О точности оценок стойкости криптопротокола CRISP

Виталий Кирюхин

ООО «СФБ Лаб», АО «ИнфоТеКС»

РусКрипто’2024
21 марта 2024

vitaly.kiryukhin@sfblaboratory.ru

СФБ ЛАБ

Криптопротокол CRISP

ГОСТ Р 71252–2024

Информационная технология
Криптографическая защита информации
Протокол защищенного обмена для индустриальных систем

ФЕДЕРАЛЬНОЕ АГЕНТСТВО
ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р 71252–2024

Информационная технология

КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ

Протокол защищенного обмена для индустриальных систем

Издание официальное

Москва
Российский институт стандартизации
2024

Вступает в силу
с 1 апреля 2024 года
взамен рекомендаций по стандартизации
Р 1 323 565.1.029–2019

CRyptographic Industrial Security Protocol

СФБ ЛАБ

Свойства безопасности

1. Целостность (имитозащита) – обязательно
2. Конфиденциальность (шифрование) – опционально
3. Защита от повторного навязывания

СФБ ЛАБ

Особенности

- Нет интерактивности (сессий), предраспределённые ключи

СФБ ЛАБ

Особенности

- Нет интерактивности (сессий), предраспределённые ключи
- Сообщение несёт всю информацию для обработки

СФБ ЛАБ

Особенности

- Нет интерактивности (сессий), предраспределённые ключи
- Сообщение несёт всю информацию для обработки
- Явная и неявная адресация

СФБ ЛАБ

Особенности

- Нет интерактивности (сессий), предраспределённые ключи
- Сообщение несёт всю информацию для обработки
- Явная и неявная адресация
- Многоадресные сообщения,
  все устройства могут использовать один и тот же ключ

CRyptographic Industrial Security Protocol

СФБ ЛАБ

Особенности

- Нет интерактивности (сессий), предраспределённые ключи
- Сообщение несёт всю информацию для обработки
- Явная и неявная адресация
- Многоадресные сообщения,
  все устройства могут использовать один и тот же ключ
- Динамический выбор криптонабора (CS)
  для каждого пакета

Общие сведения

Протокол CRISP:

- описывает совокупность полей и правил их формирования
- может использоваться с любым протоколом передачи данных, способным доставить сформированные данные адресатам
- возлагает на защищаемую систему задачу доставки пакетов, в т.ч. адресацию и маршрутизацию

Структура пакета

	Имя	Назначение	Длина (бит)	
1	`Ext.KeyId.`	Флаг	1	Заголовок *H*
2	`Version`	Версия	15	
3	`CS`	Криптонабор	8	
4	`KeyId`	Номер ключа	от 8 до 1024	
5	`SeqNum` (SN)	Номер пакета	48	
6	`PayloadData`	Содержимое	переменная	
7	`ICV`	Имитовставка	переменная	

Максимальная длина пакета = 2048 байт

Минимальная длина доп. данных = 10 байт + имитовставка

Алгоритм отправителя

1. Выбираются ключ K, текст P, криптонабор CS

Алгоритм отправителя

СФБ ЛАБ

1. Выбираются ключ K, текст P, криптонабор CS
2. Счётчик SN увеличивается на 1

Алгоритм отправителя

1. Выбираются ключ K, текст P, криптонабор CS
2. Счётчик SN увеличивается на 1
3. Вычисляются ключи K_{MAC} и возможно K_{ENC}

$$(K_{ENC}, K_{MAC}) = \mathrm{KDF}(K, prms),\ \text{а } prms \text{ включает } CS, S_{ID},\ \text{и т.д.}$$

Алгоритм отправителя

1. Выбираются ключ K, текст P, криптонабор CS
2. Счётчик SN увеличивается на 1
3. Вычисляются ключи K_{MAC} и возможно K_{ENC}

   $(K_{ENC}, K_{MAC}) = \mathrm{KDF}(K, prms)$, а $prms$ включает CS, S_{ID}, и т.д.

4. Формируется заголовок H

Алгоритм отправителя

1. Выбираются ключ K, текст P, криптонабор CS
2. Счётчик SN увеличивается на 1
3. Вычисляются ключи K_{MAC} и возможно K_{ENC}

   $(K_{ENC}, K_{MAC}) = \mathrm{KDF}(K, prms)$, а $prms$ включает CS, S_{ID}, и т.д.

