О свойствах алгоритма S3G-128 при использовании усеченной хэш-функции «Стрибог»

В.А. Кирюхин

ООО «СФБ Лаб», АО «ИнфоТеКС»

РусКрипто'2022
23 марта 2022

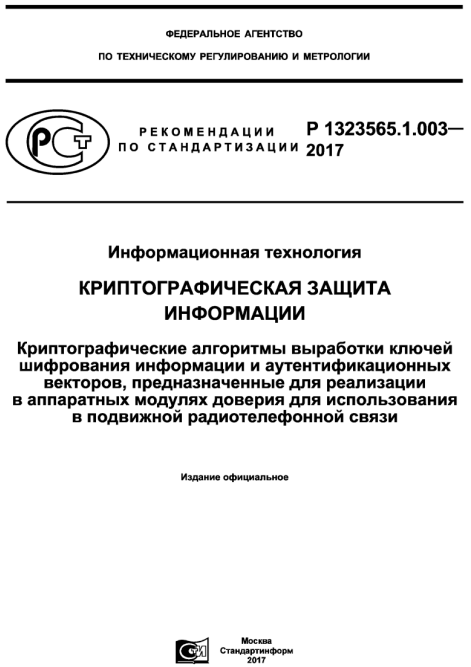
vitaly.kiryukhin@sfblaboratory.ru

Алгоритмы S3G-128 и S3G-256

Ключевые алгоритмы

$$\mathrm{S3G}(K, T) = \mathrm{H}(K|T)$$

на основе хэш-функции Стрибог-512



ФЕДЕРАЛЬНОЕ АГЕНТСТВО
ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

РЕКОМЕНДАЦИИ ПО СТАНДАРТИЗАЦИИ Р 1323565.1.003–2017

Информационная технология

КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ

Криптографические алгоритмы выработки ключей шифрования информации и аутентификационных векторов, предназначенные для реализации в аппаратных модулях доверия для использования в подвижной радиотелефонной связи

Издание официальное

Москва
Стандартинформ
2017

Р 1323565.1.003-2017 Информационная технология. Криптографическая защита информации. Криптографические алгоритмы выработки ключей шифрования информации и аутентификационных векторов, предназначенные для реализации в аппаратных модулях доверия для использования в подвижной радиотелефонной связи – Москва: Стандартинформ, 2017

Алгоритмы S3G-128 и S3G-256

Хэш-значение $\mathsf{H}(K|T)$ усекается до $s \leq n = 512$ бит и может являться:

- кодом аутентификации
- доказательством владения секретным ключом
- производным ключом (ключами)

Текст T содержит сведения об алгоритме, о назначении результата, об операторе связи. Может содержать случайные числа и другую информацию.

Требования

Полагаем, что T может *адаптивно выбираться нарушителем*.
$\mathsf{H}(K|\cdot)$ должен быть неотличим от псевдослучайной функции (PRF).
Если это так, то $\mathsf{H}(K|\cdot)$
$\Rightarrow$ стойкая схема имитозащиты;
$\Rightarrow$ стойкая схема выработки производных ключей;
$\Rightarrow$ и т.д.

Алгоритмы S3G-128 и S3G-256

Хэш-значение $\mathsf{H}(K|T)$ усекается до $s \leq n = 512$ бит и может являться:

- кодом аутентификации
- доказательством владения секретным ключом
- производным ключом (ключами)

Текст T содержит сведения об алгоритме, о назначении результата, об операторе связи. Может содержать случайные числа и другую информацию.

Требования

Полагаем, что T может *адаптивно выбираться нарушителем*.
$\mathsf{H}(K|\cdot)$ должен быть неотличим от псевдослучайной функции (PRF).
Если это так, то $\mathsf{H}(K|\cdot)$
$\Rightarrow$ стойкая схема имитозащиты;
$\Rightarrow$ стойкая схема выработки производных ключей;
$\Rightarrow$ и т.д.

Алгоритмы S3G-128 и S3G-256

Хэш-значение $\mathrm{H}(K|T)$ усекается до $s \leq n = 512$ бит и может являться:

- кодом аутентификации
- доказательством владения секретным ключом
- производным ключом (ключами)

Текст T содержит сведения об алгоритме, о назначении результата, об операторе связи. Может содержать случайные числа и другую информацию.

Требования

Полагаем, что T может *адаптивно выбираться нарушителем*.
$\mathrm{H}(K|\cdot)$ должен быть неотличим от псевдослучайной функции (PRF).
Если это так, то $\mathrm{H}(K|\cdot)$
$\Rightarrow$ стойкая схема имитозащиты;
$\Rightarrow$ стойкая схема выработки производных ключей;
$\Rightarrow$ и т.д.

Алгоритмы S3G-128 и S3G-256

Характеристики

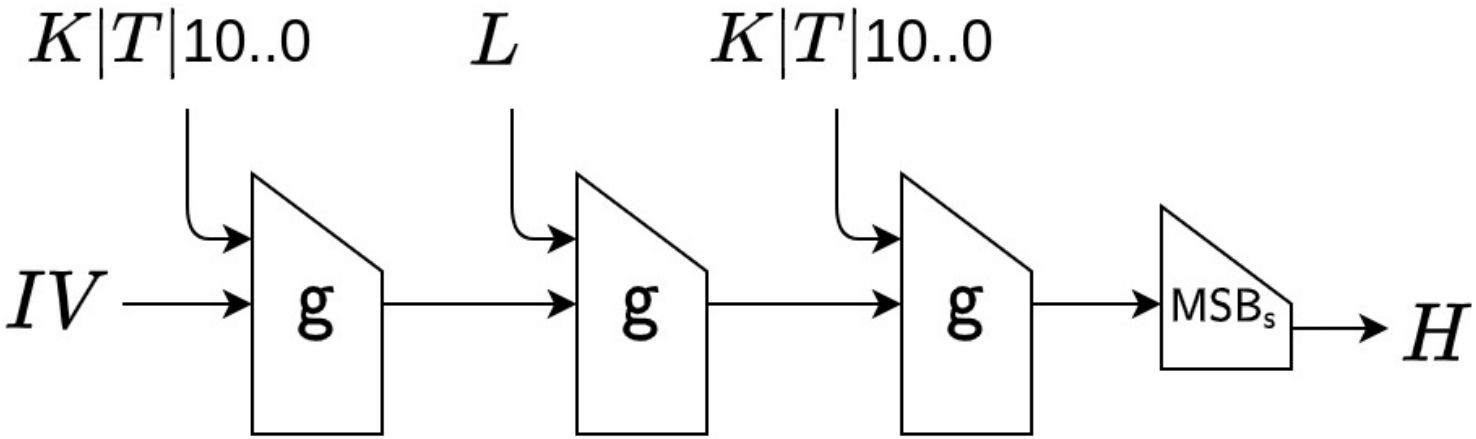
S3G-128:

