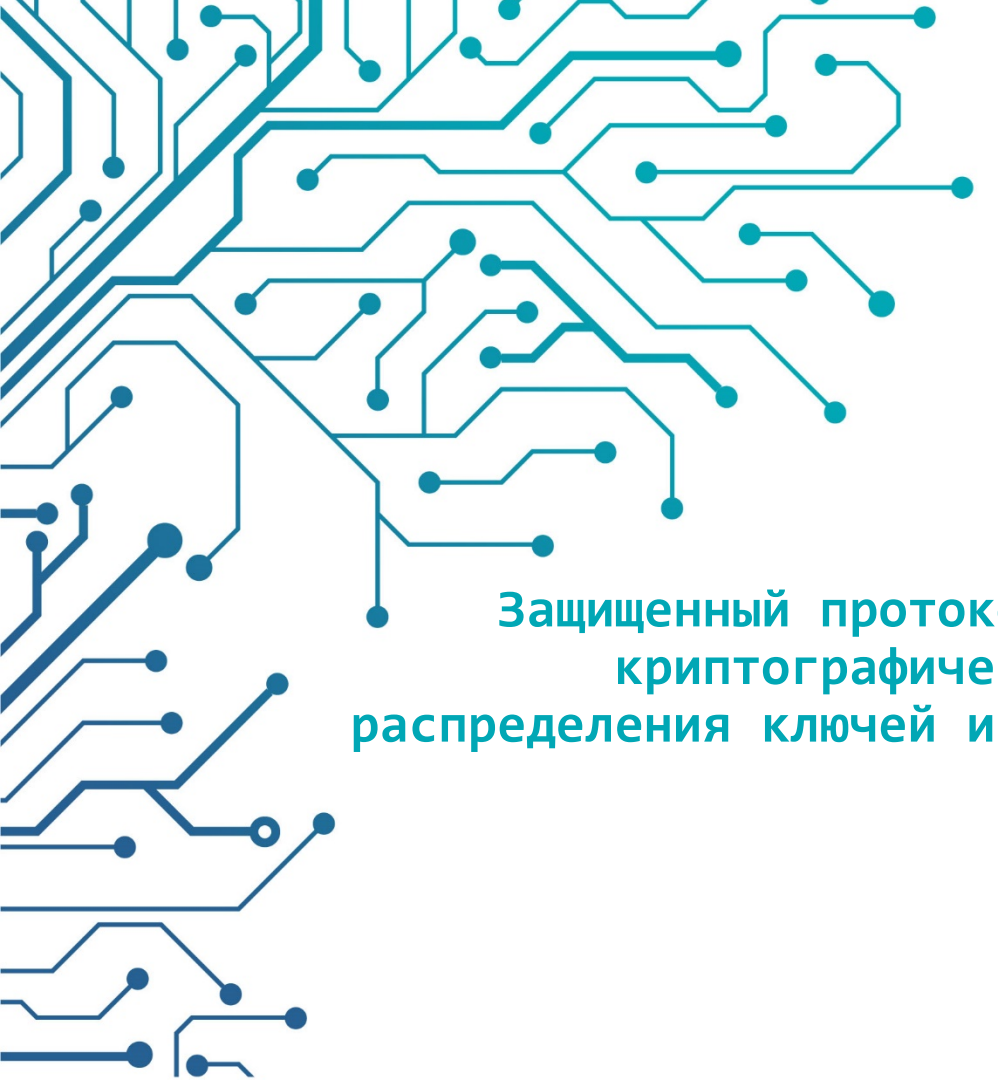
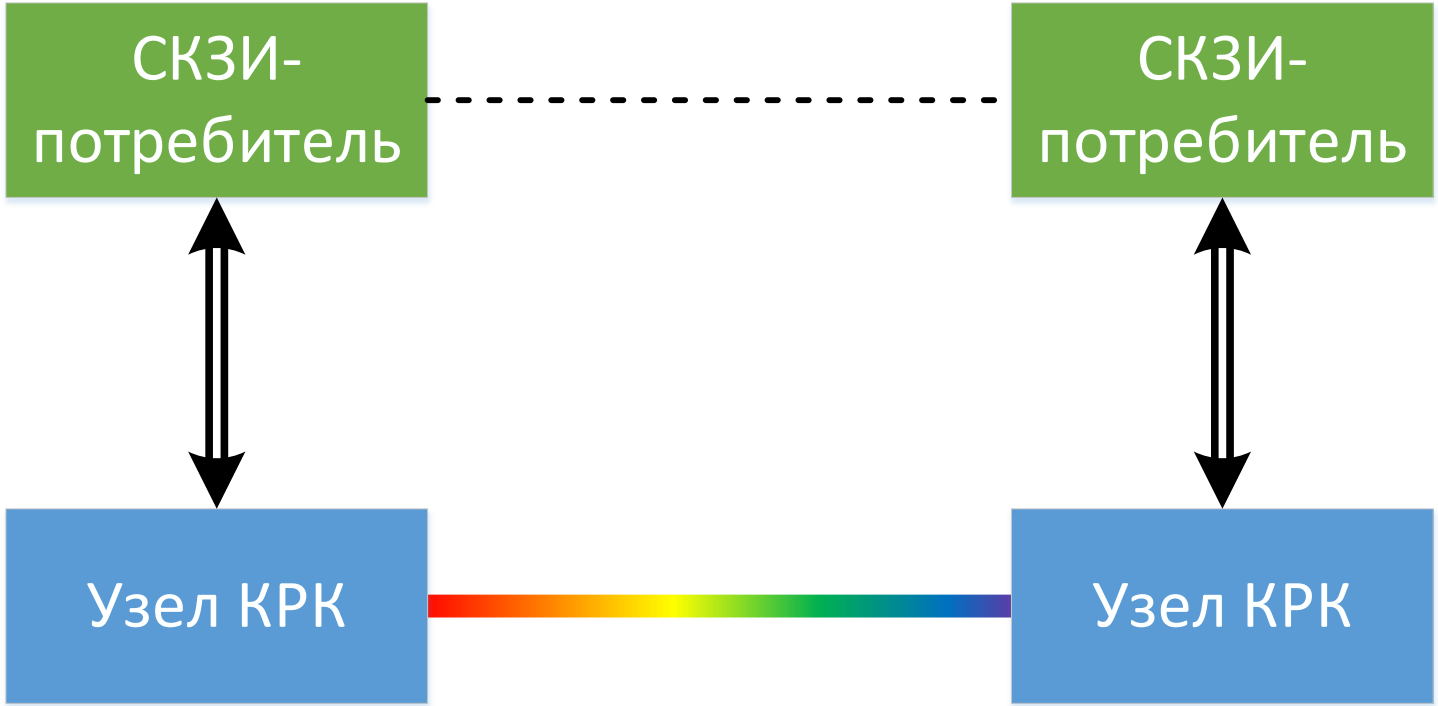


