Об одном подходе к оценке нагрузки на ключ на примере протоколов CRISP и IPLIR

Виталий Кирюхин

ООО «СФБ Лаб», АО «ИнфоТеКС»

РусКрипто’2025
20 марта 2025

vitaly.kiryukhin@sfblaboratory.ru

СФБ ЛАБ

Типичная модель из «доказуемой стойкости»

СФБ ЛАБ

Требование

Преобладание ε в задаче различения «реальная система» или «идеальная система» меньше критического значения.

Типичная модель из «доказуемой стойкости»

СФБ ЛАБ

Требование

Преобладание ε в задаче различения «реальная система» или «идеальная система» меньше критического значения.

Альтернативная формулировка

Вероятность p успешной атаки хоть на какого-нибудь одного из μ пользователей/ключей меньше критического значения.

Типичная модель из «доказуемой стойкости»

СФБ ЛАБ

Требование

Преобладание ε в задаче различения «реальная система» или «идеальная система» меньше критического значения.

Альтернативная формулировка

Вероятность p успешной атаки хоть на какого-нибудь одного из μ пользователей/ключей меньше критического значения.

Это жёсткое требование при использовании низкоресурсных криптоалгоритмов...

Пример

СФБ ЛАБ

Условия

μ ***независимых*** ключей $K_1,\ldots,K_\mu$. Каждый ключ K_i защищает ***два*** сообщения M_i и $\widetilde{M}_i$ с помощью «Магмы» в режиме CMAC.

Пример

СФБ ЛАБ

Условия

μ ***независимых*** ключей $K_1,\ldots,K_\mu$. Каждый ключ K_i защищает ***два*** сообщения M_i и $\widetilde{M}_i$ с помощью «Магмы» в режиме CMAC.

Атака

Противник наблюдает пары «сообщение, имитовставка»,

$$\begin{array}{cccccc} M_1, T_1 & M_2, T_2 & \ldots & M_j, T_j & \ldots & M_\mu, T_\mu \\ \widetilde{M}_1, \widetilde{T}_1 & \widetilde{M}_2, \widetilde{T}_2 & \ldots & \widetilde{M}_j, \widetilde{T}_j & \ldots & \widetilde{M}_\mu, \widetilde{T}_\mu \end{array}$$

Коллизия $T_j = \widetilde{T}_j$ даёт построить подделку при j-м ключе.

Вероятность успеха $p \approx \mu \cdot 2^{-64}$.

Пример

СФБ ЛАБ

Атака

[...] Вероятность успеха $p \approx \mu \cdot 2^{-64}$

Пример

СФБ ЛАБ

Атака

[...] Вероятность успеха $p \approx \mu \cdot 2^{-64}$

Вывод

В такой системе можно использовать только $\mu \ll 2^{64}$ ключей, а достижение этой границы делает дальнейшую эксплуатацию системы *недопустимой*!

Проблема

СФБ ЛАБ

- Даже в «льготных» условиях примера ограничение жёсткое (2^{60} блоков $\approx$ 400 Гбит/с за 5 лет)

Проблема

СФБ ЛАБ

- Даже в «льготных» условиях примера ограничение жёсткое (2^{60} блоков $\approx$ 400 Гбит/с за 5 лет)
- В реальных протоколах нагрузка на ключ много больше пары блоков/сообщений – ограничение гораздо жёстче

Проблема

СФБ ЛАБ

- Даже в «льготных» условиях примера ограничение жёсткое (2^{60} блоков $\approx$ 400 Гбит/с за 5 лет)
- В реальных протоколах нагрузка на ключ много больше пары блоков/сообщений – ограничение гораздо жёстче
- Аналогичная ситуация для других режимов работы шифра (в т.ч. BBB) и угроз дешифрования/различения

Два возможных решения

СФБ ЛАБ

№1. Отказ от низкоресурсных криптоалгоритмов

Используем только алгоритмы с большим размером ключа/состояния – «Кузнечик», «Стрибог» и т.д.

Два возможных решения

СФБ ЛАБ

№1. Отказ от низкоресурсных криптоалгоритмов

Используем только алгоритмы с большим размером ключа/состояния – «Кузнечик», «Стрибог» и т.д.

