О нулевой практической значимости «Атаки определения ключа полнораундового блочного шифра ГОСТ 28147-89 с нулевой трудоемкостью и памятью»

В.И. Рудской

rudskoy_vladimir@mail.ru

2 апреля 2010 года

Алгоритм блочного шифрования ГОСТ 28147-89

- Длина информационного блока 64 бита
- Длина ключа 256 бит, $K = (K_1, ..., K_8)$
- Схема Фейстеля, 32 итерации, $P_i = L_i || R_i$

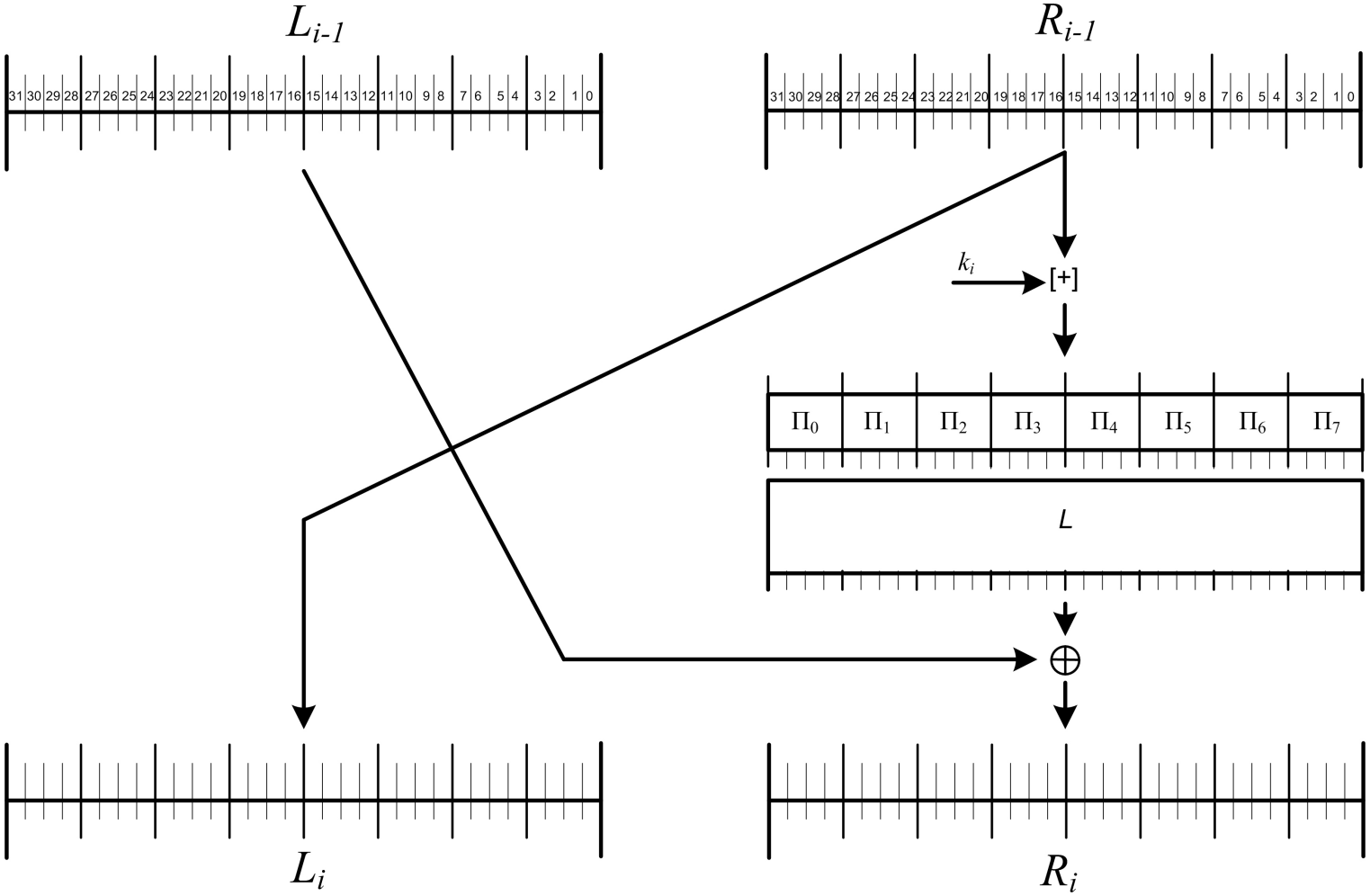
$$\begin{cases} L_i = R_{i-1} \\ R_i = L_{i-1} \oplus L(\Pi(R_{i-1} \boxplus k_i)) \end{cases}$$

При зашифровании:

$$\begin{cases} k_i = K_{(i-1) \mod 8+1}, & i \in \overline{1, 24}; \\ k_i = K_{32-i+1}, & i \in \overline{25, 32}. \end{cases}$$

При расшифровании:

$$\begin{cases} k_i = K_i, & i \in \overline{1, 8}; \\ k_i = K_{(32-i) \mod 8+1}, & i \in \overline{9, 32}. \end{cases}$$


L_{i-1}
R_{i-1}
31 30 29 28 27 26 25 24 23 22 21 20 19 18 17 16 15 14 13 12 11 10 9 8 7 6 5 4 3 2 1 0
k_i
[+]
Π_0 Π_1 Π_2 Π_3 Π_4 Π_5 Π_6 Π_7
L
L_i
R_i

Метод связанных ключей

- Сильное предположение о возможностях противника *или* предположение о маловероятном событии
- Использование в сочетании с другими методами (разностный метод, метод «бумеранга»,...)
- «Сильные» результаты и множество публикаций.
- В частности, Fleischmann, Gorsky, Hühne, Lucks «Key recovery attack on full GOST Block Cipher with zero time and memory»
- Сомнительная практическая значимость

Предположения о противнике

- Противник имеет возможность выполнять зашифрование и расшифрование выбранных текстов на неизвестном ему ключе K
- Противник имеет возможность выполнять зашифрование и расшифрование выбранных текстов на некотором количестве неизвестных связанных с K ключах $K_i = f_i(K)$, где функции f_i определяются противником или известны ему

Например $K_i = K \oplus \Delta K_i$

Метод «бумеранга» (D. Wagner, 1999)

Разностное соотношение $\alpha \to \beta$ для f,

$$f(x) \oplus f(x \oplus \alpha) = \beta$$

Разностная характеристика

$$p^f_{\alpha,\beta} = \mathbf{P}\{f(x) \oplus f(x \oplus \alpha) = \beta\}$$

Утверждение 1

Пусть f — биективно и

$$\mathbf{P}\{f(x) \oplus f(x \oplus \alpha) = \beta\} = p.$$

Тогда для f^{-1} и $\beta \to \alpha$

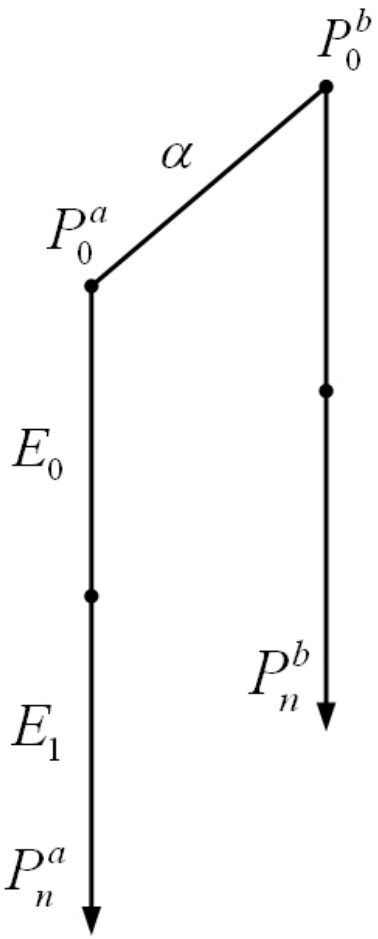
$$\mathbf{P}\{f^{-1}(x) \oplus f^{-1}(x \oplus \beta) = \alpha\} = p.$$

