестоимость**, достигаемые благодаря простым схемотехническим решениям и малым аппаратным затратам, не требующим привлечения адресуемой памяти и дорогостоящей процессорной обработки.

6. **Масштабируемость**, от супермалых блоков длиной 8 бит и до супербольших, длиной в 512 и более бит, достигаемая за счет использования экспоненциально нарастающих, лавинных эффектов и механизмов распространения влияния бит.

7. **Структурная гибкость**, от возможности комплексирования блоков и использования наращиваемой модульной архитектуры, до возможности построения целостных сетевых систем любой сложности.

8. **Открытость и прозрачность** для экспертного анализа, наличие общей методики комплексной оценки стохастической надежности и криптографической стойкости разрабатываемых приложений.

9. **Глубина и ширина охвата**, вытекающая из фундаментального и высокопродуктивного характера используемой теоретической базы, высокого уровня обобщения и формализации, унификации и стандартизации оптимальных решений.

Исходя из приоритетов научно-технической деятельности Компании и потребностей рынка, к настоящему времени наиболее детально отработаны решения, связанные с построением генераторов (псевдо) случайных чисел, используемых в системах управления ключами и поточного шифрования, включая основанные на симметричной криптографии протоколы и задачи проведения идентификации, односторонней и взаимной аутентификации объектов, хеширования и выработки показателей контроля целостности информации.

В основу ***RA***-технологий положены «Способ придания реальному объекту рандомизационных свойств и рандомизационная система», нашедших свое отражение в заявке на международный патент PCT/RU03/00141, 7 апреля 2003 года.

3. Инструментальные средства *RA*-технологий

Исходя из требований, предъявляемым к элементам современных криптографических систем, на основе ***RA***-технологий, проведена разработка и апробация широкого класса математических алгоритмов и вычислительных программ, пригодных для их самостоятельного использования в программных продуктах и аппаратной реализации соответствующих им рандомизационных устройств, объединенных под общим названием – ***инструментальные средства RA***-технологий.

Инструментальные средства ***RA***-технологий рассчитаны на перспективу и включают в себя, следующие (сопровождаемые не строгими определениями) компоненты:

Дихотомический оператор – рандомизационный оператор, способный порождать путем последовательных его итераций, одну иди несколько, так называемых *дихотомических последовательностей*, составленных из неотрицательных целых двоичных чисел 0,1,2 …, разрядностью $\boldsymbol{n}$, обладающих свойствами присущим битам последовательности, формируемым на основе ординарных счетчиков, типа $\boldsymbol{x}_i = \boldsymbol{x}_{i-1} \pm \boldsymbol{c}$.

Нелинейный счетчик *(дихотомический счетчик)* – рандомизационный генератор инкрементного или декрементного типа $\boldsymbol{x}_i = \boldsymbol{x}_{i-1} \pm \boldsymbol{c}$, предназначенный для формирования простейшей дихотомической последовательности, путем последовательных итераций составляющего его простейшего дихотомического оператора.

Дихотомический генератор – рандомизационный генератор, построенный на основе дихотомических счетчиков, с дихотомическим оператором, предусматривающим ускоренное распространение влияния младших битов на старшие, предназначенный для формирования одной или нескольких сложно устроенных дихотомических последовательностей, одновременно, с периодом повторения 2^n.

Генератор ключевого потока *(рандомизационный, бесповторный)* – стохастический генератор, предназначенный для формирования бесповторных последовательностей неотрицательных целых двоичных чисел, с периодом повторения 2^n, путем биективных (взаимно однозначных) преобразований исходных для них дихотомических последовательностей.

Односторонний оператор *(рандомизационный)* – стохастический оператор от многих двоичных переменных, построенный на основе дихотомических операторов, предназначенный для получения необратимого образа преобразований по одному из своих аргументов, за счет недетерминированного характера изменения множества остальных его аргументов.

Генератор гаммы *(рандомизационный)* – стохастический генератор, построенный на основе односторонних операторов, предназначенный для формирование равноповторных последовательностей неотрицательных целых двоичных чисел, с периодом не менее заданного.

Однонаправленный оператор *(рандомизационный)* – стохастический оператор от многих двоичных переменных, образуемый путем конечного числа последовательных итераций *(раундов)* входящего в его состав одностороннего оператора.

В контексте стохастических (рандомизационных) систем, псевдослучайные ***PR****-функции* и *операторы* аутентификации, ***хеш****-функции* и *операторы*, ***MAC****-функции* и *операторы* сжатия данных и выработки показателей контроля целостности информации – рассматриваются как специальный класс однонаправленных операторов, именуемых ***рандомизационными агрегатами***.

Функционально законченные компоненты инструментальных средств ***RA***-технологий именуются ***криптографическими примитивами*** стохастической криптографии.

4. Первоочередные задачи реализации *RA*-технологий

Среди первоочередных задач внедрения ***RA***-технологий, как наиболее перспективных с точки зрения продвижения решений компании на рынок, отводится задачам защиты материальных объектов от клонирования, фальсификации и подделки, предотвращению попыток жульничества, воровства и других несанкционированных действий на основе технологий RFID:

- защита продукции от клонирования, фальсификации и подделки;
- осуществление мелких денежных расчетов и платежей;
- маркировка и контроль ресурса оборудования, устройств, узлов и деталей, снаряжения, оружия и боеприпасов;
- защита транспортных средств от хищений (угонов), дистанционное выявление похищенных средств;
- электронное клеймение растений, животных, скота и птицы;
- защита и заверение документов и ценных бумаг;
- защита национальной валюты**;**
- другие задачи, включая задачи предотвращения несанкционированного доступа и организации пропускного режима.

