О вычислительных подходах к оценке вероятности дифференциалов в низкоресурсных XSPL-преобразованиях

В.А. Кирюхин

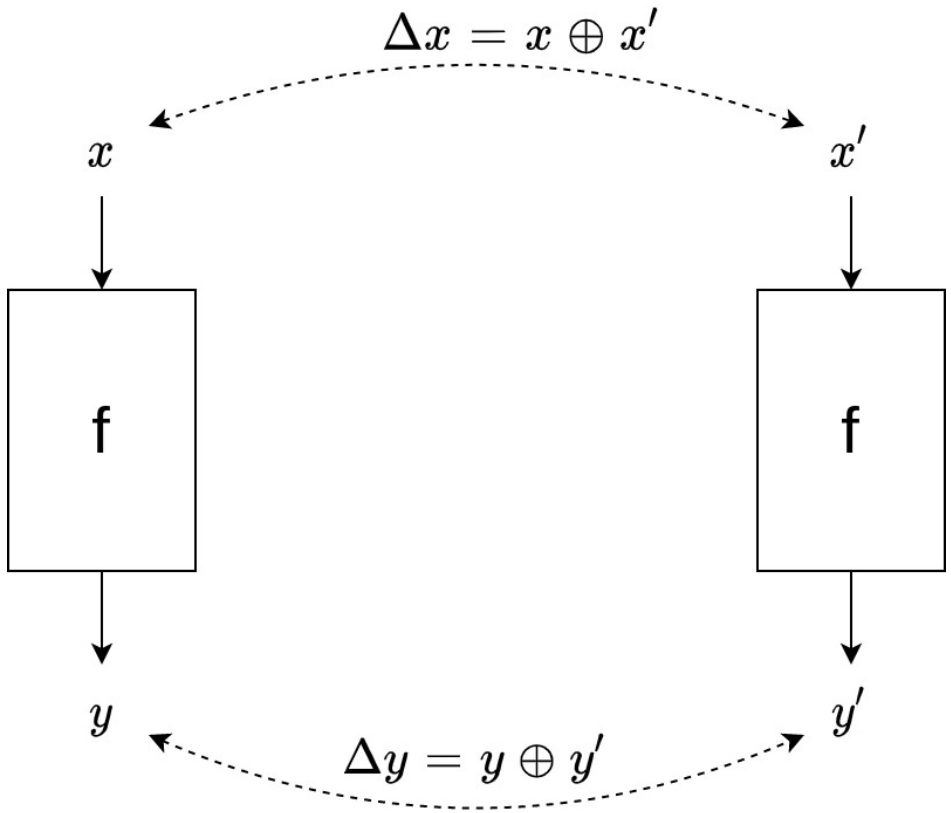
ООО «СФБ Лаб», ОАО «ИнфоТеКС»

РусКрипто'2021
25 марта 2021

vitaly.kiryukhin@sfblaboratory.ru

Дифференциальный криптоанализ

- Один из наиболее известных и универсальных способов криптоанализа
- Основа метода – наблюдение за преобразованиями разности $\Delta x = x \oplus x'$ входных блоков x и x'



Дифференциальный криптоанализ

Стойкость к дифференциальному методу определяется максимумом

$$\mathrm{DP}_{\mathsf{f}}(\Delta x, \Delta y) = \mathsf{Pr}(\mathsf{f}(x) \oplus \mathsf{f}(x \oplus \Delta x) = \Delta y)$$

– вероятности получить на выходе $\mathsf{f}(x)$ разность Δy при условии, что на входе была разность Δx

Для *зависящих от ключа* преобразований $\mathsf{F}_K(x)$ рассматривается **усредненная** вероятность

$$\mathrm{EDP}_{\mathsf{F}}\left(\Delta x, \Delta y\right) = 2^{-\kappa} \sum_{K \in V^{\kappa}} \mathsf{Pr}\left(\mathsf{F}_K(x) \oplus \mathsf{F}_K(x \oplus \Delta x) = \Delta y\right).$$

Дифференциальный криптоанализ

Стойкость к дифференциальному методу определяется максимумом

$$\mathrm{DP}_{\mathsf{f}}(\Delta x, \Delta y) = \mathsf{Pr}(\mathsf{f}(x) \oplus \mathsf{f}(x \oplus \Delta x) = \Delta y)$$

– вероятности получить на выходе $\mathsf{f}(x)$ разность Δy при условии, что на входе была разность Δx

Для *зависящих от ключа* преобразований $\mathsf{F}_K(x)$ рассматривается **усредненная** вероятность

$$\mathrm{EDP}_{\mathsf{F}}\left(\Delta x, \Delta y\right) = 2^{-\kappa} \sum_{K \in V^{\kappa}} \mathsf{Pr}\left(\mathsf{F}_K(x) \oplus \mathsf{F}_K(x \oplus \Delta x) = \Delta y\right).$$

Дифференциальный криптоанализ
Disclaimer

Здесь и далее используется **предположение**: раундовые ключи выбираются случайно и равновероятно (**Марковская модель**)

[Lai X., Massey J.L., Murphy S.
Markov ciphers and differential cryptanalysis – 1991]

