КРИПТОНИТ

Криптографические механизмы в технологии RFID

Бельский Владимир

Заместитель руководителя лаборатории криптографии

Технология RFID. Описание

RFID (Radio Frequency Identification)

Радиочастотная идентификация

Частоты

LF	• 125-134 кГц
HF	• 13,56 МГц
UHF	• 433 МГц • 860-960 МГц
Micro	• 2,45 ГГц

Стандарты

- ISO 18000
- ISO 14443
- ISO 15693
- ISO 10536

СКУД

Транспорт

Оплата

Маркировка

Удобно

Дешево

Просто

Технология RFID. Дилемма

СКУД

Транспорт

Маркировка

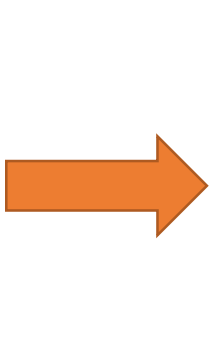
Оплата услуг

Электронные паспорта

Учет

БЕЗОПАСНОСТЬ!

Криптография



- Не просто
- Не дешево
- Не удобно

- Место криптографии в технологии RFID?
- Какой он «Российский вектор развития криптографии в RFID»?

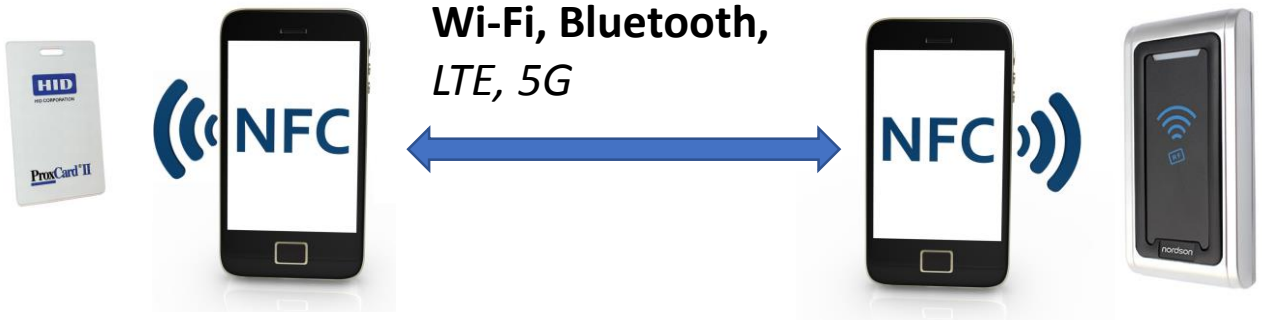
Безопасность RFID. Атаки на RFID

Клонировать почти любую карту СКУД	• За 10 минут возле метро (сами делали)
Изготовить универсальный ключ для всех номеров отеля	• Есть готовые инструкции, нужен рутованный телефон и 10$ устройство с aliexpress
Проехать бесплатно по Тройке	• Скрипт с github и телефон с андроид
Считать любую информацию с карты Mifare Classic	• Любой считыватель и компьютер с линуксом

Атаки:

- Клонирование
- Отслеживание
- Трекинг
- Повторное использование
- Экранирование
- Нарушение работы

Relay атака на RFID



Таким образом:

- **Угоняют машины**
- **Проникают в помещения**
- **Снимают деньги с карт**

Методы защиты:

- Строгое соблюдение стандартов

ISO 14443 определяет **Frame waiting time** – время ожидание ответа. Диапазон от 300 мкс до 5 с.