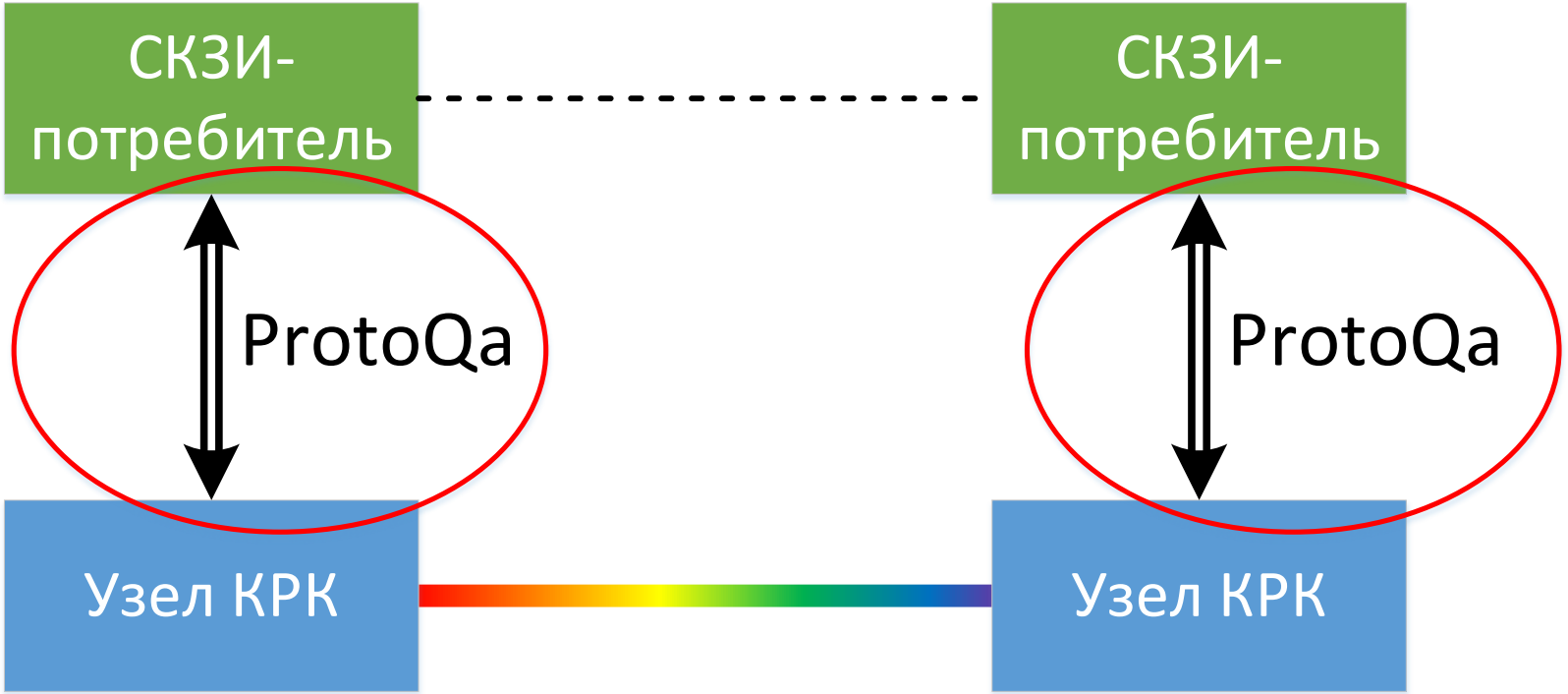
Защищенный протокол взаимодействия квантово-криптографической аппаратуры выработки и распределения ключей и средства криптографической защиты информации (ProtoQa)