Дифференциальный криптоанализ

$\mathrm{E}_K(x)$ – n-битное преобразование

Чем **ближе** максимум

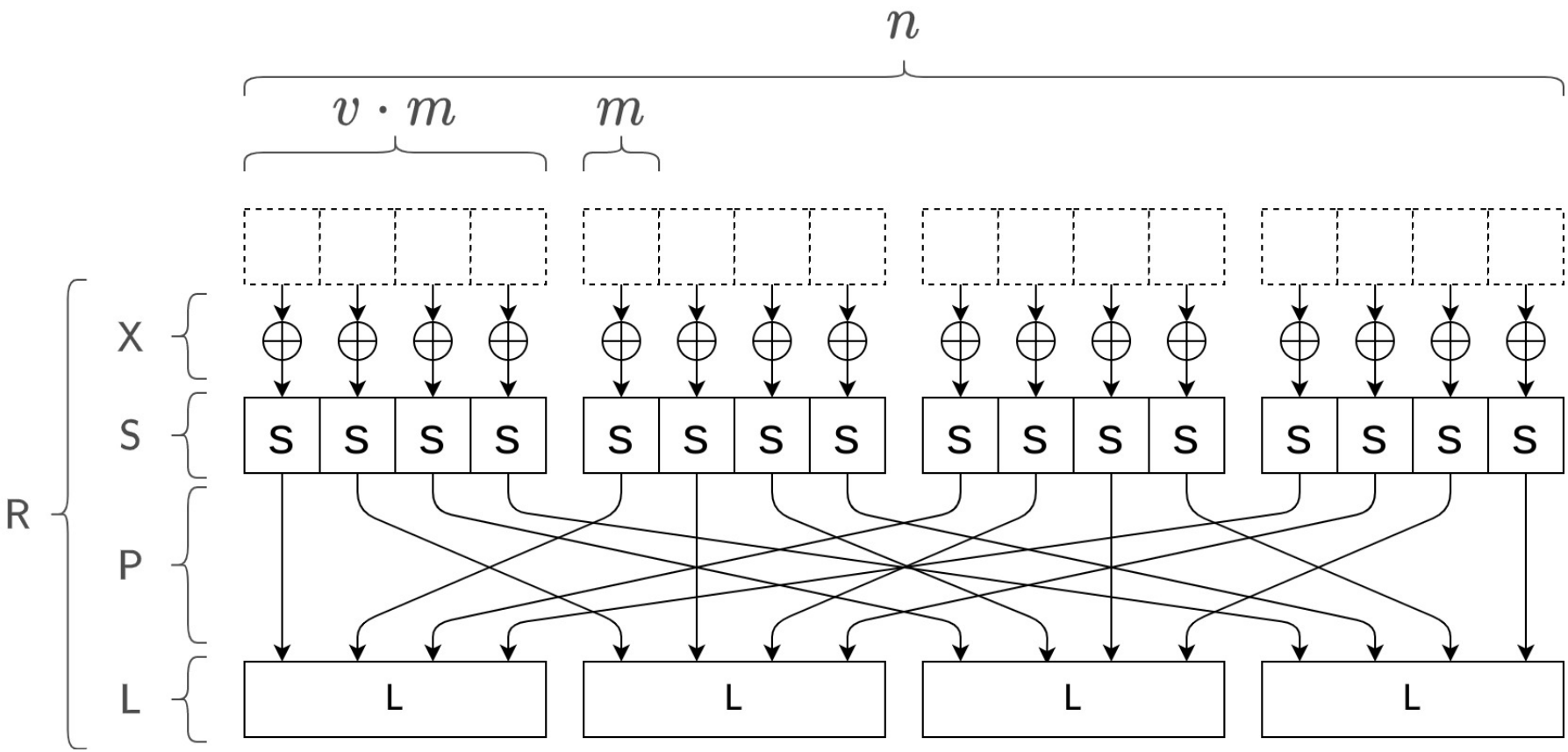
$$\mathrm{MEDP} = \max_{\Delta x, \Delta y \neq 0} \mathrm{EDP}_{\mathrm{E}_K}(\Delta x, \Delta y) > 2^{-n}$$

к

$$2^{-n},$$

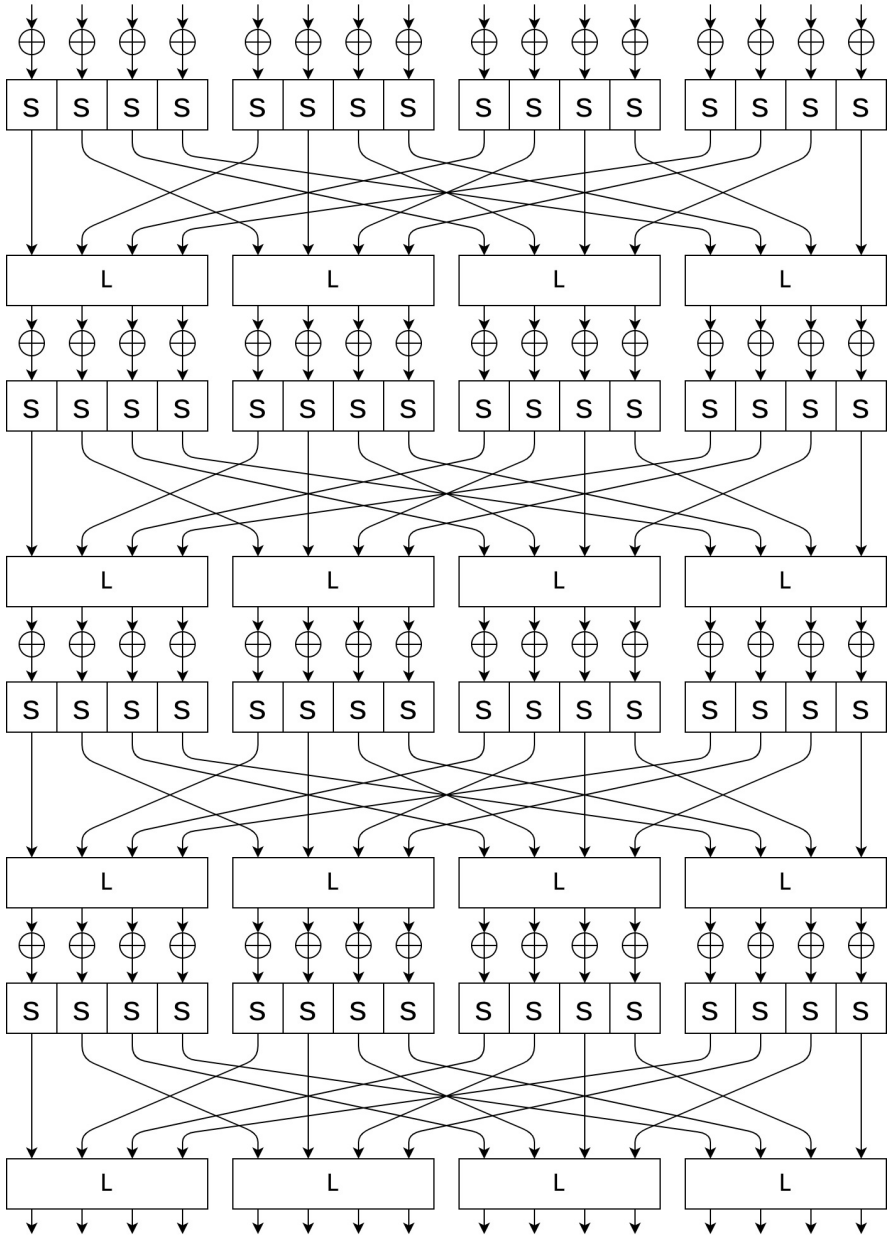
тем **более стойким** является E_K к дифференциальному методу