Защита продукции от клонирования, фальсификации и подделки может быть эффективно осуществлена в системе защиты товарного рынка от фальсифицированной и контрафактной продукции. Выбор Компанией решения этой задачи в качестве ***темы первого плана*** далеко не случаен и обусловлен следующими факторами:

Во-первых, задача защиты товарного рынка от фальсифицированной и контрафактной продукции, сама по себе актуальна и вместе с другими задачами ***в системе регулирования товарного рынка***, способна совершить экономический переворот в сфере производства и реализации товаров на рынке.

Во-вторых, в основе защиты лежит идея привлечения широких слоев населения к контролю товарного рынка, на основе общедоступных в пунктах продажи и недорогих индивидуальных устройств проверки подлинности приобретаемого товара. По сути, в отличие от предпо-

читаемых ныне силового давления и сдерживающих властных ограничений, тем самым подключаются дополнительные сильные механизмы, позволяющие осуществить последовательный и взвешенный переход от малоэффективного ведомственного государственного контроля, ***к широкомасштабному действенному общественному контролю товарного рынка***.

В-третьих, по общему мнению специалистов, без прорыва в области производства дешевых (печатных, пластиковых, кремниевых) радиочастотных меток и недорогих устройств проверки подлинности меток, а также достижений Компании в области ***минималисткой криптографии***, предполагающей реализацию в условиях крайнего дефицита ресурсов устойчивых к "взлому" криптографических устройств, действенное и рентабельное решение задачи защиты продукции от клонирования, фальсификации и подделки, не представляется возможным.

5. Состояние *RA*-технологий

Объективно, ***RA***-технологии характеризуются малой известностью и своей относительной молодостью, если судить исходя из даты регистрации заявка на международный патент, а это 2003 год, когда открытая публикация не коммерчески значимой части материалов стала возможной. На самом деле, технология не так уж и молода, если принять во внимание более чем десятилетний период разработки, предшествующий оформлению и подаче международной заявки.

С внедрением ***RA***-технологий, а также разрабатываемых на их основе устройств и систем, по мнению специалистов по системной аналитике, схемотехническим решениям и криптографии связаны следующие ***риски***:

1. Неосуществимость механизмов интеграции элементов систем и протоколов защиты.
2. Невозможность аппаратной реализации решений и достижения их надлежащих технических и стоимостных показателей. Уязвимость устройств к сторонним атакам.
3. Компрометация статистической надежности и криптографической стойкости предлагаемых инструментальных средств.

Для обоснования и подтверждения практической реализуемости ***RA***-технологий, в 2004-2005 г., совместно с **Московским комитетом по науке и технологиям** была проведена промежуточная НИОКР, по теме ***Система контроля сертификационных меток промышленных товаров***, на основе технологий RFID. Система получила свое дальнейшее развитие в ***Концепции регулирования товарного рынка*** и исследовательской работе проведенной Компанией по ***Обеспечению безопасности технологий RFID***.

Обращаясь к теоретическим основам ***RA***-технологий прозвучавших в секционном докладе, заключениям экспертов и дополнительным решениям по устранению замечаний, а также к результатам разработки, рассчитанного на различные вычислительные платформы набора инструментальных средств и их машинного моделирования, по представленным *типичным открытым решениям*, можно сделать следующие общие выводы:

1. Разработанные на основе ***RA***-технологий генераторы ключевого потока и многоуровневые протоколы управления ключами, позволяют организовать сетевую обработку, необходимую для построения сложных распределенных систем, интеграции и защиты ее элементов.
2. Инструментальные средства представляемые Компанией допускают эффективную аппаратную реализацию в условиях крайнего дефицита ресурсов. Построенные на их основе устройства, фактически обладают предельно высокой производительностью и требуют малых аппаратных затрат, не сказывающихся на рентабельности их производства.
3. Устройства, разрабатываемые на основе ***RA***-технологий, за счет параметризации и полного параллелизма не уязвимы к сторонним атакам. Зависимость секретных ключей от существенных внешних признаков защищаемых объектов и многоуровневые протоколы защиты мастер ключей, делает их устойчивыми и к физическому взлому.
4. Инструментальные средства обладают статистической надежностью, подтверждаемой на основе проверенных пакетов статистических тестов, достаточной для их практического использования.

5. Имитационное статистическое моделирование линейных, дифференциальных и корреляционных атак, представленных инструментальными средствами криптографических примитивов, дает основание предполагать о возможности достижения необходимого уровня криптографической стойкости построенных на их основе устройств.

Как следует из представленных положений, в зону рисков попадают инструментальные средства, к которым предъявляются высокие требования к их криптографической стойкости, а имитационное моделирование не дает гарантий выполнения этого требования.

Результаты имитационного моделирования подтверждаются на примере криптографического анализа 32-х разрядного алгоритма односторонней аутентификации, проведенного известным всем экспертом фирмы **ЛанКрипто**, Ивановым Александром Евгеньевичем. Результаты анализа допускают масштабирование и распространение, на другие криптографические платформы и примитивы односторонней и взаимной аутентификации, псевдослучайные функции и операторы, а также, при введении соответствующих усилений и на генераторы гаммы, хеш-функции и операторы выработки показателей контроля целостности информации. А это, без учета генераторов ключевого потока, фактически вся и значительная часть инструментальных средств стохастической криптографии, причем часть, находящаяся в зоне особо сильных криптографических рисков.