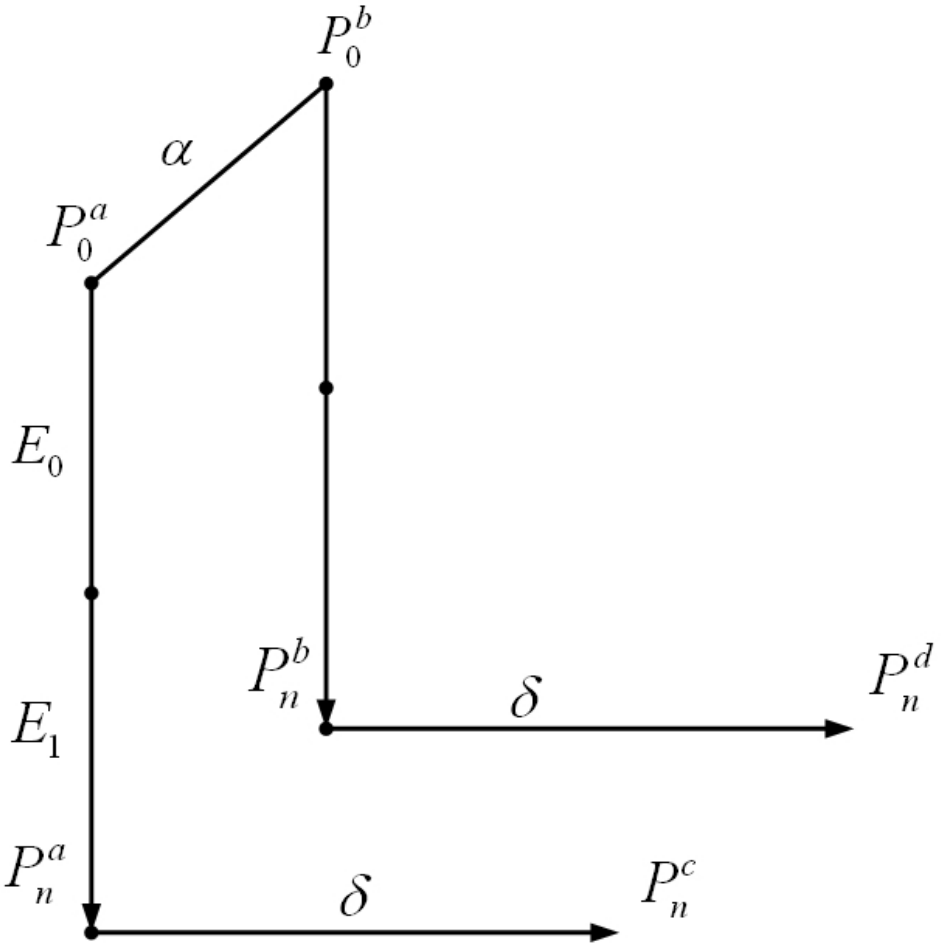
1. Построение соотношения $\alpha \to \beta$ для $E = E_K(P)$ (или его части) с достаточно большим значением $p^E_{\alpha,\beta}$
2. Накопление материала (distinguisher step): (P, P')

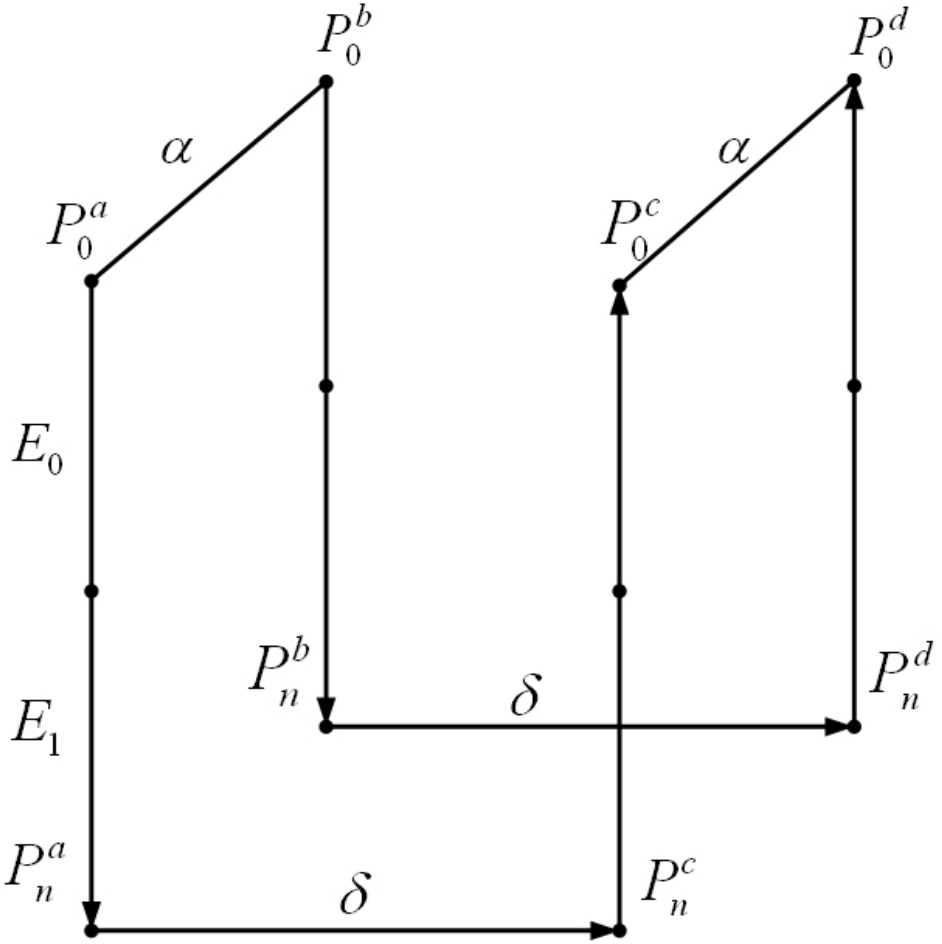
$$\begin{cases} P \oplus P' = \alpha \\ E(P) \oplus E(P') = \beta \end{cases}$$