XSPL-преобразование: раунд



	m	v	n
AES	8	4	128
PHOTON P_{100}	4	5	100

XSPL-преобразование: 4 раунда



Дифференциалы и дифф. пути

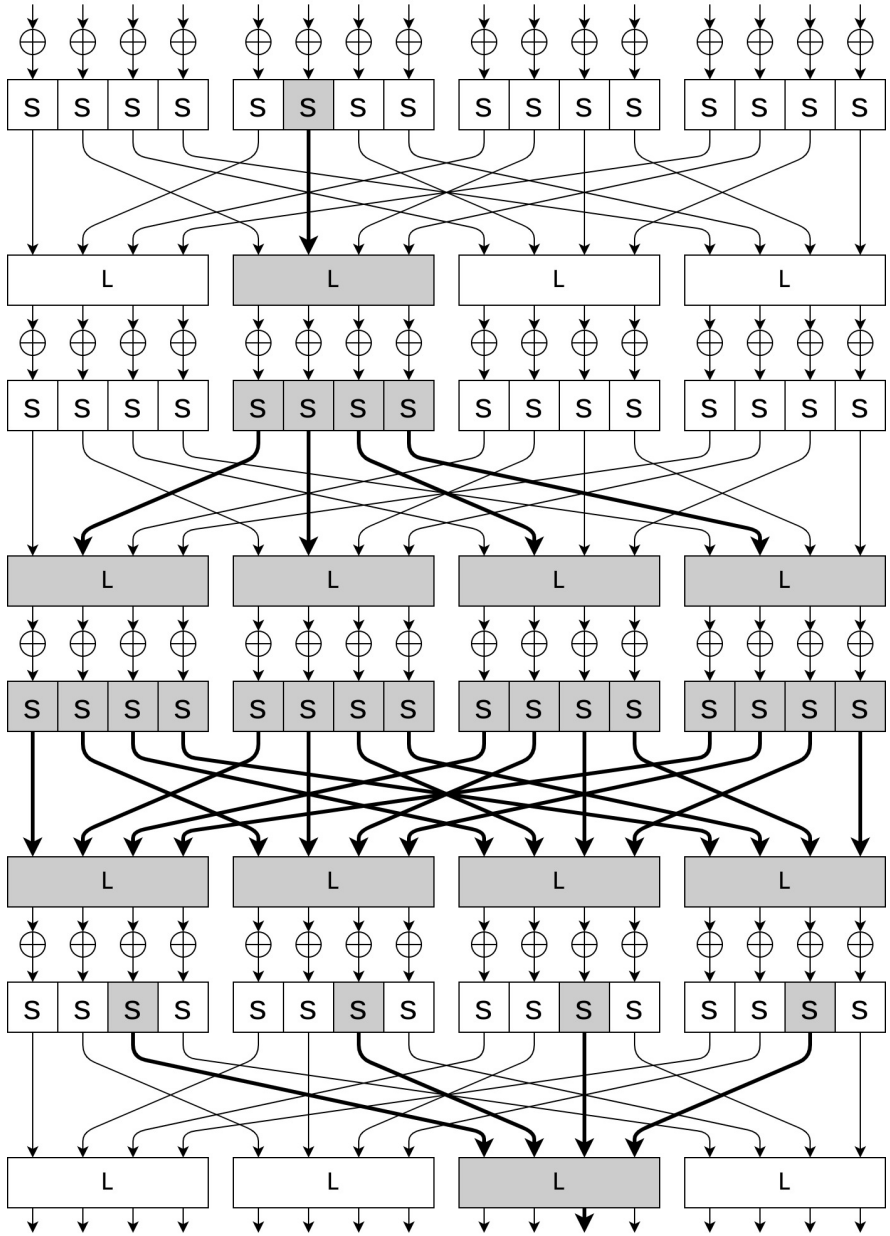
Дифференциальный **путь** = последовательность разностей

$$\Omega = \Delta x \to \Delta_1 \to \Delta_2 \to \ldots \to \Delta y$$

Дифференциал = совокупность путей

$$(\Delta x, \Delta y) = \{\Omega_i : \Delta x \to \Delta_1^{(i)} \to \Delta_2^{(i)} \to \ldots \to \Delta y\}$$

Дифференциальный путь



Дифференциальный путь

Максимальная вероятность перехода $\Delta x \xrightarrow{\mathsf{s}} \Delta y$ через Sbox

$$p = \max_{\Delta x, \Delta y \in V^m \setminus 0} \mathrm{DP}_{\mathsf{s}}(\Delta x, \Delta y) = \Pr(\mathsf{s}(x) \oplus \mathsf{s}(x \oplus \Delta x) = \Delta y)$$

Минимальное число активных Sbox'ов для 4-х раундов

$$\theta \geq (v+1)^2$$

Оценка на дифф. путь $\Omega = \Delta x \to \Delta_1 \to \Delta_2 \to \ldots \to \Delta y$

$$\mathrm{EDCP}(\Omega) \leq p^\theta$$

	p	v	θ	$\mathrm{EDCP}(\Omega)$
AES	$4/256$	4	25	2^{-150}
PHOTON P_{100}	$4/16$	5	36	2^{-72}

$\Rightarrow$ оценки много меньше 2^{-n} при большом числе раундов

Дифференциальный путь

Максимальная вероятность перехода $\Delta x \xrightarrow{\mathsf{s}} \Delta y$ через Sbox

$$p = \max_{\Delta x, \Delta y \in V^m \setminus 0} \mathrm{DP}_{\mathsf{s}}(\Delta x, \Delta y) = \Pr(\mathsf{s}(x) \oplus \mathsf{s}(x \oplus \Delta x) = \Delta y)$$

Минимальное число активных Sbox'ов для 4-х раундов

$$\theta \geq (v+1)^2$$

Оценка на дифф. путь $\Omega = \Delta x \to \Delta_1 \to \Delta_2 \to \ldots \to \Delta y$

$$\mathrm{EDCP}(\Omega) \leq p^\theta$$

	p	v	θ	$\mathrm{EDCP}(\Omega)$
AES	$4/256$	4	25	2^{-150}
PHOTON P_{100}	$4/16$	5	36	2^{-72}

$\Rightarrow$ оценки много меньше 2^{-n} при большом числе раундов

Дифференциальный путь

Максимальная вероятность перехода $\Delta x \xrightarrow{\mathsf{s}} \Delta y$ через Sbox

$$p = \max_{\Delta x, \Delta y \in V^m \setminus 0} \mathrm{DP}_{\mathsf{s}}(\Delta x, \Delta y) = \Pr(\mathsf{s}(x) \oplus \mathsf{s}(x \oplus \Delta x) = \Delta y)$$

Минимальное число активных Sbox'ов для 4-х раундов

$$\theta \geq (v+1)^2$$

Оценка на дифф. путь $\Omega = \Delta x \to \Delta_1 \to \Delta_2 \to \ldots \to \Delta y$

$$\mathrm{EDCP}(\Omega) \leq p^\theta$$

	p	v	θ	$\mathrm{EDCP}(\Omega)$
AES	$4/256$	4	25	2^{-150}
PHOTON P_{100}	$4/16$	5	36	2^{-72}

$\Rightarrow$ оценки много меньше 2^{-n} при большом числе раундов

Дифференциальный путь

Максимальная вероятность перехода $\Delta x \xrightarrow{\mathsf{s}} \Delta y$ через Sbox

$$p = \max_{\Delta x, \Delta y \in V^m \setminus 0} \mathrm{DP}_{\mathsf{s}}(\Delta x, \Delta y) = \Pr(\mathsf{s}(x) \oplus \mathsf{s}(x \oplus \Delta x) = \Delta y)$$

Минимальное число активных Sbox'ов для 4-х раундов

$$\theta \geq (v+1)^2$$

Оценка на дифф. путь $\Omega = \Delta x \to \Delta_1 \to \Delta_2 \to \ldots \to \Delta y$

$$\mathrm{EDCP}(\Omega) \leq p^\theta$$

	p	v	θ	$\mathrm{EDCP}(\Omega)$
AES	$4/256$	4	25	2^{-150}
PHOTON P_{100}	$4/16$	5	36	2^{-72}

$\Rightarrow$ оценки много меньше 2^{-n} при большом числе раундов

Дифференциал

Дифференциал $(\Delta x, \Delta y)$ – совокупность путей
Получить оценку гораздо сложнее!