№2. Более слабые модели/требования

Заведомо соглашаемся, что ущерб системе может быть нанесён, но он должен быть *достаточно малым*

Два возможных решения

СФБ ЛАБ

№1. Отказ от низкоресурсных криптоалгоритмов

Используем только алгоритмы с большим размером ключа/состояния – «Кузнечик», «Стрибог» и т.д.

№2. Более слабые модели/требования

Заведомо соглашаемся, что ущерб системе может быть нанесён, но он должен быть *достаточно малым*

С первым всё понятно, что можно сказать про второе?

Ослабляем требования

СФБ ЛАБ

Задача различения

Было ε: «реальная система» или «идеальная система»

Стало ε_j^*: «реальная система» или

«реальная система, но при j-м ключе идеальная»

Ослабляем требования

СФБ ЛАБ

Задача различения

Было ε: «реальная система» или «идеальная система»

Стало ε_j^*: «реальная система» или

«реальная система, но при j-м ключе идеальная»

Вероятность нарушения свойств безопасности

Было p: … хоть при каком-нибудь одном из μ ключей

Стало p_j^*: … при конкретном j-м ключе

Физический смысл

Для большинства типов угроз

$$p_j^* \leq \varepsilon_j^*$$

$$p^* = \max_{1 \leq j \leq \mu}(p_j^*) \leq \varepsilon^* = \max_{1 \leq j \leq \mu}(\varepsilon_j^*)$$

Физический смысл

Для большинства типов угроз

$$p_j^* \leq \varepsilon_j^*$$

$$p^* = \max_{1 \leq j \leq \mu}(p_j^*) \leq \varepsilon^* = \max_{1 \leq j \leq \mu}(\varepsilon_j^*)$$

Среднее число ключей β, при которых нарушены свойства безопасности, ограничено

$$\beta \leq \mu \cdot p^* \leq \mu \cdot \varepsilon^*$$

а тогда ε^* – верхняя оценка на **долю** таких ключей.

Физический смысл

Ослабление требований:

- число ключей, при которых нарушены свойства безопасности, заведомо ***ненулевое***, $\beta > 0$
- но их средняя доля ***мала***, $\beta/\mu \leq \pi$

Зависимые ключи

СФБ ЛАБ

- Всё просто, когда ключи *независимы*

  $\Rightarrow$ Оценка ε при $\mu = 1$ равна ε^* при произвольном μ

Зависимые ключи

- Всё просто, когда ключи *независимы*

  $\Rightarrow$ Оценка ε при $\mu = 1$ равна ε^* при произвольном μ

- Сложнее, когда они порождены *ключевым деревом*

  $\Rightarrow$ При оценке ε_j^* нужно учесть сведения противника обо всех остальных ключах

Модели для протоколов типа «KDF + AEAD»

Обобщённый протокол

СФБ ЛАБ

- Однонаправленная передача «отправитель → получатель»
- Распределённый внешним образом ключ K
- KDF формирует из базового ключа μ производных
- Каждый производный защищает q^* пакетов
- Сам протокол – специфический AEAD-режим

Обобщённый протокол – Generic Protocol

$$\mathrm{GP} : \mathbf{K} \times (\mathbf{N}_{\mathrm{KDF}} \times \mathbf{N}_{\mathrm{AE}}) \times \mathbf{A} \times \mathbf{P} \to \mathbf{C} \times \mathbf{T}$$

$$\mathrm{KDF} : \mathbf{K} \times \mathbf{N}_{\mathrm{KDF}} \to \mathbf{K}_{\mathrm{AE}}$$

$$\mathrm{AE} : \mathbf{K}_{\mathrm{AE}} \times \mathbf{N}_{\mathrm{AE}} \times \mathbf{A} \times \mathbf{P} \to \mathbf{C} \times \mathbf{T}$$

Модель для AEAD-схем

NAE – Nonce-based Authenticated Encryption

$$\mathrm{Adv}_{\mathrm{AE}}^{NAE}(A) = \Pr\left(K \xleftarrow{\mathrm{u}} \mathbf{K} : A^{\mathrm{AE}_K, \mathrm{AE}_K^{-1}} \Rightarrow 1\right) - \Pr\left(A^{\$,\perp} \Rightarrow 1\right)$$

Оракул $ возвращает «идеальную гамму».

Оракул $\perp$ возвращает символ ошибки «$\perp$».

q запросов (N, A, P) к отправителю $S \in \{\mathrm{AE}_K, \$\}$.

v запросов (N, A, C, T) к получателю $R \in \{\mathrm{AE}_K^{-1}, \perp\}$.