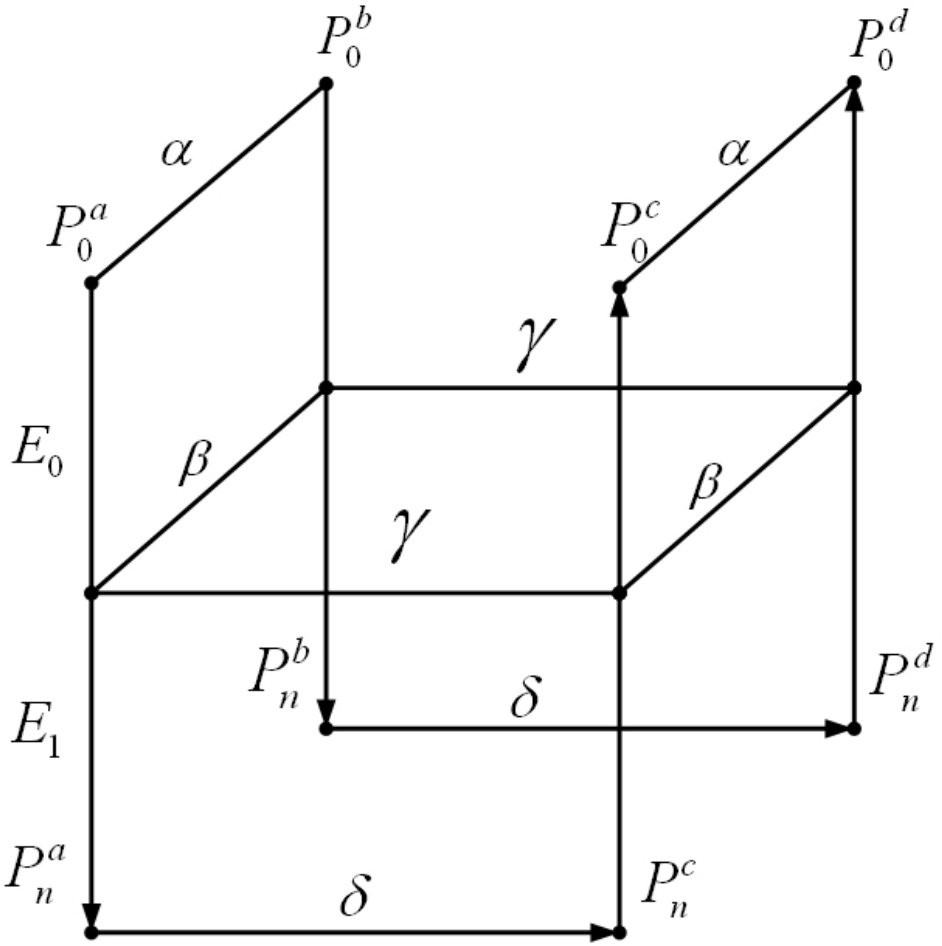
3. Определение ключа (key recovery step)

- Невозможно построить разностное соотношение для E
- Алгоритм шифрования E представим в виде $E = E_0 \circ E_1$
- Известны разностные соотношения
  $E_0 : \ \alpha \to \beta$, с характеристикой p
  $E_1 : \ \gamma \to \delta$, с характеристикой q


P_0^b
α
P_0^a
E_0
P_n^b
E_1
P_n^a


P_0^b
α
P_0^a
E_0
P_n^b
δ
P_n^d
E_1
P_n^a
δ
P_n^c


P_0^b
P_0^d
α
α
P_0^a
P_0^c
E_0
P_n^b
δ
P_n^d
E_1
P_n^a
δ
P_n^c


P_0^b
P_0^d
α
α
P_0^a
P_0^c
γ
E_0
β
β
γ
P_n^b
P_n^d
δ
E_1
P_n^a
δ
P_n^c

Если условие $P_0^c \oplus P_0^d = \alpha$ выполнено, то предполагается

- Для E_0 на паре (P_0^a, P_0^b) выполнилось соотношение $\alpha \to \beta$,
- Для E_0 на паре (P_0^c, P_0^d) выполнилось соотношение $\alpha \to \beta$,
- Для E_1^{-1} на паре (P_n^a, P_n^c) выполнилось соотношение $\delta \to \gamma$,
- Для E_1^{-1} на паре (P_n^b, P_n^d) выполнилось соотношение $\delta \to \gamma$.

Вероятность выполнения $(pq)^2$

Четверку $(P_0^a, P_0^b, P_0^c, P_0^d)$ будем называть «разностным квартетом».

Метод «бумеранга», использующий связанные ключи

Рассматриваются четыре связанных ключа K^i, $i \in \{a, b, c, d\}$

$$\Delta K^* = K^a \oplus K^b = K^c \oplus K^d,$$

$$\Delta K' = K^a \oplus K^c = K^b \oplus K^d$$

Зашифрование и расшифрование P^i проводится на ключе K^i

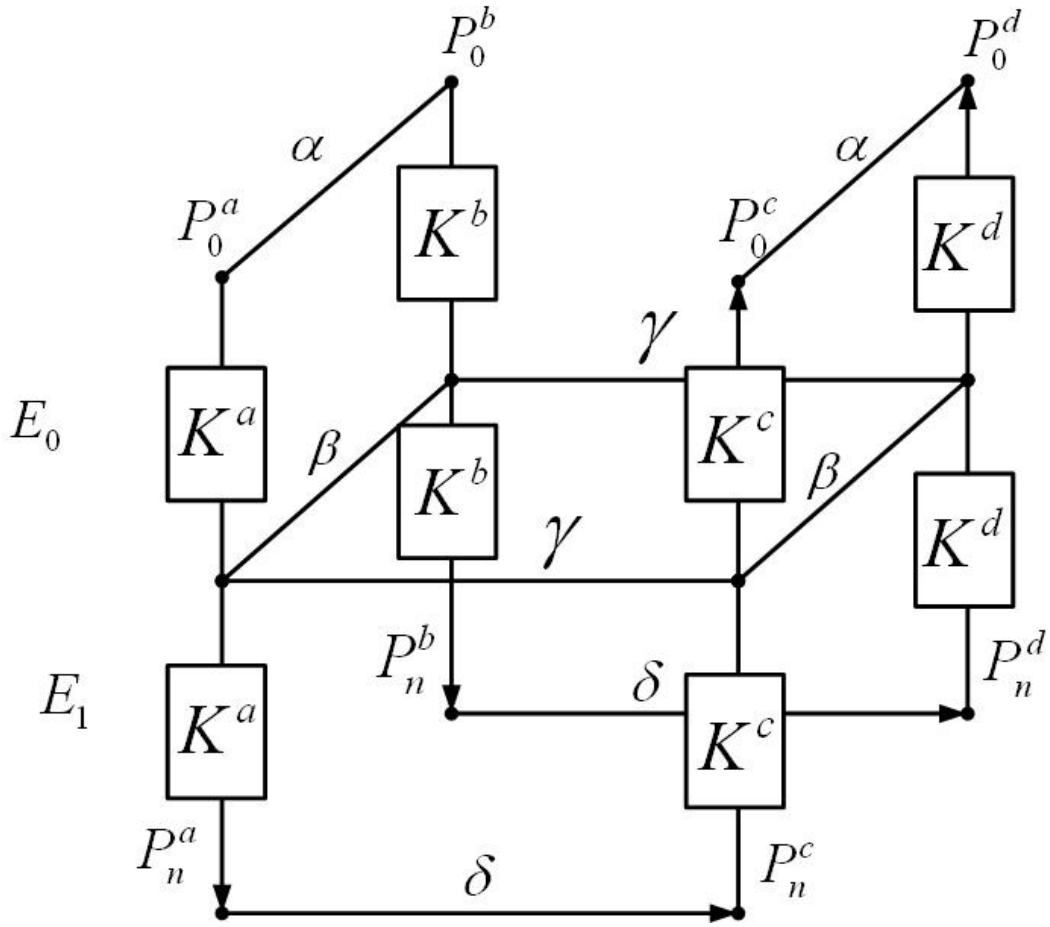
Рассмотрим преобразование

$$f(X||K) = E_K(X)||K$$

Для него верно утверждение 1

«Разностное соотношение $\alpha \to \beta$ на связанных ключах K^i и K^j»:

$$(\alpha, K^i \oplus K^j) \to (\beta, K^i \oplus K^j)$$


P_0^b
P_0^d
α
α
P_0^a
K^b
P_0^c
K^d
γ
E_0
K^a
β
K^b
K^c
β
K^d
γ
P_n^b
P_n^d
E_1
δ
K^a
K^c
P_n^a
δ
P_n^c

Применение метода к алгоритму ГОСТ 28147-89 (Fleischmann, Gorsky, Hühne, Lucks)

Рассматриваются четыре связанных ключа $K^i \in V_{256}$, $K^i = (k_1^i, \ldots, k_8^i)$, $k_j^i \in V_{32}$, $i \in \{a, b, c, d\}$, $j \in \overline{1, 8}$:

$$\Delta K^* = K^a \oplus K^b = K^c \oplus K^d = (e_{31}, 0, e_{31}, 0, e_{31}, 0, e_{31}, 0),$$

$$\Delta K' = K^a \oplus K^c = K^b \oplus K^d = (e_{31}, 0, 0, 0, 0, 0, 0, 0),$$

E_0 - первые 24 итерации; E_1 - последние 8 итераций.
Будем обозначать $P_j^i = (L_j^i, R_j^i)$
Рассматриваются разностные соотношения:

$$E_0 : \qquad ((0, e_{31})||\Delta K^*) \to ((0, e_{31})||\Delta K^*), \qquad p = 1,$$

$$E_1^{-1} : \qquad ((e_7, 0)||\Delta K') \to ((0, 0)||\Delta K'), \qquad q = 2^{-3}.$$

Рассмотрим две первые итерации зашифрования $P_0^a = (L_0^a, R_0^a)$ и $P_0^b = (L_0^b, R_0^b)$, $P_0^a \oplus P_0^b = (0, e_{31})$.

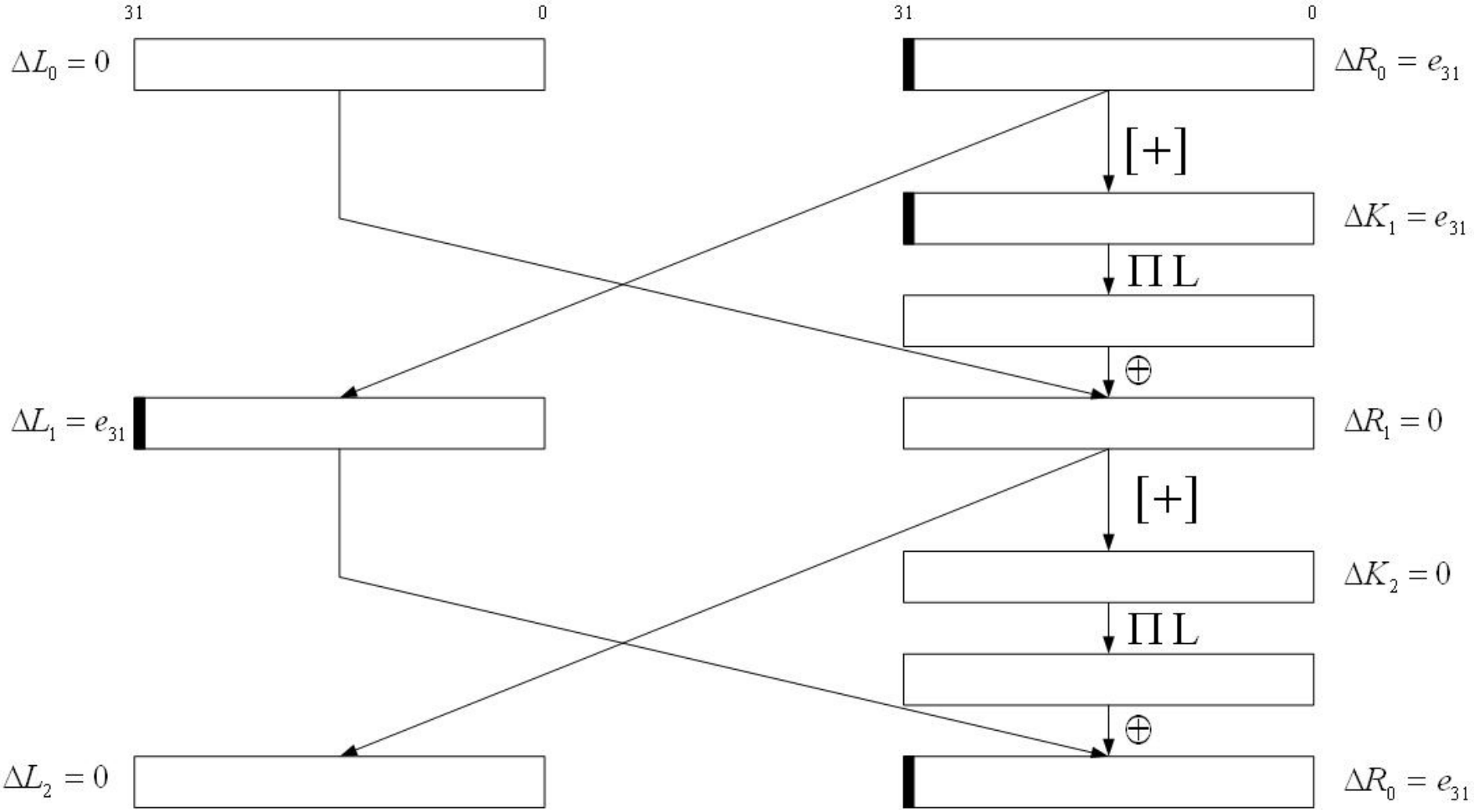
$$\begin{cases} \Delta L_1 = \Delta R_0 = e_{31} \\ \Delta R_1 = \mathbf{L}\Pi(R_0^a \boxplus k_1^a) \oplus \mathbf{L}\Pi((R_0^a \oplus e_{31}) \boxplus (k_1^a \oplus e_{31})) = 0 \end{cases}$$

$$\begin{cases} \Delta L_2 = \Delta R_1 = 0 \\ \Delta R_2 = \Delta L_1 \oplus \mathbf{L}\Pi(R_1^a \boxplus k_2^a) \oplus \mathbf{L}\Pi(R_1^a \boxplus k_2^a) = e_{31} \end{cases}$$

$(0, e_{31}) \to (0, e_{31})$ выполнилось для двух итераций E_0 с вероятностью $p' = 1$

$$\Downarrow$$

выполнится для всего E_0 с вероятностью $p = 1$.