AES

$$\mathrm{MEDP}_{\mathrm{AES}} \leq 2^{-113\ldots} \Rightarrow \text{ больше чем } 2^{-128}$$

[Keliher L., Sui J.
Exact Maximum Expected Differential and Linear Probability for 2-Round Advanced Encryption Standard (AES) – 2007]

PHOTON P_{100}

$$\mathrm{MEDP}_{\mathrm{PHOTON}} \leq 2^{-50} \Rightarrow \text{ больше чем } 2^{-100}$$

[Jian G., Peyrin T., Poschmann A.
The PHOTON Family of Lightweight Hash Functions – CRYPTO 2011]

... и эти оценки НЕ уменьшаются при увеличении числа раундов

Дифференциал

Дифференциал $(\Delta x, \Delta y)$ – совокупность путей
Получить оценку гораздо сложнее!

AES

$$\mathrm{MEDP}_{\mathrm{AES}} \leq 2^{-113\ldots} \Rightarrow \text{ больше чем } 2^{-128}$$

[Keliher L., Sui J.
Exact Maximum Expected Differential and Linear Probability for 2-Round Advanced Encryption Standard (AES) – 2007]

PHOTON P_{100}

$$\mathrm{MEDP}_{\mathrm{PHOTON}} \leq 2^{-50} \Rightarrow \text{ больше чем } 2^{-100}$$

[Jian G., Peyrin T., Poschmann A.
The PHOTON Family of Lightweight Hash Functions – CRYPTO 2011]

... и эти оценки НЕ уменьшаются при увеличении числа раундов

Дифференциал

Дифференциал $(\Delta x, \Delta y)$ – совокупность путей
Получить оценку гораздо сложнее!

AES

$$\mathrm{MEDP}_{\mathrm{AES}} \leq 2^{-113\ldots} \Rightarrow \text{ больше чем } 2^{-128}$$

[Keliher L., Sui J.
Exact Maximum Expected Differential and Linear Probability for 2-Round Advanced Encryption Standard (AES) – 2007]

PHOTON P_{100}

$$\mathrm{MEDP}_{\mathrm{PHOTON}} \leq 2^{-50} \Rightarrow \text{ больше чем } 2^{-100}$$

[Jian G., Peyrin T., Poschmann A.
The PHOTON Family of Lightweight Hash Functions – CRYPTO 2011]

... и эти оценки НЕ уменьшаются при увеличении числа раундов

Дифференциал

Дифференциал $(\Delta x, \Delta y)$ – совокупность путей
Получить оценку гораздо сложнее!

AES

$$\mathrm{MEDP}_{\mathrm{AES}} \leq 2^{-113\ldots} \Rightarrow \text{ больше чем } 2^{-128}$$

[Keliher L., Sui J.
Exact Maximum Expected Differential and Linear Probability for 2-Round Advanced Encryption Standard (AES) – 2007]

PHOTON P_{100}

$$\mathrm{MEDP}_{\mathrm{PHOTON}} \leq 2^{-50} \Rightarrow \text{ больше чем } 2^{-100}$$

[Jian G., Peyrin T., Poschmann A.
The PHOTON Family of Lightweight Hash Functions – CRYPTO 2011]

... и эти оценки НЕ уменьшаются при увеличении числа раундов

Задача

Оценить стойкость четырех раундов преобразования $\mathsf{R}^4(x) = (\mathsf{LPSX})^4(x)$ – получить верхнюю оценку на

$$\mathrm{MEDP}_{\mathsf{R}^4} = \max_{\Delta x, \Delta y \neq 0} \mathrm{EDP}_{\mathsf{R}^4}(\Delta x, \Delta y)$$

Низкоресурсные XSPL обладают меньшими размерами блока/подблока/подстановки $\Rightarrow$ будем использовать вычислительные методы, недоступные для «тяжелых» преобразований

Переход к эквивалентной задаче

Воспользуемся:

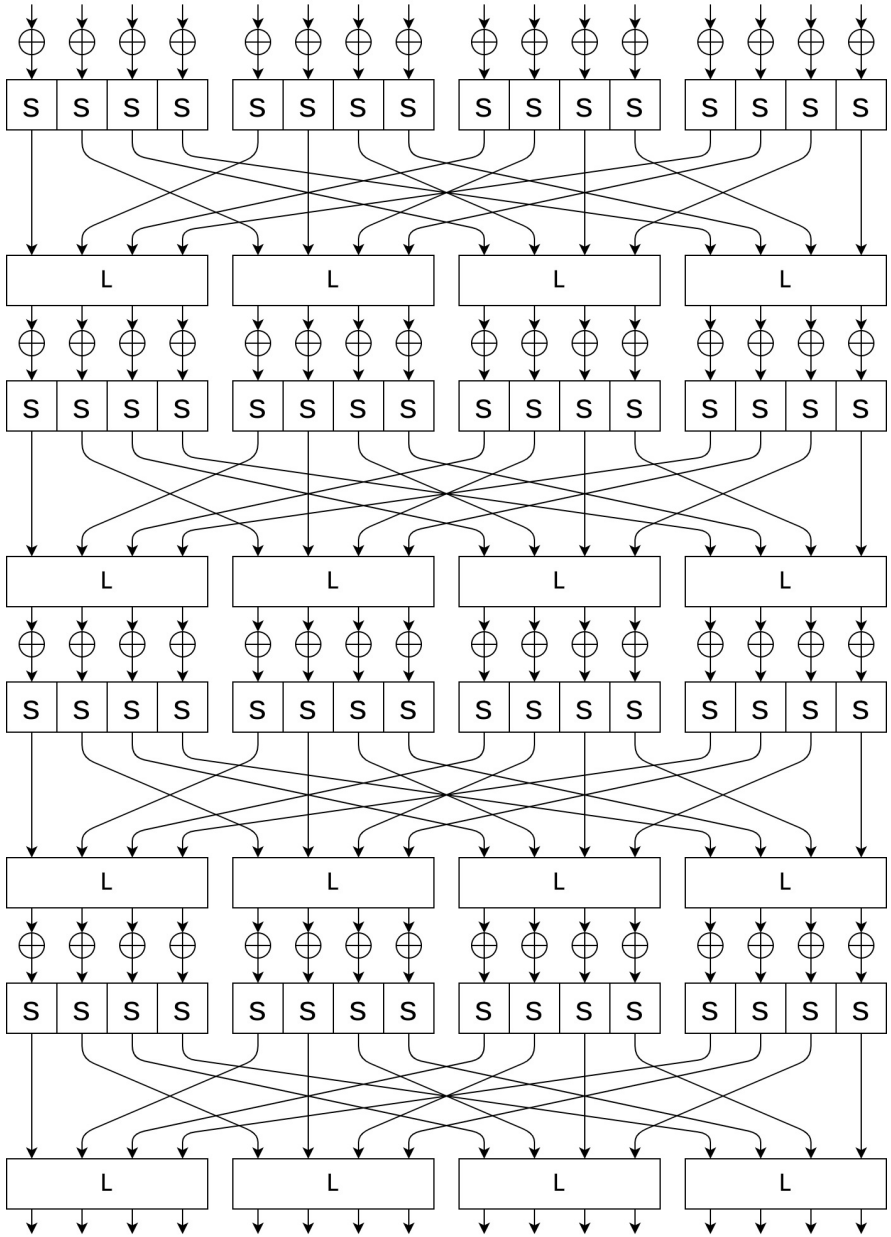
- свойством $\mathsf{PSX}(x) = \mathsf{SXP}(x)$
- линейностью P и L