Науменко Антон Павлович, ООО СФБ Лаб
Бородин Михаил Алексеевич, АО Инфотекс

Введение



Введение


СКЗИ-потребитель
СКЗИ-потребитель
ProtoQa
ProtoQa
Узел КРК
Узел КРК

Базовые принципы

Эксплуатационные

- Протокол построен по принципу «запрос-ответ».
- Протокол допускает эффективные программные и аппаратные реализации.
- Возможность расширения протокола под конкретного производителя.
- Опциональный набор команд и параметров (можно не реализовывать команды, которые не будут использоваться).

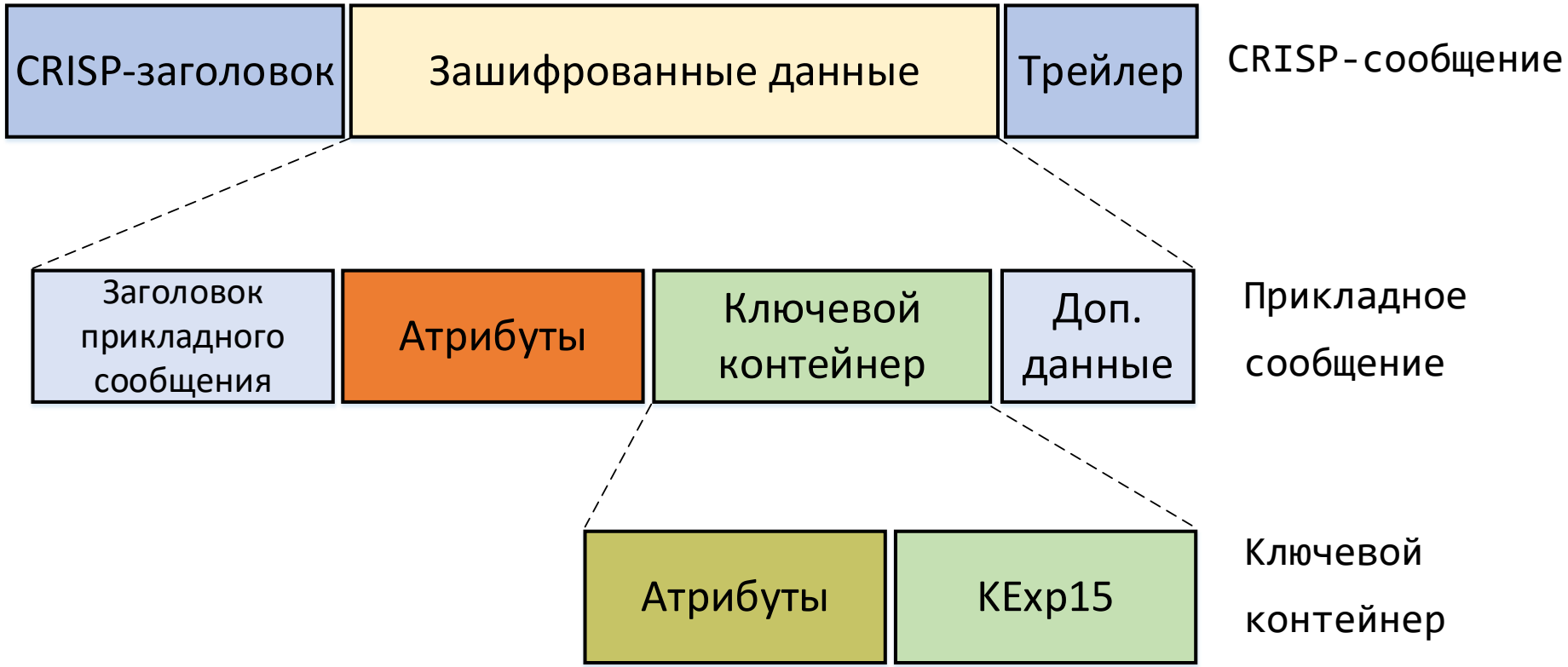
Криптографические

- Инкапсуляция прикладных сообщений внутри CRISP-сообщения.
- Используются только симметричные механизмы.
- Необходимо предварительное распределение ключей для протокола CRISP и для защиты ключевых контейнеров.
- Защита от навязывания ранее переданных сообщений.

Этапы работы протокола

1. Согласование параметров работы между СКЗИ-потребителем и узлом КРК.
2. Обычное функционирование протокола.
3. Отключение СКЗИ-потребителя от узла КРК.

Порядок формирования сообщений



Формат CRISP-сообщения

Номер поля	Наименование поля		Длина поля в битах
1	Заголовок	ExternalKeyIdFlag	1
2		Version	15
3		CS	8
4		KeyId	328
5		SeqNum	48
6	PayloadData		Переменная (≤15856)
7	ICV		Зависит от значения CS

1. **ExternalKeyIdFlag**: «0», значения KeyId достаточно для правильного определения базового ключа.
2. **Version**: «0», указано в рекомендациях на текущий момент.
3. **CS**: Например «1», набор MAGMA-CTR-CMAC. Для обеспечения конфиденциальности и имитозащиты сообщения.