- Протокол secure distance bounding

$$\text{Dist} = \frac{\Delta t - \delta}{2} \cdot c$$

- Шапочка из фольги

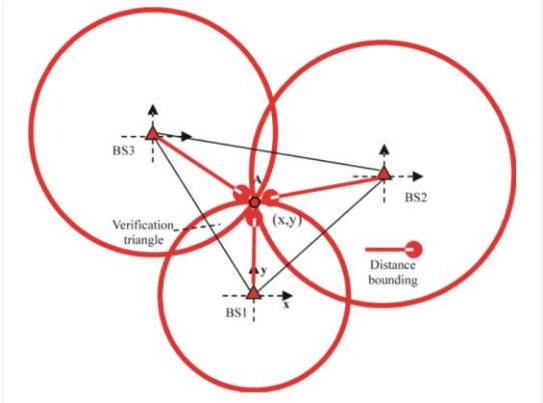
Безопасность RFID. Новые аспекты безопасности

Приватность

Можно проследить путь человека, товара, импланта.

Анонимность

Получить идентификатор с RFID-билета, е-паспорта или карточки СКУД.



Этические вопросы

У всего на свете будет свой идентификатор – не всем это подходит.

Безопасность RFID. Реакция рынка

Никак!

(самая популярная, к сожалению)

Принимают новые стандарты, в том числе по безопасности

Разрабатывают новые методы защиты, в том числе криптографические

Убирают с рынка уязвимые устройства **(ооочень медленно)**

- Более 70% всех карточек RFID выпускается Mifare (NXP), в том числе Тройка
- Большинство RFID меток вообще не используют механизмы безопасности
- Существуют карты, которые используют CRYPTO-1

Задачи криптографических механизмов в рамках RFID

1. **Аутентификация метки (основная задача)**
2. Аутентификация считывающего устройства
3. Взаимная аутентификация
4. Отправление аутентифицированного сообщения (обеспечение целостности)
5. Отправление зашифрованного сообщения (обеспечение конфиденциальности)
6. Отправление сообщения, зашифрованного в режиме аутентифицированного шифрования (целостность и конфиденциальность)
7. Распределение ключей
8. Генерация псевдослучайных чисел

Криптографические механизмы в RFID. Теория за 30 лет

Придумывают низкоресурсные крипто-алгоритмы

- Grain-128, Present-80, Simon, Spec, МАГМА!

Разработали алгоритмы аутентификации для RFID

- OSK, YA-TRAP, O-TRAP, LRP-PTCA, TBPA, SPA, LMAP и M^2 AP, HB (и его варианты)

Протоколы аутентификации и идентификации с обеспечением приватности

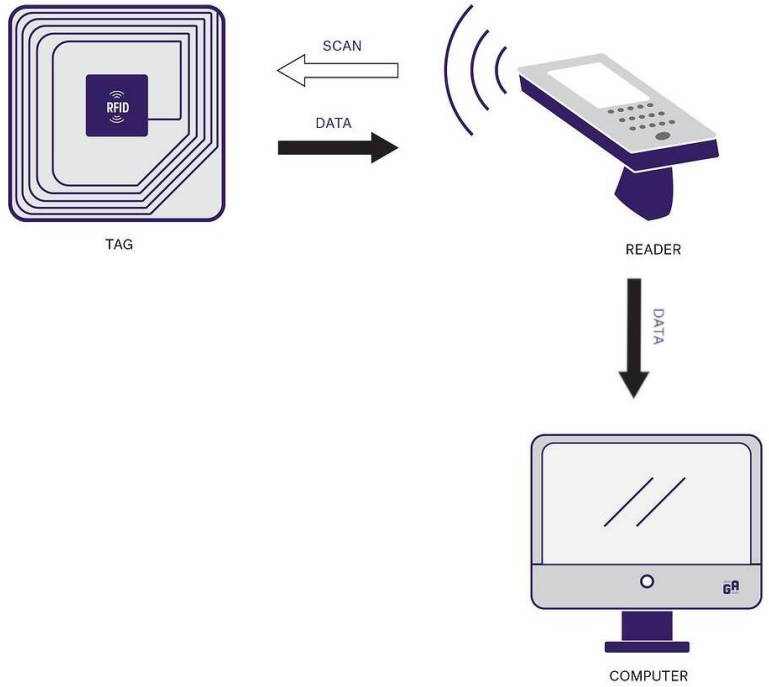
- EP-UAP, DRAP, GUPA, HBA, HBA+

Создают модели безопасности

- Privacy Models for RFID (S.Vaudenay), RFID formal privacy model (Ouafi and Phan)

Принимают новые стандарты

- ISO 29167



Криптографические механизмы в технологии RFID. ISO версия

Стандартизация в рамках ISO. Стандарт ISO 29167.