- ключ – 128 бит
- текст от 159 до 383 бит
- ключ и текст всегда помещаются **в один 512-битный блок**

S3G-256:

- ключ – 128 или 256 бит
- текст от 344 до 680 бит
- ключ и текст всегда помещаются в два 512-битных блока

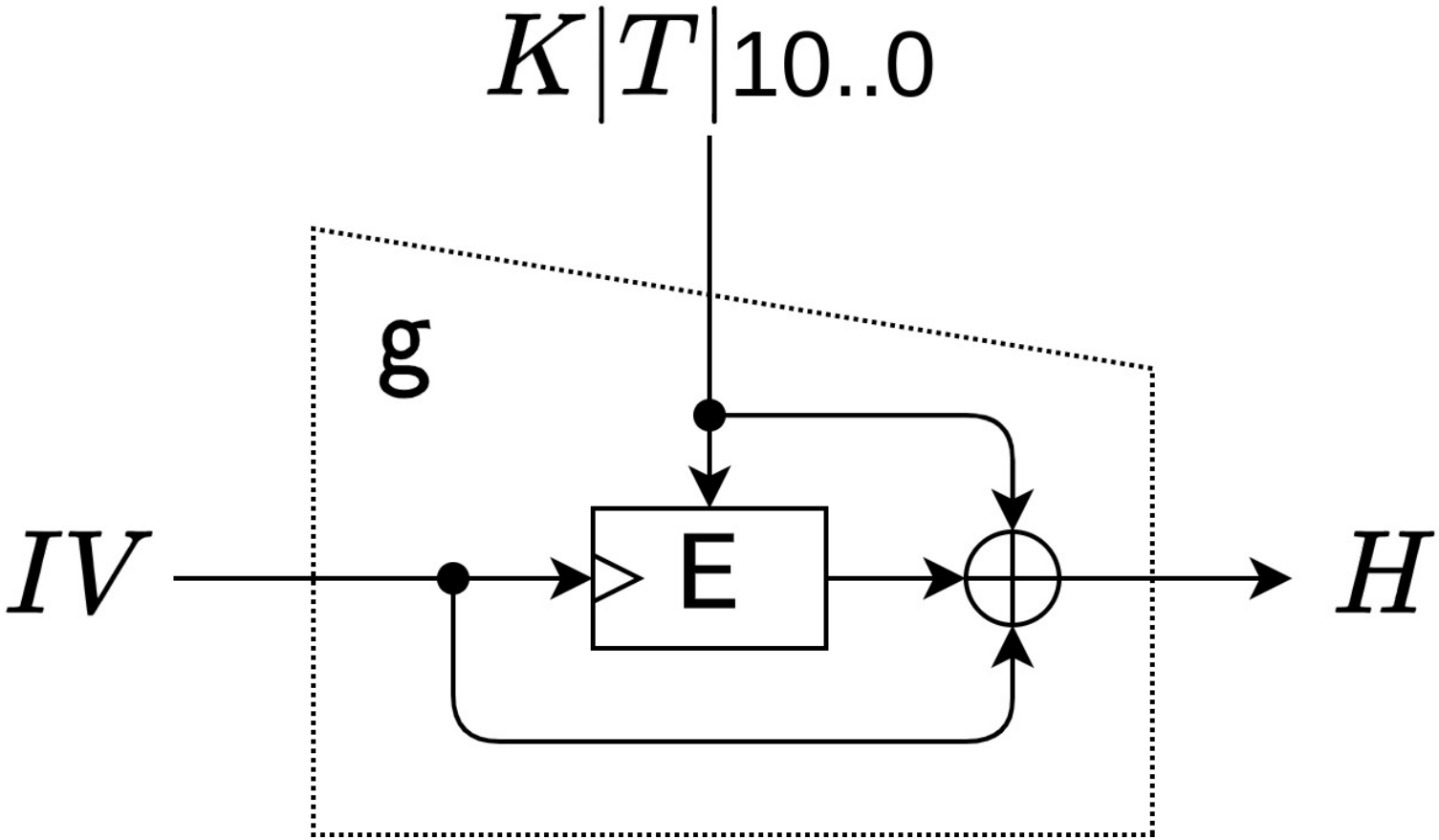
Алгоритм S3G-128



3 вызова функции сжатия:
– ключ и текст с учётом дополнения 10..0
– битовая длина
– контрольная сумма = единственному блоку