Перейдём к преобразованию «эквивалентному относительно дифференциального метода»

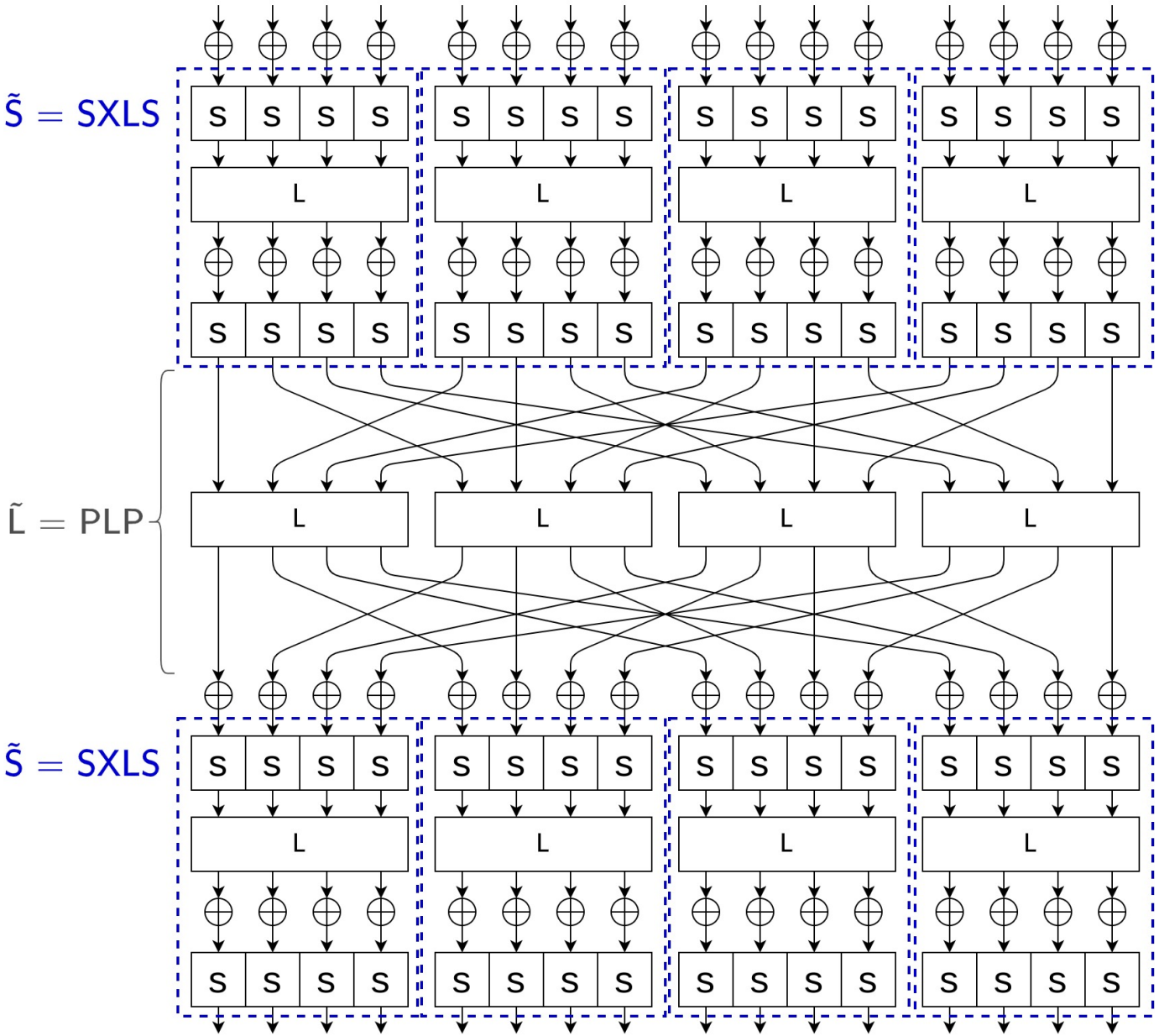
$$\widetilde{\mathsf{E}}(x) = \mathsf{SXLSX}\ \mathsf{PLP}\ \mathsf{SXLSX}(x)$$

$$\max_{\Delta x, \Delta y \neq 0} \mathrm{EDP}_{\widetilde{\mathsf{E}}}(\Delta x, \Delta y) = \max_{\Delta x, \Delta y \neq 0} \mathrm{EDP}_{\mathsf{R}^4}(\Delta x, \Delta y)$$

Исходное преобразование $\mathrm{R}^4(x) = (\mathrm{LPSX})^4(x)$



Преобразование $\widetilde{E}(x)$



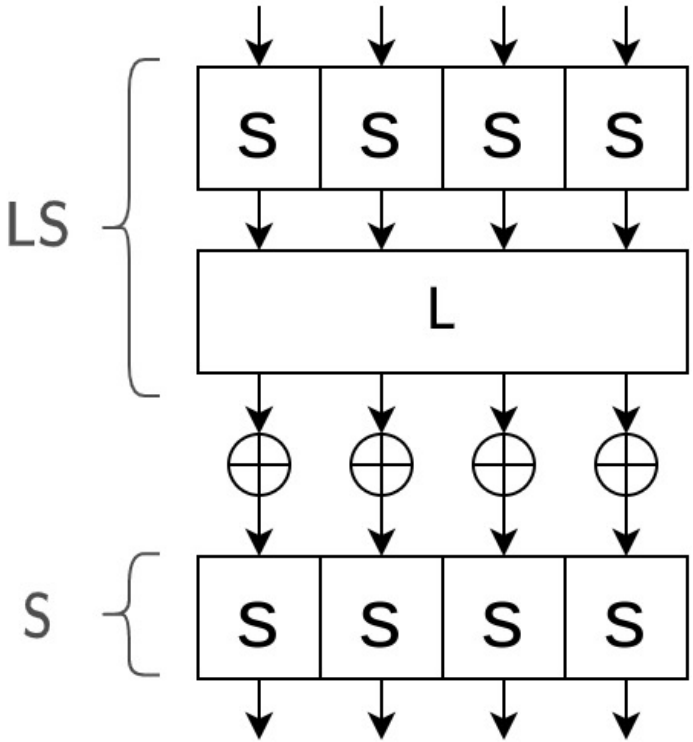
Преобразование $\widetilde{\mathsf{E}}(x)$

$\widetilde{\mathsf{E}}(x)$ – двухраундовое XS~~P~~L-преобразование

1. Нелинейный слой – $\widetilde{\mathsf{S}} = \mathsf{SXLS}$
   – v SuperSbox'ов по vm бит
2. Линейный слой – $\widetilde{\mathsf{L}} = \mathsf{PLP}$
   – максимально рассеивающее над $(V^{vm})^v$, $\mathcal{B}_{\widetilde{\mathsf{L}}} = v + 1$