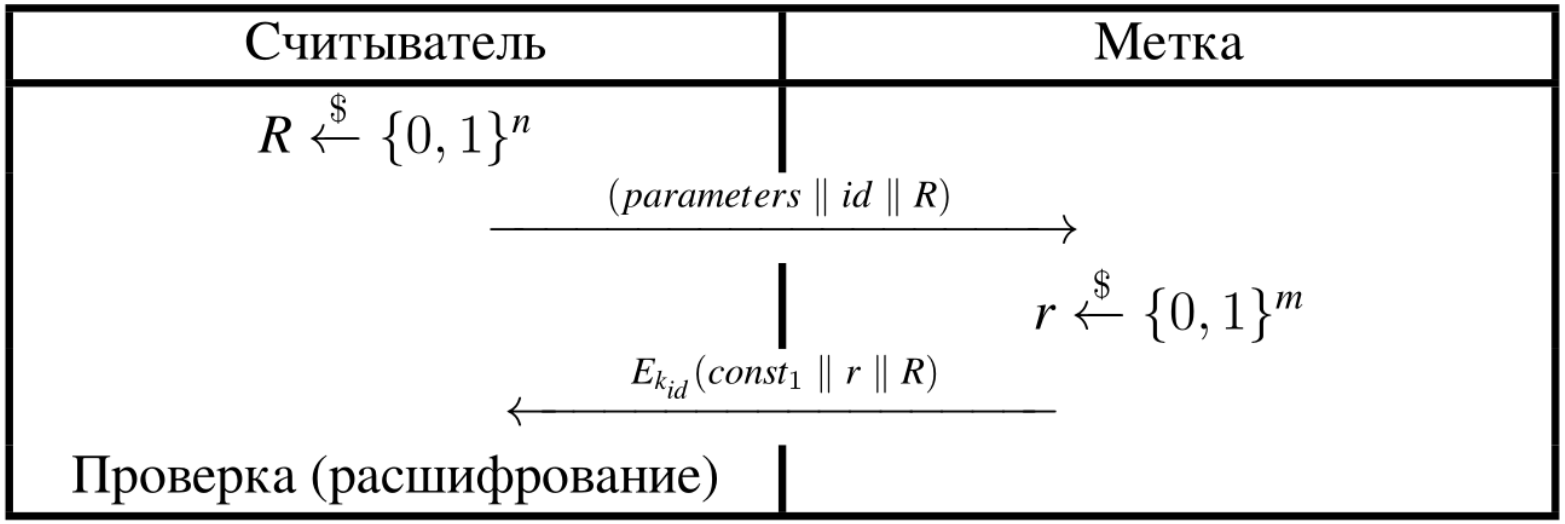
- AES-128 (CBC)
- AES OFB
- PRESENT-80
- ECC-DH
- Grain-128A
- XOR
- ECDSA-ECDH
- RAMON
- SIMON
- SPECK

	AES-128	AES OFB	ECDSA-ECDH	SIMON
Аутентификация метки	+	+	-	+
Аутентификация считывателя	+	+	-	+
Взаимная аутентификация	+	+	+	+
Аутентификация сообщения	+	-	-	+
Шифрование сообщения	+	-	-	-
Аутентифицирующее шифрование	+	-	-	+
Обновление ключей	-	+	-	+
Распределение ключей	-	-	+	-

Особенности алгоритмов

- Аутентификация метки и считывателя происходит в основном по ISO 9798-4
- Самый распространенный вариант - AES-128

Общая схема аутентификации RFID (по стандартам ISO)