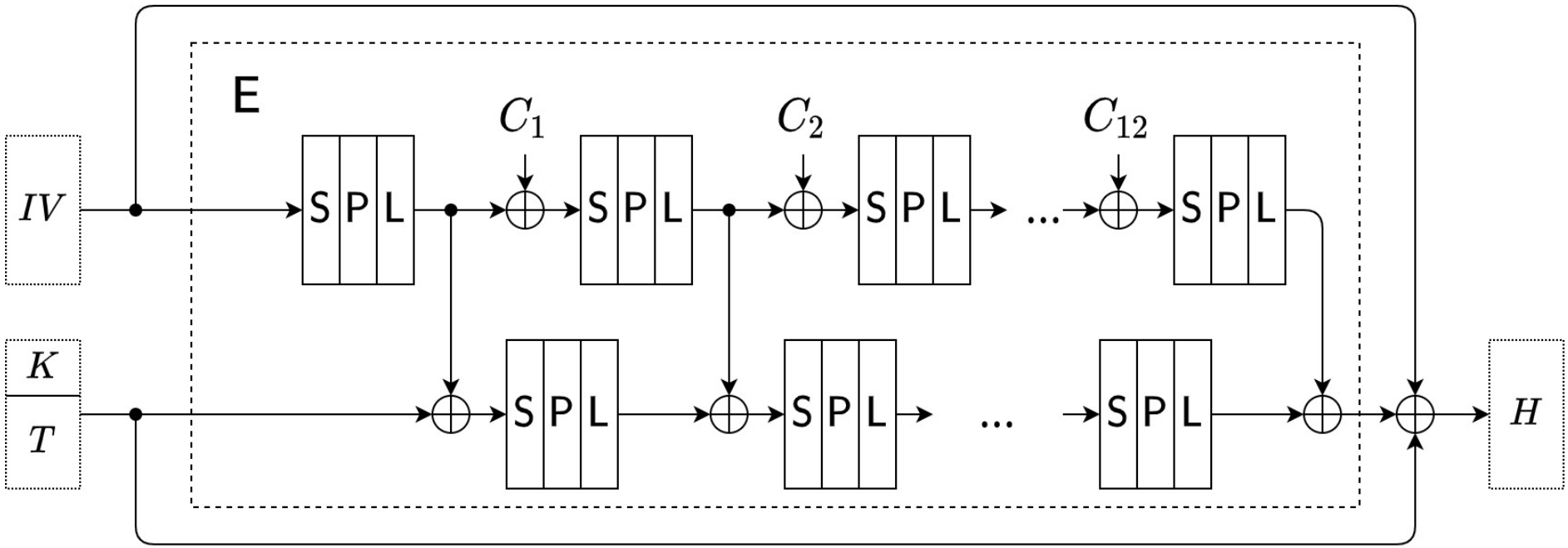
Усеченная версия?

Будет ли стойким S3G-128, если вместо H использовать однократный вызов функции сжатия g?



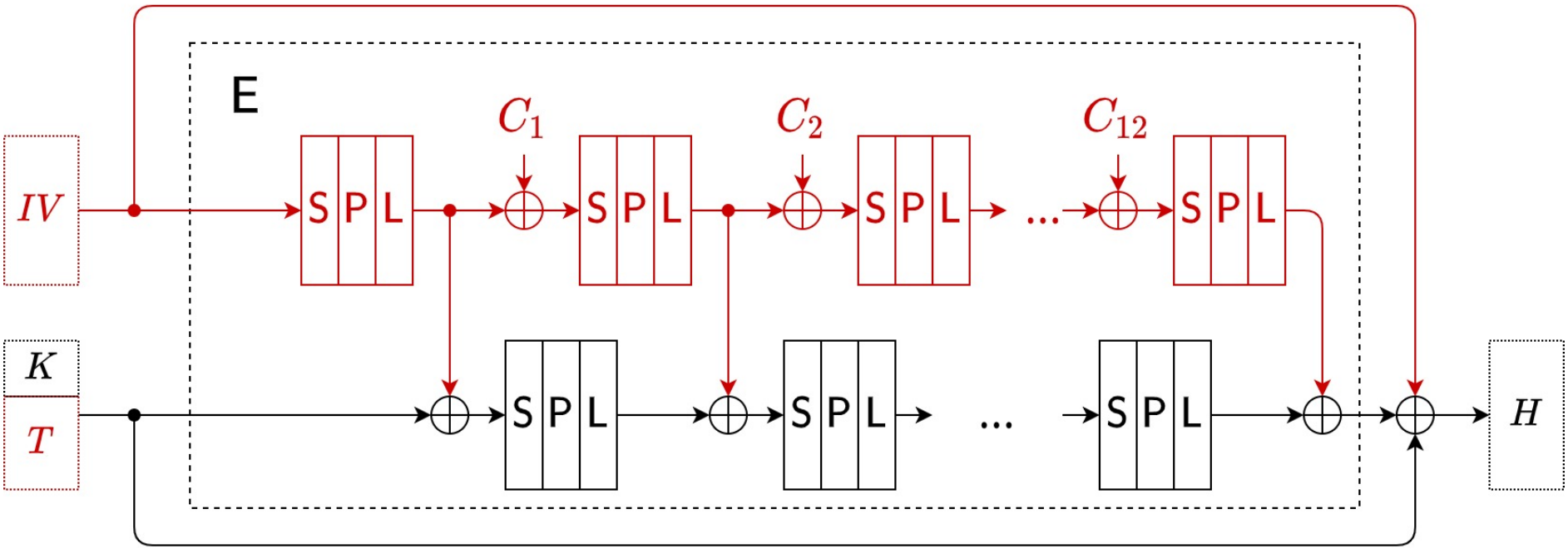
Функция сжатия

- конструкция Миагучи-Пренеля
- блочный XSPL-шифр E
- размер блока и ключа по $n = 512$ бит