4. Формируется заголовок H
5. Если CS обеспечивает шифрование,
   - тогда $C = \mathrm{Enc}(K_{ENC}, IV, P)$, $IV = \mathrm{lsb}_{32}(SN)$
   - иначе, $C = P$

Алгоритм отправителя

1. Выбираются ключ K, текст P, криптонабор CS
2. Счётчик SN увеличивается на 1
3. Вычисляются ключи K_{MAC} и возможно K_{ENC}

   $(K_{ENC}, K_{MAC}) = \mathrm{KDF}(K, prms)$, а $prms$ включает CS, S_{ID}, и т.д.

4. Формируется заголовок H
5. Если CS обеспечивает шифрование,
   - тогда $C = \mathrm{Enc}(K_{ENC}, IV, P)$, $IV = \mathrm{lsb}_{32}(SN)$
   - иначе, $C = P$
6. Вычисляется имитовставка $T = \mathrm{MAC}(K_{MAC}, H||C)$

Алгоритм отправителя

СФБ ЛАБ

1. Выбираются ключ K, текст P, криптонабор CS
2. Счётчик SN увеличивается на 1
3. Вычисляются ключи K_{MAC} и возможно K_{ENC}

   $(K_{ENC}, K_{MAC}) = \mathrm{KDF}(K, prms)$, а $prms$ включает CS, S_{ID}, и т.д.

4. Формируется заголовок H
5. Если CS обеспечивает шифрование,
   - тогда $C = \mathrm{Enc}(K_{ENC}, IV, P)$, $IV = \mathrm{lsb}_{32}(SN)$
   - иначе, $C = P$
6. Вычисляется имитовставка $T = \mathrm{MAC}(K_{MAC}, H||C)$
7. Отправляется пакет вида (H, C, T)

Криптонаборы

CS	Название	Имит.	Шифр.	Имитовставка
1	MAGMA-CTR-CMAC	+	+	32
2	MAGMA-NULL-CMAC	+	–	32
3	MAGMA-CTR-CMAC8	+	+	64
4	MAGMA-NULL-CMAC8	+	–	64

- используется только «Магма» [ГОСТ Р 34.12-2015]
- один KDF на основе CMAC для всех криптонаборов, производный ключ защищает $q = 2^{13}$ пакетов
- шифрование – CTR [ГОСТ Р 34.13-2015]
- имитозащита – CMAC [ГОСТ Р 34.13-2015]
- «шифрование затем имитозащита» – EncThenMAC

Результаты анализа

СФБ ЛАБ

CTCrypt 2023

- доказательство стойкости протокола в релевантной модели угроз за счёт сведения к стойкости шифра «Магма»
- оценки ***сверху*** на *преобладание* в задаче различения, а следовательно, на *вероятность* нарушения свойств безопасности (конфиденциальности и целостности)

Верхние оценки

Преобладание противника ограничено:

$$\mathrm{Adv}_{\mathrm{CRISP}} \lessapprox \mathrm{Adv}_{\mathrm{KDF}}(\kappa) + \kappa \cdot \left(\mathrm{Adv}_{\mathrm{CMAC}}(q, l) + \mathrm{Adv}_{\mathrm{CTR}}(q, l)\right)$$

κ – число производных ключей
$q \leq 2^{13}$ – число пакетов, защищаемых на одном пр.ключе
$l \leq 2^{8}$ – максимальная длина пакета (в 64-битных блоках)

Kiryukhin V.

On security aspects of CRISP

CTCrypt 2023

Оценки точные?

Преобладание/вероятность успеха противника:

- доказуемая стойкость – оценка **сверху**
- атаки – оценка **снизу**

Оценки точные?

Преобладание/вероятность успеха противника:

- доказуемая стойкость – оценка **сверху**
- атаки – оценка **снизу**

Построим атаки – продемонстрируем **точность** оценок.

Атака на конфиденциальность – бесключевое чтение.
Атака на целостность – навязывание.