4. **KeyId**: $«10101000»_b$, идентификатор ключа задается в следующих 40-а байтах.
5. **SeqNum**: Номер сообщения между участниками, задается независимо для каждого направления.
6. **PayloadData**: Прикладное сообщение.
7. **ICV**: Имитозащита полей 1-6.

Формат заголовка прикладного сообщения

Номер поля	Название поля	Размер
1	Ver	1 байт
2	SenderID	16 байт
3	DestinID	16 байт
4	SessionID	4 байта
5	MsgType	1 байт

1. **Ver**: «0», текущая версия.
2. **SenderID**: идентификатор отправителя сообщения.
3. **DestinID**: идентификатор получателя сообщения.
4. **SessionID**: Идентификатор пары сообщений (запрос-ответ) между участниками, задается независимо для каждого направления запросов.
5. **MsgType**: Тип сообщения.

Типы прикладных сообщений

Код	Описание	Классификация
0x01	Запрос согласования параметров	Запрос/ответ согласования параметров
0x02	Ответ на запрос согласования параметров	
0x03	Запрос нового ключа	Виды запросов на получение ключа
0x04	Запрос зарезервированного ключа	
0x05	Запрос нового или зарезервированного ключа	
0x06	Ответ на запрос получения ключа	Ответ на запрос получения ключа
0x07	Запрос случайного числа	Запрос/ответ на получение случайного числа
0x08	Ответ на запрос случайного числа	
0x09	Запрос передачи данных служебного канала	Запрос передачи данных служебного канала
0x0A	Запрос типа информационное сообщение	Информационные сообщения
0x00	Ответ с кодом отчета	
…	…	…

Механизмы защиты

Протокол CRISP

Конфиденциальность

- Шифрование прикладных сообщений, при CS=1 используется БШ «Магма» в режиме гаммирования по ГОСТ 34.13-2018.