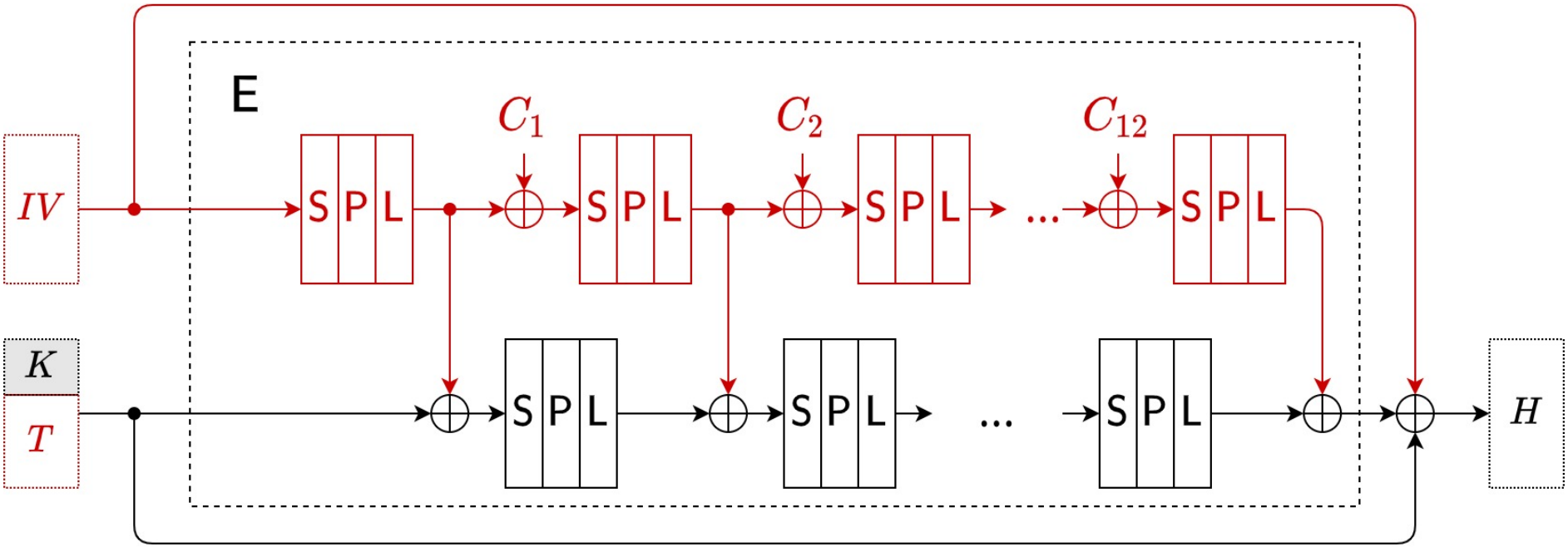
Функция сжатия в S3G-128

- все раундовые ключи шифра E известны нарушителю
- вход T адаптивно выбирается нарушителем



Функция сжатия в S3G-128

Секретный ключ K:
– является частью входа
– частично «закрывает» выход



Конструкция

По сути анализ сводится к

$$\mathrm{S3G}'(K, T) = \Pi(K|T) \oplus (K|T) = H$$

- $\Pi : V^{512} \to V^{512}$ – публично известная подстановка
- ключ K длины $k = 128$ бит
- вход T длины $m = 384$ бита (с учётом дополнения)

Анализ

1. Доказуемая стойкость
   (оценка **сверху** на возможности нарушителя)
2. Универсальные методы
   (оценка **снизу** на возможности нарушителя)
3. Специальные методы
   (учёт специфических слабостей конкретной схемы)

Анализ

1. Доказуемая стойкость
   (оценка **сверху** на возможности нарушителя)
2. Универсальные методы
   (оценка **снизу** на возможности нарушителя)
3. Специальные методы
   (учёт специфических слабостей конкретной схемы)

Анализ

1. Доказуемая стойкость
   (оценка **сверху** на возможности нарушителя)
2. Универсальные методы
   (оценка **снизу** на возможности нарушителя)
3. Специальные методы
   (учёт специфических слабостей конкретной схемы)

Доказуемые свойства

Покажем, что S3G′ – стойкая псевдослучайная функция (PRF) в **предположении** о том, что подстановка Π является случайно и равновероятно выбранной.

(эвристическая модель идеальной подстановки, как в SHA-3 и других «губках»)

Доказуемые свойства

Нарушитель моделируется интерактивным вероятностным алгоритмом, который может
отправлять запросы к $\Pi(\cdot)$, $\Pi^{-1}(\cdot)$ и $\mathrm{S3G}'(K,\cdot)$:

- t – число обращений к Π и Π^{-1}
  (количество «вычислительных ресурсов»)
- q – число обращений к $\mathrm{S3G}'(K,\cdot)$
  (количество адаптивно выбираемых пар вход/выход (T,H))

Доказуемые свойства

Преобладание нарушителя $\mathcal{A}$ определяется как разность вероятностей:

$$\begin{aligned}\mathrm{Adv}^{PRF}_{\mathsf{S3G}'}(\mathcal{A}) = \Pr(&\Pi \xleftarrow{\mathrm{R}} Perm(V^{512}), K \xleftarrow{\mathrm{R}} V^{128},\\ &\mathcal{A}^{\mathsf{S3G}'(K,\cdot),\Pi(\cdot),\Pi^{-1}(\cdot)} \Rightarrow 1)\\ -\\ \Pr(&\Pi \xleftarrow{\mathrm{R}} Perm(V^{512}), \rho \xleftarrow{\mathrm{R}} Func(V^{384}, V^{512}),\\ &\mathcal{A}^{\rho(\cdot),\Pi(\cdot),\Pi^{-1}(\cdot)} \Rightarrow 1)\end{aligned}$$

Доказуемые свойства

Теорема

Для преобразования S3G′ (при условии истинности эвристического предположения о равновероятном выборе П) преобладание любого нарушителя с ресурсами t и q ограничено сверху

$$\mathrm{Adv}^{PRF}_{\mathrm{S3G}'}(t, q) \leq \frac{t}{2^{k-1}} + \frac{q^2}{2^{m-2}},$$

длина ключа $k = 128$, длина входа $m = 384$.