Не смотря на полученные вполне достаточные для практической реализации результаты, представленный алгоритм аутентификации предполагает ряд усилений, не учтенных в атаке, позволяющих существенным образом улучшить его статистические и криптографические показатели. Из них, особенно эффективна замена алгоритма его нелинейным аналогом, позволяющая устранить присущие линейным системам серьезные недостатки.

В качестве первой, наиболее приоритетной задачи предполагающей развитие минималисткой криптографии, предполагается реализация ***Проекта обеспечения безопасности технологий RFID***. Центральным местом проекта, является разработка протокола и криптографического примитива проверки подлинности (аутентификации) меток RFID. В качестве такого примитива используются рандомизационные агрегаты, разработанные Компанией.

6. Рандомизационные агрегаты

По определению, рандомизационные агрегаты, определенные на множестве m двоичных входов – модификаторов H и множестве n выходов Z, порождают семейство однонаправленных псевдослучайных ***PR-операторов*** $\mathcal{F}_m = \{f_K(H)\}_{K \in \Omega_K}$ (Рис.2), а при одном выходе ***PR-функций*** $\mathcal{F} = \{f_K(H)\}_{K \in \Omega_K}$ (Рис.1), определенных на множестве состояний $\Upsilon = \Upsilon_H \times \Upsilon_K$.

Здесь, $\Omega_K = \{K\}$ и $\Omega_H = \{H\}$ – множества всех допустимых ключей K и модификаторов H, а Υ_H и Υ_K пространства модификации и состояний, соответственно, формируемые $\Upsilon_H = \mathcal{H}(\Omega_H)$ и $\Upsilon_K = \mathcal{K}(\Omega_K)$ по пространство модификаторов Ω_H, и ключевому пространству Ω_K.

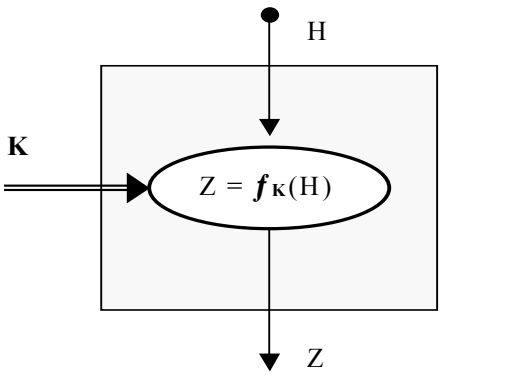


Рис. 1. Одномерная ***PR***-функция

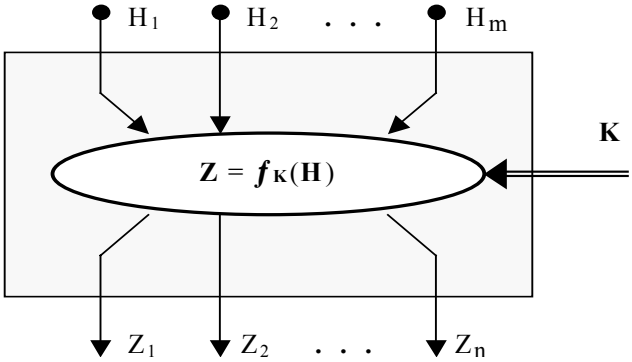


Рис. 2. Многомерный ***PR***-оператор

На основе W^q-агрегатов, при открытом ключе K могут быть построены, соответственно, одномерные и многомерные ***хеш-функции и операторы***, при секретном ключе – ***MAC-функции и операторы*** выработки показателей контроля целостности информации.

По открытым ключам – модификаторам (синхропосылки) $\boldsymbol{H}_0$, устанавливаемых прямо или по открытому ключу $\boldsymbol{K}_0$, можно перестраивать работу W^q-агрегатов.

Исходя из общих криптографических требований, в этом случае необходимо, чтобы несущественные линейные изменения $\boldsymbol{H}_0$ на входе W^q-агрегатов, приводили к существенным нелинейным изменениям на их выходе.

Рандомизационные агрегаты с косвенным выходом – $\boldsymbol{Z}_q = \boldsymbol{G}_q \oplus \boldsymbol{V}_q$, после завершения q раундов, гарантирующих установленный уровень криптографической безопасности и модификации выходной переменной $\boldsymbol{G}_q = \boldsymbol{G}_q \oplus \boldsymbol{W}_q$, где $\boldsymbol{W}_q$ – рандомизационная переменная D-оператора $(\boldsymbol{W}_q \neq \boldsymbol{V}_q)$, допускают перевод в режим поточного шифрования n-битовых блоков данных $\boldsymbol{I}_i$

$$\boldsymbol{O}_i = \boldsymbol{G}_{q+i} \oplus \boldsymbol{I}_i \qquad (i = \overline{1,m})$$

или режим расшифрования поступающей информации $\boldsymbol{O}_i$

$$\boldsymbol{I}_i = \boldsymbol{G}_{q+i} \oplus \boldsymbol{O}_i,$$

но при этом, число шифрируемых блоков m не должно сказываться на общей криптографической стойкости агрегата.

7. Протокол односторонней аутентификации

Аутентификация, происшедшее от греч. *authentikos* – аутентичный (действительный, подлинный, соответствующий подлинному), в общесистемном контексте предполагает наличие субъекта и означает проверку подлинности противостоящего ему объекта.

Если при этом момент имеет место такое же обратное действие, аутентификация называется *взаимной*, если нет – *односторонней*.

Последовательность действий, заканчивающаяся подтверждением подлинности объекта, именуется ***протоколом односторонней аутентификации***.

В криптографическом аспекте, протокол аутентификации предполагает проверку на соответствие секрета имеющегося у субъекта и секрета скрытого в аутентифицируемом объекте. В симметричной (минималисткой, стохастической) криптографии, собственно методами и положениями которой мы руководствуемся, этот секрет задается, защищенным от компрометации и разглашения уникальным ***ключом аутентификации***.