Атака на конфиденциальность

Верхняя оценка

Оценка сверху для преобладания в задаче различения

$$\mathrm{Adv}_{\mathrm{CTR}}(q, l) \lessapprox \frac{(q \cdot l)^2}{2^{n+1}}$$

квадратично зависит от числа защищаемых блоков.

Известные методы

Без изменений применяем существующие методы дешифрования режима CTR

Lavrikov I. V., Shishkin V. A.

How much data may be safely processed on one key in different modes?

Матем. вопр. криптогр., 10:2, 2019

Leurent G., Sibleyras F.

The Missing Difference Problem, and its Applications to Counter Mode Encryption

2018

Условия

СФБ ЛАБ

- Задача – найти значение секретного блока $S \in \mathbf{S}$
- Каждый пакет шифруется
- В каждом пакете
  - половина блоков – известные зашифрованные блоки OT
  - половина блоков с зашифрованным секретом S

Алгоритм

- Пусть **S** состоит из двух элементов, к примеру **S** = {0...0, 1...1}
- Знаем $ql/2$ блоков гаммы Γ_i
- Знаем $ql/2$ блоков «гамма+секрет» $\tilde{\Gamma}_j \oplus S$
- Для любых (i, j) верно $\Gamma_i \oplus (\tilde{\Gamma}_j \oplus S) \neq S$
- Ожидаем, что найдётся пара (i, j): $\Gamma_i \oplus (\tilde{\Gamma}_j \oplus S) = S' \in \mathbf{S}$
- Значение секрета $S \in \mathbf{S} \setminus \{S'\}$

Нижняя оценка

Вероятность успешного бесключевого чтения при $|\mathbf{S}| = 2$ и при конкретном производном ключе

$$p_1 \approx \left(\frac{q \cdot l}{2}\right)^2 \cdot \frac{1}{2^n} = 2^{-24},$$

при каком-нибудь из κ производных ключей

$$p_\kappa \approx \kappa \cdot p_1 \approx \frac{1}{2} \cdot \kappa \cdot \mathrm{Adv}_{\mathrm{CTR}}(q, l).$$

Нижняя оценка

Вероятность успешного бесключевого чтения при $|\mathbf{S}| = 2$ и при конкретном производном ключе

$$p_1 \approx \left(\frac{q \cdot l}{2}\right)^2 \cdot \frac{1}{2^n} = 2^{-24},$$

при каком-нибудь из κ производных ключей

$$p_\kappa \approx \kappa \cdot p_1 \approx \frac{1}{2} \cdot \kappa \cdot \mathrm{Adv}_{\mathrm{CTR}}(q, l).$$

При $|\mathbf{S}| \geq 4$, вероятность успеха p_1 *много меньше* 2^{-n}.

Вывод: бесключевое чтение *малоэффективно* для существующих криптонаборов протокола CRISP.

Атака на целостность

Верхняя оценка

Оценка сверху для преобладания в задаче различения

$$\mathrm{Adv}_{\mathrm{CMAC}}(q, l) \lessapprox \frac{16q^2 + ql^2 + 4ql}{2^n} \approx \frac{16q^2}{2^n}$$

почти не зависит от длины пакета ($l \leq 2^8$)

Chattopadhyay S., Jha A., Nandi M.
Towards Tight Security Bounds for OMAC, XCBC and TMAC
2022

Проблема

НЕ работает стандартная атака на CMAC/HMAC вида:
– запросить имитовставки T_i к q сообщениям M_i
– найти коллизию $T_i = T_j$, $i \neq j$
– запросить дополнительно сообщение $M_i||B$, получить T'
– построить подделку $M_j||B$ с имитовставкой T'

Проблема

НЕ работает стандартная атака на CMAC/HMAC вида:
– запросить имитовставки T_i к q сообщениям M_i
– найти коллизию $T_i = T_j$, $i \neq j$
– запросить дополнительно сообщение $M_i||B$, получить T'
– построить подделку $M_j||B$ с имитовставкой T'

Причина

Каждое сообщение обладает уникальным номером,
из коллизии для $SN_i||M_i$ и $SN_j||M_j$
НЕ следует коллизия для $SN_{q+1}||M_i$ и $SN_{q+2}||M_j$.