Доказуемые свойства

Идея доказательства

1. Анализ биективного преобразования

$$\mathsf{B}(K, T) = \Pi(K|T) \oplus (K|0^m)$$

2. Отличие $\mathsf{B}(K, T)$ от случайной подстановки

$$\begin{aligned}\mathrm{Adv}_{\mathsf{B}}^{PRP}(\mathcal{A}) = \Pr(&\Pi \xleftarrow{\mathrm{R}} Perm(V^{512}), K \xleftarrow{\mathrm{R}} V^{128},\\ &\mathcal{A}^{\mathsf{B}(K,\cdot),\Pi(\cdot),\Pi^{-1}(\cdot)} \Rightarrow 1)\\ -\\ \Pr(&\Pi \xleftarrow{\mathrm{R}} Perm(V^{512}), \widetilde{\Pi} \xleftarrow{\mathrm{R}} Perm(V^{512}),\\ &\mathcal{A}^{\widetilde{\Pi}(0^m|\cdot),\Pi(\cdot),\Pi^{-1}(\cdot)} \Rightarrow 1)\end{aligned}$$

Доказуемые свойства

Идея доказательства

3. Ситуации неотличимы, пока две подстановки $\widetilde{\Pi}$ и Π можно «хранить в одной» – у них не пересекаются ни множество запрошенных входов, ни множества запрошенных выходов.

Нарушитель имеет t пар за счет запросов к $\Pi(\cdot)$, $\Pi^{-1}(\cdot)$

$$(X_1, W_1), (X_2, W_2), \ldots, (X_t, W_t) \in V^n \times V^n,$$

и q пар за счёт запросов к $\mathsf{B}(K, \cdot)$

$$(T_1, Y_1), (T_2, Y_2), \ldots, (T_q, Y_q) \in V^m \times V^n,$$

и каждой паре (T_i, Y_i) соответствует

$$(\overline{X}_i = K|T_i, \overline{W}_i = Y_i \oplus K|0^m).$$

В итоге:

$$\mathrm{Adv}_{\mathsf{B}}^{PRP}(\mathcal{A}) \leq \Pr\left(\{X_1, ..., X_t\} \cap \left\{\overline{X}_1, \ldots, \overline{X}_q\right\} \neq \emptyset\right) +$$

$$\Pr\left(\{W_1, ..., W_t\} \cap \left\{\overline{W}_1, \ldots, \overline{W}_q\right\} \neq \emptyset\right) \leq \frac{t}{2^k} + \left(\frac{t}{2^k} + \frac{q^2}{2^{m-1}}\right)$$

Доказуемые свойства

Идея доказательства

5. Мера отличимости случайной подстановки и случайной функции оценивается с помощью «PRP-PRF Леммы» (по «парадоксу дней рождения»)

$$\mathrm{Adv}_{\mathsf{B}}^{PRF}(t,q) \leq \mathrm{Adv}_{\mathsf{B}}^{PRP}(t,q) + \frac{q^2}{2^{n+1}} \leq \frac{t}{2^{k-1}} + \frac{q^2}{2^{m-2}}.$$

Доказуемые свойства

Следствие 1 – стойкая имитозащита

При использовании S3G′ для формирования s-битных имитовставок **вероятность** навязывания хотя бы одного ложного сообщения за ν попыток ограничена сверху

$$\mathrm{Adv}^{SUF}_{\mathrm{S3G}'}(t,q,\nu) \leq \mathrm{Adv}^{PRF}_{\mathrm{S3G}'}(t,q) + \frac{\nu}{2^s} \leq \frac{t}{2^{k-1}} + \frac{q^2}{2^{m-2}} + \frac{\nu}{2^s}$$

Вероятность навязывания зависит от:

- вычислительной мощности нарушителя;
- числа попыток навязывания;
- длины имитовставки;

но почти НЕ зависит от объема обрабатываемого материала.

Доказуемые свойства

Должно быть выполнено

$$\mathrm{Adv}^{SUF}_{\mathrm{S3G}'}(t, q, 1) \leq \frac{t}{2^{k-1}} + \frac{q^2}{2^{m-2}} + \frac{1}{2^s} < \pi_{\mathrm{mac}},$$

где π_{mac} – максимально допустимое значение вероятности однократного навязывания сообщения.

Р 1323565.1.005 – 2017 Информационная технология. Криптографическая защита информации. Допустимые объёмы материала для обработки на одном ключе при использовании некоторых вариантов режимов работы блочных шифров в соответствии с ГОСТ Р 34.13-2015

Доказуемые свойства

Следствие 2 – стойкость к восстановлению ключа

Вероятность определения секретного ключа ограничена сверху

$$\mathrm{Adv}^{KR}_{\mathrm{S3G}'}(t,q) \le \mathrm{Adv}^{PRF}_{\mathrm{S3G}'}(t,q) + \frac{1}{2^n} \le \frac{t}{2^{k-1}} + \frac{q^2}{2^{m-2}} + \frac{1}{2^n}$$

Доказуемые свойства

Должно быть выполнено

$$\mathrm{Adv}^{KR}_{\mathrm{S3G}'}(t,q) \leq \frac{t}{2^{k-1}} + \frac{q^2}{2^{m-2}} + \frac{1}{2^n} < \pi_{\mathrm{enc}},$$

где π_{enc} – максимально допустимое значение вероятности эффективного применения методов криптографического анализа.

Р 1323565.1.005 – 2017 Информационная технология. Криптографическая защита информации. Допустимые объёмы материала для обработки на одном ключе при использовании некоторых вариантов режимов работы блочных шифров в соответствии с ГОСТ Р 34.13-2015

Доказуемые свойства

Пример – стойкость схемы выработки производных ключей

Пусть ключи вырабатываются по правилу

$$\mathrm{S3G}'(K,1)\,|\,\mathrm{S3G}'(K,2)\,|\,\ldots\,|\,\mathrm{S3G}'(K,q),$$

суммарно $q \cdot n$ бит ключевого материала

Доказуемые свойства

Пример – стойкость схемы выработки производных ключей

Рассмотрим гипотетический генератор G, который:
– с вероятностью p порождает $q \cdot n$ нулевых бит (сбой)
– с вероятностью $(1 - p)$ порождает $q \cdot n$ «идеальных» бит

$$\mathrm{Adv}_{\mathsf{G}}^{PRG}(q) \leq p + \frac{1}{2^{qn}} \approx p$$

Сбой = раскрытие всех производных ключей: должно быть выполнено

$$p < \pi_{\mathrm{enc}},$$

а тогда и **целесообразно** ограничить

$$\mathrm{Adv}_{\mathsf{S3G}'}^{PRG}(t, q) \leq \mathrm{Adv}_{\mathsf{S3G}'}^{PRF}(t, q) \leq \frac{t}{2^{k-1}} + \frac{q^2}{2^{m-2}} < \pi_{\mathrm{enc}},$$

ориентируясь на G как на *худший случай*.