В статье ***Security and Privacy Aspects of Low-Cost Radio Frequency Identification Systems***, группы пользующихся мировой известностью экспертов **Weis S., Sarma S., Rivest R.** и **Engels D.**, опубликованной In Security in Pervasive Computing, 2003, рассматривается несколько схем обеспечения безопасности в системах RFID, как сред с крайним дефицитом ресурсов.

Из известных в настоящий момент симметричных криптографических схем, ***теоретически самый сильный вариант***, основан на псевдослучайных ***PR***-функциях. При этом исходят из положений, что каждая привязываемая к защищаемому объекту радиочастотная метка использует вместе со считывающим устройством уникальный секретный ключ $\boldsymbol{k}$, из ключевого пространства $\boldsymbol{K}$, и поддерживает множество псевдослучайных функций $\mathcal{F} = \{f_k\}_{k \in K}$.

<u>В выводах статьи отмечается</u>.

Область исследований, которые принесут большую пользу безопасности и конфиденциальности RFID – это разработка аппаратно эффективных криптографических хэш-функций, симметричного шифрования, *MAC* (кодов аутентификации сообщений) и генераторов случайных чисел. Общие достижения в производстве схем и развитии RFID понизят затраты и позволят выделять больше ресурсов для функций безопасности. Разработка эффективных реализаций совершенных односторонних и псевдослучайных функций является также весьма важным направлением исследований.

Констатируется, что обеспечение сильных криптографических примитивов в требуемом ценовом диапазоне 0,05-0,1$ на настоящий момент – ***нереалистичная задача***.

Между тем, представленные в прилагаемой Презентации расчеты предполагаемых аппаратных затрат и проведенный анализ решений, включая криптографический, позволяют заключить, что

RA-технологии и разработанные на их основе рандомизационные агрегаты и другие криптографические примитивы, способны поддерживать множество ***PR***-функций и операторов криптографической стойкости, вполне достаточной для обеспечения необходимого уровня безопасности и конфиденциальности систем RFID. Причем систем, построенных не только, как предполагали авторы, на основе ***менее критичных*** кремниевых меток, но и ***более критичных*** пластиковых и ***сверх критичных*** печатных меток RFID.

Рассмотрим более подробно Протокол проведения односторонней аутентификации и составляющие его компоненты. При этом будем считать, что составляющие его положения согласованы, а компоненты законно зарегистрированы и проверены – сертифицированы.
Аутентификатор *(односторонний)* – сертифицированное встраиваемое устройство, осуществляющее по секретному ключу аутентификации ***A***, криптографическое преобразование поступившего на его вход ***N***-разрядного случайного двоичного числа ***R***, именуемого ***маркером состояния***, в ***код аутентификации C***, той же разрядности.

Аутентификаторы строится на основе ***N***-разрядных W^q-агрегатов, порождающих PR_N-функцию, вида:

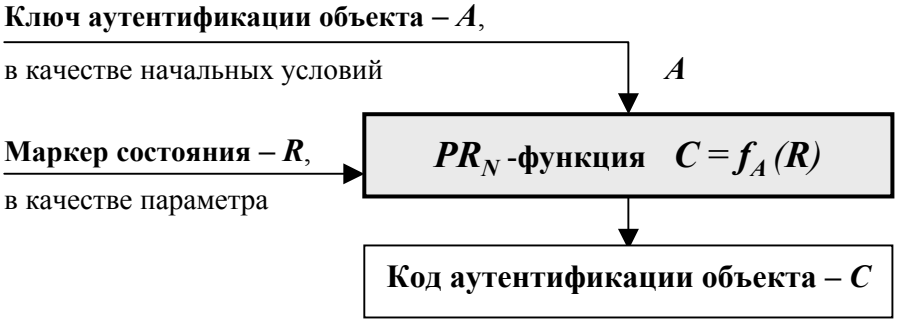


Рис. 3. Формирование кода аутентификации объекта

Генератор ключа аутентификации – сертифицированное встраиваемое устройство, осуществляющее по секретному мастер-ключу ***K*** категории принадлежности объекта, криптографическое преобразование поступившего на его вход ***M***-разрядного двоичного модификатора ***H***, отражающего существенные структурные и внешние признаки защищаемого объекта, в секретный ключ аутентификации ***A***.

Генераторы ключей аутентификации строится на основе ***M***-разрядных W^q-агрегатов, при этом ***M*** значительно больше ***N***, порождающих PR_M-функцию, вида:

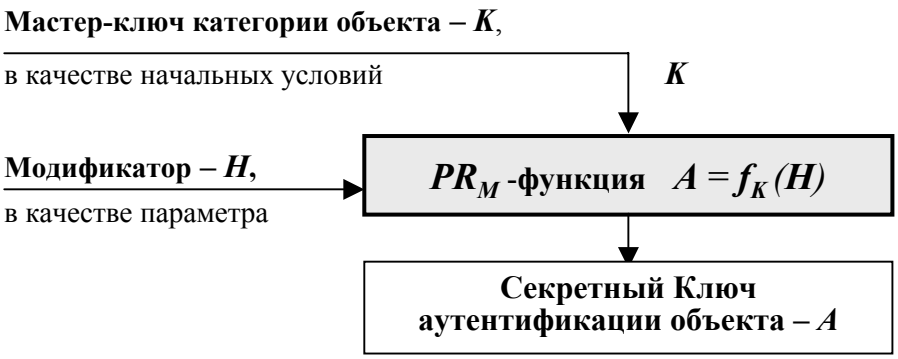


Рис. 4. Формирование секретного ключа аутентификации объекта

Верификатор – сертифицированное устройство (индивидуальное, общее, специальное), предназначенное для установления подлинности сертифицированных объектов.

