Анализ подходов к построению протоколов RFID для защиты от атак пересылки

Чичаева Анастасия

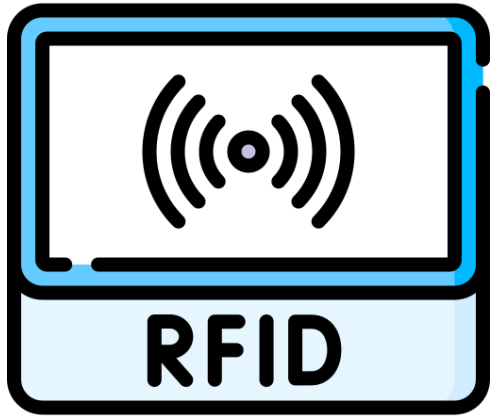
Специалист-исследователь,
Лаборатория криптографии

РусКрипто’2023

КРИПТОНИТ

Атаки пересылки

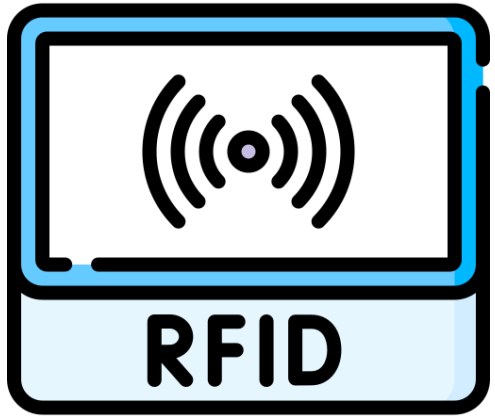
КРИПТОНИТ



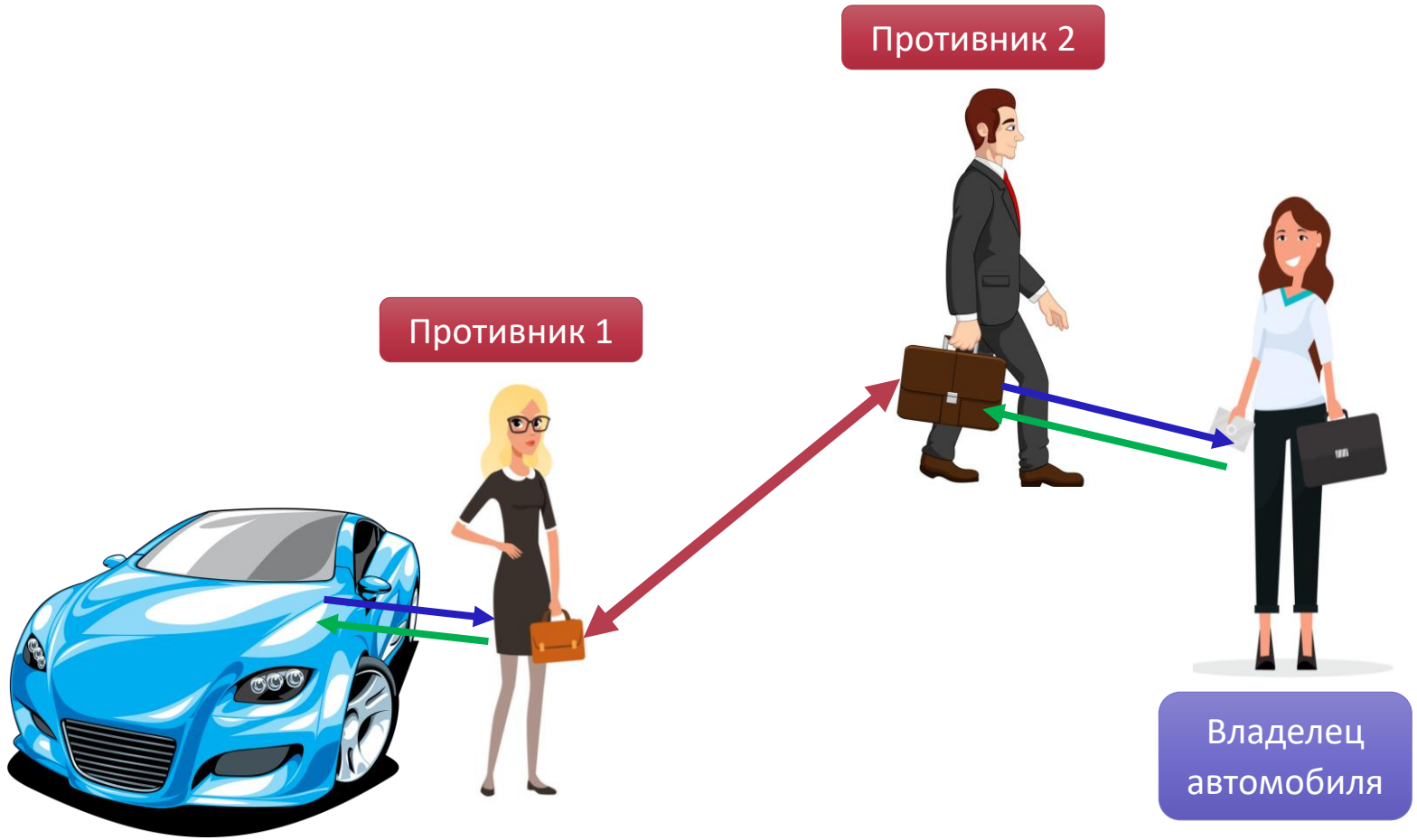
!!!Важно расстояние !!!

Атаки пересылки

КРИПТОНИТ



!!!Важно расстояние !!!



Атаки с присутствием «честной» метки

КРИПТОНИТ

АТАКА ПЕРЕСЫЛКИ (relay attack)

Пассивный противник пересылает сообщения без изменения.

АТАКА МАФИОЗИ (mafia fraud)

Активный противник может не только пересылать, но и модифицировать сообщения.