Модель для обобщённого протокола

Задача различения при ключе с номером j.

NAE* – Nonce-based Authenticated Encryption

$$\mathrm{Adv}^{NAE*}_{\mathrm{GP}}(A) = \max_{j \in \mathbf{N}_{\mathrm{KDF}}} \Big(\Pr(K \xleftarrow{\mathrm{u}} \mathbf{K} : A^{S_1, R_1}(j) \Rightarrow 1) - \Pr(K \xleftarrow{\mathrm{u}} \mathbf{K} : A^{S_0, R_0}(j) \Rightarrow 1) \Big)$$

$(S_1, R_1) = (\mathrm{GP}_K, \mathrm{GP}_K^{-1})$ – всегда «реальные»

$$(S_0, R_0) = \begin{cases} (\mathrm{GP}_K, \mathrm{GP}_K^{-1}), & \text{при } N_{\mathrm{KDF}} \neq j \text{ «реальные»} \\ (\$, \perp), & \text{при } N_{\mathrm{KDF}} = j, \text{ «идеальные»} \end{cases}$$

Модели для KDF

PRF

$$\mathrm{Adv}_{\mathrm{F}}^{PRF}(A) = \Pr(K \xleftarrow{u} \mathbf{K} : A^{\mathrm{F}_K} \Rightarrow 1) -$$
$$- \Pr(\mathrm{R} \xleftarrow{u} \mathrm{Func}(\mathbf{X}, \mathbf{Y}) : A^{\mathrm{R}} \Rightarrow 1)$$

К оракулу делается q запросов.

PRF*

$$\mathrm{Adv}_{\mathrm{F}}^{PRF*}(A) = \Pr(K \xleftarrow{u} \mathbf{K}; : A^{\mathrm{F}_K, \mathrm{F}_K} \Rightarrow 1) -$$
$$- \Pr(K \xleftarrow{u} \mathbf{K}; \mathrm{R} \xleftarrow{u} \mathrm{Func}(\mathbf{X}, \mathbf{Y}) : A^{\mathrm{R}, \mathrm{F}_K} \Rightarrow 1)$$

К первому оракулу – r запросов, ко второму – q запросов.
Запросы к оракулам не повторяются.

Результаты

СФБ ЛАБ

Было: Теорема 1

$$\mathrm{Adv}^{NAE}_{\mathrm{GP}}(t, \mu q^*, \mu v^*) \leq \mathrm{Adv}^{PRF}_{\mathrm{KDF}}(t', \mu) + \mu \cdot \mathrm{Adv}^{NAE}_{\mathrm{AE}}(t', q^*, v^*)$$

Стало: Теорема 2

$$\mathrm{Adv}^{NAE*}_{\mathrm{GP}}(t, \mu q^*, \mu v^*) \leq \mathrm{Adv}^{PRF*}_{\mathrm{KDF}}(t', \mu) + \mathrm{Adv}^{NAE}_{\mathrm{AE}}(t', q^*, v^*)$$

- μ – число производных ключей
- $q = \mu \cdot q^*$ – общее число защищаемых пакетов
- $v = \mu \cdot v^*$ – общее число попыток навязывания
- q^* – число пакетов, защищаемых на производном ключе
- v^* – число попыток навязывания при каждом производном

Результаты

Как ослабление модели повлияло на оценки?

1. Исчез сомножитель μ
2. Ослаблены требования к KDF,
   модель PRF заменяется на PRF*

Оценки для KDF

Требования к KDF

СФБ ЛАБ

Было: модель PRF

Совокупность из μ производных ключей неотличима от совокупности «идеальных».

Требования к KDF

Было: модель PRF

Совокупность из μ производных ключей неотличима от совокупности «идеальных».

Стало: модель PRF*

Производный ключ с номером j неотличим от «идеального», когда противнику известны все остальные «реальные».