Известные методы

Адаптируем существующие атаки под специфику протокола

Brincat K., Mitchel C.

New CBC-MAC forgery attacks

ACISP 2001

Mitchel C.

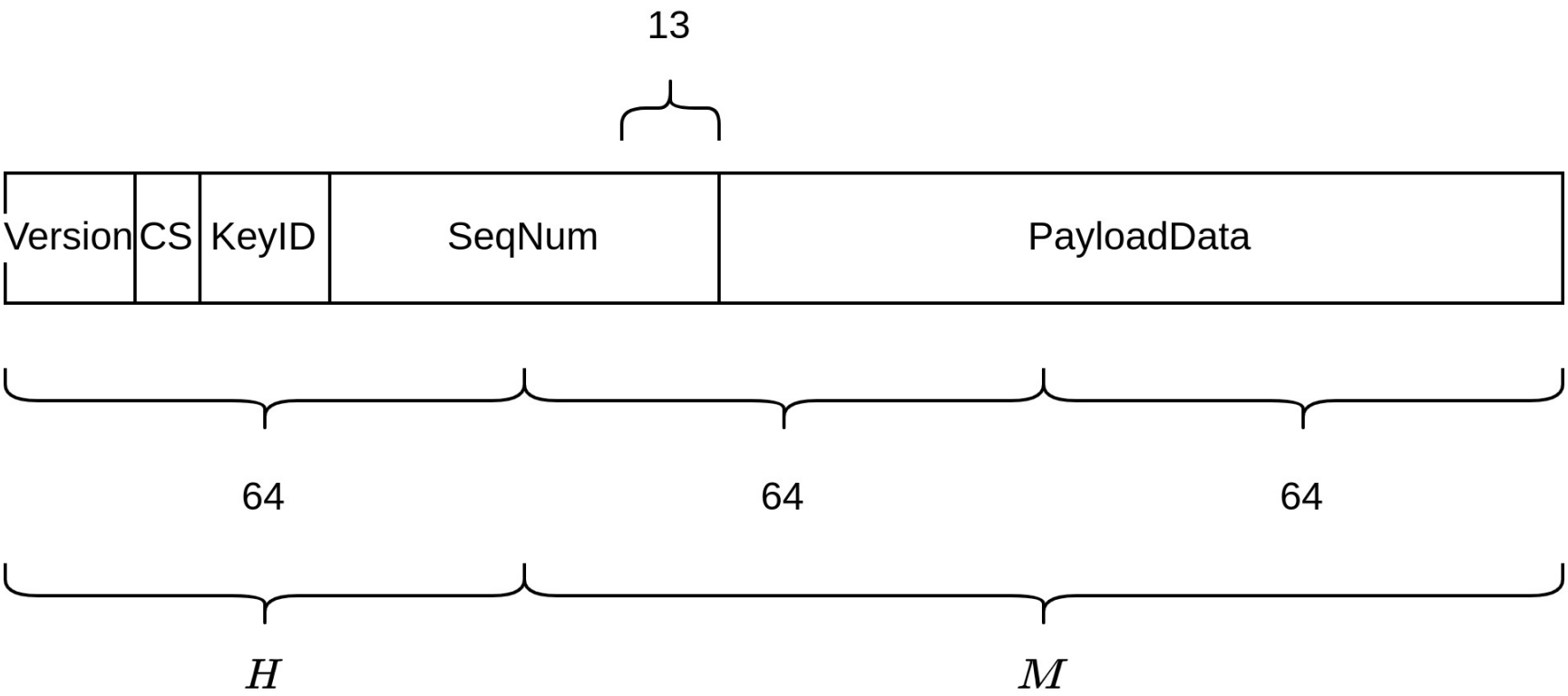
Partial Key Recovery Attacks on XCBC, TMAC and OMAC