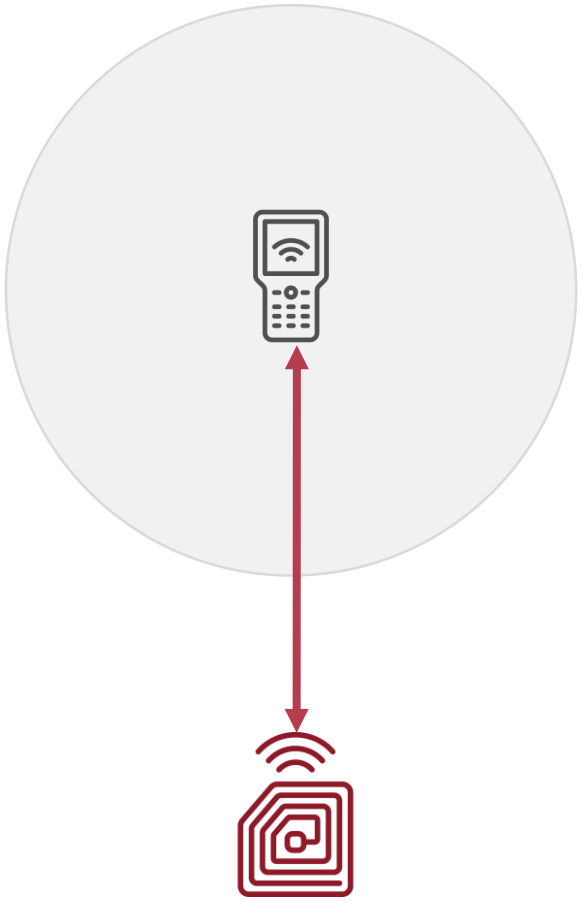
АТАКА ЧЕЛОВЕК ПОСЕРЕДИНЕ (Man-in-the-Middle attack)

Противник действует в два этапа: сначала следит за взаимодействием легитимных участников, затем реализует атаку мафиози

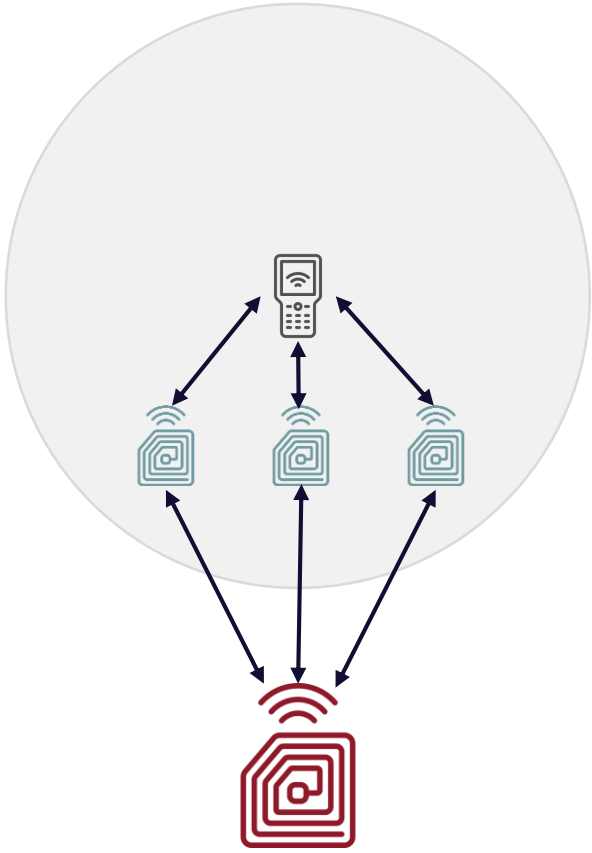
Атаки с присутствием «нечестной» метки

КРИПТОНИТ

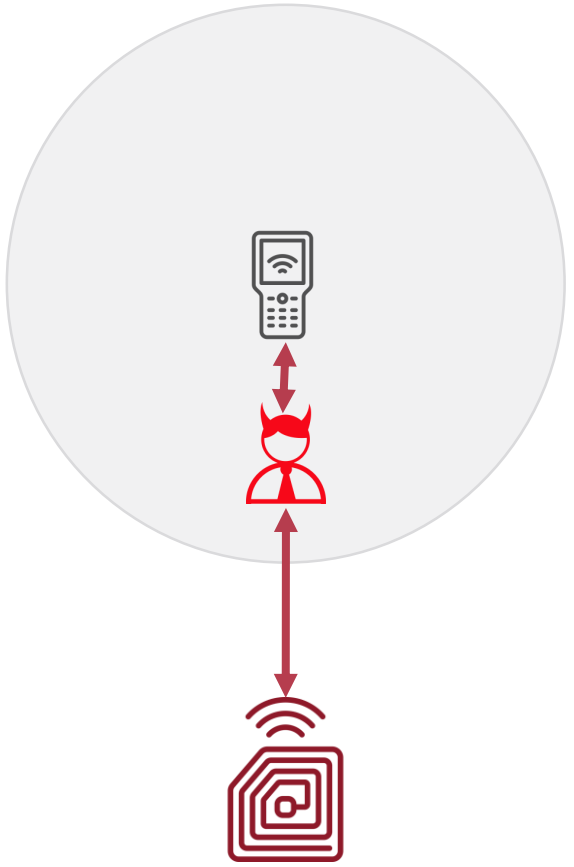
ПОДДЕЛКА РАССТОЯНИЯ
(distance fraud)



ПОДДЕЛКА РАССТОЯНИЯ С ИСПОЛЬЗОВАНИЕМ ДРУГИХ ЛЕГИТИМНЫХ УЧАСТНИКОВ
(distance hijacking)



АТАКА ТЕРРОРИСТА
(terrorist fraud)



Технические меры защиты

- Экранирование RFID метки
- Дополнительные действия владельца RFID метки
- Использование GPS
- Измерение времени ответа
  - ➢ Протоколы оценки расстояния (distance-bounding)

Протоколы оценки расстояния

КРИПТОНИТ

Протоколы оценки расстояния учитывают скорость распространения сигнала в среде и на основе времени передачи и приема сообщения оценивают близость доказывающего участника.

Особенность протоколов оценки расстояния — наличие **быстрой фазы**, где проверяющий отправляет запросы доказывающему и получает ответы на них, замеряя время между отправкой запроса и получением ответа.

