Исследование применимости метода связанных ключей к упрощенной модификации шифра Кузнечик

Гончаренко Кирилл Сергеевич

21 марта 2017 г.

Данная работа посвящена криптоанализу модификации шифра Кузнечик с использованием метода связанных ключей. Описана атака на версию с 4 раундами шифрования и урезанного ключевого расписания, позволяющая полностью найти мастер-ключ за 2^{12} шифрований при стольких же связанных ключах.

Немного о методе связанных ключей

Метод свзянных ключей был впервые предложен Е. Бихамом в работе [5].
Криптоаналитик может использовать дополнительные пары ключей, которые связаны между собой известным отношением (в некоторых вариациях – сам задавать это отношение). Часто это отношение является просто побитовым сложением с заранее заданной константой.
Важно отметить - сами ключи не известны, а известно только соотношение между ними.

Некоторые результаты, полученные с использованием метода связанных ключей

Метод связанных ключей широко применяется для криптоанализа различных блочных шифров. Так, например:

- В работах [6] и [7] были обозначены идеи примемения метода связанных ключей для различных шифров, например, IDEA, Triple-DES, Biham-DES и многих других.
- В работе [2] представлена атака с использованием усовершенствованной атаки типа бумеранг (в которой используются связанные ключи), существенно снижающая стойкость шифров AES-192 и AES-256. Для последнего была представлена атака, восстанавливающая полностью ключ за $2^{99,5}$ шифрований.
- В работе [3] была представлена модифицированная атака из [4] также с использованием атаки типа бумеранг, которая полностью восстанавливает ключ ГОСТ 28147-89.

Используемые обозначения

$\mathbb{F}$ – конечное поле $GF(2)[x]/p(x)$, где $p(x) = x^8 + x^7 + x^6 + x + 1 \in GF(2)[x]$; элементы поля $\mathbb{F}$ представляются целыми числами, причем элементу $z_0 + z_1\theta + \ldots + z_7\theta^7 \in \mathbb{F}$ соответствует число $z_0 + 2 \cdot z_1 + \ldots + 2^7 \cdot z_7$, где $z_i \in 0, 1$, $i = 0, 1, \ldots, 7$ и θ обозначает класс вычетов по модулю $p(x)$, содержащий x;

$Vec_s : \mathbb{Z}_{2^s} \to V_s$ – биективное отображение, сопоставляющее элементу кольца $\mathbb{Z}_{2^s}$ его двоичное представление, т.е. для любого элемента $z \in \mathbb{Z}_{2^s}$, представленного в виде $z = z_0 + 2 \cdot z_1 + \ldots + 2^{s-1} \cdot z_{s-1}$, где $z_i \in 0, 1$, $i = 0, 1, \ldots, s-1$, выполнено равенство $Vec_s(z) = z_{s-1}|| \ldots ||z_1||z_0$;

$Int_s : V_s \to \mathbb{Z}_{2^s}$ – отображение, обратное к отображению Vec_s, т.е. $Int_s = Vec_s^{-1}$;

$\Delta : V_8 \to \mathbb{F}$ – биективное отображение, сопоставляющее двоичной строке из V_8 элемент поля $\mathbb{F}$ следующим образом: строке $z_7|| \ldots ||z_1||z_0$, $z_i \in 0, 1$, $i = 0, 1, \ldots, 7$, соответствует элемент $z_0 + z_1 \cdot \theta + \ldots + z_7 \cdot \theta^7 \in \mathbb{F}$;

$\nabla : \mathbb{F} \to V_8$ – отображение, обратное к отображение Δ, т.е. $\nabla = \Delta^{-1}$.

Используемые преобразования

В качестве нелинейного биективного преобразования выступает подстановка $\pi = Vec_8 \pi' Int_8 : V_8 \to V_8$, где $\pi' : \mathbb{Z}_{2^8} \to \mathbb{Z}_{2^8}$. Значения подстановки π' записаны ниже в виде массива
$\pi' = (\pi'(0), \pi'(1), \ldots, \pi'(255))$:

$$\pi' = (252, 238, 221, 17, 207, 110, 49, 22, 251, 196, 250, 218, 35, 197, 4, 77, 233, 119, 240, 219, 147, 46, 153, 186, 23, 54, 241, 187, 20, 205, 95, 193, 249, 24, 101, 90, 226, 92, 239, 33, 129, 28, 60, 66, 139, 1, 142, 79, 5, 132, 2, 174, 227, 106, 143, 160, 6, 11, 237, 152, 127, 212, 211, 31, 235, 52, 44, 81, 234, 200, 72, 171, 242, 42, 104, 162, 253, 58, 206, 204, 181, 112, 14, 86, 8, 12, 118, 18, 191, 114, 19, 71, 156, 183, 93, 135, 21, 161, 150, 41, 16, 123, 154, 199, 243, 145, 120, 111, 157, 158, 178, 177, 50, 117, 25, 61, 255, 53, 138, 126, 109, 84, 198, 128, 195, 189, 13, 87, 223, 245, 36, 169, 62, 168, 67, 201, 215, 121, 214, 246, 124, 34, 185, 3, 224, 15, 236, 222, 122, 148, 176, 188, 220, 232, 40, 80, 78, 51, 10, 74, 167, 151, 96, 115, 30, 0, 98, 68, 26, 184, 56, 130, 100, 159, 38, 65, 173, 69, 70, 146, 39, 94, 85, 47, 140, 163, 165, 125, 105, 213, 149, 59, 7, 88, 179, 64, 134, 172, 29, 247, 48, 55, 107, 228, 136, 217, 231, 137, 225, 27, 131, 73, 76, 63, 248, 254, 141, 83, 170, 144, 202, 216, 133, 97, 32, 113, 103, 164, 45, 43, 9, 91, 203, 155, 37, 208, 190, 229, 108, 82, 89, 166, 116, 210, 230, 244, 180, 192, 209, 102, 175, 194, 57, 75, 99, 182)$$

Линейное преобразование задается отображением $\ell : V_8^{16} \to V_8$, которое определяется следующим образом:

$$\ell(a_{15}, \ldots, a_0) = \nabla(148 \cdot \Delta(a_{15}) + 32 \cdot \Delta(a_{14}) + 133 \cdot \Delta(a_{13}) + 16 \cdot \Delta(a_{12}) +$$
$$194 \cdot \Delta(a_{11}) + 192 \cdot \Delta(a_{10}) + 1 \cdot \Delta(a_9) + 251 \cdot \Delta(a_8) + 1 \cdot \Delta(a_7) + 192 \cdot \Delta(a_6)$$
$$194 \cdot \Delta(a_5) + 16 \cdot \Delta(a_4) + 133 \cdot \Delta(a_3) + 32 \cdot \Delta(a_2) + 148 \cdot \Delta(a_1) + 1 \cdot \Delta(a_0))$$

для любых $a_i \in V_8,], i = 0, 1, \ldots, 15$, где операции сложения и умножения осуществляются в поле $\mathbb{F}$, а константы являются элементами поля.

При реализации алгоритмов зашифрования и расшифрования используются следующие преобразования:

$\mathbf{X[k]} : \mathbf{V_{128}} \to \mathbf{V_{128}}$	– $\mathbf{X[k](a)} = \mathbf{k} \oplus \mathbf{a}$, где $k, a \in V_{128}$;
$\mathbf{S} : \mathbf{V_{128}} \to \mathbf{V_{128}}$	– $\mathbf{S(a)} = \mathbf{S(a_{15}} \| \ldots \| \mathbf{a_0}) = \pi(\mathbf{a_{15}}) \| \ldots \| \pi(\mathbf{a_0})$, где $a = a_{15} \| \ldots \| a_0 \in V_{128}$, $a_i \in V_8$, $i = 0, 1, \ldots, 15$;
$R : V_{128} \to V_{128}$	– $R(a) = R(a_{15} \| \ldots \| a_0) = \ell(a_{15}, \ldots, a_0) \| a_{15} \| \ldots \| a_1$, где $a = a_{15} \| \ldots \| a_0 \in V_{128}$, $a_i \in V_8$, $i0, 1 \ldots 15$;
$\mathbf{L} : \mathbf{V_{128}} \to \mathbf{V_{128}}$	– $L(a) = R^{16}(a)$, где $a \in V_{128}$ (линейное преобразование);
$F[k] : V_{128} \times V_{128} \to V_{128} \times V_{128}$	– $F[k](a_1, a_0) = LSX[k](a_1) \oplus a_0, a_1)$, где k, a_0, $a_1 \in V_{128}$.

Ключевое расписание

Алгоритм развертывания ключа использует итерациооные константы $\mathbf{C_i} \in V_{128}$, $i = 1, 2, \ldots, 32$, которые определены следующим образом:

$$\mathbf{C_i} = \mathbf{L(i)},\ i = 1, 2, \ldots, 32.$$

Итерационные ключи $\mathbf{K_i} \in V_{128}$, $i = 1, 2, \ldots 10$, вырабатываются на основе ключа
$K = k_{255}|| \ldots ||k_0 \in V_{256}$, $k_i \in V_1$, $i = 0, 1, \ldots, 255$, и определяются равенствами:

$$\mathbf{K_1} = \mathbf{k_{255}}||\ldots||\mathbf{K_{128}};$$

$$\mathbf{K_2} = \mathbf{k_{127}}||\ldots||\mathbf{k_0};$$

$$(\mathbf{K_{2i+1}}, \mathbf{K_{2i+2}}) = \mathbf{F}[\mathbf{C_{8(i-1)+8}}]\ldots\mathbf{F}[\mathbf{C_{8(i-1)+1}}](\mathbf{K_{2i-1}}, \mathbf{K_{2i}}), \quad i = 1, 2, 3, 4.$$

$$i = 1 : (K_3, K_3) = F[C_8]F[C_7]\ldots F[C_2]F[C_1](K_1, K_2)$$

Алгоритм зашифрования / расшифрования

Алгоритм зашифрования в зависимости от значений итерационных ключей $K_i \in V_{128}$, $i = 1, 2, \ldots, 10$, реализует подстановку $\mathbf{E}_{\mathbf{K_1},\ldots,\mathbf{K_{10}}}$, заданную на множестве V_{128} в соответствии с равенством

$$\mathbf{E}_{\mathbf{K_1},\ldots,\mathbf{K_{10}}}(\mathbf{a}) = \mathbf{X}[\mathbf{k_{10}}]\mathbf{LSX}[\mathbf{K_9}]\ldots\mathbf{LSX}[\mathbf{K_2}]\mathbf{LSX}[\mathbf{K_1}](\mathbf{a}),$$

где $a \in V_{128}$.