2005

Условия атаки

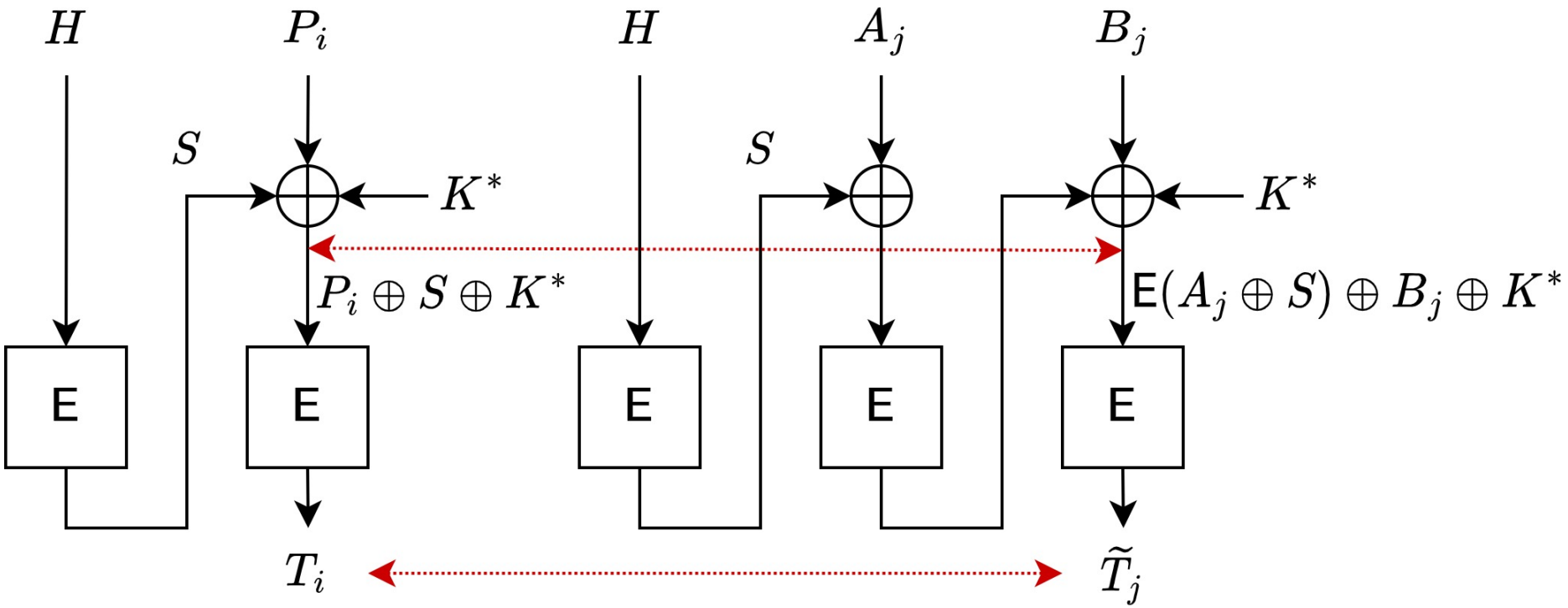
Известные сообщения с ограничениями на структуру:

- первые несколько блоков заголовка *H* зафиксированы
- блоки *M* содержат биты `SeqNum` и `PayloadData`
- поле `PayloadData` может быть *зашифровано*