31
0
31
0
$\Delta L_0 = 0$
$\Delta R_0 = e_{31}$
[+]
$\Delta K_1 = e_{31}$
П L
$\Delta L_1 = e_{31}$
$\Delta R_1 = 0$
[+]
$\Delta K_2 = 0$
П L
$\Delta L_2 = 0$
$\Delta R_0 = e_{31}$

$$E_1^{-1}: \qquad ((e_7,0)||\Delta K') \to ((0,0)||\Delta K'), \qquad q = 2^{-3}.$$

Выполнение разностного соотношения равносильно равенству

$$L_{32}^a \oplus \mathbf{L}\Pi(R_{32}^a \boxplus k_1^a) = L_{32}^c \oplus \mathbf{L}\Pi(R_{32}^c \boxplus k_1^c).$$

С учетом $L_{32}^c = L_{32}^a \oplus e_7$, $R_{32}^a = R_{32}^c$, $k_1^c = k_1^a \oplus e_{31}$ равносильно

$$\mathbf{L}\Pi(R_{32}^a \boxplus k_1^a) \oplus \mathbf{L}\Pi(R_{32}^a \boxplus (k_1^a \oplus e_{31})) = L_{32}^a \oplus L_{32}^a = e_7,$$

или, что то же самое

$$\Pi(R_{32}^a \boxplus k_1^a) \oplus \Pi((R_{32}^a \boxplus k_1^a) \oplus e_{31}) = e_{28}.$$

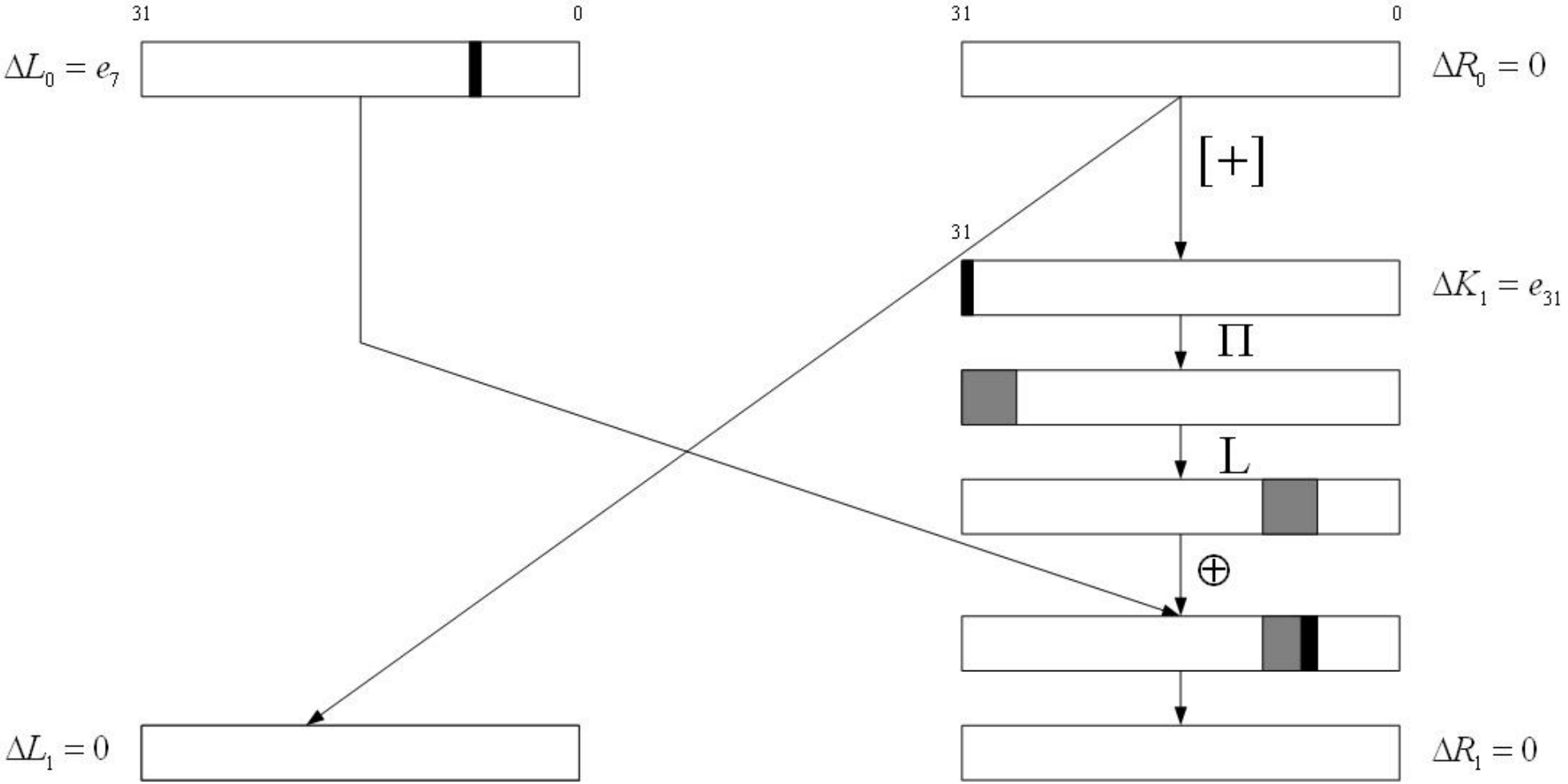
$\pi : V_4 \to V_4$-подстановка, действующая на старших битах

$$\pi(\overline{R_{32}^a \boxplus k_1^a}) \oplus \pi((\overline{R_{32}^a \boxplus k_1^a}) \oplus e_3) = e_0,$$

т.е. разностное соотношение $e_3 \to e_0$ для подстановки π, $q = 2^{-3}$.

Для произвольных подстановок: $e_3 \to \omega, \quad q \neq 0$
Для E_1^{-1} следует рассматривать разностное соотношение

$$(\mathbf{L}[\omega, 0, ..., 0], 0) \to (0,0).$$


31
0
$\Delta L_0 = e_7$
31
0
$\Delta R_0 = 0$
[+]
31
$\Delta K_1 = e_{31}$
П
L
⊕
$\Delta L_1 = 0$
$\Delta R_1 = 0$