Целостность и аутентичность

- Имитозащита всех полей CRISP-сообщения, при CS=1 используется БШ «Магма» в режиме выработки имитовставки по ГОСТ 34.13-2018.

Защита от повторов

- Использование «скользящего окна» принятых сообщений.

Диверсификация ключей

- Контроль нагрузки на ключ/данные; диверсификация с использованием БШ «Магма» в режиме выработки имитовставки по ГОСТ 34.13-2018.

Прикладные сообщения

Конфиденциальность и целостность ключа и опционально случайных чисел

- Использование ключевых контейнеров KExp15 с БШ «Кузнечик» или «Магма».

Защита от повторов

- Возрастающий счётчик номеров запросов в каждом направлении (**SessionID**).
- Идентификаторы целевых ключей формируются в узлах КРК, метки этих ключей могут формироваться в СКЗИ-потребителях.
- Предусмотрены поля, которые позволяют организовать контроль нагрузки на ключ/данные; и синхронно осуществлять смену ключей защиты контейнеров.

Обоснование стойкости. Базовые криптомеханизмы

«Магма» (ГОСТ 28147-89)

Свойство «отражения»

- 2^{32} пар открытый-шифрованный текст
- 2^{225} операций опробования

Свойство «неподвижная точка»

- 2^{64} пар открытый-шифрованный текст
- 2^{193} операций опробования

Обоснование стойкости. «Кузнечик»

Раунды	Атака	Материал	Время	Память
2	Многомерные невозможные дифф.	5	2^{13}	2^{7}
3	Многомерные невозможные дифф.	11	2^{72+8t}	2^{71-8t}
	Многомерные н.д. + Интегральная	2^{8}	2^{16}	2^{20}
4	Многомерные невозможные дифф.	21	2^{137}	2^{136}
		21	2^{144}	2^{129}
	Многомерные н.д. + Интегральная	2^{8}	2^{144}	2^{20}
		2^{8}	2^{136}	2^{129}
4	Multiset-Algebraic	2^{56}	2^{56}	O(1)
5	MitM	2^{113}	$2^{159.3}$	2^{154}
5	Multiset-Algebraic	2^{120}	2^{120}	O(1)
6	MitM	2^{113}	2^{231}	2^{218}
6	Multiset-Algebraic	2^{128}	$2^{133.5}$	O(1)
7	Multiset-Algebraic	2^{128}	$2^{154.5}$	2^{140}
9	Тотальное опробование	4	2^{256}	O(1)

Обоснование стойкости. Алгоритм выработки производных ключей

Теорема. Пусть алгоритм *CMAC* использует блочный шифр $E: V_k \times V_n \to V_n$ (обозначим такое преобразование $CMAC[E]$), тогда

$$Adv^{PRF}_{CMAC[E]}(t, q, \sigma) \leq Adv^{PRP}_{E}(t', q') + \frac{4\sigma^2}{2^n},$$

где:

t – вычислительные ресурсы противника;

q – число адаптивных запросов, которые противник может отправить оракулу;

σ – суммарная длина всех запросов (в блоках);

$t' = t + c \cdot \sigma \approx t$, где c – константа, зависящая от модели вычисления;

$q' = \sigma + 1$.

Обоснование стойкости. Алгоритм выработки производных ключей

Определение. Преобладанием противника $\mathcal{A}$ в модели KDF для ключевой функции $F: V_k \times V_{\leq l} \to V_{n \cdot m}$ назовём

$$Adv_F^{KDF}(\mathcal{A}) = \left| Pr\left(K \xleftarrow{R} V_k : \mathcal{A}^{F(\cdot)} \Rightarrow 1\right) - Pr\left(\mathcal{A}^{\$(\cdot)} \Rightarrow 1\right) \right|,$$

где $\$(\cdot)$ – оракул, возвращающий последовательности двоичных независимых равновероятных случайных величин длины $n \cdot m$ бит.

Если значение $\mathrm{Adv}_{\mathrm{F}}^{KDF}(\mathcal{A})$ мало, то можно говорить, что для противника $\mathcal{A}$ схема выработки производных ключей неотличима от *«генератора идеальной гаммы»*.