Доказуемые свойства

Пример – стойкость схемы выработки производных ключей

Рассмотрим гипотетический генератор G, который:
– с вероятностью p порождает $q \cdot n$ нулевых бит (сбой)
– с вероятностью $(1 - p)$ порождает $q \cdot n$ «идеальных» бит

$$\mathrm{Adv}_{\mathsf{G}}^{PRG}(q) \leq p + \frac{1}{2^{qn}} \approx p$$

Сбой = раскрытие всех производных ключей: должно быть выполнено

$$p < \pi_{\mathrm{enc}},$$

а тогда и **целесообразно** ограничить

$$\mathrm{Adv}_{\mathsf{S3G}'}^{PRG}(t, q) \leq \mathrm{Adv}_{\mathsf{S3G}'}^{PRF}(t, q) \leq \frac{t}{2^{k-1}} + \frac{q^2}{2^{m-2}} < \pi_{\mathrm{enc}},$$

ориентируясь на G как на *худший случай*.

Универсальные методы

- Определение секретного ключа – тотальное опробование (вероятность успеха $\approx t \cdot 2^{-k}$ при $q = 1$)
- Различитель - парадокс дней рождения (вероятность успеха $\approx q^2 \cdot 2^{-(n+1)}$)

Универсальные методы

- Определение секретного ключа – тотальное опробование (вероятность успеха $\approx t \cdot 2^{-k}$ при $q = 1$)
- Различитель - парадокс дней рождения (вероятность успеха $\approx q^2 \cdot 2^{-(n+1)}$)

Специальные методы

Можно ли воспользоваться слабостями реальной П для построения более эффективных методов?

Это сложная задача:

- в П используется «тяжёлый» 12-раундовый XSPL-шифр
- размер блока $n = 512$ бит
- трудоемкость универсального метода – 2^{128} операций

Удалось построить атаки на:

- 5 раундов – с практической трудоемкостью (интегральный метод)
- 6 раундов – трудоемкость $2^{112} < 2^{128}$ операций

Специальные методы

Можно ли воспользоваться слабостями реальной П для построения более эффективных методов?

Это сложная задача:

- в П используется «тяжёлый» 12-раундовый XSPL-шифр
- размер блока $n = 512$ бит
- трудоемкость универсального метода – 2^{128} операций

Удалось построить атаки на:

- 5 раундов – с практической трудоемкостью (интегральный метод)
- 6 раундов – трудоемкость $2^{112} < 2^{128}$ операций

Специальные методы

Можно ли воспользоваться слабостями реальной П для построения более эффективных методов?

Это сложная задача:

- в П используется «тяжёлый» 12-раундовый XSPL-шифр
- размер блока $n = 512$ бит
- трудоемкость универсального метода – 2^{128} операций

Удалось построить атаки на:

- 5 раундов – с практической трудоемкостью (интегральный метод)
- 6 раундов – трудоемкость $2^{112} < 2^{128}$ операций

Атака на 6 из 12 раундов

Метод согласования с использованием многомерных дифференциальных соотношений

Формируем:

- набор текстов $T_0, ..., T_d$, которые отличаются только в одном байте

Получаем:

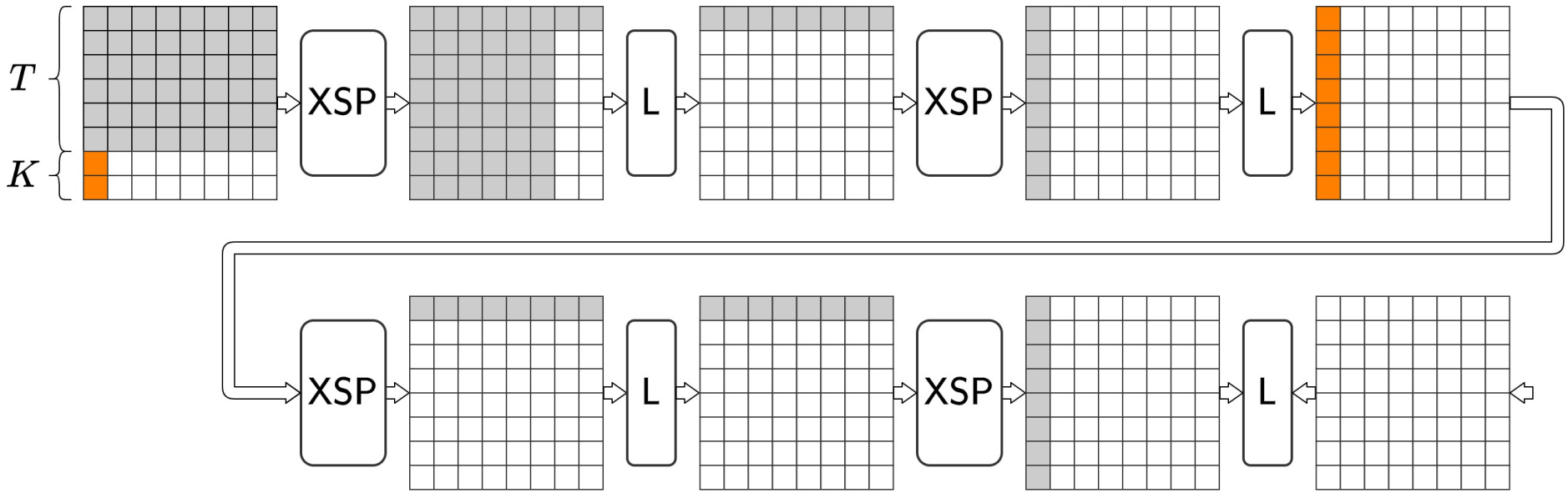
- d-разность $\boldsymbol{\delta T} = (T_0 \oplus T_1, T_0 \oplus T_2, \ldots, T_0 \oplus T_d)$ на входе
- d-разность $\boldsymbol{\delta H} = (H_0 \oplus H_1, H_0 \oplus H_2, \ldots, H_0 \oplus H_d)$ на выходе