Упрощенная версия Кузнечика

В данной модификации ключевое расписание использует лишь 2 раунда сети Фейстеля при выработке нового раундового ключа, т.е. $(K_3, K_4) = F[C_2]F[C_1](K_1, K_2)$. Кроме того, количество раундов шифрования снижено до 4.

$$K_3 = K_1 \oplus LSX[C_2](K_2 \oplus LSX[C_1](K_1))$$
$$K_4 = K_2 \oplus LSX[C_1](K_1)$$
$$\hat{E}_{K_1,K_2}(m) = X[K_4]LSX[K_3]LSX[K_2]LSX[K_1](m)$$

Необходимые обозначения

Обозначим за $F_i(\delta)$ вектор $L(\delta \lll 8i)$, где $\delta \in V_8$. Таким образом, поскольку L линейное,
$\forall x \in V_{128} : L(x \oplus (0 \dots 0, \underbrace{\delta}_{i}, 0 \dots 0)) = L(x) \oplus F_i(\delta)$

Через A^i обозначим i-ый 8-битный блок $A \in V_{128}$. Таким образом, $A = (A^{15}, \dots, A^0)$

Атака, позволяющая восстановить $K_1^l, l = \overline{0, 15}$:

1. Выбираем открытый текст $m = C_1$
2. Для всех возможных $k = \overline{0, 255}$:
   2.1 Выбираем 2 пары связанных ключей:
   $(K_1, K_2), (\mathbf{K'_{1,l}}, \mathbf{K''_{j,l}}) = (\mathbf{K_1} \oplus \mathbf{1} \lll \mathbf{8l}, \mathbf{K_2} \oplus \mathbf{F_l(j)})$, где j таково, что $\pi(k \oplus C_1^l) \oplus \pi(k \oplus C_1^l \oplus 1) = j$ и
   $(K_1, K_2), (\mathbf{K'_{6,l}}, \mathbf{K''_{\hat{j},l}}) = (\mathbf{K_1} \oplus \mathbf{6} \lll \mathbf{8l}, \mathbf{K_2} \oplus \mathbf{F_l(\hat{j})})$, где $\hat{j}$ таково, что $\pi(k \oplus C_1^l) \oplus \pi(k \oplus C_1^l \oplus 6) = \hat{j}$
   2.2 Если $L^{-1}(\hat{E}_{K_1,K_2}(m) \oplus \hat{E}_{K'_{1,l},K''_{j,l}}(m)) = (0, \ldots, 0, \underbrace{a}_{l}, 0, \ldots, 0)$
   и
   $L^{-1}(\hat{E}_{K_1,K_2}(m) \oplus \hat{E}_{K'_{6,l},K''_{\hat{j},l}}(m)) = (0, \ldots, 0, \underbrace{b}_{l}, 0, \ldots, 0)$ для некоторых $a, b \in V_8$, то записываем в память данный k. Если нашлось несколько k, для которых этот пункт выполнен, сохраняем их в массив возможных значений.
3. Присвоить K_1^l значение k (если подходящих значений несколько, создать копию разгаданной части ключа для каждого варианта).

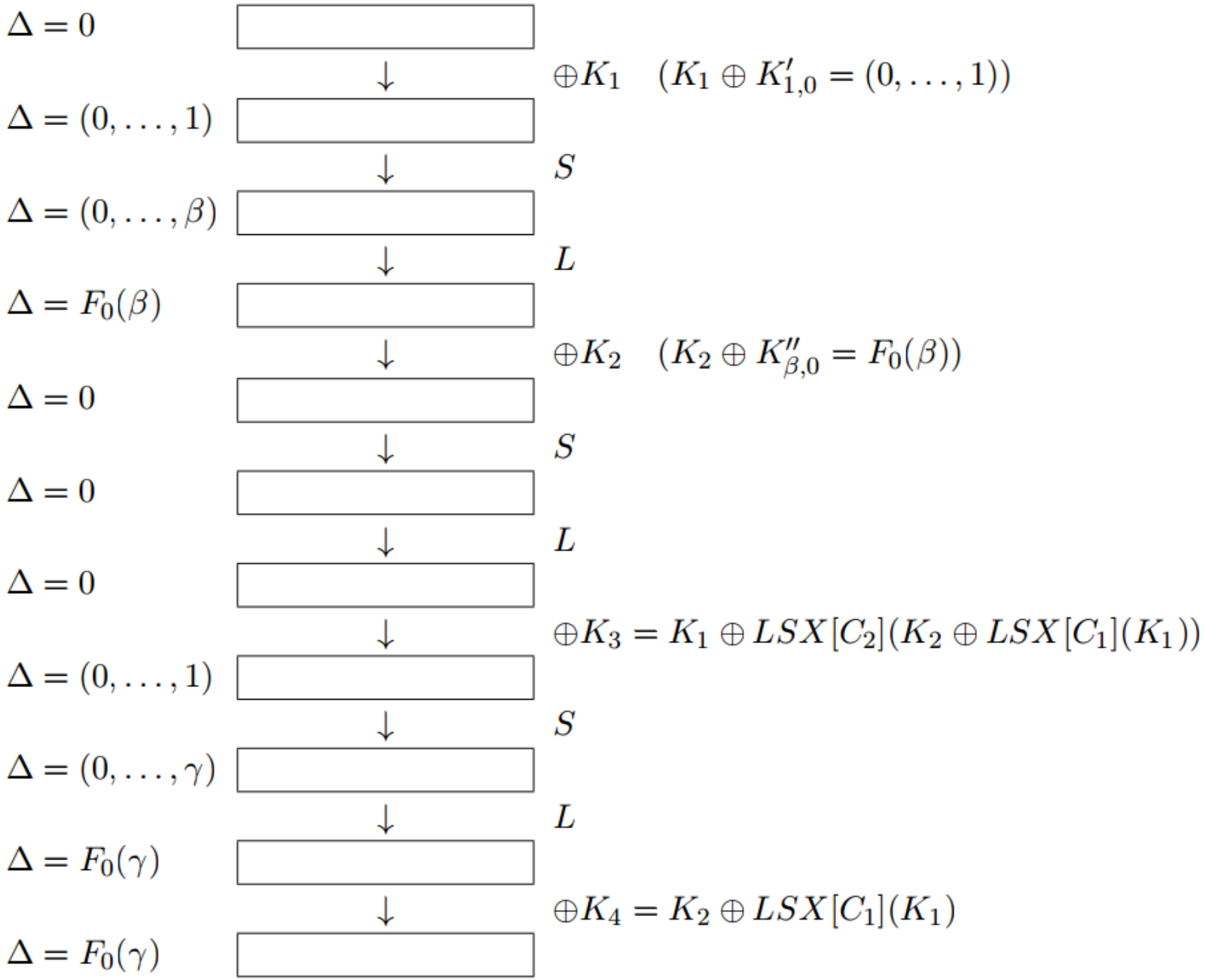
Атака, позволяющая восстановить K_2 при известном K_1:

1. Выбираем открытый текст
   $m = (C_1^{15}, C_1^{14}, \ldots, C_1^2, C_1^1, \pi^{-1}(\pi(C_1^0 \oplus K_1^0) \oplus 2) \oplus K_1^0)$
2. $K_2 = \hat{E}_{K_1,K_2}(m) \oplus LSX[C_1](K_1) \oplus LS(K_1)$

Обоснование первой атаки

Для примера рассмотрим часть атаки на K_1^0: пусть $C_1^0 \oplus K_1^0 = \alpha$, и $\pi(\alpha) \oplus \pi(\alpha \oplus 1) = \beta$

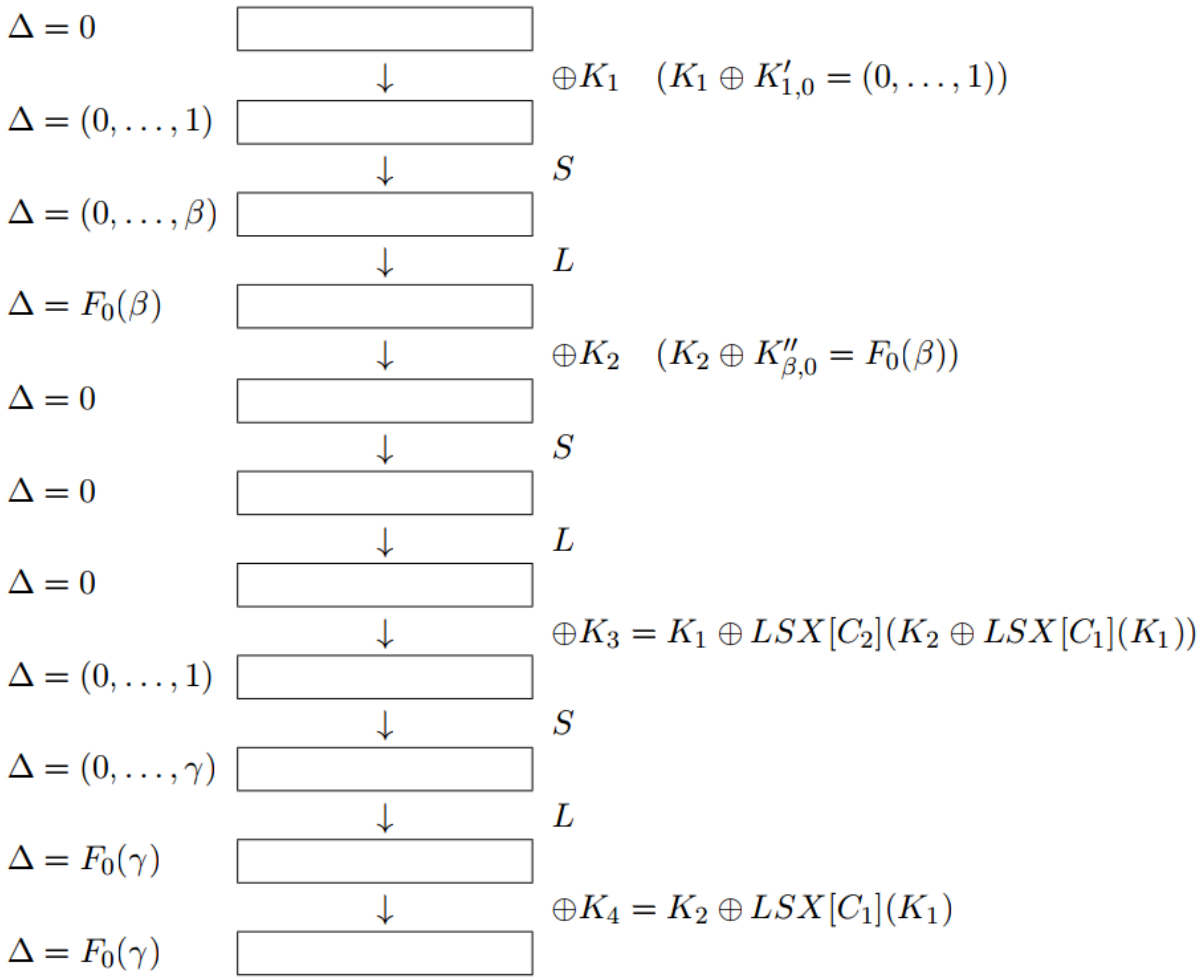
Рис. 1 демонстрирует работу $\hat{E}$ для пары ключей $(K'_{1,0}, K''_{\beta,0})$. Δ обозначает разность внутренних состояний для двух процедур шифрования.