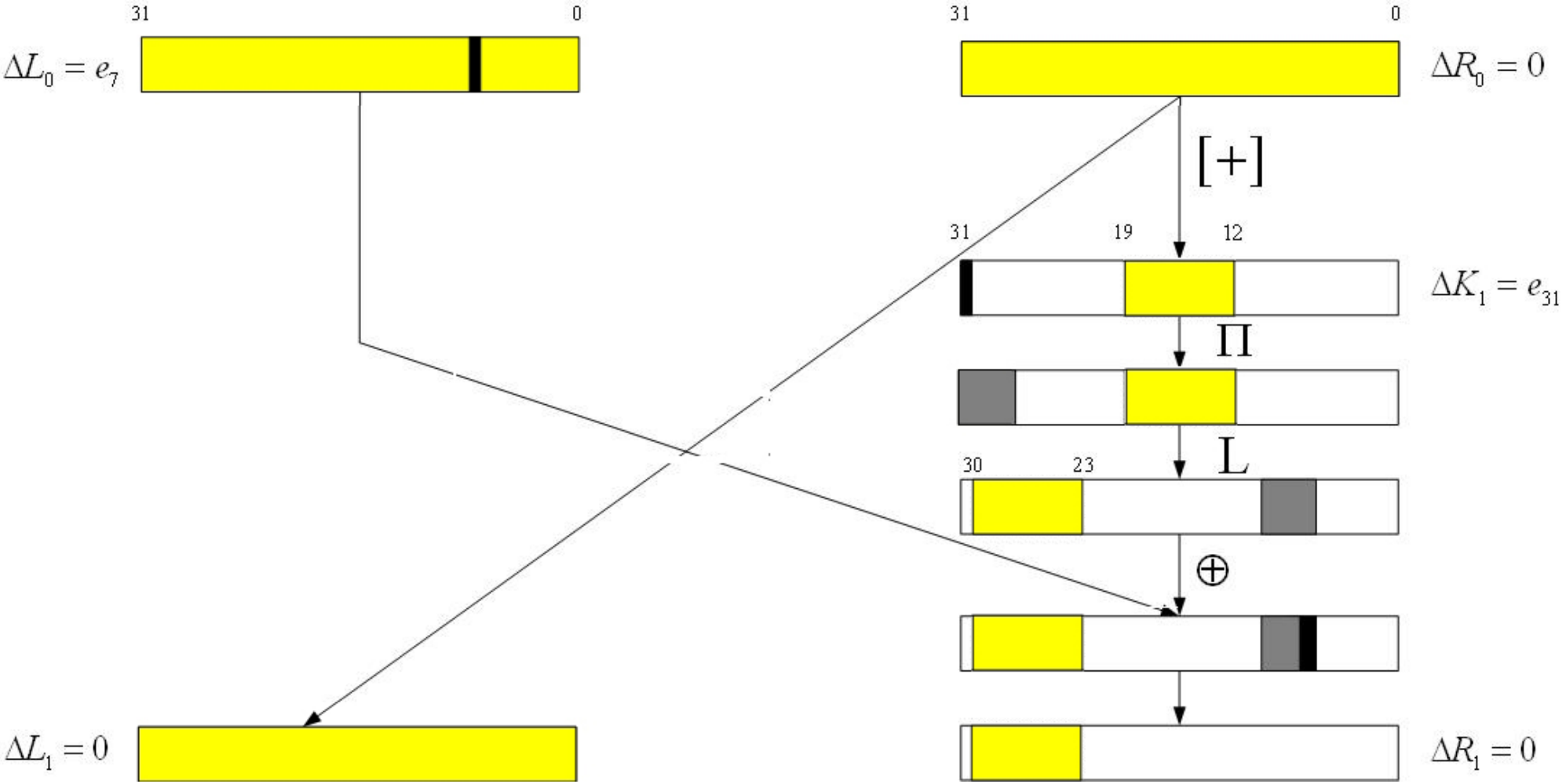
Алгоритм 1

1. Выбирается $2^{5.5}$ пар P_0^a и $P_0^b = P_0^a \oplus (0, e_{31})$.
2. Зашифрование на связанных ключах $P_{32}^a = E(P_0^a, K^a)$, $P_{32}^b = E(P_0^b, K^b)$.
3. Вычисляются $P_{32}^c = P_{32}^a \oplus (e_7, 0)$, $P_{32}^d = P_{32}^b \oplus (e_7, 0)$
4. Расшифрование на связанных ключах $P_0^c = E^{-1}(P_{32}^c, K^c)$, $P_0^d = E^{-1}(P_{32}^d, K^d)$
5. Проверяется $P_0^c \oplus P_0^d \stackrel{?}{=} (0, e_{31})$. Если выполнено, то в Θ сохраняется разностный квартет $(P_0^a, P_0^b, P_0^c, P_0^d)$.
6. Опробуются 8 бит ключа k_1^a в позициях с 12 по 19. Вычисляются $k_1^c = k_1^a \oplus e_{31}$, $k_1^b = k_1^a$, $k_1^d = k_1^b \oplus e_{31}$.
   - 6.1 Для каждого $(P_0^a, P_0^b, P_0^c, P_0^d) \in \Theta$ вычисляются $\overline{P}_{31}^a, \overline{P}_{31}^b, \overline{P}_{31}^c, \overline{P}_{31}^d$.
   - 6.2 Проверяется $\overline{P}_{31}^a \oplus \overline{P}_{31}^c \stackrel{?}{=} (0, 0)$ и $\overline{P}_{31}^b \oplus \overline{P}_{31}^d \stackrel{?}{=} (0, 0)$.
   - 6.3 Если выполнено, то счетчик опробуемого набора увеличивается на 1.
7. Выбираются $k_1^a, k_1^b, k_1^c, k_1^d$ с наибольшим значением счетчика.
8. Для каждого выбранного k_1^a остальные $256 - 8 = 248$ бит находятся тотальным перебором. Если истинный ключ найден, то выполнение завершается. Иначе выбирается другое k_1^a и повторяется тотальный перебор.

Анализ метода

«...The data and time complexity of Step 5 to **8** are negligible...»

Вычислим максимально возможное число бит P_{31}^i.
Очевидно, что $L_{31}^i = R_{32}^i$.
Можно вычислить $(k_1^i \boxplus R_{32}^i)[12 \sim 19]$ с точностью до возможного бита переноса.
Следовательно можно вычислить $R_{31}^i[23 \sim 30]$.
Т.к. $k_1^i[12 \sim 19] = k_1^j[12 \sim 19]$ и $R_{32}^i[12 \sim 19] = R_{32}^j[12 \sim 19]$ для всех $i, j \in \{a, b, c, d\}$.
Следовательно условие 6.3 выполнено для любого опробуемого набора.
В результате алгоритм сводится к опробованию всех возможных ключей.


31
0
$\Delta L_0 = e_7$
31
0
$\Delta R_0 = 0$
[+]
31
19
12
$\Delta K_1 = e_{31}$
Π
L
30
23
⊕
$\Delta L_1 = 0$
$\Delta R_1 = 0$

Алгоритм 2

1.-5. Накопление материала $(P_0^a, P_0^b, P_0^c, P_0^d)$ и $(P_{32}^a, P_{32}^b, P_{32}^c, P_{32}^d)$ в Θ

6. Опробуются 8 бит k_1^a **с 24 по 31**. Вычисляются $k_1^c = k_1^a \oplus e_{31}$, $k_1^b = k_1^a$, $k_1^d = k_1^b \oplus e_{31}$.