Особенности:

- Метка умеет только шифровать и не умеет расшифровывать;
- Размеры n и m зависят от длины блока алгоритма шифрования E;
- Существуют варианты протокола односторонней аутентификации метки (TAM), односторонней аутентификации считывателя (IAM), и взаимной аутентификации (MAM);
- Существует вариант протокола с передачей информации (TAM2) и без передачи информации (TAM1);

Отечественные криптографические алгоритмы в RFID

Магма (размер блока 64 бита)

R – 40 бит, r – 20 бит

+ Скорость работы
+ Необходимые ресурсы

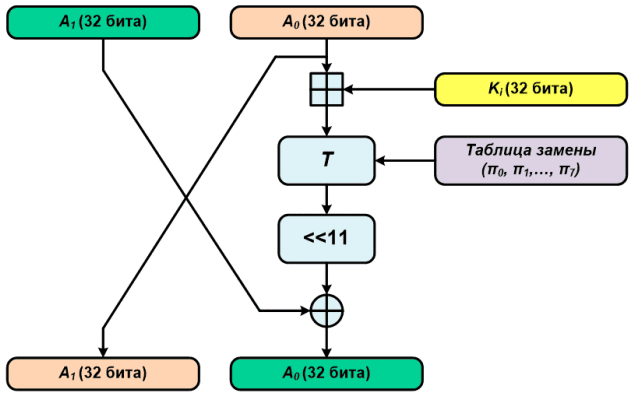
- «Размеры» случайных чисел

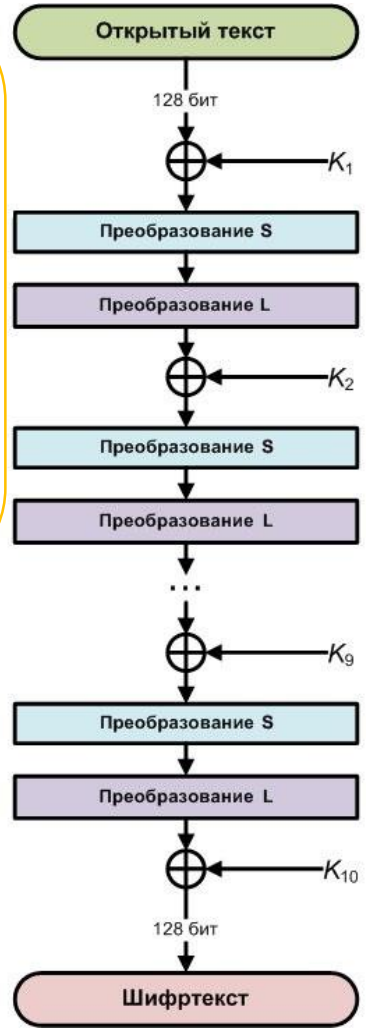
Кузнечик (размер блока 128 бит)