$\Delta = 0$
$\oplus K_1 \quad (K_1 \oplus K'_{1,0} = (0, \ldots, 1))$
$\Delta = (0, \ldots, 1)$
S
$\Delta = (0, \ldots, \beta)$
L
$\Delta = F_0(\beta)$
$\oplus K_2 \quad (K_2 \oplus K''_{\beta,0} = F_0(\beta))$
$\Delta = 0$
S
$\Delta = 0$
L
$\Delta = 0$
$\oplus K_3 = K_1 \oplus LSX[C_2](K_2 \oplus LSX[C_1](K_1))$
$\Delta = (0, \ldots, 1)$
S
$\Delta = (0, \ldots, \gamma)$
L
$\Delta = F_0(\gamma)$
$\oplus K_4 = K_2 \oplus LSX[C_1](K_1)$
$\Delta = F_0(\gamma)$

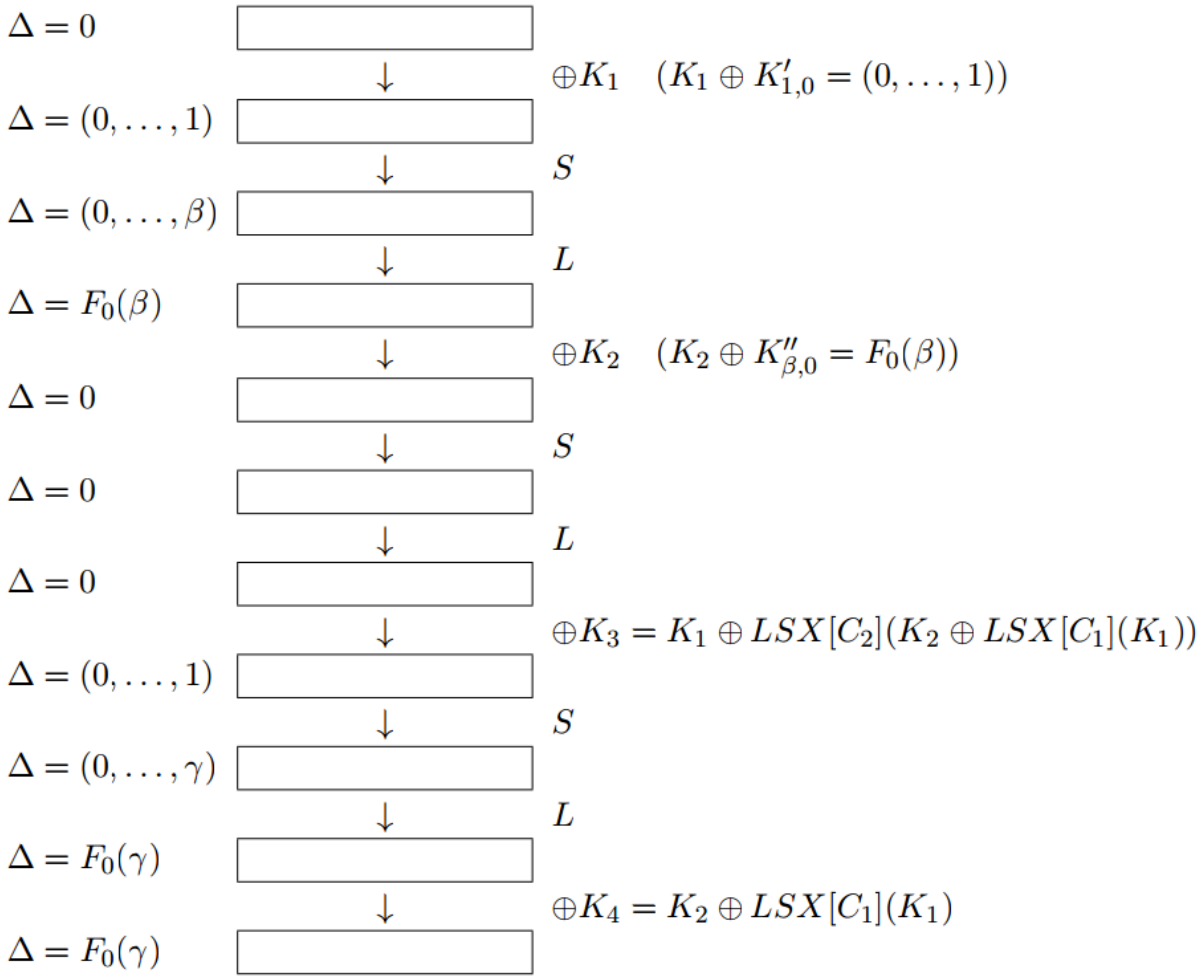
1. Выбираем открытый текст $m = C_1$
2. Для всех возможных $k = \overline{0, 255}$:
   - 2.1 Выбираем 2 пары связанных ключей:
     $(K_1, K_2), (\mathbf{K'_{1,0}}, \mathbf{K''_{j,0}}) = (\mathbf{K_1} \oplus \mathbf{1}, \mathbf{K_2} + \mathbf{F_0(j)})$, где j таково, что $\pi(k \oplus C_1^0) \oplus \pi(k \oplus C_1^0 \oplus 1) = j$ и
     $(K_1, K_2), (\mathbf{K'_{6,0}}, \mathbf{K''_{\hat{j},0}}) = (\mathbf{K_1} \oplus \mathbf{6}, \mathbf{K_2} + \mathbf{F_0(\hat{j})})$, где $\hat{j}$ таково, что $\pi(k \oplus C_1^0) \oplus \pi(k \oplus C_1^0 \oplus 6) = \hat{j}$
   - 2.2 Если $L^{-1}(\hat{E}_{K_1,K_2}(m) \oplus \hat{E}_{K'_{1,0},K''_{j,0}}(m)) = (0, \ldots, 0, a)$ и $L^{-1}(\hat{E}_{K_1,K_2}(m) \oplus \hat{E}_{K'_{6,0},K''_{\hat{j},0}}(m)) = (0, \ldots, 0, b)$ для некоторых $a, b \in V_8$, то отмечаем данный k.
3. Присвоить K_1^0 значение k

$$K_3 = K_1 \oplus LSX[C_2](K_2 \oplus LSX[C_1](K_1))$$
$$K_4 = K_2 \oplus LSX[C_1](K_1)$$
$$\hat{E}_{K_1,K_2}(m) = X[K_4]LSX[K_3]LSX[K_2]LSX[K_1](m)$$

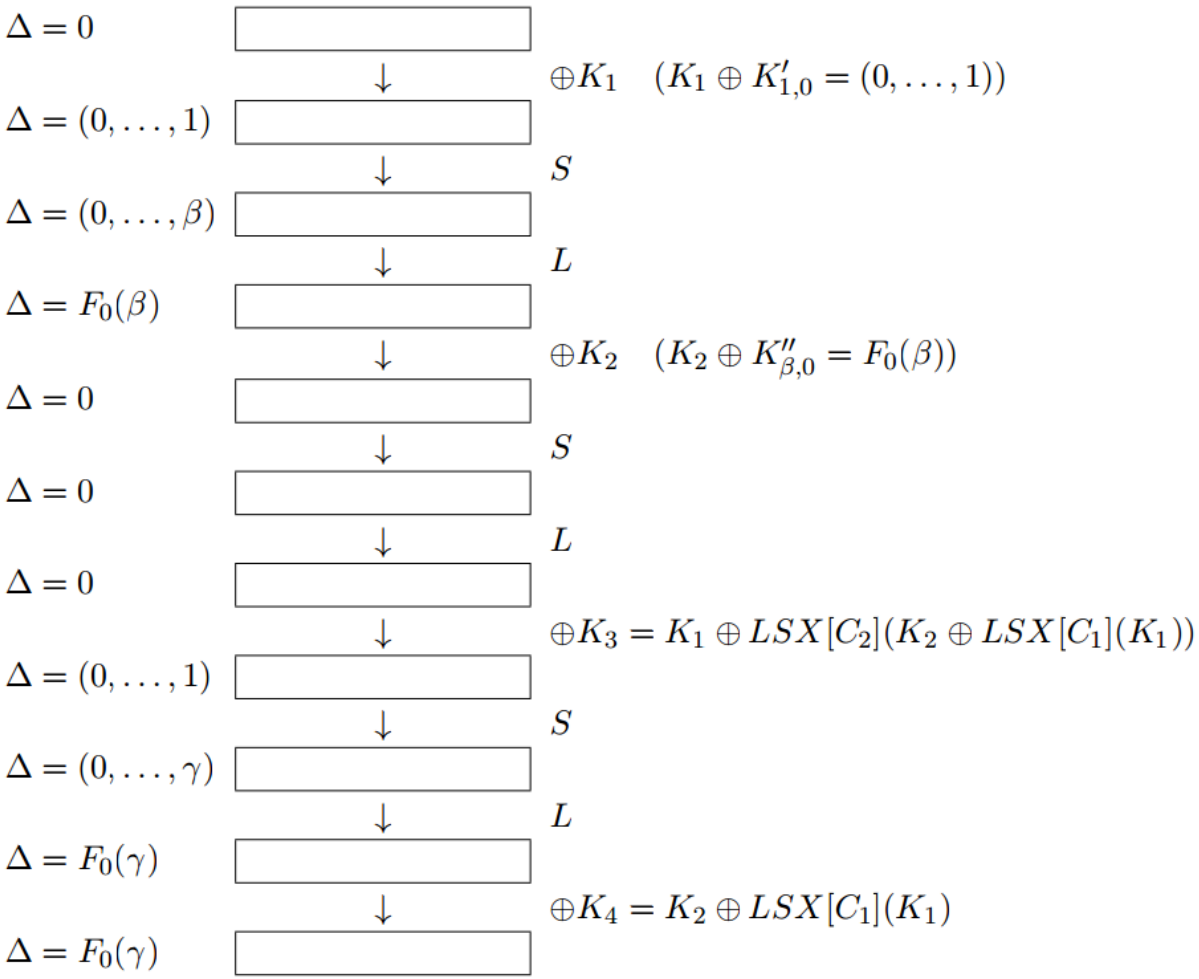
0. На вход подаются одинаковые открытые тексты m, поэтому изначально внутренние состояния идентичны ($\Delta = 0$).



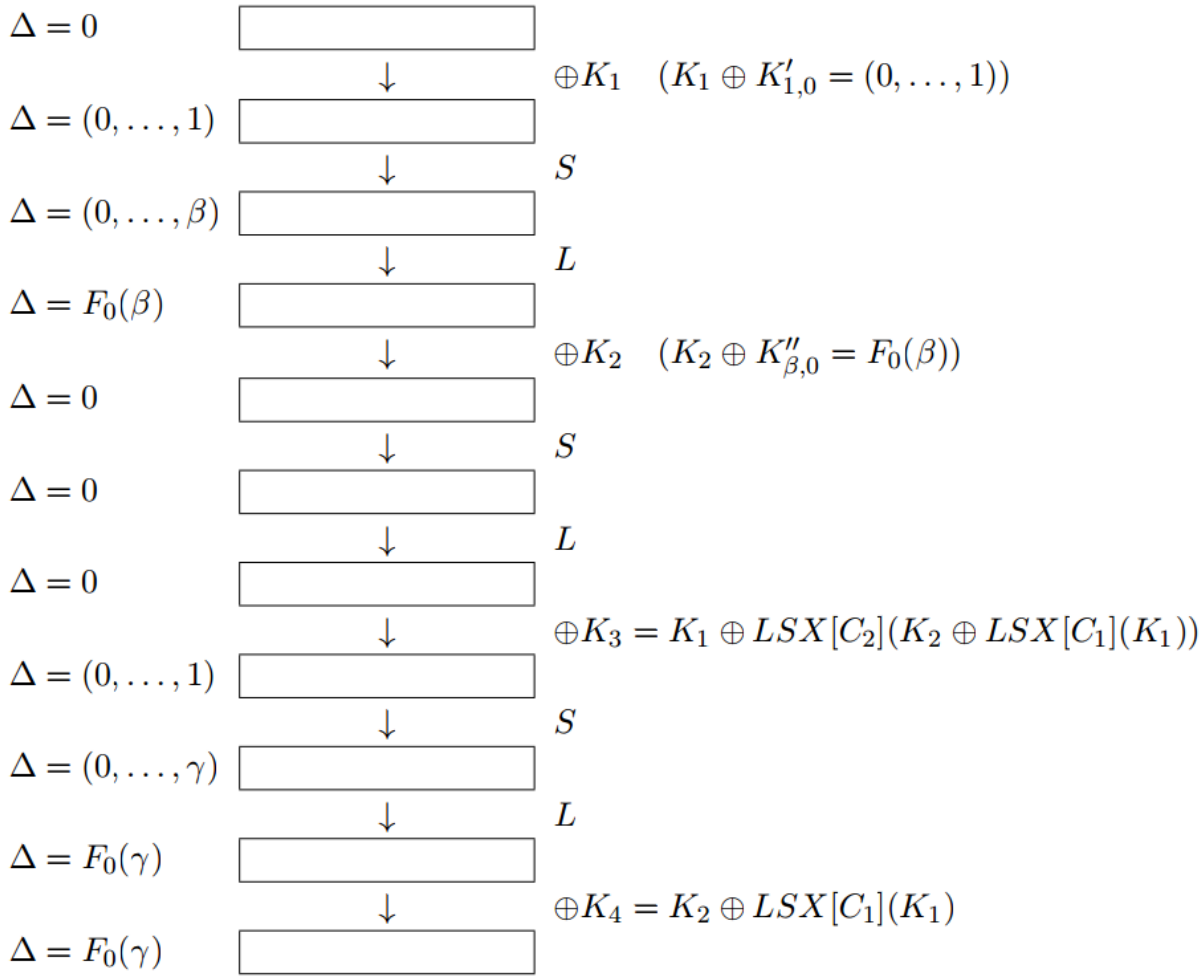
1. После побитово го сложения с первым раундовым ключом $\Delta = K_1 \oplus K'_{1,0} = (0, \ldots, 1)$.