Пример: CTR

KDF – режим гаммирования CTR

Шифр «Магма», $k = 256$, $n = 64$, $r = \frac{k}{n} = 4$, $\mu = \frac{q}{r}$,

$$K_1 || \ldots || K_\mu = \mathrm{E}_K(0) \,||\, \mathrm{E}_K(1) \,||\, \ldots \,||\, \mathrm{E}_K(q-1)$$

Пример: CTR

KDF – режим гаммирования CTR

Шифр «Магма», $k = 256$, $n = 64$, $r = \frac{k}{n} = 4$, $\mu = \frac{q}{r}$,

$$K_1||...||K_\mu = \mathrm{E}_K(0) \,||\, \mathrm{E}_K(1) \,||\, ... \,||\, \mathrm{E}_K(q-1)$$

PRF: «все реальные или все идеальные»

При $\pi_{\text{enc}} = 2^{-10}$, $r = 4$, $q = \mu \cdot r$ из

$$\mathrm{Adv}_{\mathrm{E}}^{PRF}(t,q) \leq \mathrm{Adv}_{\mathrm{E}}^{PRP}(t',q) + \frac{q \cdot (q-1)}{2^{n+1}} \lessapprox \frac{\mu^2 \cdot r^2}{2^{n+1}}$$

получаем $\mu \leq 2^{25}$ производных ключей.

Пример: CTR

KDF – режим гаммирования CTR

Шифр «Магма», $k = 256$, $n = 64$, $r = \frac{k}{n} = 4$, $\mu = \frac{q}{r}$,

$$K_1||...||K_\mu = \mathrm{E}_K(0) \,||\, \mathrm{E}_K(1) \,||\, ... \,||\, \mathrm{E}_K(q-1)$$

PRF*: «j-й реальный или идеальный, остальные реальны»

При $\pi_{\text{enc}} = 2^{-10}$, $r = 4$, $q = \mu \cdot r$ из

$$\mathrm{Adv}_{\mathrm{E}}^{PRF*}(t, q, r) \le 2 \cdot \mathrm{Adv}_{\mathrm{E}}^{PRP}(t', q + r) + \frac{q \cdot r}{2^n - r} + \frac{r \cdot (r-1)}{2^{n+1}} \approx\lesssim \frac{\mu \cdot r^2}{2^n}$$

получаем $\mu \le 2^{50}$ производных ключей.

Пример: CMAC

СФБ ЛАБ

Утверждение

Для алгоритма CMAC в отсутствии ограничений на вид входа оценки в моделях PRF и PRF* **одинаковы**.

Пример: CMAC

СФБ ЛАБ

Утверждение

Для алгоритма CMAC в отсутствии ограничений на вид входа оценки в моделях PRF и PRF* **одинаковы**.

KDF-CMAC

$$\begin{aligned}\text{KDF-CMAC}(K, X) = &\text{CMAC}(K, 1||X) \;||\\ &\text{CMAC}(K, 2||X) \;||\\ &\ldots\\ &\text{CMAC}(K, r||X)\end{aligned}$$

Типичные ограничения:

1. Запросы противника неадаптивны
2. Длина входа зафиксирована
3. Первый блок ненулевой

Пример: CMAC

Теорема

Для противника, ограниченного *неадаптивными* (na) запросами фиксированной длины с первым ненулевым блоком

$$\mathrm{Adv}^{na\text{-}PRF^*}_{\mathrm{CMAC}}(t,q,r,l) \le 2 \cdot \mathrm{Adv}^{PRP}_{\mathrm{E}}(t',\sigma) + \frac{7qrl + 7r^2l + 5ql + 5rl}{2^n} + \frac{24qrl^4}{2^{2n}}$$

Пример: CMAC

Теорема

Для противника, ограниченного *неадаптивными* (*na*) запросами фиксированной длины с первым ненулевым блоком

$$\mathrm{Adv}^{na\text{-}PRF^*}_{\mathrm{CMAC}}(t,q,r,l) \le 2\cdot \mathrm{Adv}^{PRP}_{\mathrm{E}}(t',\sigma) + \frac{7qrl + 7r^2l + 5ql + 5rl}{2^n} + \frac{24qrl^4}{2^{2n}}$$

Следствие

При $\pi_{\mathrm{enc}} = 2^{-10}$, $r = 4$, $q = \mu \cdot r$, $l \le 8$,

$$\mathrm{Adv}^{na\text{-}PRF^*}_{\mathrm{KDF\text{-}CMAC}}(t,q,r,l) \lessapprox \frac{2^6 \cdot \mu \cdot r^2}{2^n},$$

получаем $\mu \le 2^{44}$ производных ключей.