R – 80 бит, r – 32 бит

+ Полное соответствие стандарту ISO
+ Высокий «уровень» безопасности

- Быстродействие и эффективность



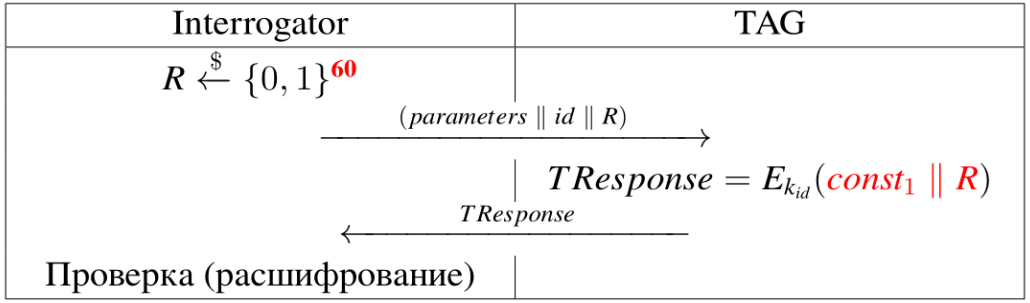


Отечественные криптографические алгоритмы в RFID

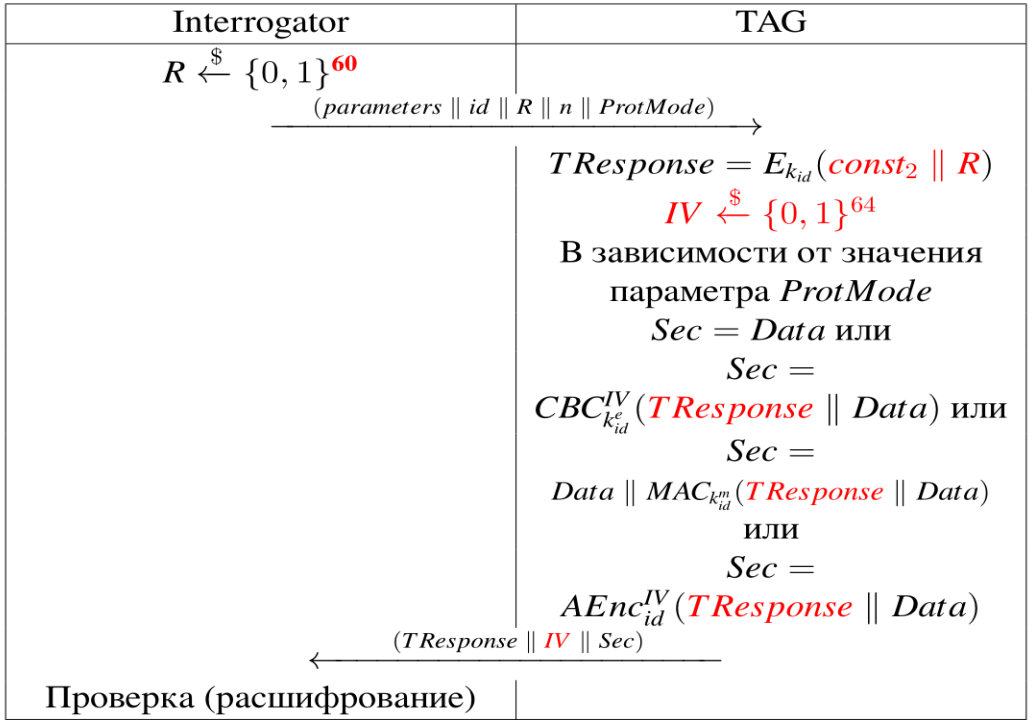
Предложен модифицированный вариант на основе алгоритма шифрования МАГМА

- ✓ Размер запроса на аутентификацию был увеличен до **60** бит, а сторона, которая проходит аутентификацию, не генерирует собственное случайное число;
- ✓ Вектор инициализации при шифровании дополнительных данных берётся случайным, а затем передаётся по открытому каналу;
- ✓ Для шифрования передаваемых данных и для аутентификации используются разные ключи.

ТАМ 1



ТАМ 2



Криптографические механизмы в технологии RFID

В соответствии с решением заседания ТК26 (24-е заседание, 14 ноября 2019г.) в рамках подкомитета 4.1 (**Криптографические механизмы для индустриальных систем**) запланирована разработка первых редакций следующих документов:

- проект Методических рекомендаций ТК26 «Информационные технологии. Технологии автоматической идентификации и сбора данных. Сервисы безопасности для радиоинтерфейсов систем радиочастотной идентификации»

- проект Методических рекомендаций ТК26 «Информационные технологии. Технологии автоматической идентификации и сбора данных. Криптографические наборы ГОСТ 34.12-2018 сервисов безопасности для радиоинтерфейсов связи»

КРИПТОНИТ

Спасибо за внимание!

Бельский Владимир,

Электронная почта: v.belsky@kryptonite.ru

Адрес в Интернет: http://kryptonite.ru/