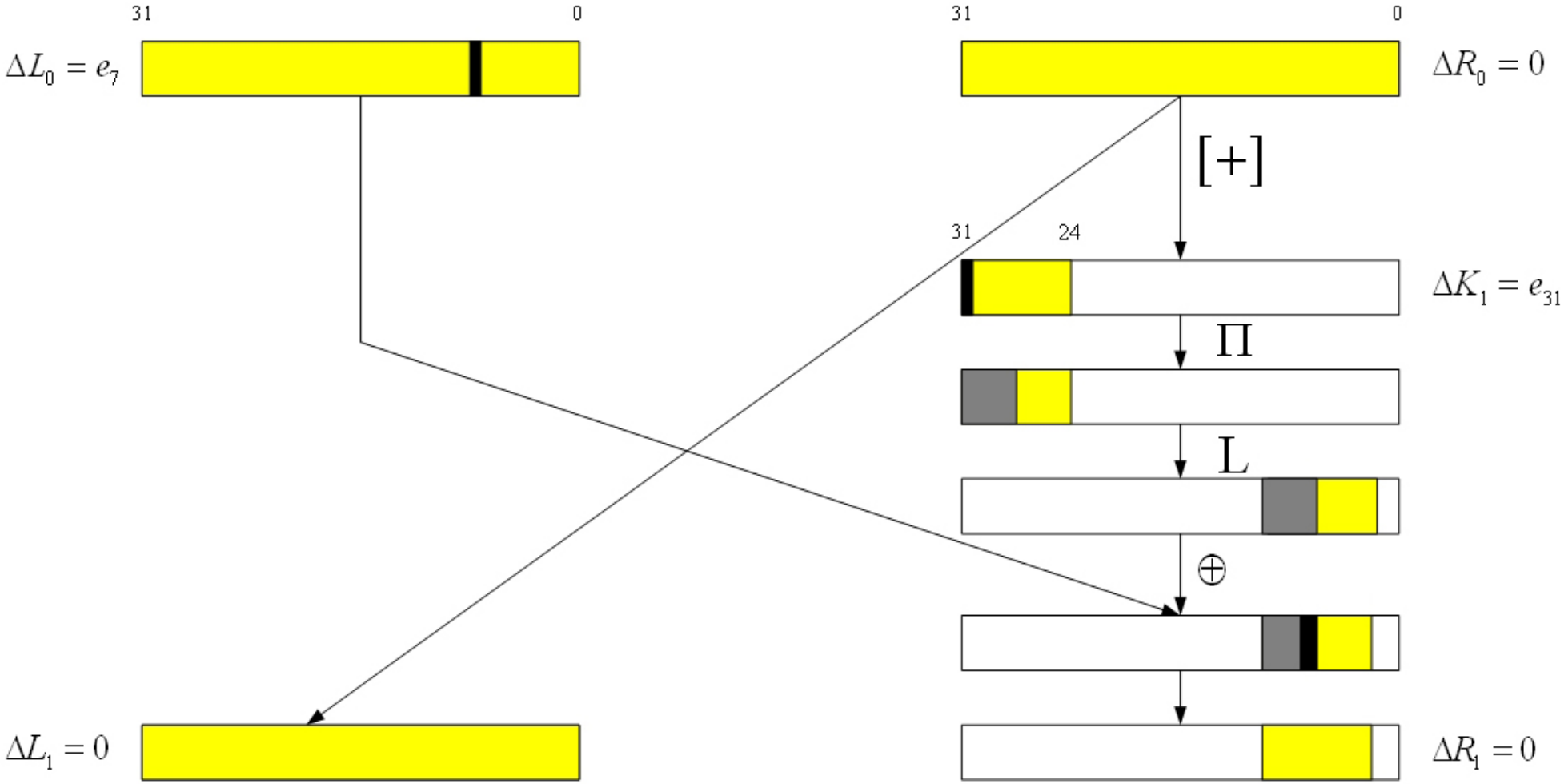
6.1. Для каждого $(P_0^a, P_0^b, P_0^c, P_0^d) \in \Theta$ вычисляются $\overline{P}_{31}^a, \overline{P}_{31}^b, \overline{P}_{31}^c, \overline{P}_{31}^d$.

6.2 Проверяется $\overline{P}_{31}^a \oplus \overline{P}_{31}^c \stackrel{?}{=} (0,0)$ и $\overline{P}_{31}^b \oplus \overline{P}_{31}^d \stackrel{?}{=} (0,0)$.

6.3 Если выполнено, то счетчик опробуемого набора увеличивается на 1.

7. Выбираются $k_1^a, k_1^b, k_1^c, k_1^d$ с наибольшим значением счетчика.

8. Для выбранного k_1^a остальные $256 - 8 = 248$ бита находятся тотальным перебором. Если истинный ключ найден, то выполнение завершается. Иначе выбирается другое k_1^a и повторяется тотальный перебор.


31
0
$\Delta L_0 = e_7$
31
0
$\Delta R_0 = 0$
[+]
31
24
$\Delta K_1 = e_{31}$
П
L
⊕
$\Delta L_1 = 0$
$\Delta R_1 = 0$

Усовершенствование алгоритма 2

k_1^a– истинный ключ, $\widehat{k_1^a}$– ложный ключ.

Замечание: k и $k \oplus e_{31}$ неразличимы

Условие отсеивания:

$P_{31}^a \oplus P_{31}^c = (0,0)$ и $P_{31}^b \oplus P_{31}^d = (0,0)$.

$$\pi((R_{32}^a \boxplus k_1^a)[28 \sim 31]) \oplus \pi((R_{32}^a \boxplus k_1^a)[28 \sim 31] \oplus e_3) = e_0,$$

$$\pi((R_{32}^a \boxplus \widehat{k_1^a})[28 \sim 31]) \oplus \pi((R_{32}^a \boxplus \widehat{k_1^a})[28 \sim 31] \oplus e_3) \neq e_0.$$