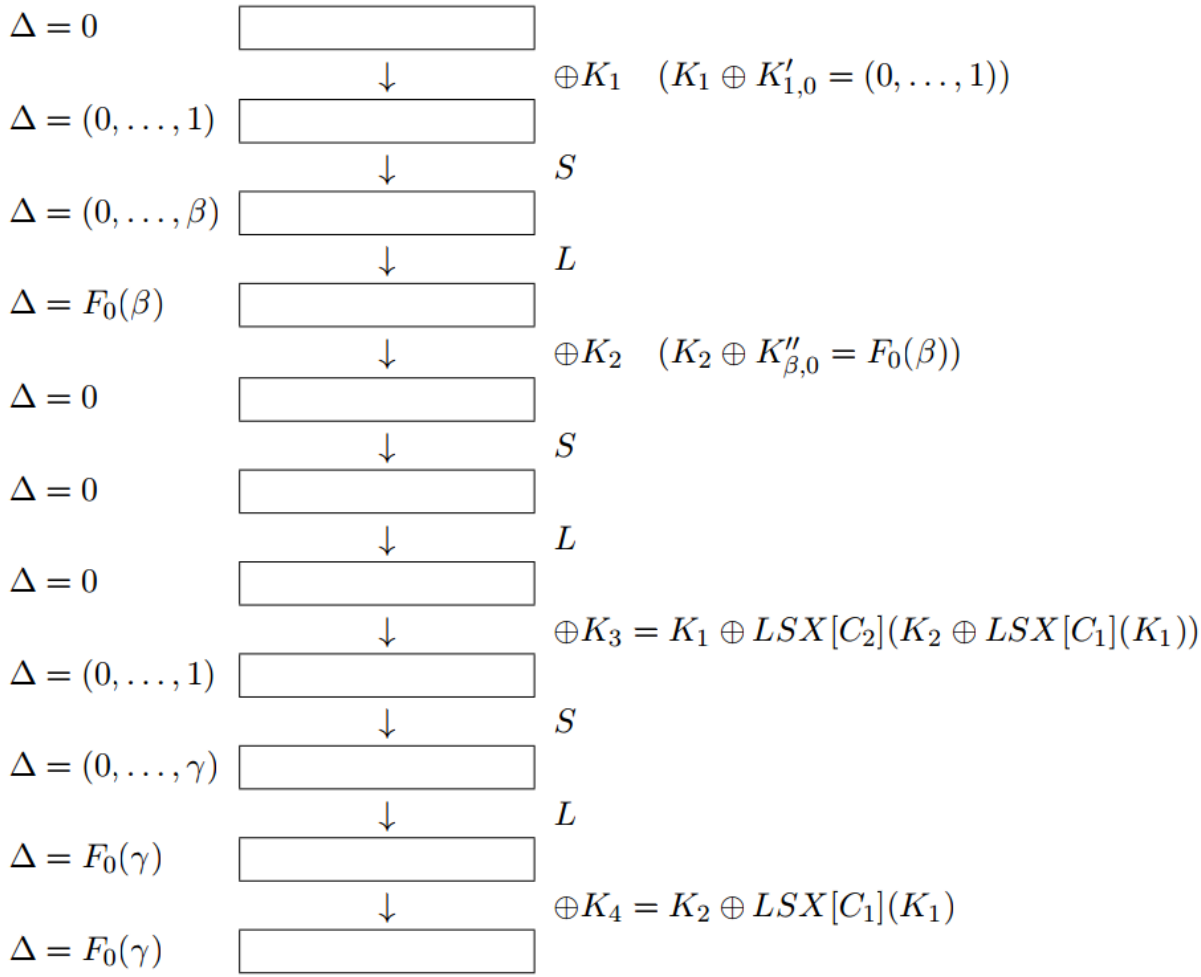
2.


$\Delta = 0$
$\oplus K_1 \quad (K_1 \oplus K'_{1,0} = (0, \ldots, 1))$
$\Delta = (0, \ldots, 1)$
S
$\Delta = (0, \ldots, \beta)$
L
$\Delta = F_0(\beta)$
$\oplus K_2 \quad (K_2 \oplus K''_{\beta,0} = F_0(\beta))$
$\Delta = 0$
S
$\Delta = 0$
L
$\Delta = 0$
$\oplus K_3 = K_1 \oplus LSX[C_2](K_2 \oplus LSX[C_1](K_1))$
$\Delta = (0, \ldots, 1)$
S
$\Delta = (0, \ldots, \gamma)$
L
$\Delta = F_0(\gamma)$
$\oplus K_4 = K_2 \oplus LSX[C_1](K_1)$
$\Delta = F_0(\gamma)$

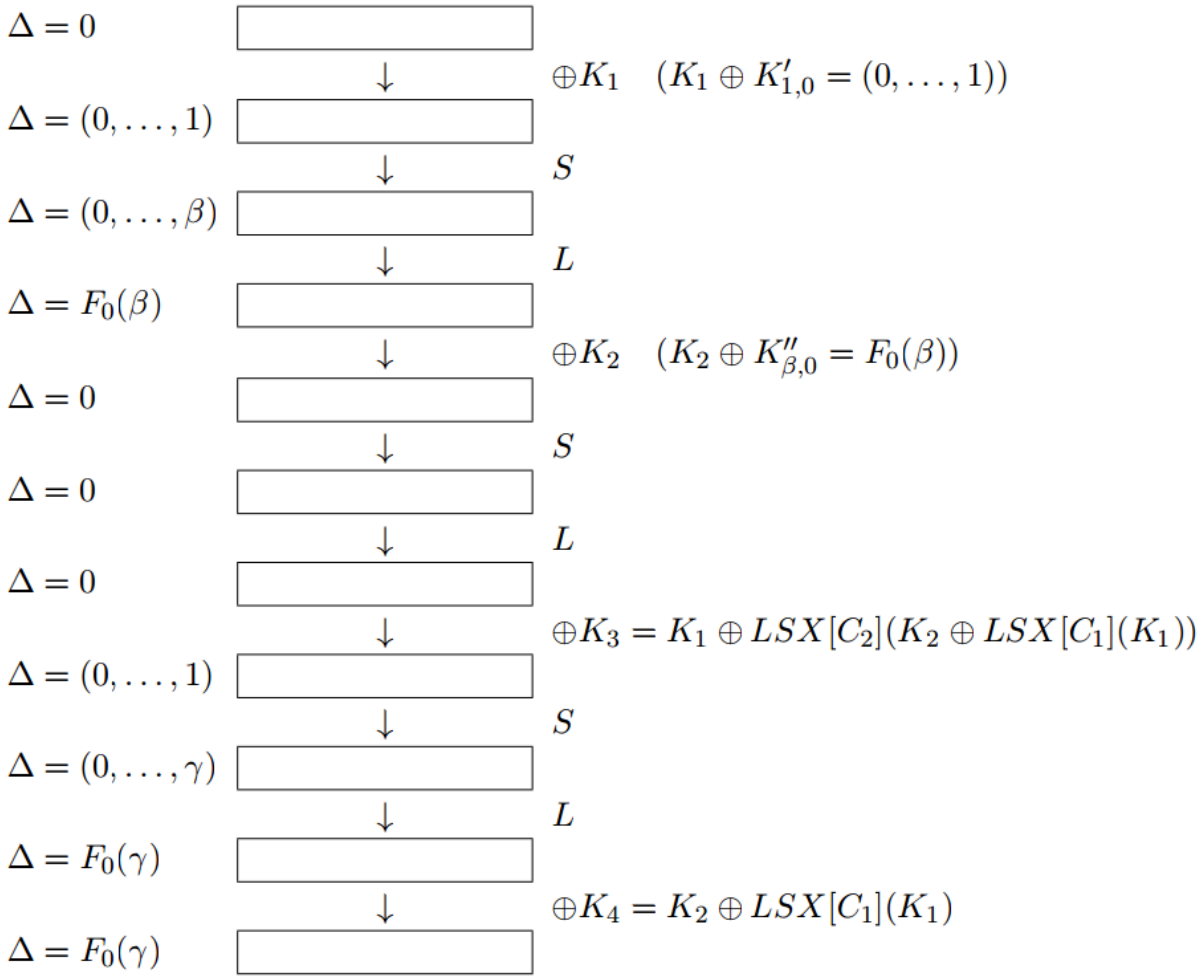
3. После линейного преобразования ненулевая разность последнего блока спровоцирует потенциально ненулевые разности в остальных блоках: $\Delta = F_0(\beta)$



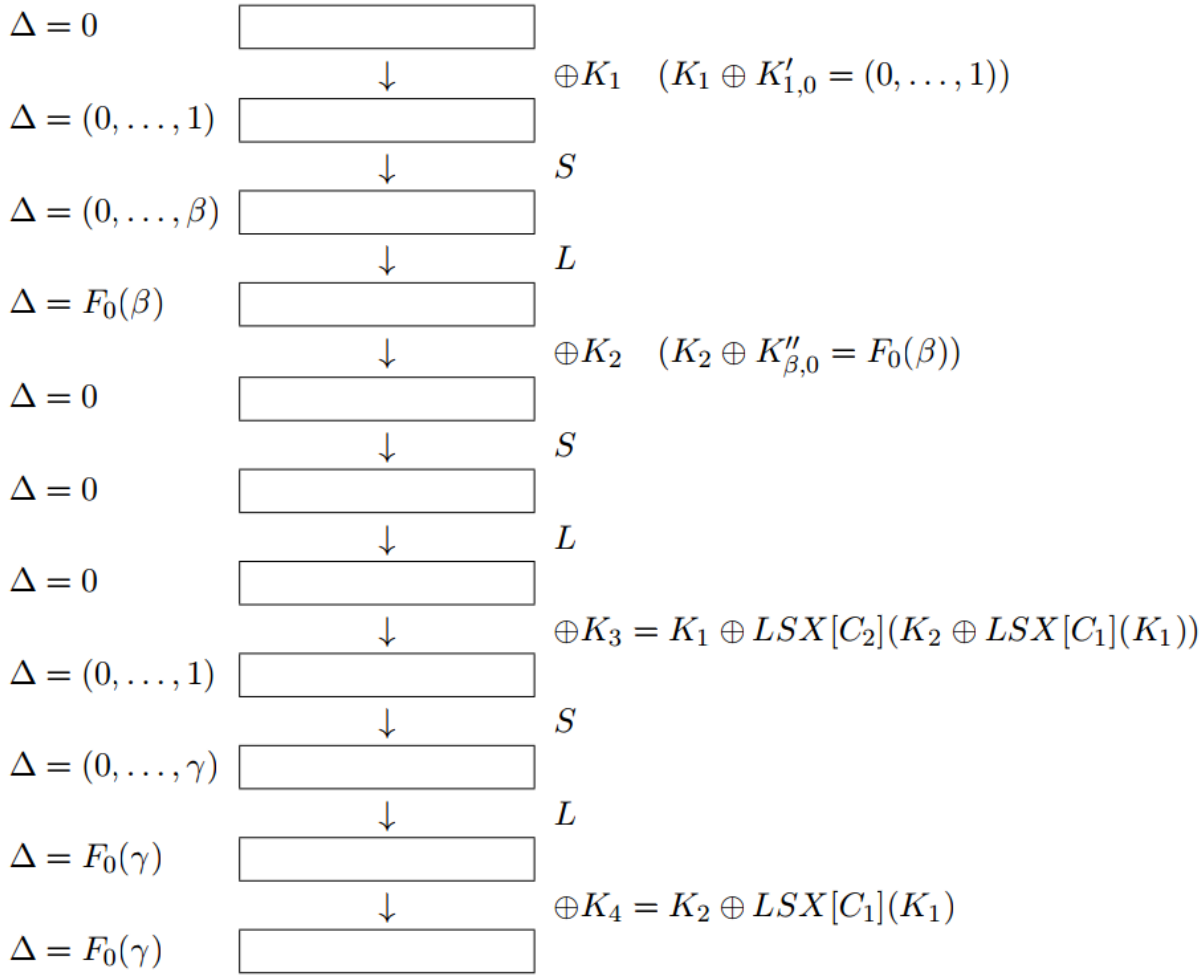
4. $K_2 \oplus K''_{\beta,0} = F_0(\beta)$, следовательно произошла локальная коллизия, и после побитового сложения со вторым раундовым ключом внутренние состояния стали идентичны. Таким образом, после побитового сложения со вторым раундовым ключом $\Delta = 0$