Классификация

КРИПТОНИТ

Протоколы типа Брандса-Шаума

Проверяющий		Доказывающий
. . . . .		
	Быстрая фаза для всех $i \in 1 \ldots m$	
$C_i \in \{0, 1\}$		$R_i \in \{0, 1\}$
Измерение времени t_i	$C_i \longrightarrow$	
Измерение времени t_i^*	$\longleftarrow R_i$	
Проверка $(t_i^* - t_i) \leqslant \Delta t_{Max}$		
. . . . .		
	Завершающая фаза	
Проверка подписи	$\longleftarrow Sign_k(C_1 \| \| R_1 \| \| \ldots \| \| C_m \| \| R_m)$	

Основное отличие – порядок выполнения быстрой фазы и фазы криптографических вычислений

Протоколы типа Ханке-Куна

Проверяющий		Доказывающий
ключ K		ключ K
	Фаза настройки параметров	
Случайное число N_a	$N_a \longrightarrow$	
	$\longleftarrow N_b$	Случайное число N_b
	$V \| \| W = H(K, N_a \| \| N_b)$ $\| \| V \| \| = \| \| W \| \| = m$	
. . . . .		
	Быстрая фаза для всех $i \in 1 \ldots m$	
$C_i \in \{0, 1\}$		
Измерение времени t_i	$C_i \longrightarrow$	
		$R_i = V_i$, если $C_i = 0$ $R_i = W_i$, если $C_i = 1$
Измерение времени t_i^*	$\longleftarrow R_i$	
Проверка корректности R_i Проверка $(t_i^* - t_i) \leqslant \Delta t_{Max}$		

Сравнение

КРИПТОНИТ

Протокол	Атака человек посередине	Distance hijacking	Атака террориста
Протокол Брандса-Шаума [1]	✓	✗	✗
Протокол Ханке-Куна [2]	✓	✓	✗
Протокол Мунилла-Пейнадо [3]	✓	✓	✗
Протокол Кима-Авойна [4]	✓	✓	✗
Протокол бинарного дерева [5]	✓	✓	✗
Протокол Рейда и др. [6]	✓	✓	✓
Протокол Швейцарский нож [7]	✓	✓	✓
Асимметричный протокол Брандса-Шаума [1]	✓	✗	✗
Протокол Водено [8]	✓	✓	✗

1. Brands S., Chaum D. Distance-bounding protocols
2. Hancke G.,Kuhn M.AnRFID Distance Bounding Protocol
3. Munilla J., Peinado A. Distance bounding protocols for RFID enhanced by using void-challenges and analysis in noisy channels
4. Kim C. H., Avoine G. RFID distance bounding protocol with mixed challenges to prevent relay attacks
5. Avoine G., TchamkertenA.Anefficient distance bounding RFID authentication protocol: balancing false-acceptance rate and memory requirement
6. J. Reid [и др.] Detecting relay attacks with timing-based protocols
7. C. H. Kim [и др.] The Swiss-Knife RFID Distance Bounding Protocol
8. Vaudenay S. Private and secure public-key distance bounding

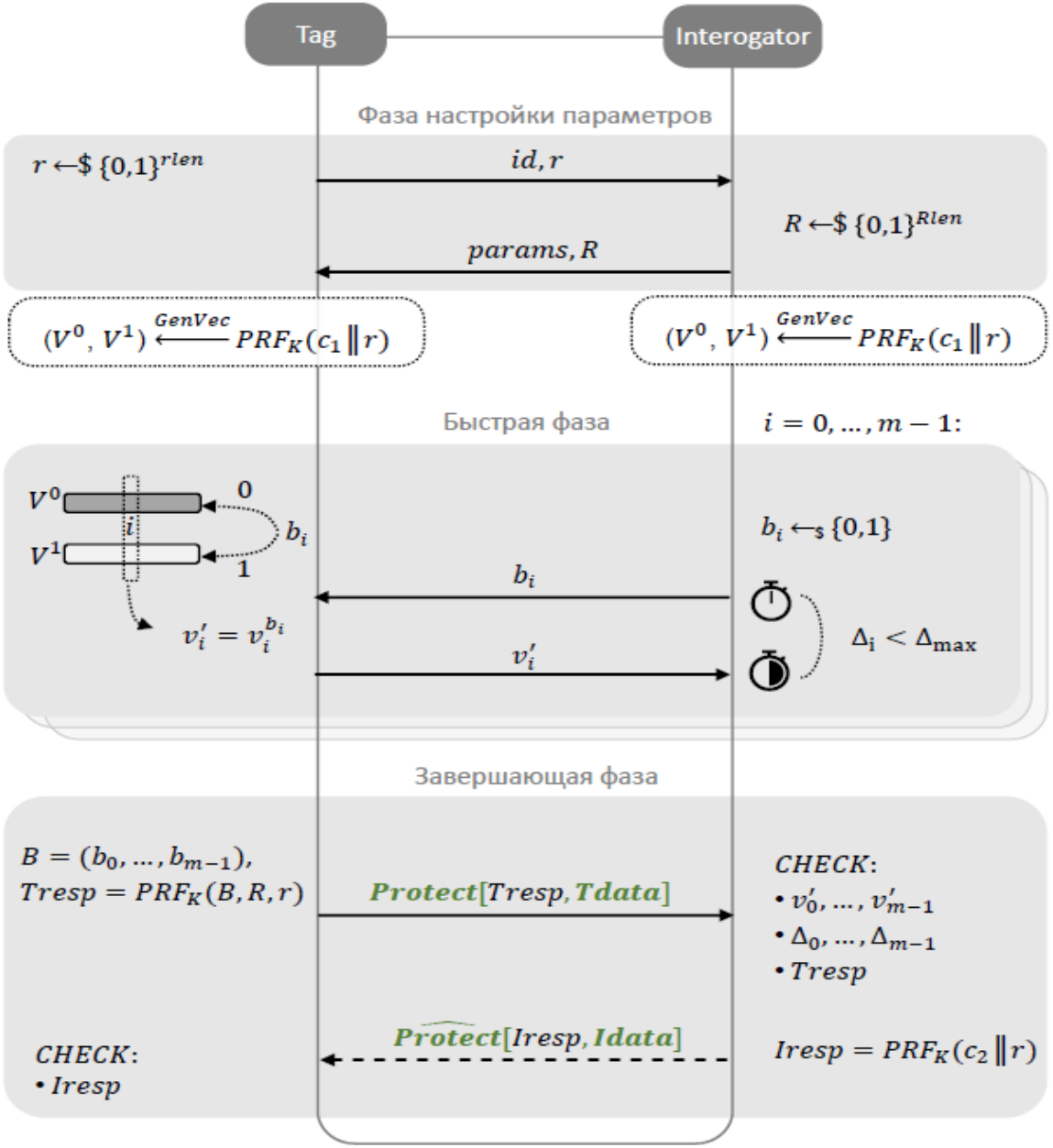
Протокол DB-RFID

DB-RFID развивает идеи протокола «Швейцарский нож».
Внесены следующие изменения:

- Убран функционал, связанный с приватностью.
- Изменен механизм выработки векторов, с целью возможности использованию prf-функций с разной длиной ключа и выхода.
- Добавлена возможность опциональной передачи дополнительных данных совместно с аутентифицирующим сообщением.