Криптопротоколы CRISP и IPlir

Криптопротокол CRISP

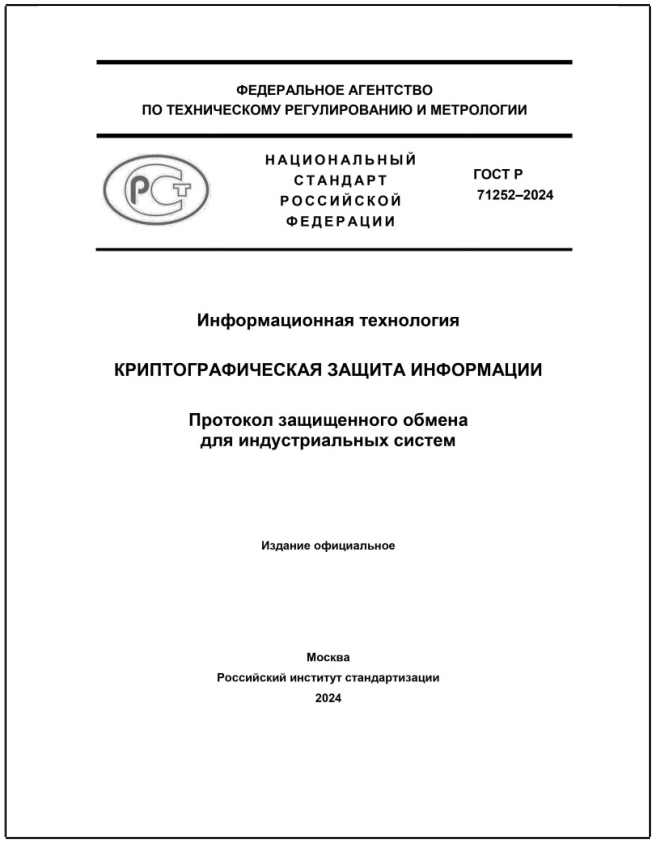
ГОСТ Р 71252–2024

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

Криптопротокол IPlir

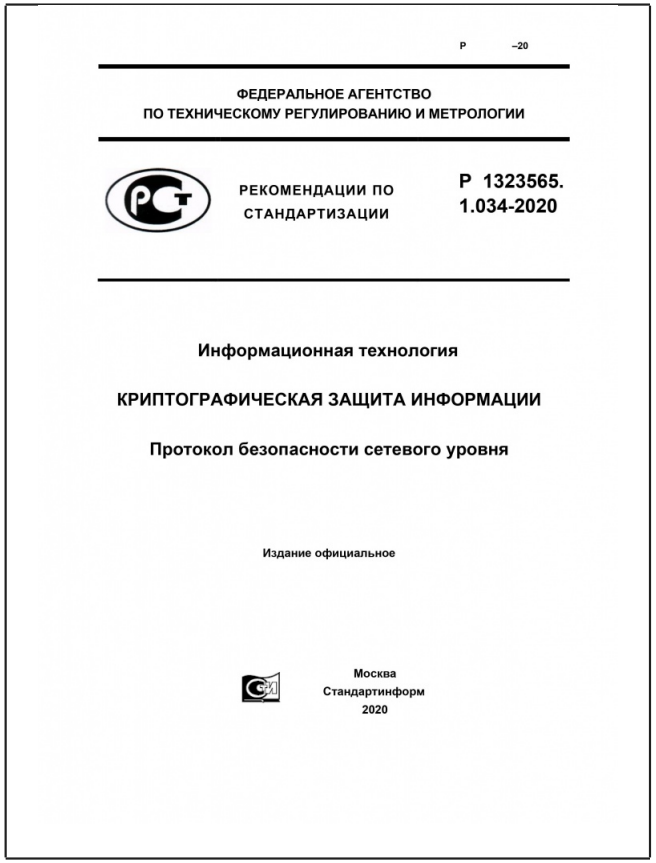
Р 1323565.1.034 — 2020

Информационная технология

Криптографическая защита информации

Протокол безопасности

сетевого уровня



Р –20

ФЕДЕРАЛЬНОЕ АГЕНТСТВО
ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

РЕКОМЕНДАЦИИ ПО СТАНДАРТИЗАЦИИ

Р 1323565.
1.034-2020

Информационная технология

КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ

Протокол безопасности сетевого уровня

Издание официальное

Москва
Стандартинформ
2020

Общие свойства

СФБ ЛАБ

- Ключи распределены внешним образом
- Отсутствует интерактивность
- Используется KDF-CMAC
- Свойства безопасности:
  - целостность
  - (опционально) конфиденциальность