Обоснование стойкости. Алгоритм выработки производных ключей

Справедлива оценка

$$\mathrm{Adv}_{\mathrm{DK}}^{KDF}(t,q) \le \mathrm{Adv}_{\mathrm{E}}^{PRP}(t',q') + \frac{196\cdot(mq)^2}{2^n},$$

где $t' \approx t$, а $q' = 7\cdot mq + 1$.

Для шифра Магма значение $\mathrm{Adv}_{\text{Магма}}^{PRP}(t',q')$ можно считать близким к вероятности успеха метода тотального опробования

$$\mathrm{Adv}_{\text{Магма}}^{PRP}(t,q) \approx \frac{t}{2^k} \approx 0$$

– пренебрежимо мало по сравнению с другим слагаемым в оценке.

Для алгоритма DK параметр q по сути определяет допустимую нагрузку на базовый ключ. Предельное значение q должно быть выбрано так, чтобы $\mathrm{Adv}_{\mathrm{DK}}^{KDF}(t,q)$ было ограничено малой величиной.

Обоснование стойкости. KExp15

Определение. Преобладанием противника $\mathcal{A}$ в модели DAE (Deterministic Authenticated Encryption) для схемы $K15 = (KExp15, KImp15)$ назовём

$$Adv_{K15}^{DAE}(\mathcal{A}) = \left| Pr\left(\left(K_{MAC}^{Exp}, K_{ENC}^{Exp}\right) \xleftarrow{R} V_k^2 : \mathcal{A}^{KExp15(\cdot,\cdot),KImp15(\cdot,\cdot)} \Rightarrow 1 \right) - \right.$$
$$\left. - Pr\left(\mathcal{A}^{\$(\cdot,\cdot),\perp(\cdot,\cdot)} \Rightarrow 1\right) \right|,$$

где

$\$(\cdot,\cdot)$ – оракул, который принимает запрос вида (IV, K) и возвращает последовательность двоичных независимых равновероятных случайных величин длины $|K| + n$ бит;

$\perp(\cdot,\cdot)$ – оракул, который возвращает ошибку на любой запрос вида $(IV, KEXP)$;

K – экспортируемый ключ $K \in V_{\leq l}$;

оракул $KExp15(\cdot,\cdot)$ принимает запрос вида (IV, K) и возвращает $KEXP$;

оракул $KImp15(\cdot,\cdot)$ принимает запрос вида $(IV, KEXP)$ и возвращает K или ошибку.

Обоснование стойкости. KExp15

Справедлива оценка

$$\mathrm{Adv}^{DAE}_{\mathrm{K15}}(t,q) \approx \frac{4(qu)^2}{2^n} + \frac{(q(u+1))^2}{2^{n+1}} + \frac{q}{2^n} < \frac{5(qu)^2}{2^n}.$$

Максимальная длина экспортируемого ключа K (или случайной последовательности) составляет 2^{11} байт.

Для шифра Кузнечик ($n = 128$, $u = 8 \cdot 2^{11}/n = 2^7$) получим

$$\mathrm{Adv}^{DAE}_{\mathrm{K15[Кузнечик]}}(t,q) < \frac{5 \cdot 2^{14} \cdot q^2}{2^{128}} < 2.5 \cdot 10^{-34} \cdot q^2.$$

Для шифра Магма ($n = 64$, $u = 8 \cdot 2^{11}/n = 2^8$) получим

$$\mathrm{Adv}^{DAE}_{\mathrm{K15[Магма]}}(t,q) < \frac{5 \cdot 2^{16} \cdot q^2}{2^{64}} < 1.8 \cdot 10^{-14} \cdot q^2.$$

Обоснование стойкости. Ограничения

Число экспортируемых ключей K при одной и той же паре базовых ключей $(K_{MAC}^{Exp}, K_{ENC}^{Exp})$ не должно превышать:

– для шифра Магма $q \leq 2^{12}$;

– для шифра Кузнечик $q \leq 2^{45}$.

Число пар производных ключей (K_{MAC}, K_{ENC}), выработанных с использованием одного и того же базового ключа протокола CRISP в рамках реализации протокола ProtoQa, не должно превышать величины:

$$q \leq 2^{15}.$$

Обоснование стойкости. Навязывание

Протокол ProtoQa является стойким к навязыванию ложных сообщений при условии реализации в конечной системе, в которой предполагается использование данного протокола, ограничения на максимальное количество сообщений с неправильной имитовставкой

Спасибо за внимание!

Подписывайтесь на наши соцсети

@infotecs.ru

@vpninfotecs

@InfoTeCS_Moscow