Электронный знак – бесконтактное или контактное электронное устройство, в память которого заносится сертификат связываемого с ним объекта и другая специальная информация, необходимая для обеспечения функционального предназначения знака и его системной интеграции.

Считывающее устройство **–** электронное устройство, включающее в себя один или несколько верификаторов и обеспечивающее реализацию установленного протокола идентификации, аутентификации и распознавания клонированных объектов, помещенное в корпус с элементами питания и индикацией результатов обработки.

Распознавание клонов в системе – наиболее трудная задача.

Следуя введенным понятиям, рассмотрим более подробно содержание Протокола.

Первоначально положим, что ключ аутентификации сформирован, как показано на Рис. 4 и записан в защищенной от внешнего проникновения памяти электронного знака, как это предусмотрено Протоколом привязки знака к защищаемому объекту и активации знака.

Предположим также, что считывающее устройство выделило один из знаков, входящих в его окружение, провело его идентификацию и по команде АУТЕНТИФИКАЦИЯ, выданной знаку, получило от знака категорию принадлежности объекта и всю другую информацию, необходимую для вычисления модификатора ***H***.

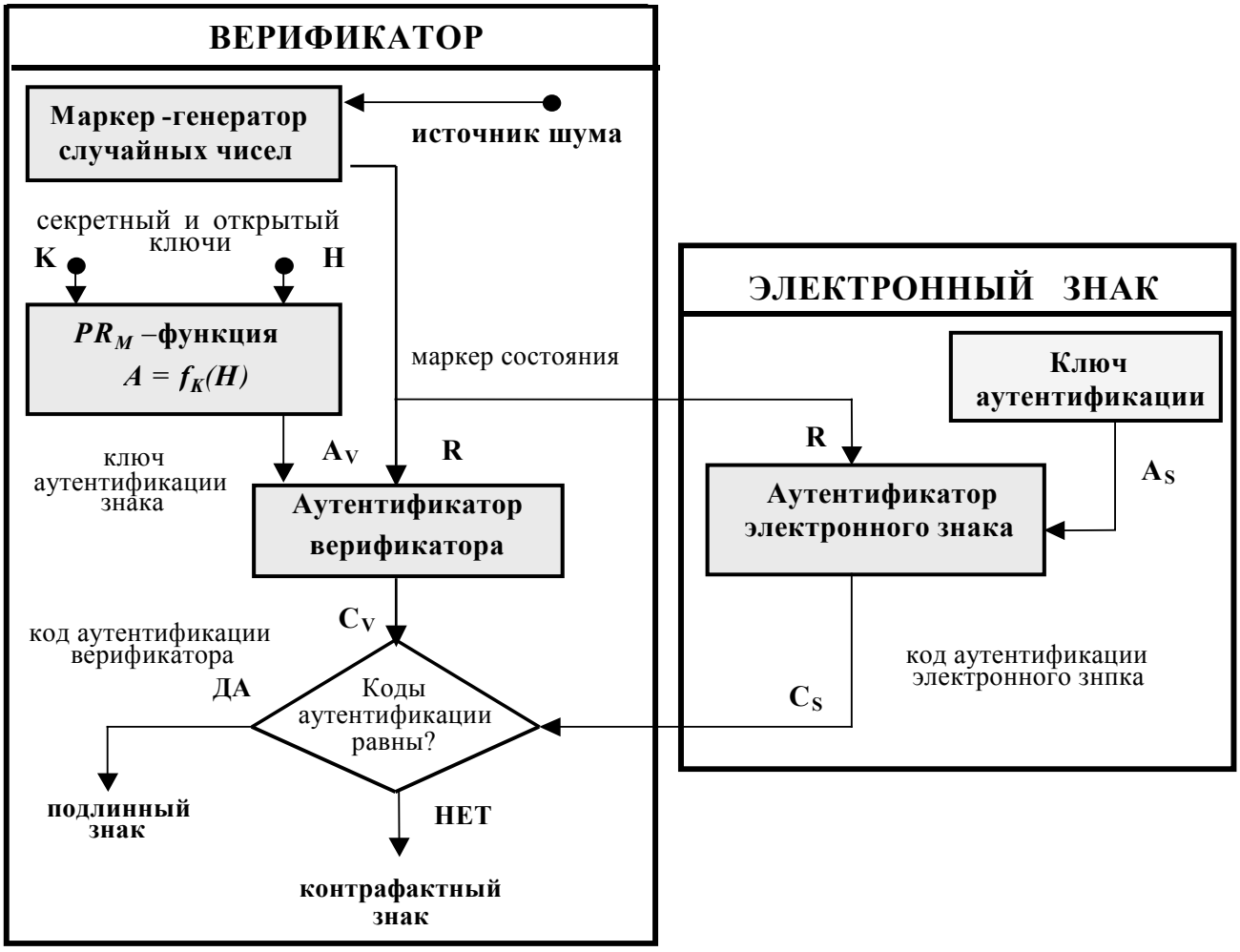


Рис. 5. Схема проведения односторонней аутентификации

После вычисления модификатора ***H*** считывающим устройством, примерный алгоритм процедуры аутентификации электронных знаков, выглядит следующим образом (Рис.5).