Оценка одного SuperSbox'a

Построим **все** дифференциалы для одного SuperSbox'a

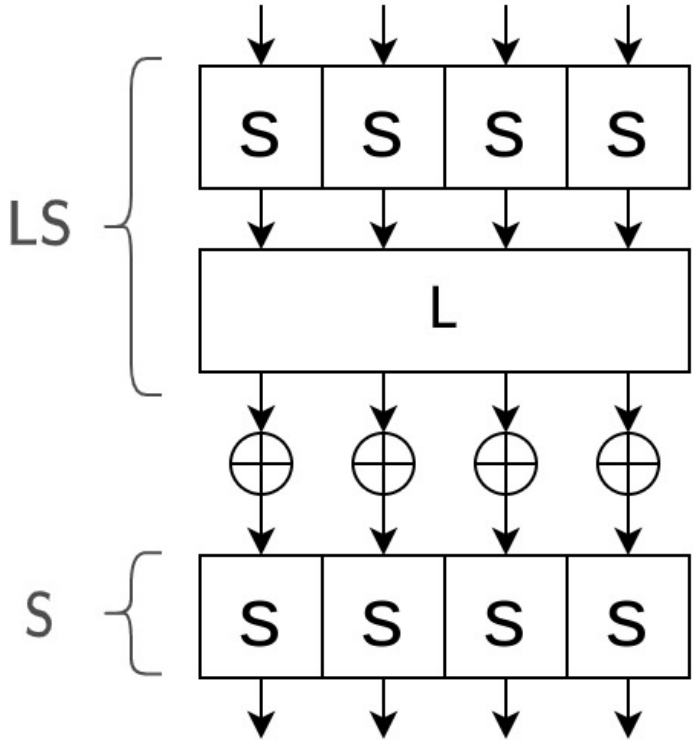


— построим матрицу

$$[\mathrm{EDP}_{\mathrm{SXLS}}(\Delta x, \Delta y)]$$

размерности $2^{vm} \times 2^{vm}$

Оценка одного SuperSbox'a – базовый подход



Перебираем блок x, разность Δx, ключ k

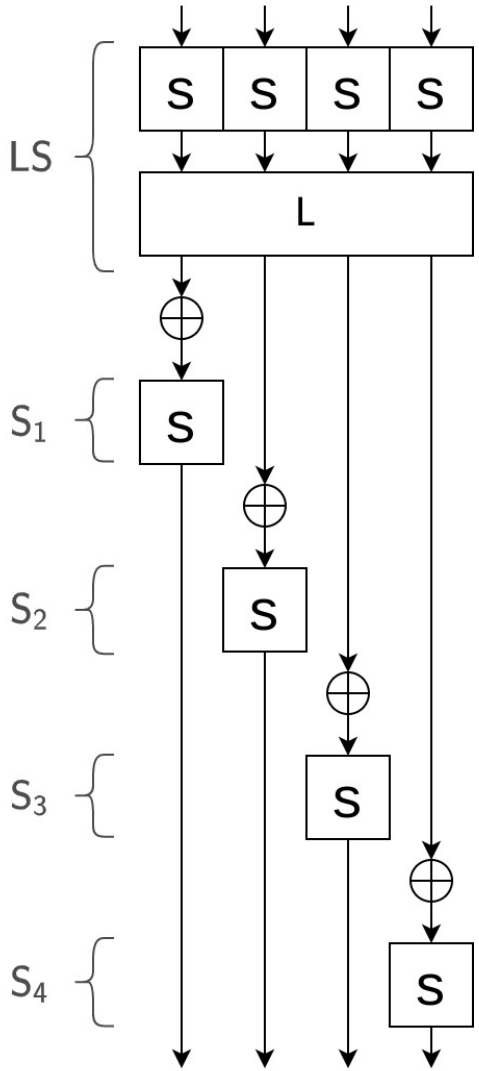
Сложность: $2^{vm} \cdot 2^{vm} \cdot 2^{vm} = 2^{3vm}$ операций

Для AES: $\left(2^{32}\right)^3 = 2^{96}$ операций

Для PHOTON P_{100}: $\left(2^{20}\right)^3 = 2^{60}$ операций

Оценка одного SuperSbox'a – эффективный подход

$S = S_v \dots S_2 S_1$ — v последовательных преобразований



Оценка одного SuperSbox'a – эффективный подход

$\mathsf{S} = \mathsf{S}_v \ldots \mathsf{S}_2\mathsf{S}_1$ — v последовательных преобразований
Матрицы $[\mathrm{DP}_{\mathsf{S}_i}(\Delta x, \Delta y)]$ будут иметь разреженный вид

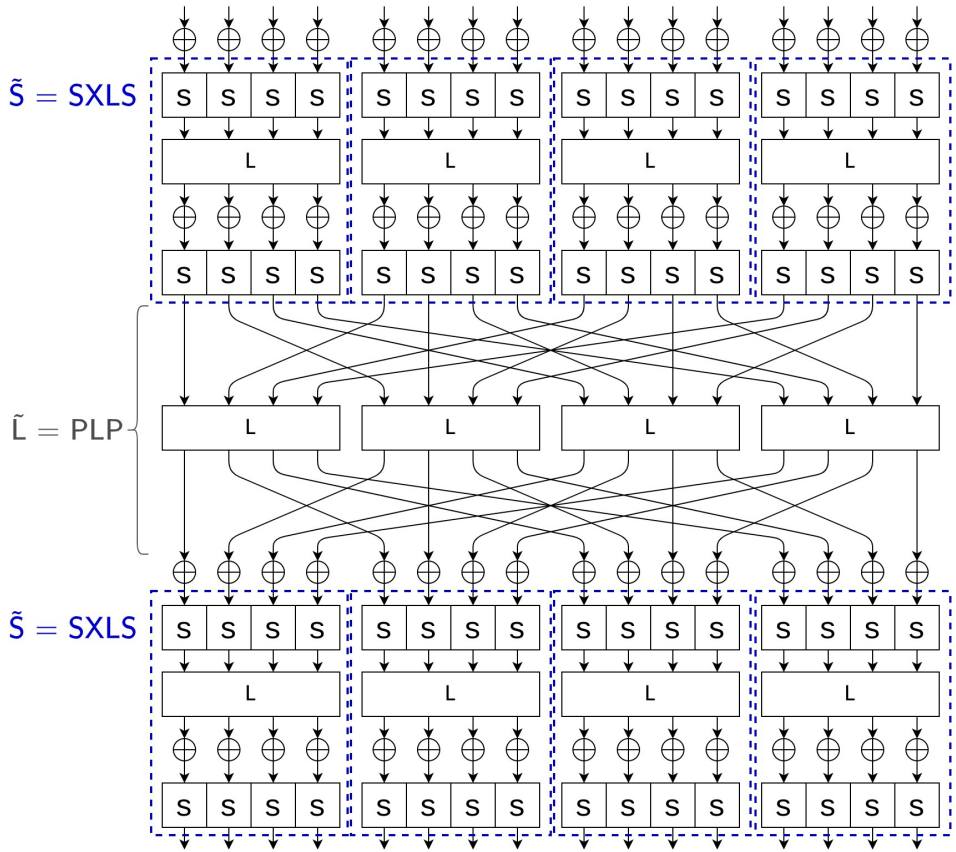
$$\begin{aligned}[\mathrm{EDP}_{\mathsf{SXLS}}(\Delta x, \Delta y)] = [\mathrm{DP}_{\mathsf{LS}}(\Delta x, \Delta y)] \times \\ \times [\mathrm{DP}_{\mathsf{S_1}}(\Delta x, \Delta y)] \times \\ \times [\mathrm{DP}_{\mathsf{S_2}}(\Delta x, \Delta y)] \times \\ \ldots \\ \times [\mathrm{DP}_{\mathsf{S}_v}(\Delta x, \Delta y)]\end{aligned}$$