Отличия IPlir и CRISP от GenericProtocol

Базовый ключ формирует производные для:

- двух линий связи «$S \to R$» и «$R \to S$» в IPlir

Отличия IPlir и CRISP от GenericProtocol

Базовый ключ формирует производные для:

- двух линий связи «$S \to R$» и «$R \to S$» в IPlir
- многих отправителей и разных криптонаборов в CRISP

Отличия IPlir и CRISP от GenericProtocol

Базовый ключ формирует производные для:

- двух линий связи «$S \to R$» и «$R \to S$» в IPlir
- многих отправителей и разных криптонаборов в CRISP

Если анализируем одну линию связи, то базовый ключ K используется *внешним* образом (на других линиях).

Дополнительно даём противнику доступ к оракулу $\mathrm{KDF}(K, \cdot)$.

IPlir

Для базового ключа заранее определены ID пары узлов и криптонабор CS. Длина входа KDF зафиксирована.

IPlir

Для базового ключа заранее определены ID пары узлов и криптонабор CS. Длина входа KDF зафиксирована.

Вывод для IPlir

Применимы оценки KDF-CMAC в модели *na-PRF**.

Для криптонабора MAGMA-MGM на одну линию связи, число производных ключей ограничено $\mu \leq 2^{42}$.

CRISP

Базовый ключ могут использовать *многие* отправители.

Их число и ID заранее *не определены*.

CRISP

Базовый ключ могут использовать *многие* отправители.

Их число и ID заранее *не определены*.

Вывод 1 для CRISP

Нарушается условие *неадаптивности* запросов к KDF.

Допустимая нагрузка на ключ увеличивается только за счёт отсутствия сомножителя μ.

[CTCrypt'23]: $\mu \leq 2^{13}$ производных и $q \leq 2^{13} \cdot 2^{13} = 2^{26}$ пакетов.

«Стало»: $\mu \leq 2^{21}$ производных и $q \leq 2^{21} \cdot 2^{13} = 2^{34}$ пакетов.

CRISP

Введём ограничения:

- все отправители и их ID выбраны до использования K
- длина ID зафиксирована

CRISP

Введём ограничения:

- все отправители и их ID выбраны до использования K
- длина ID зафиксирована

Вывод 2 для CRISP

Условие *неадаптивности* запросов к KDF выполнено.

Применимы оценки KDF-CMAC в модели *na-PRF**.

[CTCrypt'23]: $\mu \leq 2^{13}$ производных и $q \leq 2^{13} \cdot 2^{13} = 2^{26}$ пакетов.

«Стало»: $\mu \leq 2^{42}$ производных и $q \leq 2^{42} \cdot 2^{13} = 2^{55}$ пакетов.

Заключение

Заключение

СФБ ЛАБ

1. Использование низкоресурсных криптоалгоритмов делает *необходимым* ослабление моделей угроз
   – ограничиваем не вероятность нанесения хоть какого-нибудь ущерба, а само «количество» ущерба

Заключение

СФБ ЛАБ

1. Использование низкоресурсных криптоалгоритмов делает *необходимым* ослабление моделей угроз
   - ограничиваем не вероятность нанесения хоть какого-нибудь ущерба, а само «количество» ущерба
2. Для протоколов типа «KDF + AEAD» ослабление позволяет:
   - снизить качественно и/или количественно требования к KDF
   - уйти от «гибридного аргумента»

Заключение

СФБ ЛАБ

1. Использование низкоресурсных криптоалгоритмов делает *необходимым* ослабление моделей угроз
   - ограничиваем не вероятность нанесения хоть какого-нибудь ущерба, а само «количество» ущерба
2. Для протоколов типа «KDF + AEAD» ослабление позволяет:
   - снизить качественно и/или количественно требования к KDF
   - уйти от «гибридного аргумента»
3. Применение подхода к протоколам IPlir и CRISP – переход границы «парадокса ДР» по числу производных ключей

Благодарю за внимание!

Виталий Кирюхин

ООО «СФБ Лаб», АО «ИнфоТеКС»

РусКрипто’2025

20 марта 2025

vitaly.kiryukhin@sfblaboratory.ru