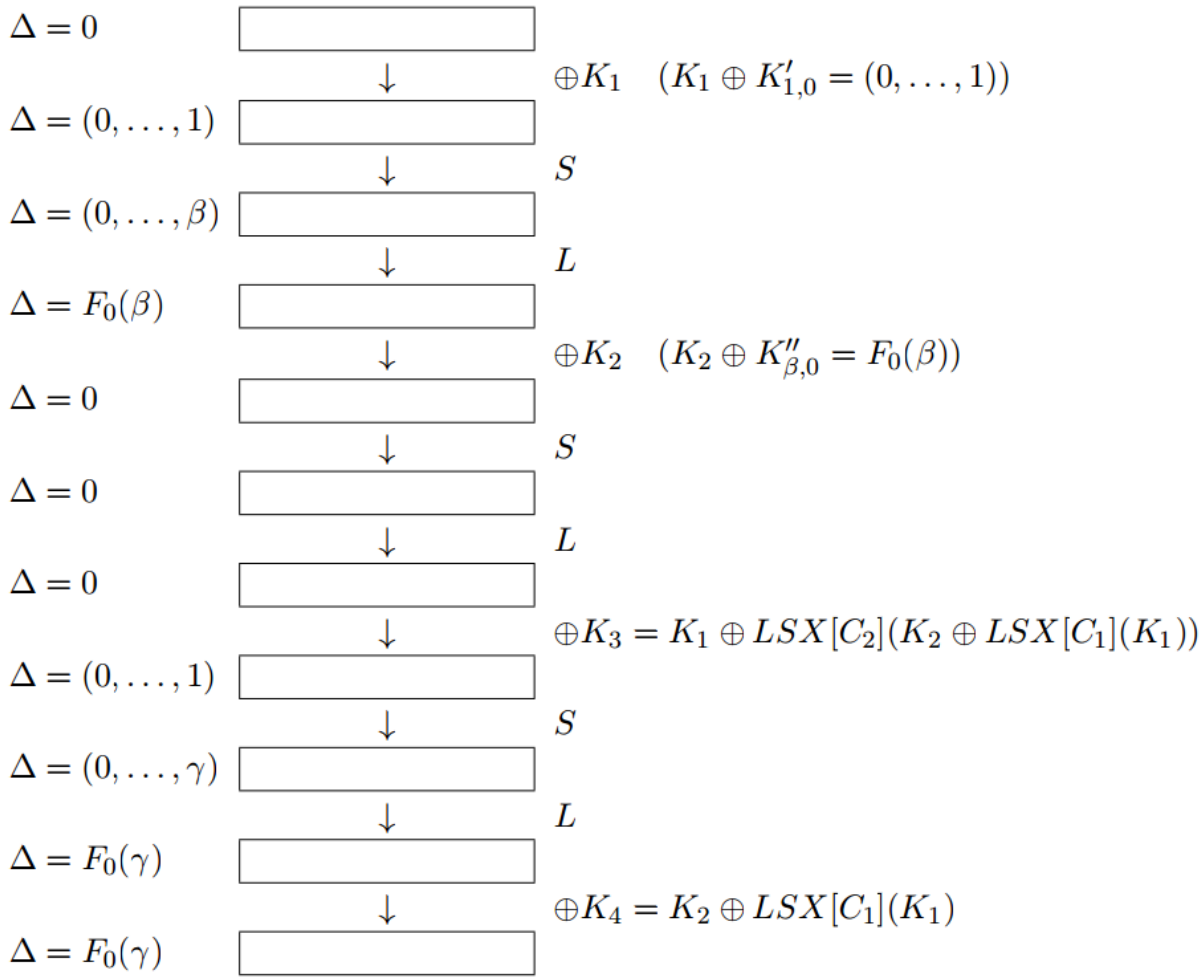
5. После нелинейного преобразования, в котором все S-блоки будут неактивны $\Delta = 0$



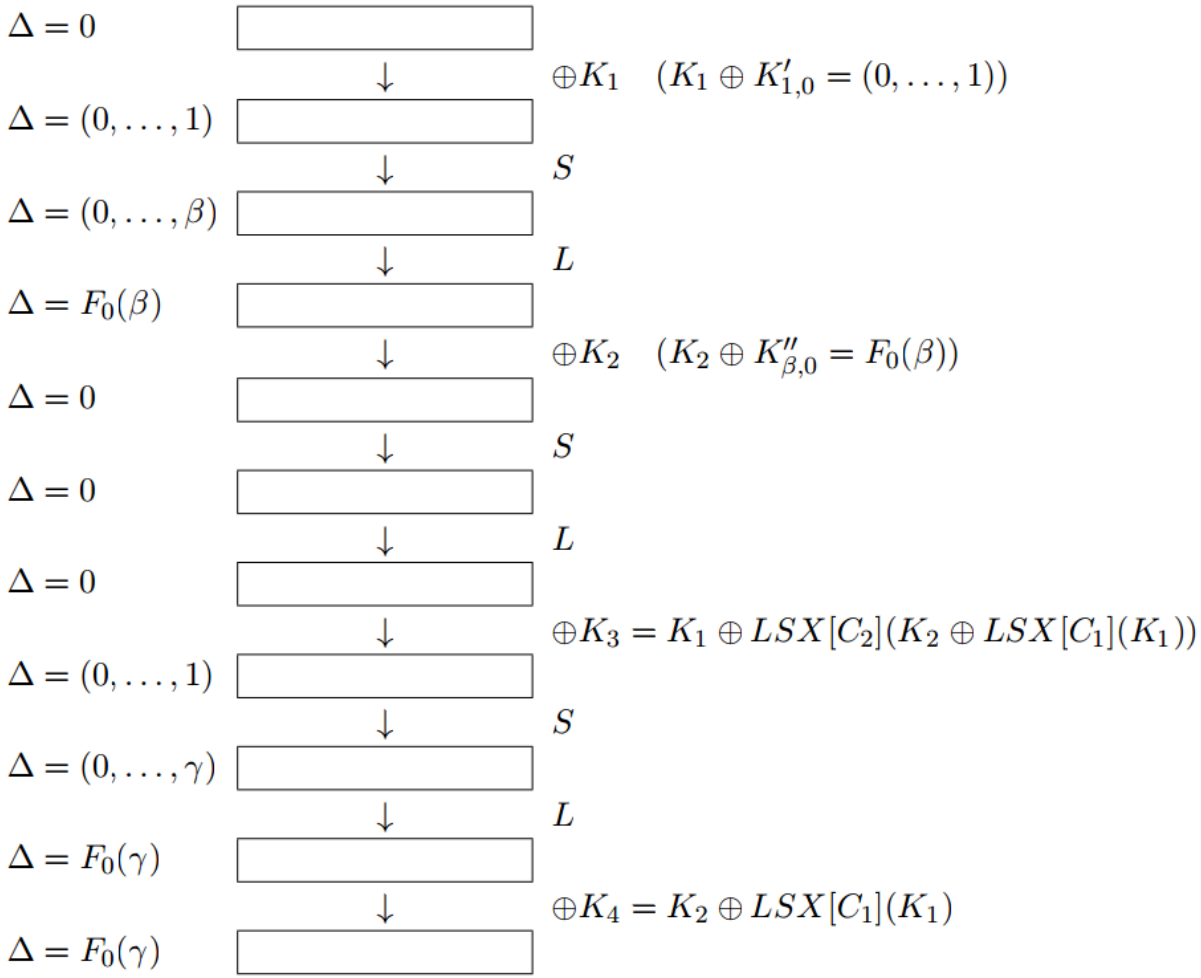
6. После линейного преобразования $\Delta = 0$



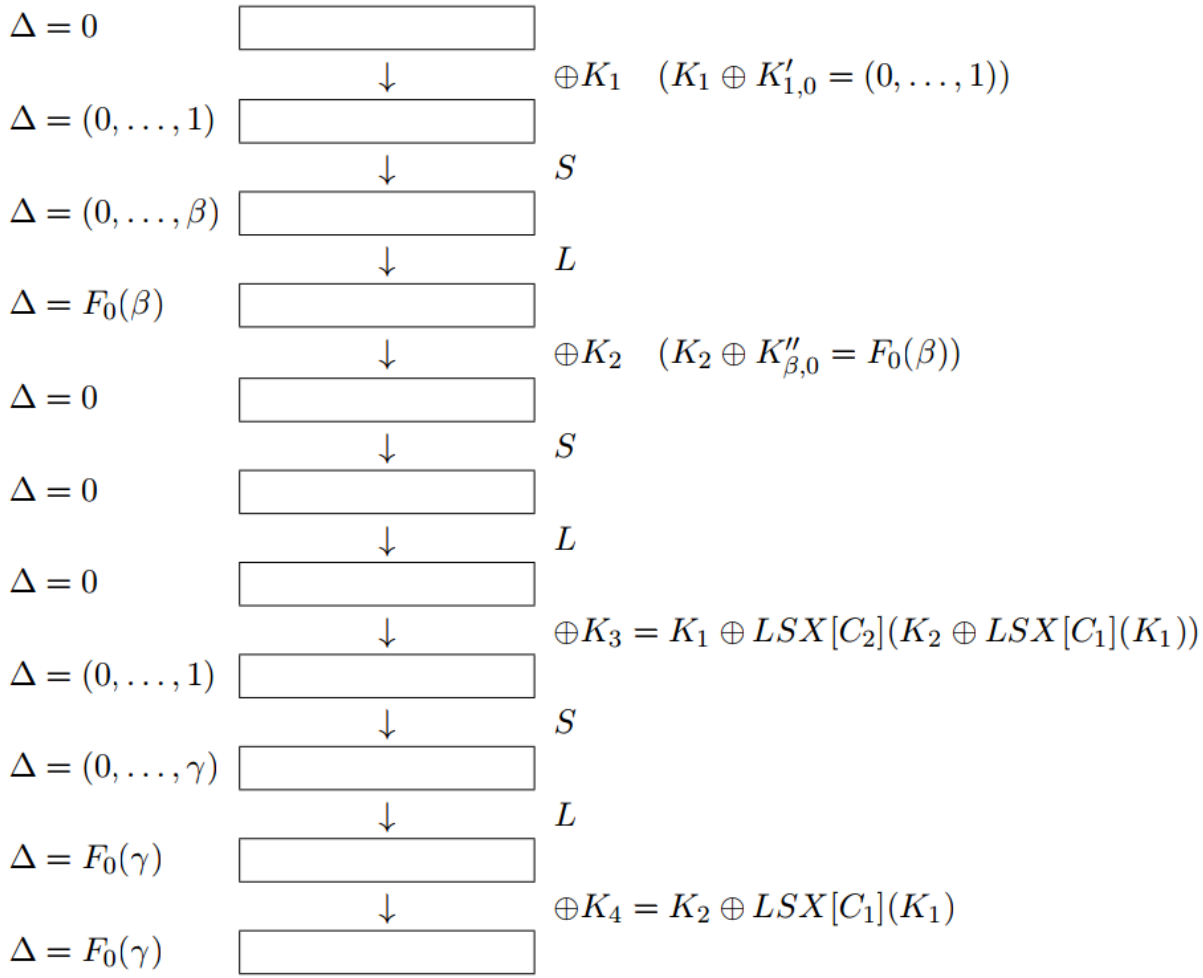
7. Поскольку $K_2 \oplus LSX[C_1](K_1) = K''_{\beta,0} \oplus LSX[C_1](K'_{1,0})$, $LSX[C_2](K_2 \oplus LSX[C_1](K_1)) = LSX[C_2](K''_{\beta,0} \oplus LSX[C_1](K'_{1,0}))$, и после следующего шага побитового сложения с ключом $\Delta = K_1 \oplus K'_{1,0} = (0, \ldots, 1)$