Сложность: $2^{2vm} \cdot 2^m \cdot v$ операций
Для PHOTON P_{100}: $\left(2^{20}\right)^2 \cdot 2^4 \cdot 5 \approx 2^{46}$ операций

Оценка четырёх раундов XSPL

- знаем все дифференциалы $\widetilde{\mathrm{S}} = \mathrm{SXLS}$
- знаем рассеивающие свойства $\widetilde{\mathrm{L}}$

$\Rightarrow$ оценим дифференциалы в 4-раундовом преобразовании



Рассмотрим два подхода...

Оценка стойкости – подход 1

Воспользуемся теоремой для оценки двухраундового XSL:

Теорема (FSE2003)

Для преобразования вида $y = \mathsf{E}(x) = \mathsf{SXLSX}(x)$ *выполнено*

$$\mathrm{MEDP}_{\mathsf{E}} = \max_{\Delta x, \Delta y \neq 0} \mathrm{EDP}_{\mathsf{E}}(\Delta x, \Delta y) \leq$$

$$\leq \max\left(\max_{\alpha \in V^m \setminus 0} \sum_{i \in V^m \setminus 0} \left(\mathrm{DP}_{\mathsf{s}}(\alpha, i)\right)^{\mathcal{B}_{\mathsf{L}}}, \max_{\beta \in V^m \setminus 0} \sum_{i \in V^m \setminus 0} \left(\mathrm{DP}_{\mathsf{s}}(i, \beta)\right)^{\mathcal{B}_{\mathsf{L}}} \right)$$

где S *состоит из параллельного применения подстановок* $\mathsf{s} : V^m \to V^m$, *а* $\mathcal{B}_{\mathsf{L}}$ *– минимальное число активных подстановок* s

Park, S., Sung, S.H., Lee, S., Lim, J.
Improving the Upper Bound on the Maximum Differential and the Maximum Linear Hull Probability for SPN Structures and AES
In: Fast Software Encryption - FSE 2003. LNCS, vol. 2887, pp. 247–260. Springer (2003).

Оценка стойкости – подход 1

Лемма

Для четырёх раундов XPSL*-преобразования справедлива оценка*

$$\mathrm{MEDP}_{\mathsf{R4}} = \max_{\Delta x, \Delta y \neq 0} \mathrm{EDP}_{\mathsf{R4}}\left(\Delta x, \Delta y\right) \leq$$

$$\leq \max \left(\max_{\alpha \in V^{vm} \setminus 0} \sum_{i \in V^{vm} \setminus 0} \left(\mathrm{EDP}_{\mathsf{SXLS}}(\alpha, i)\right)^{\mathcal{B}_{\mathbf{PLP}}}, \right.$$

$$\left. \max_{\beta \in V^{vm} \setminus 0} \sum_{i \in V^{vm} \setminus 0} \left(\mathrm{EDP}_{\mathsf{SXLS}}(i, \beta)\right)^{\mathcal{B}_{\mathbf{PLP}}} \right).$$

Оценка стойкости – подход 1

Идея доказательства леммы:

- примененить теорему (FSE2003) к преобразованию $\widetilde{\mathsf{E}}(x) = \widetilde{\mathsf{S}}\mathsf{X}\widetilde{\mathsf{L}}\widetilde{\mathsf{S}}\mathsf{X}(x)$
- вместо бесключевой $\mathsf{s} : V^m \to V^m$ рассмотреть зависящую от ключа $\mathsf{SXLS} : V^{vm} \times V^{vm} \to V^{vm}$
- вместо вероятности $\mathrm{DP}\left(\Delta x, \Delta y\right)$ рассмотреть усреднённую вероятность $\mathrm{EDP}\left(\Delta x, \Delta y\right)$

Оценка стойкости – подход 1

Идея доказательства леммы:

- примененить теорему (FSE2003) к преобразованию $\widetilde{\mathrm{E}}(x) = \widetilde{\mathrm{S}}\mathrm{X}\widetilde{\mathrm{L}}\widetilde{\mathrm{S}}\mathrm{X}(x)$
- вместо бесключевой $\mathrm{s} : V^m \to V^m$ рассмотреть зависящую от ключа $\mathrm{SXLS} : V^{vm} \times V^{vm} \to V^{vm}$
- вместо вероятности $\mathrm{DP}\left(\Delta x, \Delta y\right)$ рассмотреть усреднённую вероятность $\mathrm{EDP}\left(\Delta x, \Delta y\right)$

Оценка стойкости – подход 1

Идея доказательства леммы:

- примененить теорему (FSE2003) к преобразованию $\widetilde{\mathrm{E}}(x) = \widetilde{\mathrm{S}}\mathrm{X}\widetilde{\mathrm{L}}\widetilde{\mathrm{S}}\mathrm{X}(x)$
- вместо бесключевой $\mathrm{s} : V^m \to V^m$ рассмотреть зависящую от ключа $\mathrm{SXLS} : V^{vm} \times V^{vm} \to V^{vm}$
- вместо вероятности $\mathrm{DP}\,(\Delta x, \Delta y)$ рассмотреть усреднённую вероятность $\mathrm{EDP}\,(\Delta x, \Delta y)$

Оценка стойкости – подход 2

Второй подход – больше вычислительных ресурсов, но более точная оценка:

Шаг 1. Получим оценку $\hat{p}_1$ на дифференциалы,
у которых активен ровно $v + 1$ SuperSbox