- Верификатор вырабатывает или использует сформированный ранее маркер состояния (случайное число) ***R*** и через считывающее устройство посылает его знаку.
- Верификатор, используя хранящийся в нем, секретный мастер-ключ ***K*** категории объекта и вычисленный считывающим устройством модификатор ***H***, вычисляет ключ A_V аутентификации электронного знака (Рис.4).

- Аутентификатор входящий в состав верификатора и аутентификатор встроенный в электронный, каждый, используя свой секретный ключ аутентификации A_V и A_S, вырабатывают свой несекретный код аутентификации C_V и C_S, соответственно.
- Код аутентификации C_S, сформированный знаком передается запросившему его считывающему устройству.
- Верификатор сравнивает код аутентификации C_S, полученный от знака, с выработанным им кодом аутентификации C_V. При несовпадении кодов – $C_V \neq C_S$, считывающее устройство сигнализирует, что знак является контрафактным.

После успешного завершения аутентификации – $C_V = C_S$, возможно следующее продолжение.

- Аутентификатор знака переводится в режим шифрования и вырабатывает гамму. Выработанной гаммой зашифровывается хранящаяся в знаке коммерчески значимая и конфиденциальная информация и передается запросившему его считывающему устройству.
- Считывающее устройство принимает и расшифровывает поступающие данные, и в соответствии с установленным протоколом передает их далее, на последующую обработку.

В целях последующего выявления фальсифицированных знаков и клонов, считывающее устройство ведет подсчет числа идентифицированных и аутентифицированных знаков.

Рассмотренный протокол односторонней аутентификации позволяет, на основе радиочастотных меток и других электронных знаков организовать эффективную и надежную защиту материальных объектов от фальсификации и подделки.

Протоколу присущи следующие недостатки:

- Не обеспечивается распознавание клонов.
- Компрометация мастер-ключа категории, ведет к компрометации системы в разделе всей категории.

Предотвращение компрометации мастер-ключей и распознавание клонов, может быть осуществлено на основе многоуровневых протоколов защиты.

8. Защита мастер-ключей от компрометации

Распознавание фальсифицированной и контрафактной продукции осуществляется аппаратно, на основе встроенного алгоритма аутентификации, позволяющего проверить подлинность связанной с товаром радиочастотной (**RF**) метки. Действительно, если исключить возможность клонирования метки и предоставить покупателю неподдельное индивидуальное устройство проверки подлинности приобретаемого им товара, то покупатель, как и в первом случае, может вполне убедиться, что он приобрел подлинный товар. Кроме этого, алгоритм аутентификации может быть легко, без дополнительных аппаратных издержек, переведен в режим шифрования. На основе шифрования коммерчески значимой, а также другой существенной информации хранящейся в RF-метках, действуя на физическом уровне можно также предотвратить утечки конфиденциальной информации.

В условиях реального рынка, целесообразность внедрения защищенных RF-меток определяется их стоимостью. По мнению аналитиков, порог рентабельности технологии RFID при маркировке недорогих товаров достигается при стоимости радиочастотных меток - 2 цента.

Во всех случаях, главным и конечным арбитром процедуры проверки подлинности товара, является Потребитель. Любое делегирование его полномочий, например “кристально честному“ продавцу или даже “абсолютно бдительному” органу инспекции, в реальных условиях недопустимо. Это брешь для проникновения на рынок фальсифицированной и контрафактной продукции.

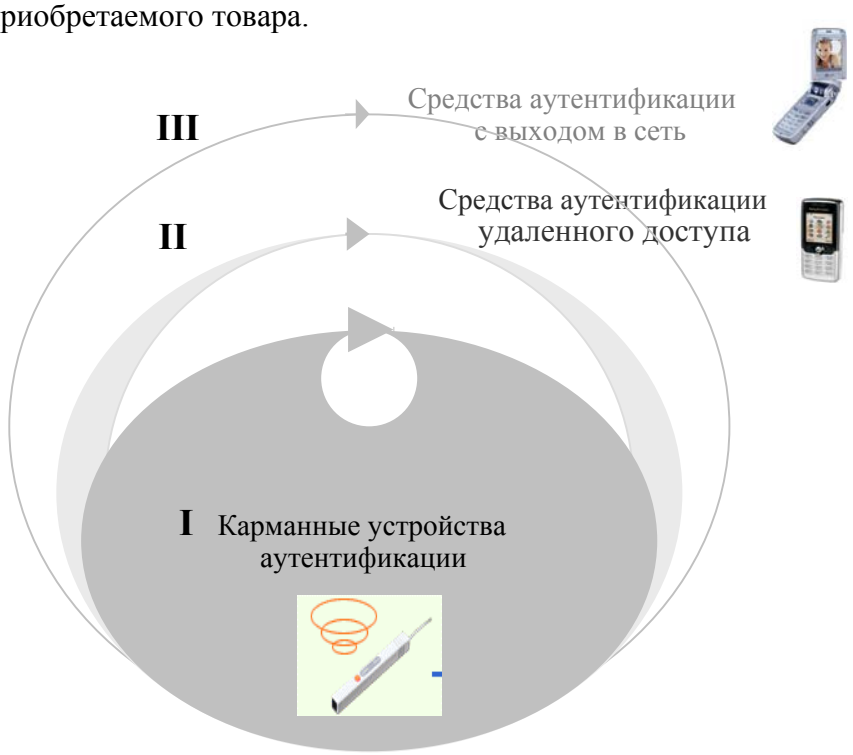
Данный метод имеет известные, в общем упомянутые ранее в предыдущем разделе 7 достоинства и недостатки.