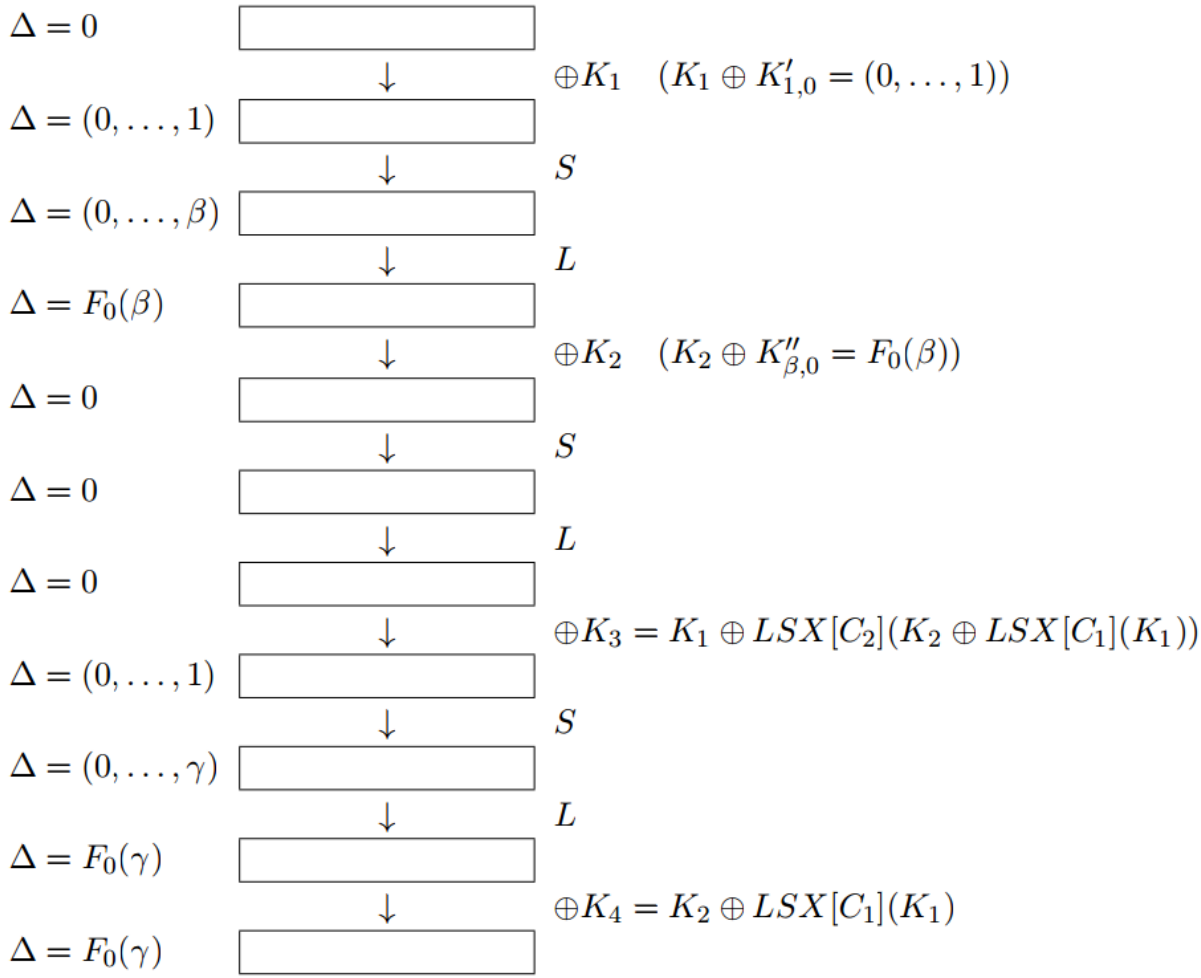
8. На следующем шаге получается лишь один активный S-блок (чем мы пользуемся на стадии различителя), и Δ переходит в неизвестную разность $(0, \ldots, \gamma)$



9. После $L\ \Delta = F_0(\gamma)$



10. $K_2 \oplus LSX[C_1](K_1) = K''_{\beta,0} \oplus LSX[C_1](K'_{1,0})$, поэтому после финального шага разность состояний (шифртекстов) Δ остается равной $F_0(\gamma)$



Различитель

Для описанных выше ключей разность шифртекстов получается равной $F_0(\gamma)$.
Пусть γ нам и не известен, однако, мы знаем, что все блоки $L^{-1}(F_0(\gamma))$, кроме нулевого, равны 0.

Заметим, однако, что если бы мы использовали только одну пару связанных ключей в шаге 2.а), то шаг различителя прошли бы все такие x, для которых $\pi(x) \oplus \pi(x \oplus 1) = \beta$.
Было экспериментально проверено, что пара $\pi(x) \oplus \pi(x \oplus 1)$, $\pi(x) \oplus \pi(x \oplus 6)$ является уникальной для всех $x = 0, 1, \ldots, 255$, т.е. не существует таких $0 \leq x < y \leq 255$, что $\pi(x) \oplus \pi(x \oplus 1) = \pi(y) \oplus \pi(y \oplus 1)$ и $\pi(x) \oplus \pi(x \oplus 6) = \pi(y) \oplus \pi(y \oplus 6)$.

Для остальных пар связанных ключей, если мы хотим определить вероятность ошибки первого рода, шифр можно рассматривать как случайную перестановку на V_{128}. При таком допущении вероятность, что для какой-то другой пары связанных ключей результат будет удовлетворять условию различителя, ограничена сверху $2^{-128} \cdot 2^8 = 2^{-120}$.

Аналогичные рассуждения верны для $l = \overline{1, 15}$
Матожидание количества дополнительных кандидатов K_1 равно $(1 + 2^{-120})^{16} - 1 \approx 2^{-116}$, так что в дальнейшем мы без существенной потери точности будем считать, что K_1 был найден единственным образом.

Атакуем K_2 при известном K_1:

1. Выбираем открытый текст
   $m = (C_1^{15}, C_1^{14}, \ldots, C_1^2, C_1^1, \pi^{-1}(\pi(C_1^0 \oplus K_1^0) \oplus 2) \oplus K_1^0)$
2. $K_2 = \hat{E}_{K_1,K_2}(m) \oplus LSX[C_1](K_1) \oplus LS(K_1)$

$$
\begin{array}{|c|l}
\hline
(C_1^{15}, C_1^{14}, \ldots, C_1^2, C_1^1, \pi^{-1}(\pi(C_1^0 \oplus K_1^0) \oplus 2) \oplus K_1^0) & \\
\hline
\downarrow & \oplus K_1 \\
\hline
(C_1^{15} \oplus K_1^{15}, \ldots, C_1^1 \oplus K_1^1, \pi^{-1}(\pi(C_1^0 \oplus K_1^0) \oplus 2)) & \\
\hline
\downarrow & S \\
\hline
SX[C_1](K_1) \oplus (0, \ldots, 0, 2) & \\
\hline
\downarrow & L \\
\hline
LSX[C_1](K_1) \oplus C_2 & \\
\hline
\downarrow & \oplus K_2 \\
\hline
X[C_2](K_2 \oplus LSX[C_1](K_1)) & \\
\hline
\downarrow & S \\
\hline
SX[C_2](K_2 \oplus LSX[C_1](K_1)) & \\
\hline
\downarrow & L \\
\hline
LSX[C_2](K_2 \oplus LSX[C_1](K_1)) & \\
\hline
\downarrow & \oplus K_3 = K_1 \oplus LSX[C_2](K_2 \oplus LSX[C_1](K_1)) \\
\hline
K_1 & \\
\hline
\downarrow & S \\
\hline
S(K_1) & \\
\hline
\downarrow & L \\
\hline
LS(K_1) & \\
\hline
\downarrow & \oplus K_4 = K_2 \oplus LSX[C_1](K_1) \\
\hline
K_2 \oplus LS(K_1) \oplus LSX[C_1](K_1) & \\
\hline
\end{array}
$$

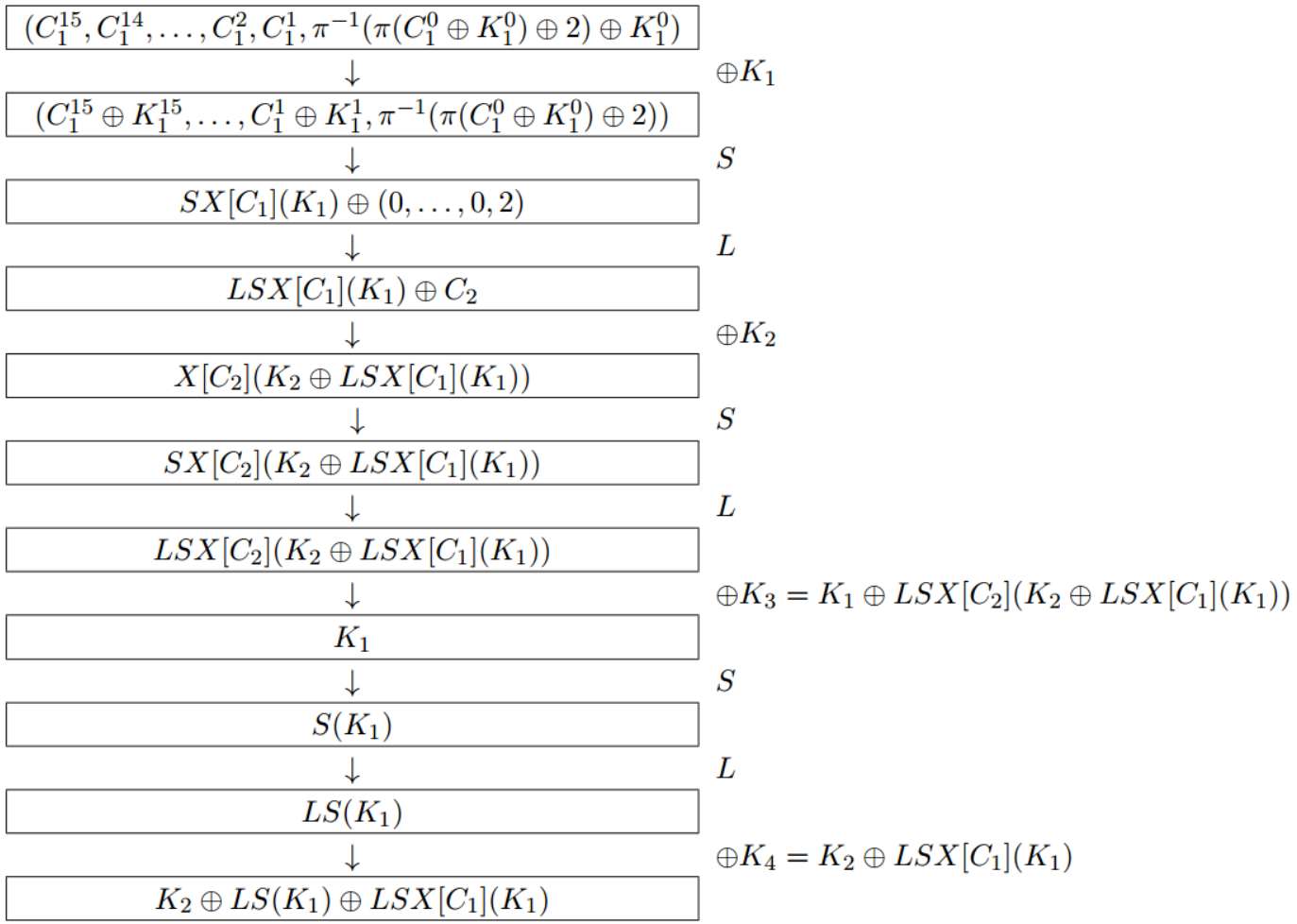
0. На вход подается
$m = (C_1^{15}, C_1^{14}, \ldots, C_1^2, C_1^1, \pi^{-1}(\pi(C_1^0 \oplus K_1^0) \oplus 2) \oplus K_1^0)$