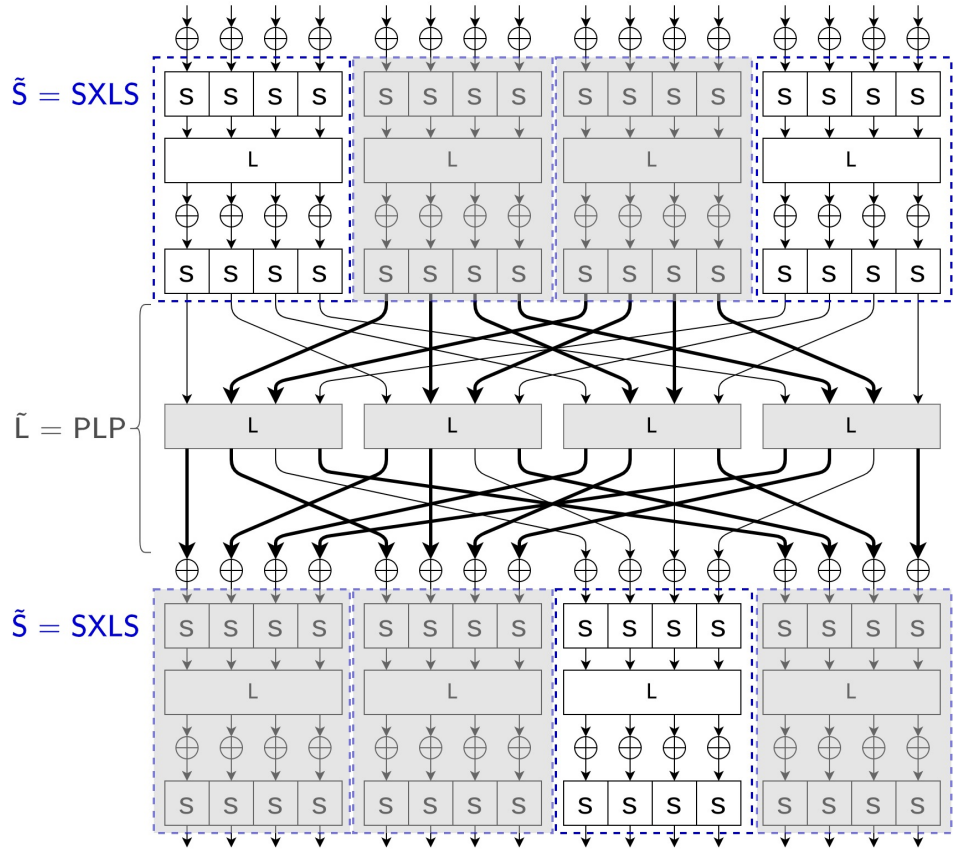
Шаг 2. Получим оценку $\hat{p}_2$ на остальные дифференциалы
($v + 2$, $v + 3$, ..., $2v$ активных)

Шаг 3:

$$\mathrm{MEDP} \leq \max(\hat{p}_1, \hat{p}_2)$$

Оценка стойкости – подход 2

Шаг 1. Получим оценку $\hat{p}_1$ на дифференциалы, у которых активен ровно $v + 1$ SuperSbox



Изображена конфигурация $c_{active} = \{2, 3, 5, 6, 8\}$, $|c_{active}| = 5 = v + 1$

Оценка стойкости – подход 2

Шаг 1. Получим оценку $\hat{p}_1$ на дифференциалы,
у которых активен ровно $v+1$ SuperSbox

- Рассмотрим каждую конфигурацию c_{active}: $\binom{2v}{v+1}$ вариантов
- Построим набор кодовых слов кода $\widetilde{\mathrm{L}} = \mathrm{PLP}$, соответствующих c_{active}: $(2^m-1)^v$ кодовых слов
- Каждый набор оценим рекурсивным алгоритмом:
  [Kiryukhin V. – Exact maximum expected differential and linear probability for 2-round Kuznyechik – CTCrypt'18]
- Максимум по всем наборам – оценка $\hat{p}_1$

Оценка стойкости – подход 2

Шаг 2. Получим оценку $\hat{p}_2$ на остальные дифференциалы ($v+2$, $v+3$, ..., $2v$ активных)

- Находим строку/столбец матрицы $[\mathrm{EDP}_{\mathrm{SXLS}}(\Delta x, \Delta y)]$ дифференциалов SuperSbox'а, которые дадут максимальную оценку $\hat{p}_2$
- Знаем показатель рассеивания $\widetilde{\mathrm{L}} = \mathrm{PLP}$ над $(V^{vm})^v$, $\mathcal{B}_{\widetilde{\mathrm{L}}} = v+1$
- Вычисляем $\hat{p}_2$ алгоритмом динамического программирования: [Kiryukhin V. – An algorithm for bounding non-minimum weight differentials in 2-round LSX-ciphers – CTCrypt'20]

Шаг 3:

$$\mathrm{MEDP} \leq \max(\hat{p}_1, \hat{p}_2)$$

Результаты

Преобразование P_{100} хэш-функции PHOTON

[Jian G., Peyrin T., Poschmann A.
The PHOTON Family of Lightweight Hash Functions
CRYPTO 2011]

Размер блока $n = 100$ бит
Размерность состояния $v \times v = 5 \times 5$
Размер подстановки $m = 4$ бита
Оценка разработчиков: $\mathrm{MEDP}_{P_{100}} \leq 2^{-50}$

Новая оценка

$$\mathrm{MEDP}_{P_{100}} \leq 2^{-67.4\ldots}$$

Результаты

Функция сжатия g хэш-функции «Мора», РусКрипто'2020

[Бондакова О.С.
Об одной низкоресурсной хэш-функции
РусКрипто'2020]

Размер блока $n = 64$ бита
Размерность состояния $v \times v = 4 \times 4$
Размер подстановки $m = 4$ бита
Аналитическая оценка: $\mathrm{MEDP}_g \leq 2^{-35.6...}$

Новая оценка

$$\mathrm{MEDP}_g \leq 2^{-47.3...}$$

Заключение

- Представлены вычислительные подходы к оценке стойкости 4-х раундов XSPL-преобразований
- В рамках предположения о независимости и равновероятности раундовых ключей:
  - Получены **верхние оценки** на вероятность дифференциала
  - Рассматриваемые оценки по меньшей мере **не возрастают** с увеличением числа раундов
  - Значение оценки определяет меру **доказуемой стойкости** к дифференциальному методу
- Получены новые оценки для:
  - Преобразования P_{100} хэш-функции PHOTON, CRYPTO 2011
  - Функции сжатия g хэш-функции «Мора», РусКрипто'2020

Заключение

- Представлены вычислительные подходы к оценке стойкости 4-х раундов XSPL-преобразований
- В рамках предположения о независимости и равновероятности раундовых ключей:
  - Получены **верхние оценки** на вероятность дифференциала
  - Рассматриваемые оценки по меньшей мере **не возрастают** с увеличением числа раундов
  - Значение оценки определяет меру **доказуемой стойкости** к дифференциальному методу
- Получены новые оценки для:
  - Преобразования P_{100} хэш-функции PHOTON, CRYPTO 2011
  - Функции сжатия g хэш-функции «Мора», РусКрипто'2020

Заключение

- Представлены вычислительные подходы к оценке стойкости 4-х раундов XSPL-преобразований
- В рамках предположения о независимости и равновероятности раундовых ключей:
  - Получены **верхние оценки** на вероятность дифференциала
  - Рассматриваемые оценки по меньшей мере **не возрастают** с увеличением числа раундов
  - Значение оценки определяет меру **доказуемой стойкости** к дифференциальному методу
- Получены новые оценки для:
  - Преобразования P_{100} хэш-функции PHOTON, CRYPTO 2011
  - Функции сжатия g хэш-функции «Мора», РусКрипто'2020

Благодарю за внимание!