Протокол состоит из трех условных фаз:

- фаза настройки параметров и выработки секретных значений;
- быстрая фаза с замером времени;
- завершающая фаза верификации, на которой стороны доказывают, что обладают общим секретом K.

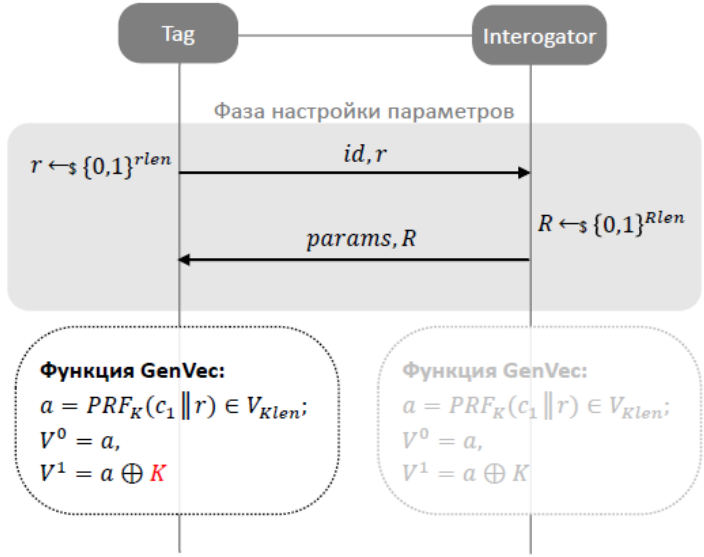


Условные обозначения:

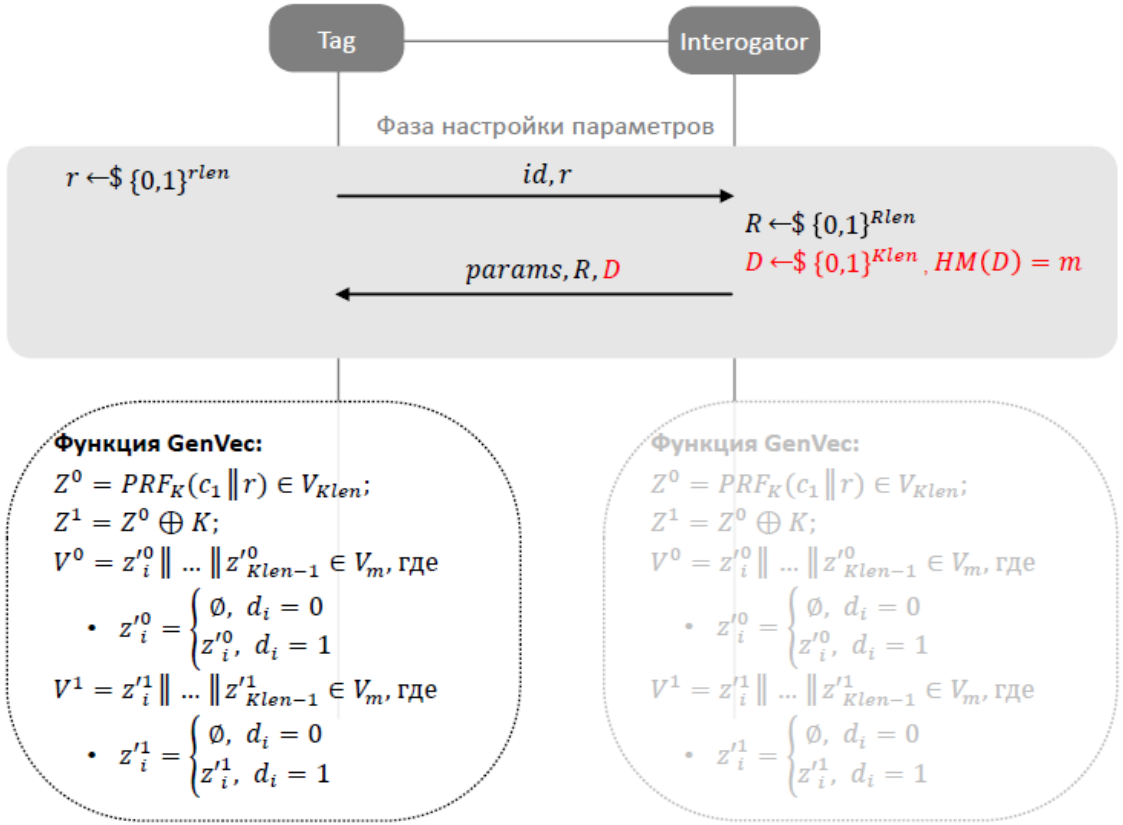
«◄- - - ·» — опциональное сообщение, пересылаемое в случае использования режима двусторонней аутентификации

Фаза настройки параметров

Генерация векторов в модели, учитывающей атаку террориста



Фаза настройки параметров

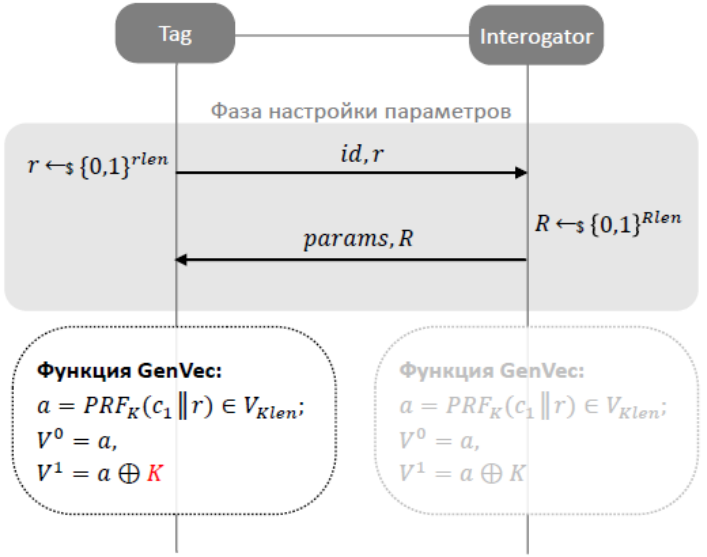


Условные обозначения:

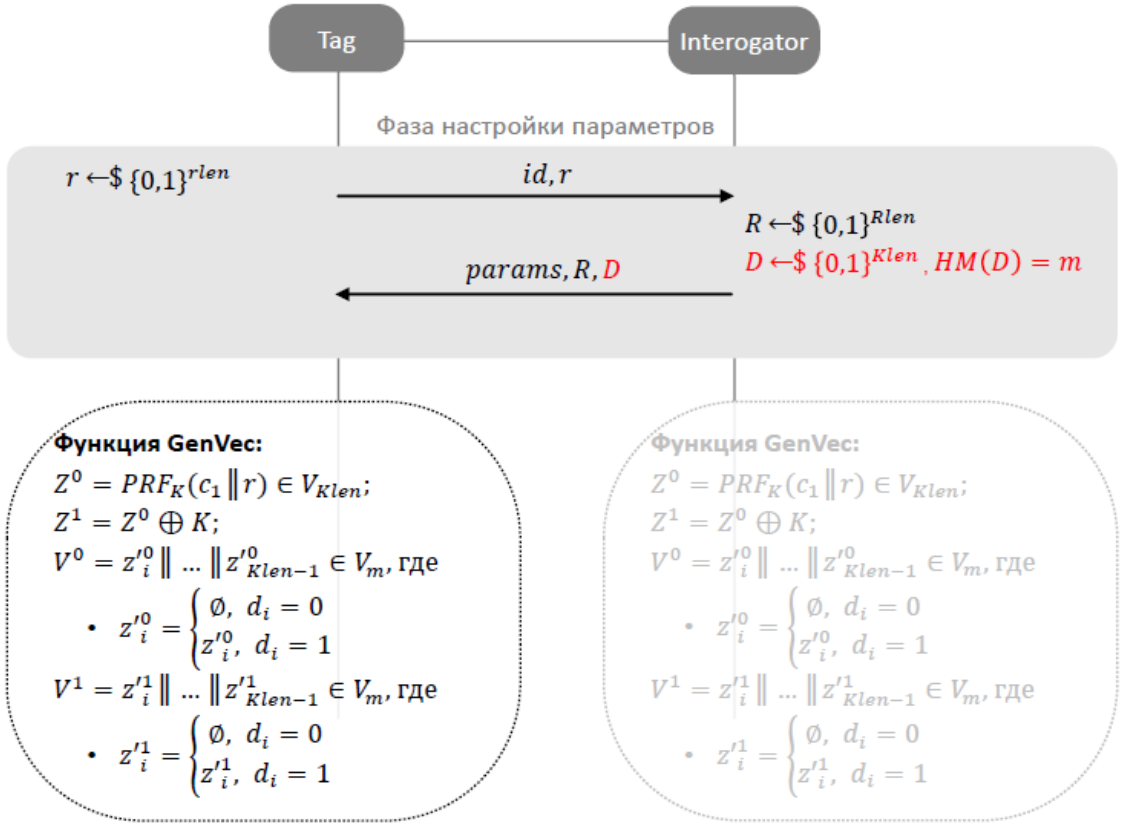
$HM(D)$ — вес Хемминга, т.е. количество битов в векторе $D = (d_0, \dots, d_{Klen-1})$, которые отличаются от 0.

Генерация векторов длины m в протоколе «Швейцарский нож»

Генерация векторов в модели, учитывающей атаку террориста



Фаза настройки параметров

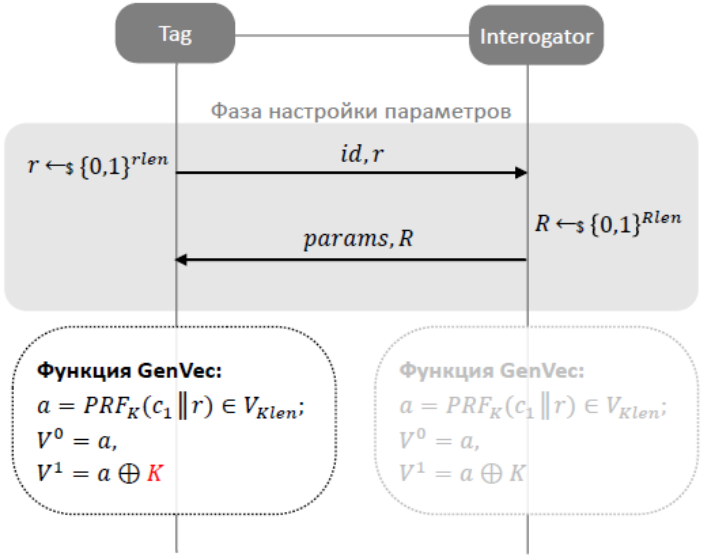


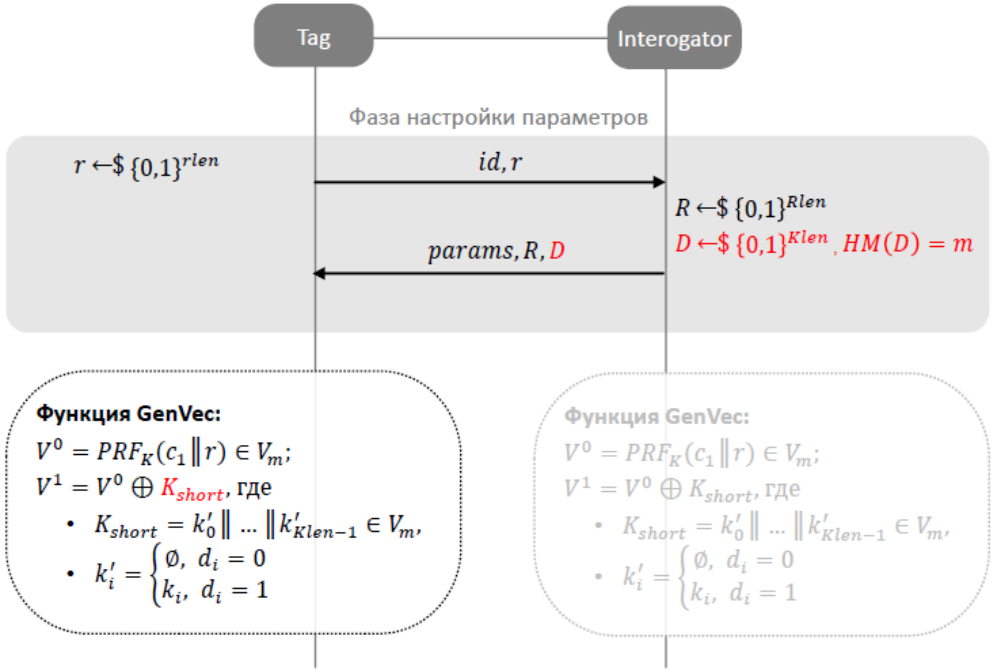
Условные обозначения:

$HM(D)$ — вес Хемминга, т.е. количество битов в векторе $D = (d_0, \dots, d_{Klen-1})$, которые отличаются от 0.

Генерация векторов длины m в протоколе «Швейцарский нож»

Генерация векторов в модели, учитывающей атаку террориста



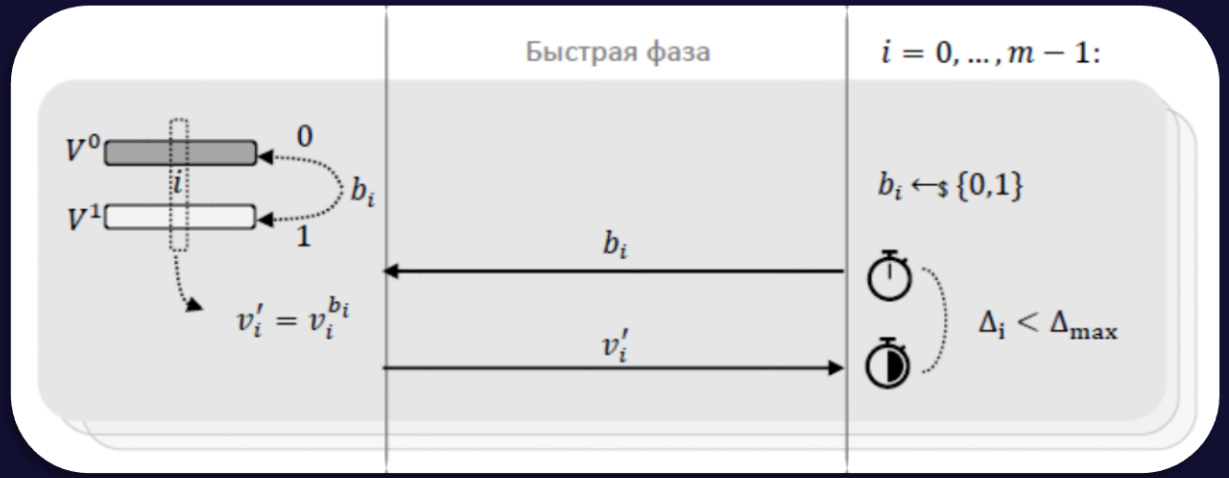


Генерация векторов в протоколе DB-RFID

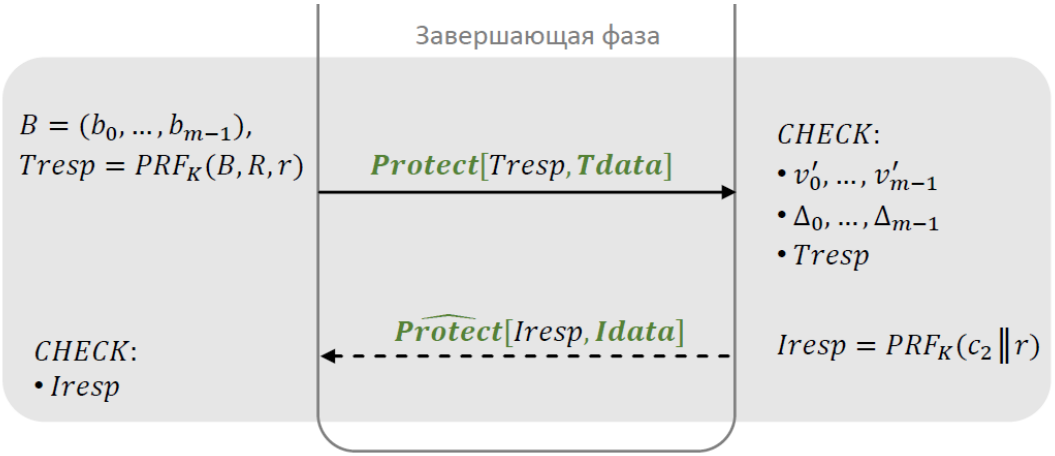
Быстрая фаза

- Во время быстрой фазы важно минимизировать любые задержки в ответе метки на сообщение считывателя. Для этого ответ метки v_i должен зависеть максимально простым образом от полученного бита b_i, но в то же время он должен опираться и на некоторую секретную информацию, выработанную в ходе первого этапа.

- За счет изменений, внесенных в функцию генерации векторов, число итераций m быстрой фазы можно сократить.