Положение кардинальным образом меняется, в следующих случаях

- наличие высоко развитой, гибкой и многоуровневой, динамичной и эффективной системы генерации и управления ключами, включая **ID** меток (собственно - ядра системы управления сертификатами),
- появление дешевых, криптографически надежно защищенных от клонирования и подделки RF-меток,
- предоставление широким слоям населения недорогих индивидуальных устройств проверки подлинности приобретаемого ими товара.

Все это можно сделать на основе ***RA***-технологий.

Ниже показан вариант распределения потоков транзакций по проверке подлинности (аутентификации) приобретаемого товара.



Представленная на рисунке система защиты от фальсифицированной и контрафактной продукции состоит из трех уровней. На первом и втором уровне системы, подлинность приобретаемого товара устанавливается непосредственно, как это предписывается Протоколом обеспечения безопасности RFID, путем проверки подлинности связанной с ним защищенной RF-метки.

На третьем – *логистическом уровне*, проверка подлинности товара, включая установление факта клонирования метки, осуществляется путем отслеживания траектории его движения от производителя к прилавку продавца. Отслеживание траектории движения объекта производится по базе данных, посредством средства аутентификации с выходом в сеть, например, мобильного телефона и встроенного в него верификатора. По указанным выше причинам, стоимость такой транзакции должна быть достаточно высока, а возможность доступа предельно ограничена.

Первый уровень является основным. Для проведения аутентификации, на этом уровне используются недорогие, сертифицированные карманные устройства, например в виде карандаша, выпускаемые изготовителем средств маркировки. В состав устройства включают одну или несколько сменяемых микросхем – верификаторов. Верификаторы разделены по категориям товаров и позволяют по скрытому в них секретному мастер-ключу категории вычислить индивидуальный секретный ключ аутентификации RF-метки и по нему, а также по специальному сеансовому ключу, установить подлинность метки. Слабым звеном этой схемы является мастер-ключ категории. Если злоумышленник может вскрыть верификатор и прочитать его мастер-

ключ, что далеко не дешево и весьма не просто сделать при наличии в микросхеме специальной активной защиты, то тогда он в принципе сможет клонировать RF-метки. Этот недостаток может быть устранен, с введением второго, так называемого «фискального» уровня защиты.

Для проведения аутентификации на втором уровне используются сертифицированные устройства аутентификации удаленного доступа (например, сотовый телефон с простой специальной приставкой), а в состав RF-метки вводится дополнительный секретный ключ аутентификации. В этом случае, информация RF-метки ретранслируется, на так называемый **сервер фискальной аутентификации** (ФАТ). Не уточняя детали, ФАТ-сервер, по скрытому в нем секретному мастер-ключу категории и случайным образом генерируемому сеансовому ключу, вычисляет код аутентификации радиочастотной метки и передает его устройству аутентификации. Устройство аутентификации устанавливает подлинность метки. По несовпадению кода от метки и кода от сервера, можно установить, что метка поддельная или имеет факт клонирования метки.

По сравнению с третьим уровнем, стоимость такой транзакции должна быть не столь высока, при этом доступ может быть не сильно ограничен.

При такой архитектуре построения системы, наряду с административной и уголовной ответственностью, на всех уровнях защиты может быть введен весьма эффективный «Протокол материального поощрения Бдительного Покупателя, за счет строгого наказания Нечестного Продавца». Чем выше уровень защиты, тем серьезнее должно быть наказание Продавца.

9. Технологические аспекты реализации систем RFID

От решения рассмотренных выше задач на основе защищенных меток и RFID технологий, будет зависеть эффективность решения не менее актуальных, во многом схожих задач:

- защита и заверение документов и ценных бумаг;
- защита национальной валюты;
- защита автотранспорта от угонов, дистанционное выявление угнанных средств;
- маркировка и контроль ресурса оборудования, устройств, механизмов, узлов и деталей;
- оплата проезда (бесконтактная) в общественном транспорте.

Как отмечают эксперты, области применения RFID-технологий неисчерпаемы, что подтверждается далеко не полным перечнем задач, готовых для начала практической разработки. При этом, как следует из представленных выше материалов, масштабы распространения RFID-технологий безграничны, особенно в условиях уменьшения себестоимости и повышения функциональных возможностей средств маркировки.

В этом русле очень перспективными выглядят печатная (органическая) электроника и беспроцессорные криптографические технологии, по производству радиочастотных меток. Например, массовое внедрение первых для маркировки недорогих штучных товаров, позволит производить дешевые обычные (незащищенные) метки по себестоимости 1 евро-цент [7], а вторые – защищенные метки, по себестоимости всего на 30-50% выше обычных [2], т.е. около 2 центов US. А это все вместе, дает возможность отказаться от штриховых кодов и позволяет по стоимости радиочастотных меток достичь порога рентабельности RFID-технологий [3].

Между тем, учитывая недостатки присущие органической электронике, там, где требуются высокая скорость и надежность обработки, включая небольшие размеры, а также функциональность и устойчивость к внешним факторам и воздействиям, без дешевых кремниевых (обычных и защищенных) радиочастотных меток [6], по себестоимости 5-10 центов, не обойтись.

В тех случаях, когда требуется привлечение адресуемой памяти и проведение сложных математических вычислений, к примеру, при использовании асимметричных криптографических алгоритмов и процедур распознавания образов, без интеллектуальных радиочастотных

(Smart) меток со встроенным процессором, себестоимостью 0.3-1$ и выше, безусловно не обойтись.

Как прогнозируют исследовательские группы ОАО "**Российская электроника**", **Hewlett-Packard**, **Hitachi, IBM**, **Intel**, **Philips** и другие, снижение себестоимости радиочастотных меток на кремниевой основе до 2-5 центов, при одновременном повышении их функциональных возможностей и опережающем развитии беспроцессорных технологий, может быть достигнуто в ближайшем десятилетии, с внедрением наноэлектронных технологий и освоением производства радиочастотных нанокремниевых меток.