Идея

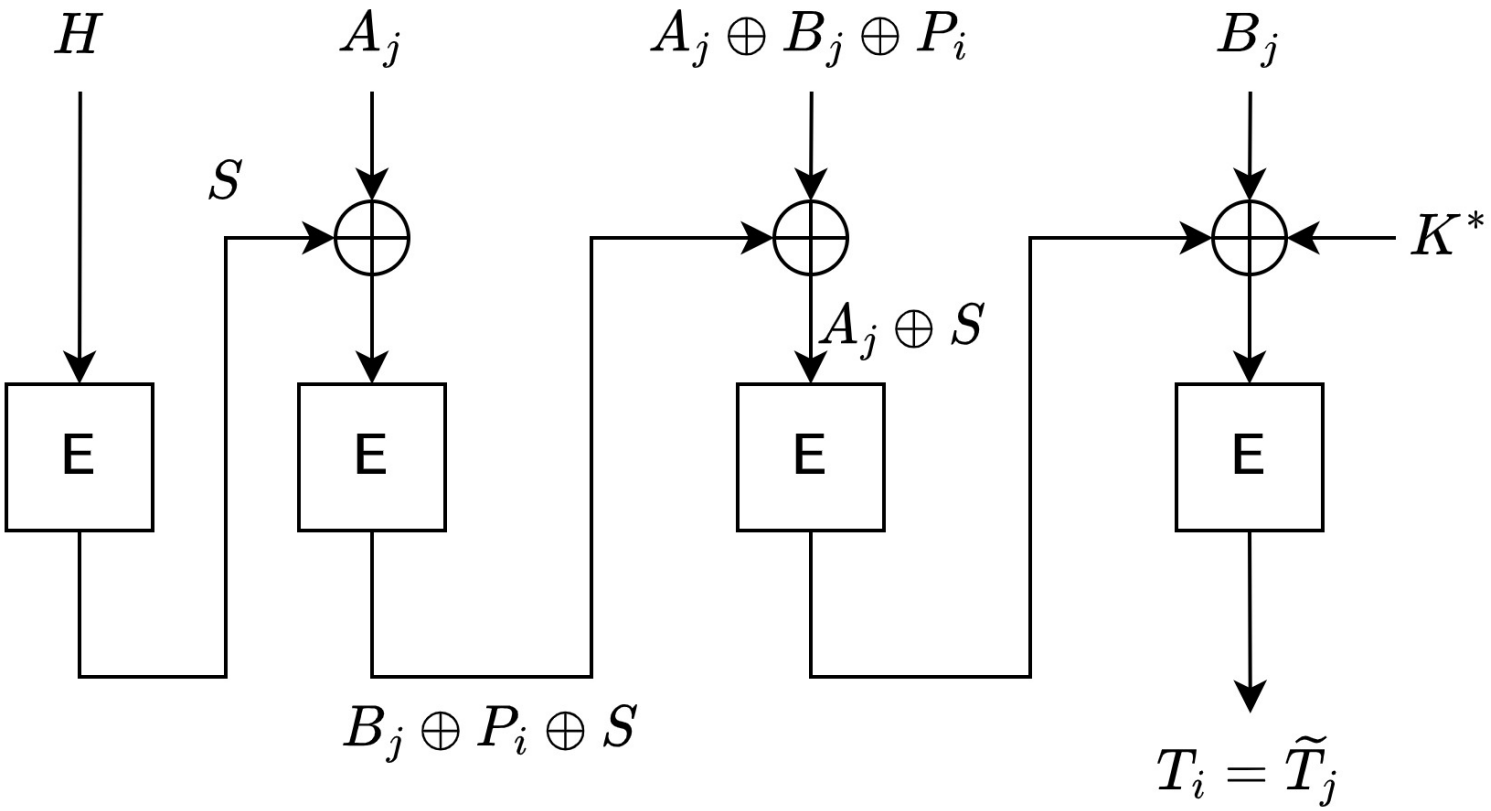
Коллизия по имитовставкам = Коллизия по состояниям



$$\mathsf{E}(A_j \oplus S) \oplus B_j = P_i \oplus S$$

Подделка путём «вставки» в центр

Блок с SeqNum (A_j) и заголовок (H) не искажаются



Алгоритм и характеристики атаки

1) Множество из $\frac{q}{2}$ сообщений $H||P_i$, имитовставки T_i
2) Множество из $\frac{q}{2}$ сообщений $H||A_j||B_j$, имитовставки $\tilde{T}_j$
3) Найдём коллизию $T_i = \tilde{T}_j$
4) Предъявим подделку *(без дополнительных запросов!)*

$$H \,||\, A_j \,||\, (A_j \oplus B_j \oplus P_i) \,||\, B_j \quad \text{с имитовставкой } T_i$$

Алгоритм и характеристики атаки

1) Множество из $\frac{q}{2}$ сообщений $H||P_i$, имитовставки T_i
2) Множество из $\frac{q}{2}$ сообщений $H||A_j||B_j$, имитовставки $\tilde{T}_j$
3) Найдём коллизию $T_i = \tilde{T}_j$
4) Предъявим подделку *(без дополнительных запросов!)*

$$H \,||\, A_j \,||\, (A_j \oplus B_j \oplus P_i) \,||\, B_j \quad \text{с имитовставкой } T_i$$