Завершающая фаза



Защита данных в протоколе DB-RFID

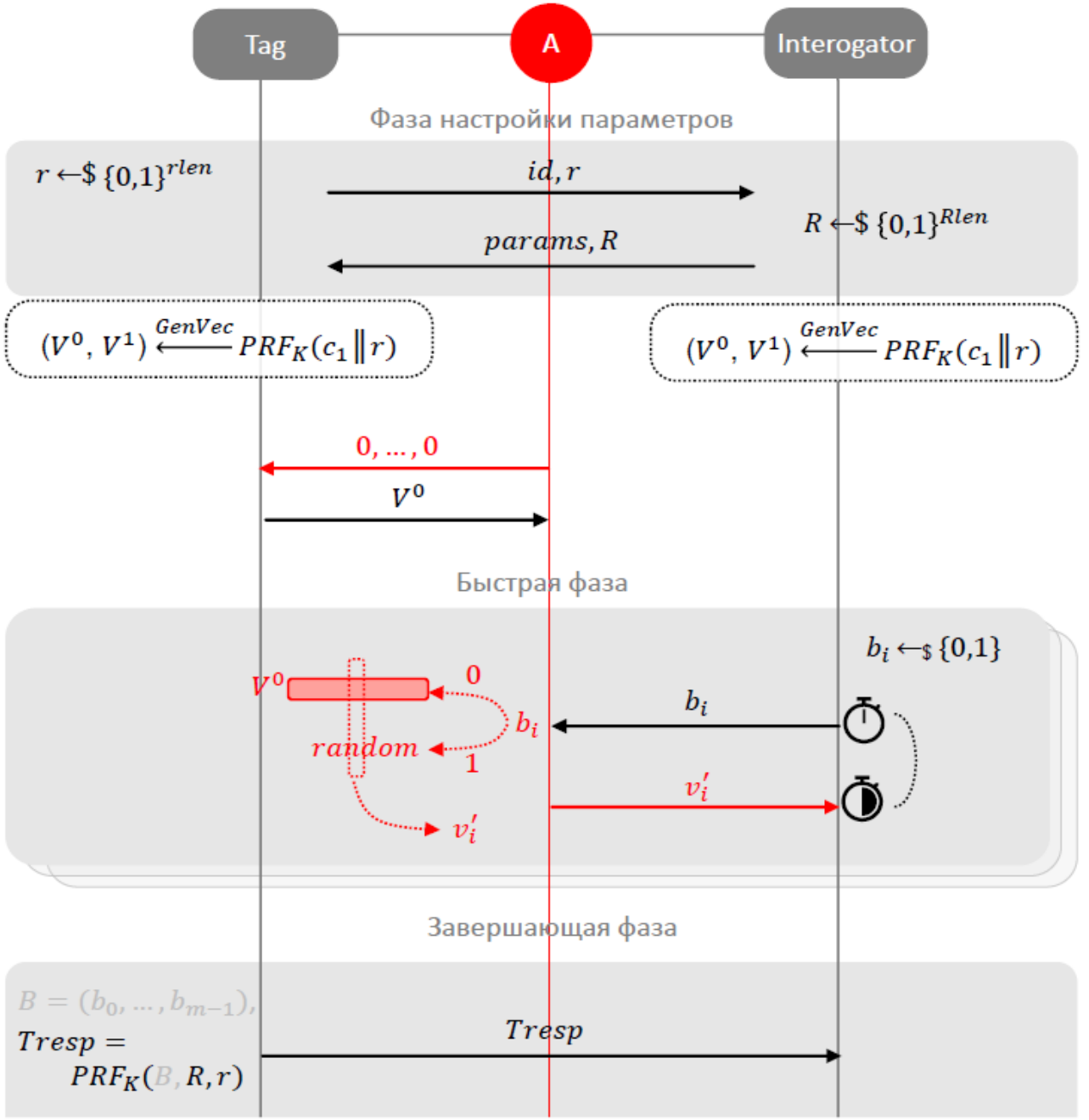
$Prot$ $Mode$	$Protect(TResp, TData)$	$\widehat{Protect}(IResp, IData)$
00	$TResp$	$IResp$
10	$TResp \parallel TData \parallel$ $\parallel MAC_{k^m}(TResp \parallel TData)$	$IResp \parallel IData \parallel$ $\parallel MAC_{k^m}(IResp \parallel IData)$
11	$IV \leftarrow\$ \{0,1\}^{64}$ $TResp \parallel CBC_{k^e}^{IV}(TData) \parallel$ $MAC_{k^m}(TResp \parallel CBC_{k^e}^{IV}(Data))$	$IV \leftarrow\$ \{0,1\}^{64}$ $IResp \parallel \widehat{CBC}_{K^e}^{IV}(IData) \parallel$ $MAC_{k^m}(IResp \parallel \widehat{CBC}_{k^e}^{IV}(IData))$

Завершающая фаза

Защита данных в протоколе DB-RFID

$Prot\ Mode$	$Protect(TResp, TData)$	$\widehat{Protect}(IResp, IData)$
00	$TResp$	$IResp$
10	$TResp \| TData \|$ $\| MAC_{k^m}(TResp \| TData)$	$IResp \| IData \|$ $\| MAC_{k^m}(IResp \| IData)$
11	$IV \leftarrow\$ \{0,1\}^{64}$ $TResp \| CBC^{IV}_{k^e}(TData) \|$ $MAC_{k^m}(TResp \| CBC^{IV}_{k^e}(Data))$	$IV \leftarrow\$ \{0,1\}^{64}$ $IResp \| \widehat{CBC}^{IV}_{K^e}(IData) \|$ $MAC_{k^m}(IResp \| \widehat{CBC}^{IV}_{k^e}(IData))$