$$
\begin{array}{|c|l}
\hline
(C_1^{15}, C_1^{14}, \ldots, C_1^2, C_1^1, \pi^{-1}(\pi(C_1^0 \oplus K_1^0) \oplus 2) \oplus K_1^0) & \\
\hline
\downarrow & \oplus K_1 \\
\hline
(C_1^{15} \oplus K_1^{15}, \ldots, C_1^1 \oplus K_1^1, \pi^{-1}(\pi(C_1^0 \oplus K_1^0) \oplus 2)) & \\
\hline
\downarrow & S \\
\hline
SX[C_1](K_1) \oplus (0, \ldots, 0, 2) & \\
\hline
\downarrow & L \\
\hline
LSX[C_1](K_1) \oplus C_2 & \\
\hline
\downarrow & \oplus K_2 \\
\hline
X[C_2](K_2 \oplus LSX[C_1](K_1)) & \\
\hline
\downarrow & S \\
\hline
SX[C_2](K_2 \oplus LSX[C_1](K_1)) & \\
\hline
\downarrow & L \\
\hline
LSX[C_2](K_2 \oplus LSX[C_1](K_1)) & \\
\hline
\downarrow & \oplus K_3 = K_1 \oplus LSX[C_2](K_2 \oplus LSX[C_1](K_1)) \\
\hline
K_1 & \\
\hline
\downarrow & S \\
\hline
S(K_1) & \\
\hline
\downarrow & L \\
\hline
LS(K_1) & \\
\hline
\downarrow & \oplus K_4 = K_2 \oplus LSX[C_1](K_1) \\
\hline
K_2 \oplus LS(K_1) \oplus LSX[C_1](K_1) & \\
\hline
\end{array}
$$

1. $State := m \oplus K_1 = (C_1^{15} \oplus K_1^{15}, \ldots, C_1^1 \oplus K_1^1, \pi^{-1}(\pi(C_1^0 \oplus K_1^0) \oplus 2))$

$$
\begin{array}{|c|l}
\hline
(C_1^{15}, C_1^{14}, \ldots, C_1^2, C_1^1, \pi^{-1}(\pi(C_1^0 \oplus K_1^0) \oplus 2) \oplus K_1^0) & \\
\hline
\downarrow & \oplus K_1 \\
\hline
(C_1^{15} \oplus K_1^{15}, \ldots, C_1^1 \oplus K_1^1, \pi^{-1}(\pi(C_1^0 \oplus K_1^0) \oplus 2)) & \\
\hline
\downarrow & S \\
\hline
SX[C_1](K_1) \oplus (0, \ldots, 0, 2) & \\
\hline
\downarrow & L \\
\hline
LSX[C_1](K_1) \oplus C_2 & \\
\hline
\downarrow & \oplus K_2 \\
\hline
X[C_2](K_2 \oplus LSX[C_1](K_1)) & \\
\hline
\downarrow & S \\
\hline
SX[C_2](K_2 \oplus LSX[C_1](K_1)) & \\
\hline
\downarrow & L \\
\hline
LSX[C_2](K_2 \oplus LSX[C_1](K_1)) & \\
\hline
\downarrow & \oplus K_3 = K_1 \oplus LSX[C_2](K_2 \oplus LSX[C_1](K_1)) \\
\hline
K_1 & \\
\hline
\downarrow & S \\
\hline
S(K_1) & \\
\hline
\downarrow & L \\
\hline
LS(K_1) & \\
\hline
\downarrow & \oplus K_4 = K_2 \oplus LSX[C_1](K_1) \\
\hline
K_2 \oplus LS(K_1) \oplus LSX[C_1](K_1) & \\
\hline
\end{array}
$$

2. $State := \pi(State) = (\pi(C_1^{15} \oplus K_1^{15}), \ldots, \pi(C_1^1 \oplus K_1^1), \pi(C_1^0 \oplus K_1^0) \oplus 2) = SX[C_1](K_1) \oplus (0, \ldots, 0, 2)$



3. $State := L(State) = LSX[C_1](K_1) \oplus C_2$

$$
\begin{array}{|c|l}
\hline
(C_1^{15}, C_1^{14}, \ldots, C_1^2, C_1^1, \pi^{-1}(\pi(C_1^0 \oplus K_1^0) \oplus 2) \oplus K_1^0) & \\
\hline
\downarrow & \oplus K_1 \\
\hline
(C_1^{15} \oplus K_1^{15}, \ldots, C_1^1 \oplus K_1^1, \pi^{-1}(\pi(C_1^0 \oplus K_1^0) \oplus 2)) & \\
\hline
\downarrow & S \\
\hline
SX[C_1](K_1) \oplus (0, \ldots, 0, 2) & \\
\hline
\downarrow & L \\
\hline
LSX[C_1](K_1) \oplus C_2 & \\
\hline
\downarrow & \oplus K_2 \\
\hline
X[C_2](K_2 \oplus LSX[C_1](K_1)) & \\
\hline
\downarrow & S \\
\hline
SX[C_2](K_2 \oplus LSX[C_1](K_1)) & \\
\hline
\downarrow & L \\
\hline
LSX[C_2](K_2 \oplus LSX[C_1](K_1)) & \\
\hline
\downarrow & \oplus K_3 = K_1 \oplus LSX[C_2](K_2 \oplus LSX[C_1](K_1)) \\
\hline
K_1 & \\
\hline
\downarrow & S \\
\hline
S(K_1) & \\
\hline
\downarrow & L \\
\hline
LS(K_1) & \\
\hline
\downarrow & \oplus K_4 = K_2 \oplus LSX[C_1](K_1) \\
\hline
K_2 \oplus LS(K_1) \oplus LSX[C_1](K_1) & \\
\hline
\end{array}
$$

4. $State := State \oplus K_2 = X[C_2](K_2 \oplus LSX[C_1](K_1))$

$$
\begin{array}{|c|l}
\hline
(C_1^{15}, C_1^{14}, \ldots, C_1^2, C_1^1, \pi^{-1}(\pi(C_1^0 \oplus K_1^0) \oplus 2) \oplus K_1^0) & \\
\hline
\downarrow & \oplus K_1 \\
\hline
(C_1^{15} \oplus K_1^{15}, \ldots, C_1^1 \oplus K_1^1, \pi^{-1}(\pi(C_1^0 \oplus K_1^0) \oplus 2)) & \\
\hline
\downarrow & S \\
\hline
SX[C_1](K_1) \oplus (0, \ldots, 0, 2) & \\
\hline
\downarrow & L \\
\hline
LSX[C_1](K_1) \oplus C_2 & \\
\hline
\downarrow & \oplus K_2 \\
\hline
X[C_2](K_2 \oplus LSX[C_1](K_1)) & \\
\hline
\downarrow & S \\
\hline
SX[C_2](K_2 \oplus LSX[C_1](K_1)) & \\
\hline
\downarrow & L \\
\hline
LSX[C_2](K_2 \oplus LSX[C_1](K_1)) & \\
\hline
\downarrow & \oplus K_3 = K_1 \oplus LSX[C_2](K_2 \oplus LSX[C_1](K_1)) \\
\hline
K_1 & \\
\hline
\downarrow & S \\
\hline
S(K_1) & \\
\hline
\downarrow & L \\
\hline
LS(K_1) & \\
\hline
\downarrow & \oplus K_4 = K_2 \oplus LSX[C_1](K_1) \\
\hline
K_2 \oplus LS(K_1) \oplus LSX[C_1](K_1) & \\
\hline
\end{array}
$$

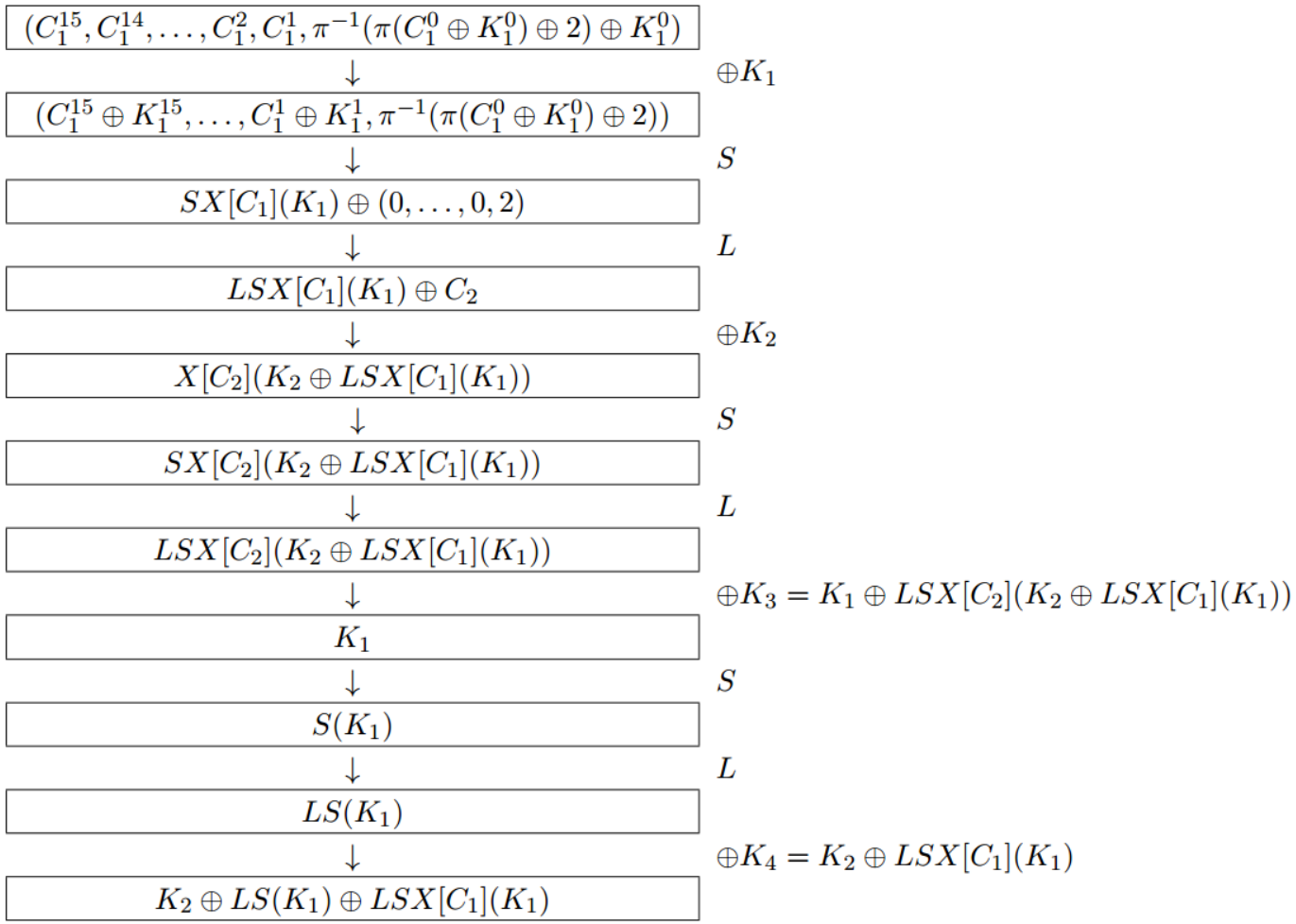
5. $State := S(State) = SX[C_2](K_2 \oplus LSX[C_1](K_1))$