Вероятность успеха при конкретном производном ключе

$$p_1 \approx \left(\frac{q}{2}\right)^2 \cdot \frac{1}{2^n} = 2^{-40},$$

при *каком-нибудь* из $к$ производных ключей

$$p_к \approx к \cdot p_1 \approx \tfrac{1}{64} \cdot к \cdot \mathrm{Adv}_{\mathrm{CMAC}}(q, l).$$

Общие замечания

СФБ ЛАБ

- Содержимое пакетов может быть ***любым*** (в т.ч. зашифрованным), ограничивается лишь длина
- Первое множество: «заголовок + один блок»
- Второе множество: «заголовок + *любые* блоки»
- Длина имитовставки равна длине блока

Атака на целостность

Определение финализирующих ключей

Условия

Сообщения имеют вид «заголовок + несколько *байт*»

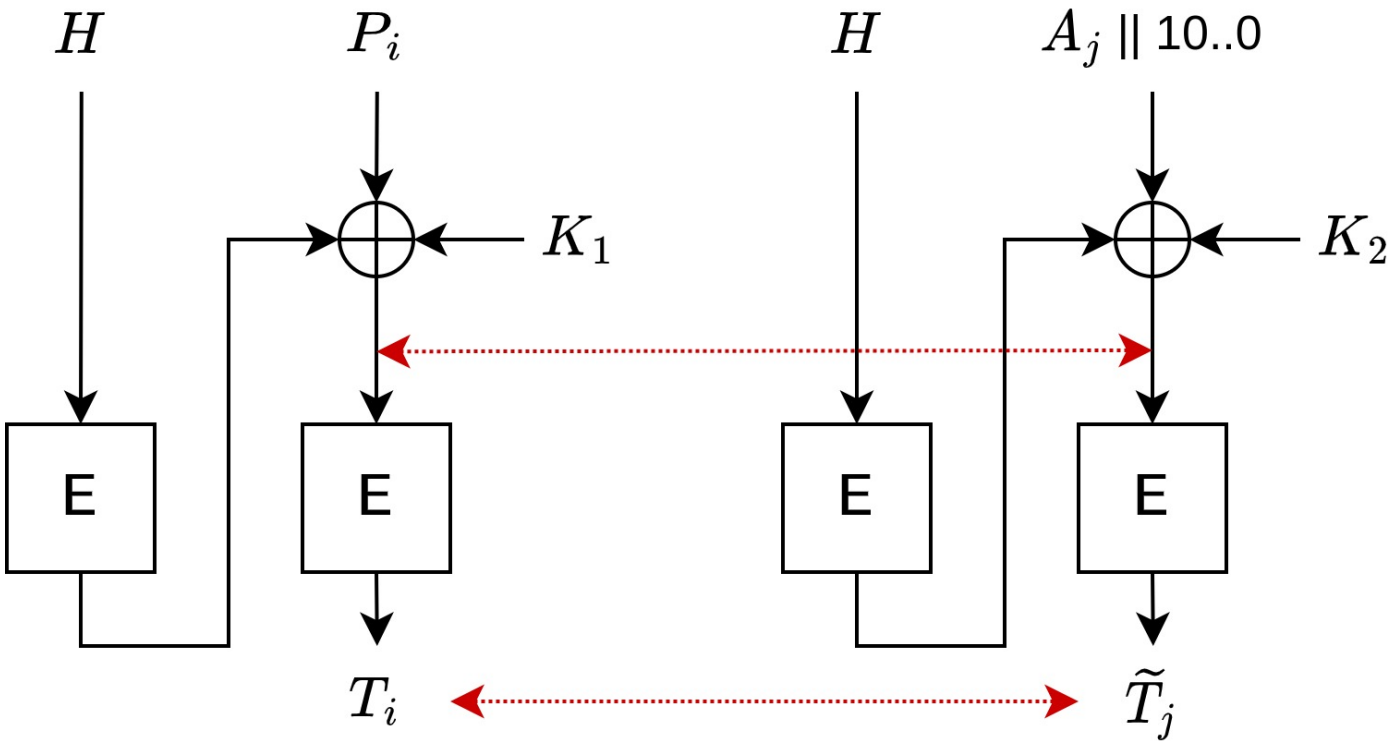
Первое множество – длина сообщений кратна n ($H||P_i$)
Второе множество – длина сообщений НЕ кратна n ($H||A_j$)