Атака



Протокол DB-RFID-GOST

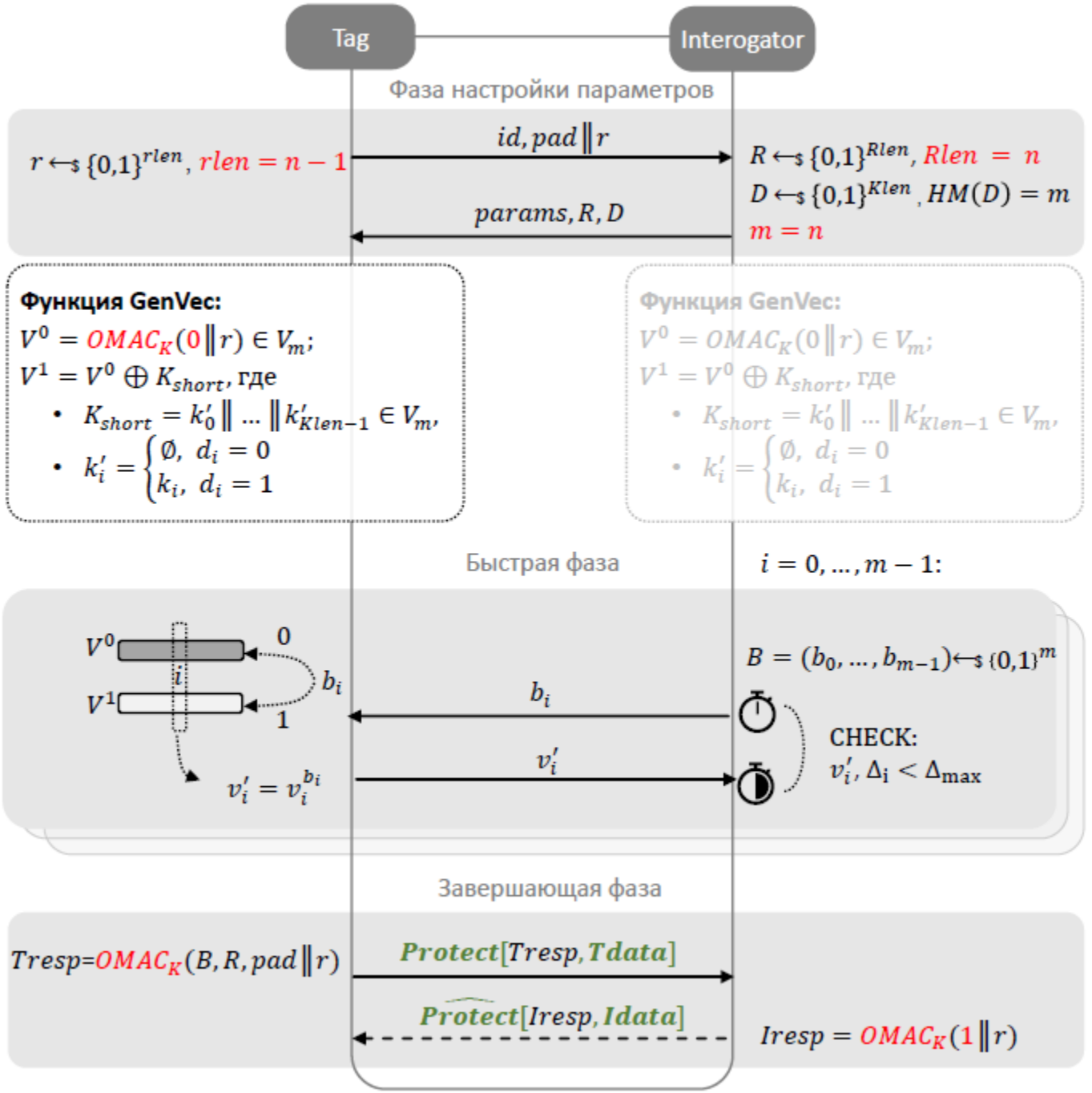
В качестве функции PRF_K можно использовать следующие механизмы:

- $OMAC_K$ — функция выработки кода аутентификации сообщения, описанная в ГОСТ 34.13-2018, на базе блочного шифра «Магма» или «Кузнечик»
- $HMAC_K$ — один из алгоритмов вычисления кода аутентификации сообщения на основе хэш-функции, определенных в Р 50.1.113-2016.

Протокол DB-RFID-GOST

В качестве функции PRF_K можно использовать следующие механизмы:

- $OMAC_K$ — функция выработки кода аутентификации сообщения, описанная в ГОСТ 34.13-2018, на базе блочного шифра «Магма» или «Кузнечик»
- $HMAC_K$ — один из алгоритмов вычисления кода аутентификации сообщения на основе хэш-функции, определенных в Р 50.1.113-2016.



Модели противника

КРИПТОНИТ

Модель Avoine [9]

Авторы выделяют несколько возможных стратегий действия противника:

- *Стратегия pre-ask:* противник до начала быстрой фазы со стороны Считывателя проводит быструю фазу с атакуемой меткой, а затем использует полученную информацию чтобы попытаться успешно пройти быструю фазу со Считывателем.
- *Стратегия post-ask:* противник проводит быструю фазу со Считывателем, а затем пытается навязать какие-либо сообщения в быстрой фазе с меткой, используя информацию, полученную ранее.
- *Стратегия early-reply:* стратегия используется в случае, когда противник пытается убедить Считыватель в том, что он находится в легитимной зоне, фактически не находясь в ней. Для этого во время быстрой фазы противник отвечает на запрос Считывателя *раньше,* чем фактически получает его, тем самым пытаясь заранее «предугадать» запрос и ответ на него.

[9] A framework for analyzing RFID distance bounding protocols / G. Avoine [и др.]

Модели противника

КРИПТОНИТ

Модель SimTF [10]

- Существует только одна метка и один считыватель
- Передача сообщений идет либо через противника, либо напрямую
- Противник всегда знает, чем закончилась сессия
- Существуют функция $clock$, моделирующая «глобальные часы»
- Понятие согласованности сессий позволяет формализовать атаку мафиози и террориста

Модель GameTF [11]

- Протокол аутентификации является стойким в модели GameTF, если любой противник, аутентифицирующийся с помощью легитимной метки-сообщника, может аутентифицироваться и без помощи метки с вероятностью, большей чем вероятность успешной аутентификации в атаке мафиози.

  В частности, отсюда следует, что информация, полученная во время атаки террориста, не увеличит вероятность успешной аутентификации в будущем)

Модель Водено [12]

- Вводится понятие расстояния (каждый участник находится в определенной точке пространства).
- Авторы применяют подход, аналогичный использующемуся в интерактивных доказательствах.

[10] A formal approach to distance-bounding RFID protocols / U. Durholz [и др.]
[11] Terrorism in distance bounding: modeling terrorist fraud resistance / *Fischlin M.*, *Onete C.*
[12] Practical and provably secure distance-bounding / *Boureanu I.*, *Mitrokotsa A.*, *Vaudenay S.*

Оценки стойкости

КРИПТОНИТ

Оценки стойкости для протокола типа «Швейцарский нож»

Модель	Оценка стойкости
Avoine, impers.	$\left(\frac{1}{2}\right)^{flen}$
Avoine, pre-ask	$\binom{m}{E}\left(\frac{1}{2}\right)^{m}$
Avoine, post-ask	$\binom{m}{E}\left(\frac{1}{2}\right)^{m}$
Avoine, terror	$\left(\frac{3}{4}\right)^{m}$
SimTF	$insecure$
GameTF	$secure$

Спасибо за внимание!

Авторы доклада:

Чичаева Анастасия

Специалист-исследователь,
Лаборатория криптографии
a.chichaeva@kryptonite.ru

Бельский Владимир

Заместитель руководителя,
Лаборатория криптографии
v.belsky@kryptonite.ru

Царегородцев Кирилл

Старший специалист-исследователь,
Лаборатория криптографии
k.tsaregorodtsev@kryptonite.ru

Шишкин Василий

Руководитель лаборатории,
Лаборатория криптографии
v.shishkin@kryptonite.ru

Результаты доклада получены в ходе выполнения НИР Академии Криптографии.