Учитывая существующее состояние микроэлектронной индустрии и рынка готовых решений, позволяющих обеспечить достаточно высокий технологический и организационный уровень защиты от клонирования и подделки кремниевых RF-меток, наращивание и конечную реализацию высокой полнофункциональной криптографической защиты можно осуществить поэтапно.

Ниже приведена таблица, построенная исходя из представленных в разделе 8 способов защиты от фальсифицированной и контрафактной продукции и широкой номенклатуры выпускаемых интегральных микросхем, идентичных общепринятым дешевым (беспроцессорным) и относительно дорогим (процессорным) типам **I-Code** и **Mifare**, соответственно, изготовляемых компанией **Philips**.

Предполагаемый порядок поэтапного внедрения дешевых радиочастотных меток

<table>
<tr><th></th><th>Простейшие (беспроцессорные)
метки на базе микрочипов типа I-Code,
себестоимостью около 5 центов и выше</th><th>Программируемые (процессорные)
метки на базе микрочипов типа Mifare,
себестоимостью около 50 центов и выше</th></tr>
<tr><td rowspan="2">I этап</td><td>Аутентификация по идентификатору метки и имени производителя</td><td rowspan="2">Аутентификация
на основе известных блочных шифров
(DES, 3DES, AES, ГОСТ 28147-89)</td></tr>
<tr><td>III (логистический) уровень обработки (раздел 8), как это предусмотрено концепцией EPCglobal</td></tr>
<tr><td rowspan="2">II этап</td><td>Аутентификация
по несекретному хеш, формируемому в зависимости от секретного мастер-ключа</td><td>Полнофункциональная аутентификация
по коду аутентификации, вырабатываемому в зависимости от секретного ключа аутентификации и несекретного сеансового ключа</td></tr>
<tr><td>Аппаратная реализация верификаторов, включая введение в простейшие метки дополнительной памяти под несекретные хеши, поддерживающих физические I и II-ой уровни обработки (раздел 8)</td><td>Эмуляция полнофункциональных верификаторов и защищенных беспроцессорных меток,
поддерживающих все три уровни обработки (раздел 8)</td></tr>
<tr><td>III этап</td><td colspan="2">Аппаратная реализация на основе интегральных кремниевых микросхем
полнофункциональных недорогих верификаторов и дешевых защищенных беспроцессорных меток себестоимостью 5-10 центов,
поддерживающих все три уровни обработки (раздел 8)</td></tr>
</table>

В настоящее время поставлено на коммерческую основу производство, включая Россию в лице ОАО «**Ангстрем**», дешевых простейших меток типа **I-Code**, а также Smart меток типа **Mifare**, отвечающих первому и второму этапу. Третий этап перспективный, рассчитан на высокую и надежную полнофункциональную защиту не только кремниевых, как в первых двух случаях, но и всех других типов радиочастотных меток и связан с освоением высокоэффективных беспроцессорных криптографических технологий [1].

Принимая во внимание сказанное, дополнительно расставляя акценты на понятиях полезных для дальнейшего развития и продвижения RFID-технологий, радиочастотные метки будем подразделять на два класса – обычные (**Prime**, беспроцессорные) и интеллектуальные (**Smart**, процессорные) RF-метки.

В свою очередь, обычные радиочастотные метки, как это предусмотрено представленными в таблице этапами наращивания полнофункциональной защиты, подразделяются,

- на ***логистические***, известные как простейшие незащищенные **RFID**-метки, продвигаемые компанией **EPCglobal**
- и защищенные, так называемые ***сертификационные*** или **RFC** (**Radio Frequency Certification**) метки.

В зависимости от используемого Протокола аутентификации (проверки подлинности), RFC-метки подразделяются на радиочастотные метки с ***открытым*** и ***секретным ключом*** аутентификации. При этом формируемые на их основе в соответствии с Протоколом открытые коды аутентификации меток, привязываются к существенным признакам защищаемого ими объекта.

В соответствии с принятым Протоколом, построенным на основе ***RA***-технологий, радиочастотные метки с секретным ключом аутентификации криптографически защищены от клонирования и подделки. В отличие от них, RF-метки с открытым ключом аутентификации криптографически защищены, только при наличии высокой технологической защиты, исключающей возможность клонирования метки. Поддержание последнего в условиях быстрого распространения RFID неосуществимо в самом ближайшем будущем.

10. Заключение

Оценивая направления развития современной криптографии, минималистская криптография интенсивно развивается. О чем свидетельствует рост публикаций, число проводимых симпозиумов, семинаров и конференций за рубежом. К сожалению, в России этому вопросу не уделяется должного внимания.

Следуя достижениям Компании, в отличие от узко специализированного представления западных специалистов, в нашем понимании **минималистская криптография** (Minimalist cryptography), как стохастическая криптография в неполной арифметике, рассчитанная на платформы генерации от 8 до 48 бит, есть полноценная, а каким либо образом “обрезанная”, как принято говорить облегченная криптография.

Для нас такая **легкая криптография** (Lightweight cryptography) – в широком смысле, частный случай минималисткой, с облегченной, исходя исключительно из условий технической эксплуатации и ограничений на число транзакций, криптографической стойкостью.

По нашему мнению, в условиях объединения усилий Российского криптографического сообщества, стохастическая криптография может стать реальной основой для завоевания передовых позиций на рынке современных криптографических технологий. Особенно это актуально в преддверии конференции **Eurocrypt** 2006.