Идея: одна коллизия по имитовставкам позволяет определить

$$K_1 = \alpha \otimes \mathrm{E}_K(0) \text{ и } K_2 = \alpha^2 \otimes \mathrm{E}_K(0)$$

– можно построить много подделок различного вида

Идея



Коллизия даёт уравнение, позволяющее найти $\mathrm{E}_K(0)$, K_1, K_2:

$$P_i \oplus K_1 = A'_j \oplus K_2,\ A'_j = A_j||10...0,$$

$$P_i \oplus A'_j = \alpha \otimes \mathrm{E}_K(0) \oplus \alpha^2 \otimes \mathrm{E}_K(0),$$

$$\mathrm{E}_K(0) = (P_i \oplus A'_j) \otimes (\alpha \oplus \alpha^2)^{-1}.$$

Атака на целостность

Короткая имитовставка

Проблема

Пусть имитовставка усекается до половины блока.

Из коллизии таких имитовставок
НЕ следует коллизия состояний.

Решение

- Используем атаку на определение ключей K_1 и K_2

Решение

- Используем атаку на определение ключей K_1 и K_2
- При каждой коллизии $T_i = \widetilde{T}_j$
  - *предполагаем* коллизию состояний $P_i \oplus K_1 = A'_j \oplus K_2$
  - находим и сохраняем в памяти $\mathrm{E}_K(0) = (P_i \oplus A'_j) \otimes (\alpha \oplus \alpha^2)^{-1}$

Решение

- Используем атаку на определение ключей K_1 и K_2
- При каждой коллизии $T_i = \widetilde{T}_j$
  - *предполагаем* коллизию состояний $P_i \oplus K_1 = A'_j \oplus K_2$
  - находим и сохраняем в памяти $\mathrm{E}_K(0) = (P_i \oplus A'_j) \otimes (\alpha \oplus \alpha^2)^{-1}$
- Если коллизия по состояниям реализуется **дважды**, то истинное значение $\mathrm{E}_K(0)$ также появится дважды, а ложные только по одному разу

Решение

- Используем атаку на определение ключей K_1 и K_2
- При каждой коллизии $T_i = \tilde{T}_j$
  - *предполагаем* коллизию состояний $P_i \oplus K_1 = A'_j \oplus K_2$
  - находим и сохраняем в памяти $\mathrm{E}_K(0) = (P_i \oplus A'_j) \otimes (\alpha \oplus \alpha^2)^{-1}$
- Если коллизия по состояниям реализуется **дважды**, то истинное значение $\mathrm{E}_K(0)$ также появится дважды, а ложные только по одному разу
- При $q \ll 2^{\frac{n}{2}}$ вероятность хотя бы двух коллизий крайне мала $\approx (\frac{q^2}{2^n})^2$

Выводы

Рассматриваемые атаки обладают значимой вероятностью успеха ($> 2^{-10}$) только если рассматривается сценарий: реализация угрозы **при любом производном ключе из многих**.

Если каждый производный ключ рассматривается **отдельно**, то вероятность успеха атак пренебрежимо мала:

- 2^{-24} для бесключевого чтения (одного бита)
- 2^{-40} для навязывания

Заключение

1. Построены атаки на целостность и конфиденциальность, показана точность оценок стойкости протокола CRISP

Заключение

СФБ ЛАБ

1. Построены атаки на целостность и конфиденциальность, показана точность оценок стойкости протокола CRISP
2. Атаки обладают малой вероятностью успеха, НЕ угрожают практической безопасности протокола

Заключение

СФБ ЛАБ

1. Построены атаки на целостность и конфиденциальность, показана точность оценок стойкости протокола CRISP
2. Атаки обладают малой вероятностью успеха, НЕ угрожают практической безопасности протокола
3. Параметры протокола выбраны консервативно, нагрузка на производный ключ мала

Благодарю за внимание!

Виталий Кирюхин

ООО «СФБ Лаб», АО «ИнфоТеКС»
РусКрипто’2024
21 марта 2024

vitaly.kiryukhin@sfblaboratory.ru