$$
\begin{array}{|c|l}
\hline
(C_1^{15}, C_1^{14}, \ldots, C_1^2, C_1^1, \pi^{-1}(\pi(C_1^0 \oplus K_1^0) \oplus 2) \oplus K_1^0) & \\
\hline
\downarrow & \oplus K_1 \\
\hline
(C_1^{15} \oplus K_1^{15}, \ldots, C_1^1 \oplus K_1^1, \pi^{-1}(\pi(C_1^0 \oplus K_1^0) \oplus 2)) & \\
\hline
\downarrow & S \\
\hline
SX[C_1](K_1) \oplus (0, \ldots, 0, 2) & \\
\hline
\downarrow & L \\
\hline
LSX[C_1](K_1) \oplus C_2 & \\
\hline
\downarrow & \oplus K_2 \\
\hline
X[C_2](K_2 \oplus LSX[C_1](K_1)) & \\
\hline
\downarrow & S \\
\hline
SX[C_2](K_2 \oplus LSX[C_1](K_1)) & \\
\hline
\downarrow & L \\
\hline
LSX[C_2](K_2 \oplus LSX[C_1](K_1)) & \\
\hline
\downarrow & \oplus K_3 = K_1 \oplus LSX[C_2](K_2 \oplus LSX[C_1](K_1)) \\
\hline
K_1 & \\
\hline
\downarrow & S \\
\hline
S(K_1) & \\
\hline
\downarrow & L \\
\hline
LS(K_1) & \\
\hline
\downarrow & \oplus K_4 = K_2 \oplus LSX[C_1](K_1) \\
\hline
K_2 \oplus LS(K_1) \oplus LSX[C_1](K_1) & \\
\hline
\end{array}
$$

6. $State := L(State) = LSX[C_2](K_2 \oplus LSX[C_1](K_1))$

$$
\begin{array}{|c|l}
\hline
(C_1^{15}, C_1^{14}, \ldots, C_1^2, C_1^1, \pi^{-1}(\pi(C_1^0 \oplus K_1^0) \oplus 2) \oplus K_1^0) & \\
\hline
\downarrow & \oplus K_1 \\
\hline
(C_1^{15} \oplus K_1^{15}, \ldots, C_1^1 \oplus K_1^1, \pi^{-1}(\pi(C_1^0 \oplus K_1^0) \oplus 2)) & \\
\hline
\downarrow & S \\
\hline
SX[C_1](K_1) \oplus (0, \ldots, 0, 2) & \\
\hline
\downarrow & L \\
\hline
LSX[C_1](K_1) \oplus C_2 & \\
\hline
\downarrow & \oplus K_2 \\
\hline
X[C_2](K_2 \oplus LSX[C_1](K_1)) & \\
\hline
\downarrow & S \\
\hline
SX[C_2](K_2 \oplus LSX[C_1](K_1)) & \\
\hline
\downarrow & L \\
\hline
LSX[C_2](K_2 \oplus LSX[C_1](K_1)) & \\
\hline
\downarrow & \oplus K_3 = K_1 \oplus LSX[C_2](K_2 \oplus LSX[C_1](K_1)) \\
\hline
K_1 & \\
\hline
\downarrow & S \\
\hline
S(K_1) & \\
\hline
\downarrow & L \\
\hline
LS(K_1) & \\
\hline
\downarrow & \oplus K_4 = K_2 \oplus LSX[C_1](K_1) \\
\hline
K_2 \oplus LS(K_1) \oplus LSX[C_1](K_1) & \\
\hline
\end{array}
$$

7. $State := State \oplus K_3 = K_1 \oplus LSX[C_2](K_2 \oplus LSX[C_1](K_1)) \oplus LSX[C_2](K_2 \oplus LSX[C_1](K_1)) = K_1$



8. $State := S(State) = S(K_1)$

$$
\begin{array}{|c|l}
\hline
(C_1^{15}, C_1^{14}, \ldots, C_1^2, C_1^1, \pi^{-1}(\pi(C_1^0 \oplus K_1^0) \oplus 2) \oplus K_1^0) & \\
\hline
\downarrow & \oplus K_1 \\
\hline
(C_1^{15} \oplus K_1^{15}, \ldots, C_1^1 \oplus K_1^1, \pi^{-1}(\pi(C_1^0 \oplus K_1^0) \oplus 2)) & \\
\hline
\downarrow & S \\
\hline
SX[C_1](K_1) \oplus (0, \ldots, 0, 2) & \\
\hline
\downarrow & L \\
\hline
LSX[C_1](K_1) \oplus C_2 & \\
\hline
\downarrow & \oplus K_2 \\
\hline
X[C_2](K_2 \oplus LSX[C_1](K_1)) & \\
\hline
\downarrow & S \\
\hline
SX[C_2](K_2 \oplus LSX[C_1](K_1)) & \\
\hline
\downarrow & L \\
\hline
LSX[C_2](K_2 \oplus LSX[C_1](K_1)) & \\
\hline
\downarrow & \oplus K_3 = K_1 \oplus LSX[C_2](K_2 \oplus LSX[C_1](K_1)) \\
\hline
K_1 & \\
\hline
\downarrow & S \\
\hline
S(K_1) & \\
\hline
\downarrow & L \\
\hline
LS(K_1) & \\
\hline
\downarrow & \oplus K_4 = K_2 \oplus LSX[C_1](K_1) \\
\hline
K_2 \oplus LS(K_1) \oplus LSX[C_1](K_1) & \\
\hline
\end{array}
$$

9. $State := L(State) = LS(K_1)$

$$
\begin{array}{|c|l}
\hline
(C_1^{15}, C_1^{14}, \ldots, C_1^2, C_1^1, \pi^{-1}(\pi(C_1^0 \oplus K_1^0) \oplus 2) \oplus K_1^0) & \\
\hline
\downarrow & \oplus K_1 \\
\hline
(C_1^{15} \oplus K_1^{15}, \ldots, C_1^1 \oplus K_1^1, \pi^{-1}(\pi(C_1^0 \oplus K_1^0) \oplus 2)) & \\
\hline
\downarrow & S \\
\hline
SX[C_1](K_1) \oplus (0, \ldots, 0, 2) & \\
\hline
\downarrow & L \\
\hline
LSX[C_1](K_1) \oplus C_2 & \\
\hline
\downarrow & \oplus K_2 \\
\hline
X[C_2](K_2 \oplus LSX[C_1](K_1)) & \\
\hline
\downarrow & S \\
\hline
SX[C_2](K_2 \oplus LSX[C_1](K_1)) & \\
\hline
\downarrow & L \\
\hline
LSX[C_2](K_2 \oplus LSX[C_1](K_1)) & \\
\hline
\downarrow & \oplus K_3 = K_1 \oplus LSX[C_2](K_2 \oplus LSX[C_1](K_1)) \\
\hline
K_1 & \\
\hline
\downarrow & S \\
\hline
S(K_1) & \\
\hline
\downarrow & L \\
\hline
LS(K_1) & \\
\hline
\downarrow & \oplus K_4 = K_2 \oplus LSX[C_1](K_1) \\
\hline
K_2 \oplus LS(K_1) \oplus LSX[C_1](K_1) & \\
\hline
\end{array}
$$

10. $State := State \oplus K_4 = K_2 \oplus LS(K_1) \oplus LSX[C_1](K_1)$

$$
\begin{array}{|c|l}
\hline
(C_1^{15}, C_1^{14}, \ldots, C_1^2, C_1^1, \pi^{-1}(\pi(C_1^0 \oplus K_1^0) \oplus 2) \oplus K_1^0) & \\
\hline
\downarrow & \oplus K_1 \\
\hline
(C_1^{15} \oplus K_1^{15}, \ldots, C_1^1 \oplus K_1^1, \pi^{-1}(\pi(C_1^0 \oplus K_1^0) \oplus 2)) & \\
\hline
\downarrow & S \\
\hline
SX[C_1](K_1) \oplus (0, \ldots, 0, 2) & \\
\hline
\downarrow & L \\
\hline
LSX[C_1](K_1) \oplus C_2 & \\
\hline
\downarrow & \oplus K_2 \\
\hline
X[C_2](K_2 \oplus LSX[C_1](K_1)) & \\
\hline
\downarrow & S \\
\hline
SX[C_2](K_2 \oplus LSX[C_1](K_1)) & \\
\hline
\downarrow & L \\
\hline
LSX[C_2](K_2 \oplus LSX[C_1](K_1)) & \\
\hline
\downarrow & \oplus K_3 = K_1 \oplus LSX[C_2](K_2 \oplus LSX[C_1](K_1)) \\
\hline
K_1 & \\
\hline
\downarrow & S \\
\hline
S(K_1) & \\
\hline
\downarrow & L \\
\hline
LS(K_1) & \\
\hline
\downarrow & \oplus K_4 = K_2 \oplus LSX[C_1](K_1) \\
\hline
K_2 \oplus LS(K_1) \oplus LSX[C_1](K_1) & \\
\hline
\end{array}
$$

Откуда получаем, что $K_2 = \hat{E}_{K_1,K_2}(m) \oplus LSX[C_1](K_1) \oplus LS(K_1)$

Для атаки на K_1^l нам требуется один открытый текст, до 512 связанных ключей и столько же шифрований. Для нахождения K_2 требуется одно зашифрование выбранного открытого текста на исходном ключе.
Итого, общая сложность алгоритма составляет 2^{12} шифрований при требовании 2^{12} связанных ключей.

Результаты численного эксперимента

Данная атака была реализована на языке Python 2.7. Программа находила ключи в среднем за 10 минут на персональном компьютере. Кроме того, за несколько часов экспериментов не было выявлено случаев, когда для K_1 нашлось несколько кандидатов.

Спасибо за внимание!

- Федеральное агенство по техническому регулированию и метрологии *Национальный стандарт Российской Федерации ГОСТ Р 34.12-2015*. Москва, Стандартинформ, 2015.
- A. Biryukov, D. Khovratovich *Related-key Cryptanalysis of the Full AES-192 and AES-256*, University of Luxembourg.
- М. А. Пудовкина, Г. И. Хоруженко, *Атака на шифрсистему ГОСТ 28147-89 с 12 свя- занными ключами*, Матем. вопр. криптогр., 2013, том 4, выпуск 2, 127-152.
- V. Rudskoy *On zero practical signifcance of "Key recovery attack on full GOST block cipher with zero time and memory"* Lomonosov Moscow State University, Faculty of Computational Mathematics and Cybernetics.
- E. Biham. *New types of cryptanalytic attacks using related keys*. J. Cryptology, 7(4):229–246, 1994.


J. Kelsey, B. Schneier, D. Wagner *Key-Schedule Cryptanalysis of IDEA, G-DES, GOST, SAFER, and Triple-DES*


J. Kelsey, B. Schneier, D. Wagner *Related-Key Cryptanalysis of 3-WAY, Biham-DES,CAST, DES-X, NewDES, RC2, and TEA*


A. Biryukov, D. Khovratovich, I. Nikolić *Examples of differential multicollisions for 13 and 14 rounds of AES-256*