Атака на 6 из 12 раундов

Метод согласования с использованием многомерных дифференциальных соотношений

Направление «вперёд»

Опробуем 16 бит ключа и 64 бита состояния

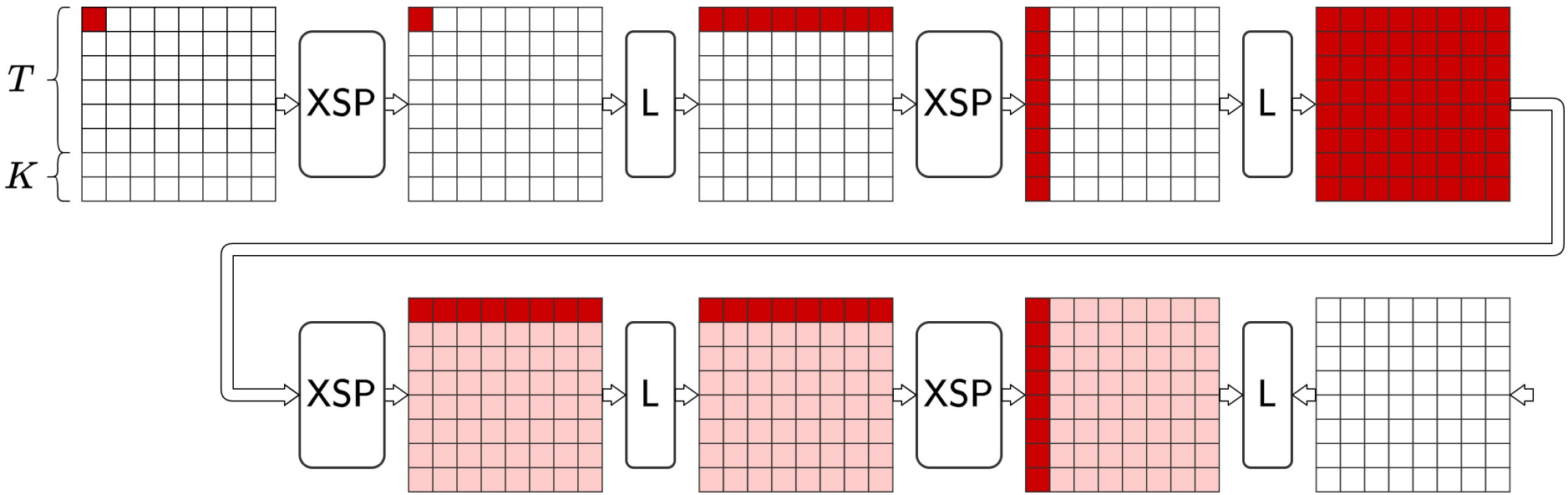


Атака на 6 из 12 раундов

Метод согласования с использованием многомерных дифференциальных соотношений

Направление «вперёд»

Получаем 2^{80} возможных вариантов d-разности

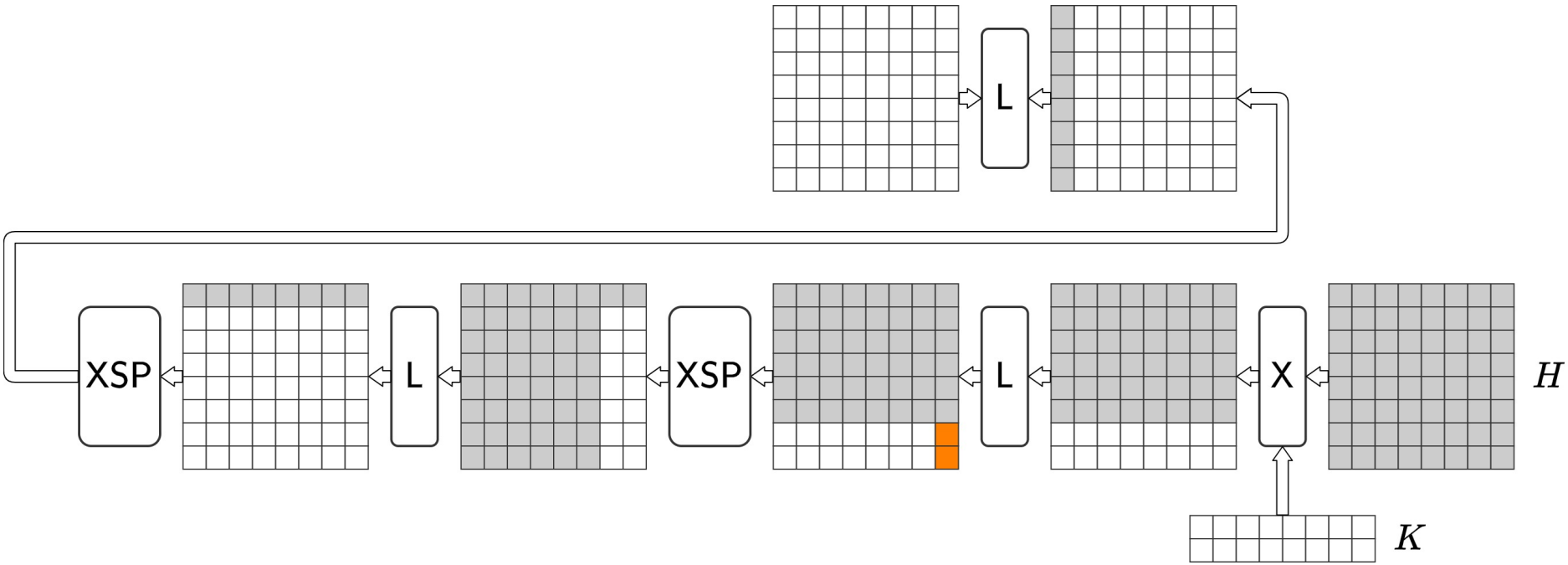


Атака на 6 из 12 раундов

Метод согласования с использованием многомерных дифференциальных соотношений

Направление «назад»