Для истинного ключа всегда выполнено

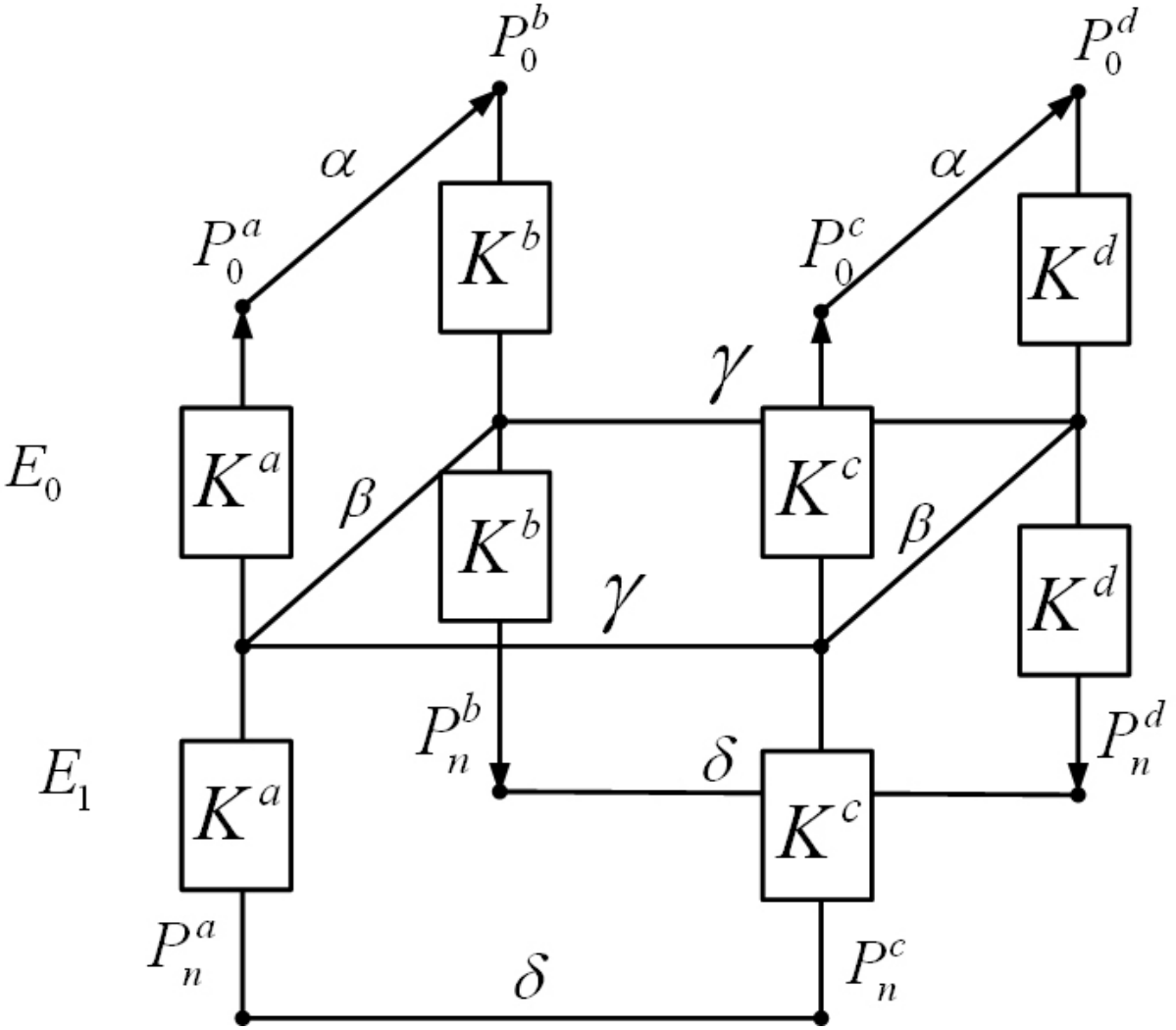
Можно определить 31 бит ключа k_1^a

Пусть $k_1^a[m+1 \sim 31] = \widehat{k_1^a}[m+1 \sim 31]$ и $k_1^a[m] \neq \widehat{k_1^a}[m]$

Если найдется разностный квартет, в котором $P_{32,m}^a$:

$$R_{32,m}^a[i] = \begin{cases} \{0,1\}_R, & i = \overline{28,31} \\ k_1^a[i] \oplus 1, & i = \overline{m+1,27}; \\ 1, & i = m; \\ 0, & i = \overline{0,m-1} \end{cases}$$

четыре старших бит суммы различны.


P_0^b
P_0^d
α
α
P_0^a
K^b
P_0^c
K^d
γ
E_0
K^a
β
K^b
K^c
β
K^d
γ
P_n^b
P_n^d
E_1
δ
K^a
K^c
P_n^a
δ
P_n^c

Алгоритм 3

1. Применяется алгоритм 2: Определяется $k_1^a[24 \sim 31]$, $k_1^a[31] = 0$

2. $i = 23$

3. выбираются 2^{10} пар шифртекстов P_{32}^a и $P_{32}^c = P_{32}^a \oplus (e_7, 0)$, где правая часть $R_{32,i}^a$, левая часть принимает 2^6 различных случайных значений.

4.-7. Накопление материала $(P_0^a, P_0^b, P_0^c, P_0^d)$ и $(P_{32}^a, P_{32}^b, P_{32}^c, P_{32}^d)$ в Θ

8. Рассматриваются $k_1^{a,(1)}, k_1^{a,(2)}$: $k_1^{a,(j)}[i+1 \sim 31] = k_1^a[i+1 \sim 31]$, $k_1^{a,(1)}[i] \neq k_1^{a,(2)}[i]$

   8.1 Вычисляются $k_1^{c,(j)} = k_1^{a,(j)} \oplus e_{31}$

   8.2 Для каждого квартета из Θ вычисляются P_{31}^a, P_{31}^c

   8.3 Проверяется $P_{31}^a \oplus P_{31}^c \stackrel{?}{=} (0,0)$ Если выполнено, то счетчик увеличивается на 1.

9. Из $k_1^{a,(1)}, k_1^{a,(2)}$ выбирается с большим значением счетчика.

10. Полагаем $k_1^a[i] = k_1^{a,(j)}[i]$.

11. Если $i > 0$, то $i = i - 1$ и переход к шагу 3. Иначе выполнение завершено, выход: ключ k_1^a

Обобщение метода

При известных $k_1^j, ..., k_t^j$ можно вычислить $P_{32-t}^j \Rightarrow$
Можно подобрать P_{32}^j так, чтобы получить нужную разность на входе $t+1$ итерации расшифрования
E_0 то же самое
E_1 редуцировано; меньшее число итераций, прежнее разностное соотношение

Используем другие квартеты связанных ключей

$$\Delta K^* = K^a \oplus K^b = K^c \oplus K^d = (e_{31}, 0, e_{31}, 0, e_{31}, 0, e_{31}, 0)$$
$$\Delta K' = K^a \oplus K^c = K^b \oplus K^d = (0, ..., \underset{t+1}{e_{31}}, ..., 0)$$

Трудоемкость метода

$2^{225} + 2^{17}$ при 4 связанных ключах

2^{26} при 18 связанных ключах

Для сравнения:

AES-256: $2^{99.5}$ при 4 связанных ключах
(Biryukov, Khovratovich)

Kasumi-128 (GSM A5/3): 2^{32} при 4 связанных ключах
(Fleischman, Gorsky, Lucks)

Теоретическая и практическая значимость результатов

«The practicality of various types of cryptanalytic attacks depends on many factors: Attacks based on few ciphertexts are better than attacks that require many ciphertexts, known plaintext attacks are better than chosen plaintext attacks, nonadaptive attacks are better than adaptive attacks, single key attacks are better than related key attacks, etc. Since it is difficult to quantify the relative importance of all these factors in different scenarios, we usually concentrate on the total running time of the attack, which is a single well defined number.»—

Biryukov, Dunkelman, Keller, Khovratovich, and Shamir
«Key Recovery Attacks of Practical Complexity on AES Variants With Up To 10 Rounds»

«Естественные» предположения

Одноключевая модель

- Один неизвестный ключ
- Ключ выбран случайно и равновероятно

Многоключевая модель

- Несколько неизвестных ключей
- Ключи выбраны случайно, равновероятно и независимо

Вероятность успеха:

$$2^{-3 \cdot 256} = 2^{-768},$$

$$2^{-17 \cdot 256} = 2^{-4352}$$

(Вероятность угадывания ключа: 2^{-256})

Модель с дополнительной информацией

Многоключевая модель с дополнительной информацией

- Несколько (явным образом) неизвестных ключей
- Имеется дополнительная информация о ключах

- Атака **НЕ** на шифр, а на систему {шифр + процедура выработки ключей}
- Стандарт ГОСТ 28147-89 не регламентирует процедуру выработки ключей

- Нельзя сравнивать с полным перебором с трудоемкостью 2^{256}
- Теоретико-информационный подход

Спасибо за внимание

Изложенные результаты доступны на
Cryptology ePrint Archive, Report 2010/111
http://eprint.iacr.org/2010/111.pdf.

Вопросы?