Параллельно 8 раз опробуем 16 бит состояния

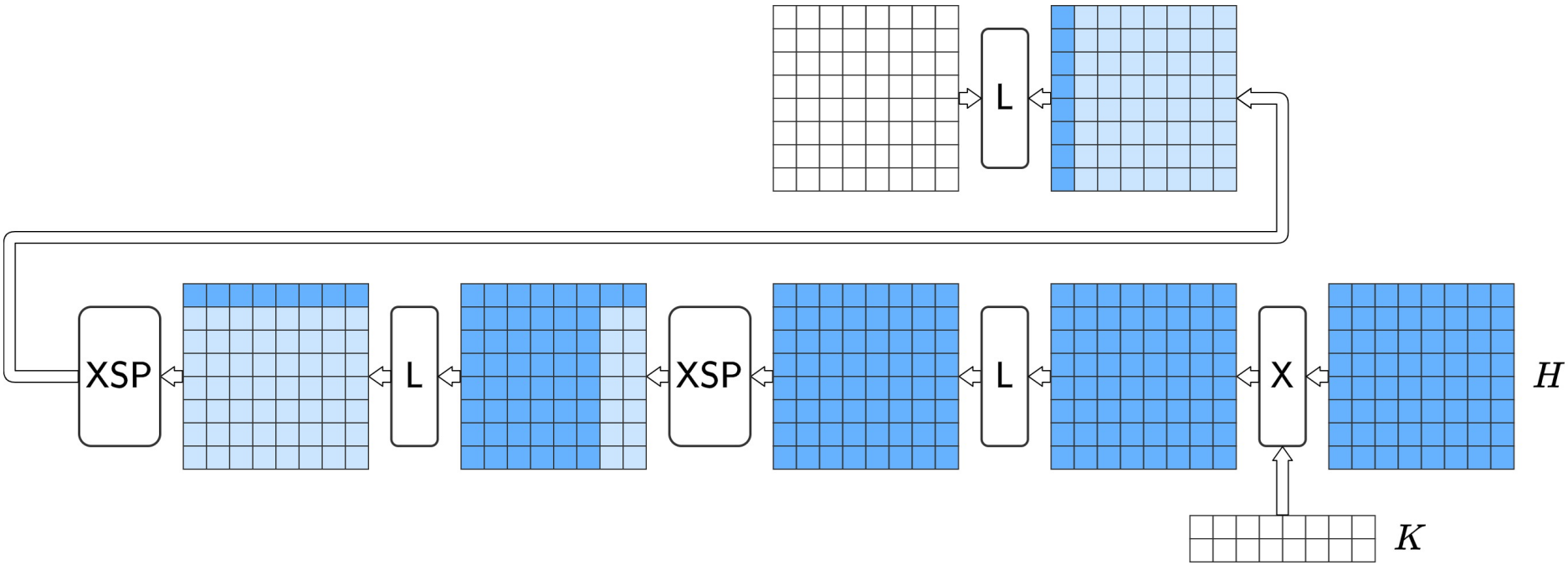


Атака на 6 из 12 раундов

Метод согласования с использованием многомерных дифференциальных соотношений

Направление «назад»

Получаем 8 множеств по 2^{16} возможных вариантов d-разности



Атака на 6 из 12 раундов

Метод согласования с использованием многомерных дифференциальных соотношений

Согласование по «строке» через L

- Исходно имеем: $\Rightarrow 2^{80} \Longleftrightarrow 2^{16 \cdot 8} \Leftarrow$
- Перегруппировываем: $\Rightarrow 2^{80} \cdot 2^{16} \Longleftrightarrow 2^{16 \cdot 7} \Leftarrow$
- Храним в памяти 2^{96} вариантов
- Перебираем 2^{112} вариантов
- При $d = 31$ получаем единственное решение (многомерный дифф. путь)
- Однозначно определяем секретный ключ

Заключение

- Рассмотрена возможность усечения S3G-128$(K, T) = \mathsf{H}(K|T)$ с трёх до одного вызова функции сжатия g
- Оценка свойств $\mathsf{g}(IV, K|T) = \Pi(K|T) \oplus (K|T)$ с точки зрения:
  - теории доказуемой стойкости
  - универсальных методов
  - специальных методов (для 6 раундов функции сжатия из 12)
- Совокупность результатов $\Rightarrow$ хорошие криптографические качества алгоритма S3G-128 в т.ч. и при использовании *усеченной* хэш-функции.

Заключение

- Рассмотрена возможность усечения S3G-128$(K, T) = \mathsf{H}(K|T)$ с трёх до одного вызова функции сжатия g
- Оценка свойств $\mathsf{g}(IV, K|T) = \Pi(K|T) \oplus (K|T)$ с точки зрения:
  - теории доказуемой стойкости
  - универсальных методов
  - специальных методов (для 6 раундов функции сжатия из 12)
- Совокупность результатов $\Rightarrow$ хорошие криптографические качества алгоритма S3G-128 в т.ч. и при использовании *усеченной* хэш-функции.

Заключение

- Рассмотрена возможность усечения S3G-128$(K, T) = \mathsf{H}(K|T)$ с трёх до одного вызова функции сжатия g
- Оценка свойств $\mathsf{g}(IV, K|T) = \Pi(K|T) \oplus (K|T)$ с точки зрения:
  - теории доказуемой стойкости
  - универсальных методов
  - специальных методов (для 6 раундов функции сжатия из 12)
- Совокупность результатов $\Rightarrow$ хорошие криптографические качества алгоритма S3G-128 в т.ч. и при использовании *усеченной* хэш-функции.

Благодарю за внимание!