НИЯУ МИФИ

Национальный исследовательский ядерный университет “МИФИ”

Кафедра №41 “Криптография и безопасность компьютерных систем”

КиБКС 41

Анализ стойкости XSL-семейства алгоритмов блочного шифрования с α-отражением к атакам двумерным методом встречи посередине

Исполнитель:

Студентка НИЯУ МИФИ Мухортова А. А.

Научный руководитель:

д. ф.-м. н., профессор ИИКС НИЯУ МИФИ Пудовкина М.А.

Москва, 2024

Содержание

- Алгоритмы блочного шифрования MANTIS и PRINCE
- XSL-семейство алгоритмов блочного шифрования с α-отражением
- Многомерный метод встречи посередине
- Атака на 8-раундовые алгоритмы семейства
- Сложность алгоритма
- Заключение

Алгоритмы блочного шифрования MANTIS и PRINCE

- MANTIS предложен на ASIACRYPT-2016.
- PRINCE предложен на CRYPTO-2012.
- Общие черты:
  - низкоресурсный,
  - свойство α-отражения,
  - алгоритм развертывания ключа,
  - длина блока 64 бита, длина ключа 128 бит, 12 раундов.
- Различия:
  - раундовая функция.

Атаки на алгоритмы блочного шифрования MANTIS и PRINCE

- MANTIS
  - Chen, S., Liu, R., Cui, T. et al. Automatic search method for multiple differentials and its application on MANTIS. // Sci. China Inf. Sci.62, 32111 (2019).
  - Dobraunig, Christoph Eichlseder, Maria Kales, Daniel Mendel, Florian. (2016). Practical Key-Recovery Attack on MANTIS5. // IACR Transactions on Symmetric Cryptology. 2016.
  - Eichlseder, M., Kales, D. (2018). Clustering Related-Tweak Characteristics: Application to MANTIS-6. // IACR Transactions on Symmetric Cryptology, 2018(2), 111–132.
- PRINCE
  - Rasoolzadeh Shahram, Raddum H˚avard. Cryptanalysis of PRINCE with Minimal Data. 2016. 01. C. 109–126.
  - Morawiecki, P. (2017). Practical attacks on the round-reduced PRINCE. // IET Information Security, 11(3), 146–151. Portico.

Алгоритмы блочного шифрования MANTIS и PRINCE

Блок открытого текста m — матрица 4×4:

$$m = m_0 || m_1 || \dots || m_{15}, \quad m \in M_4\big(V_4(2)\big),$$

$$m_i \in V_4(2),\ i \in \{0, \dots, 15\},$$

$V_m(2^n)$ – m-мерное векторное пространство над $GF(2^n)$,

$M_n(A)$ – множество квадратных матриц размера $n \times n$, элементы из множества A.

Алгоритмы блочного шифрования MANTIS и PRINCE

Алгоритм развертывания ключа:

$$k = k_0 \,||\, k_1 \quad \rightarrow \quad k' = k_0 \,||\, k'_0 \,||\, k_1, \qquad \text{где } k'_0 = (k_0 >>> 1) \oplus (k_0 >> 63)$$

$$k \in V_{128}(2), \qquad k_0, k'_0, k_1 \in V_{64}(2), \qquad k' \in V_{192}(2)$$

Свойство α-отражения:

$$E^{-1}(p, k') = E(p, k''),$$

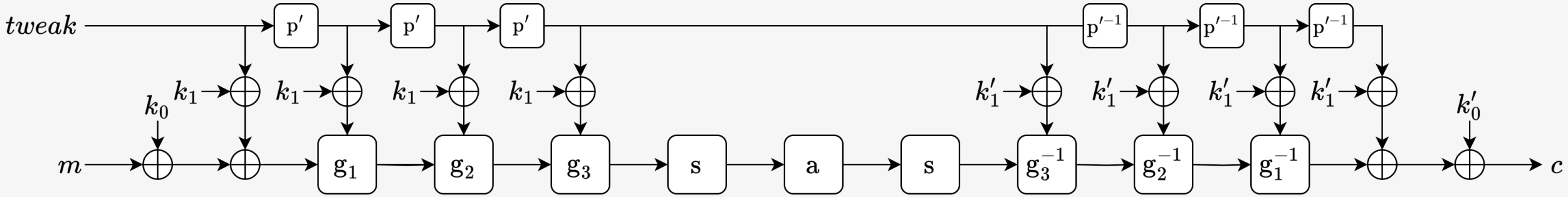
где $k'' = f(k', \alpha)$ — сопряжённый ключ.

$$f(k', \alpha) = k'_0 \,||\, k_0 \,||\, k_1 \oplus \alpha.$$

Для PRINCE $\alpha = 0xc0ac29b7c97c50dd.$

Для MANTIS $\alpha = 0x243f6a8885a308d3.$

Алгоритм блочного шифрования MANTIS



Раундовая функция $g_i: V_{64}(2) \to V_{64}(2)$, $\quad g_i(x) = a \circ p \circ h_{k_i} \circ h_{c_i} \circ s\,(x)$,

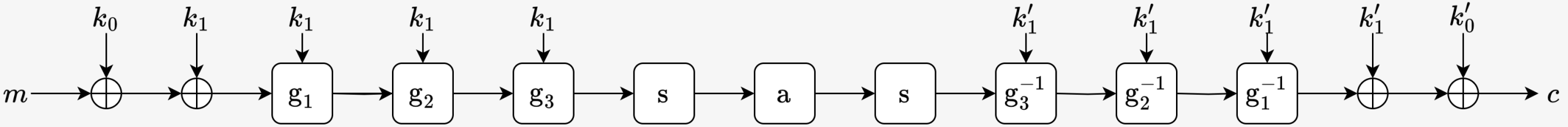
s — S-box,

h_i — побитовое сложение с i,

p — перестановка,

a — линейное преобразование, задающееся инволютивной матрицей.

Алгоритм блочного шифрования PRINCE



Раундовая функция $g_i: V_{64}(2) \to V_{64}(2)$, $\quad g_i(x) = h_{k_i} \circ h_{c_i} \circ p \circ a \circ s\,(x)$,

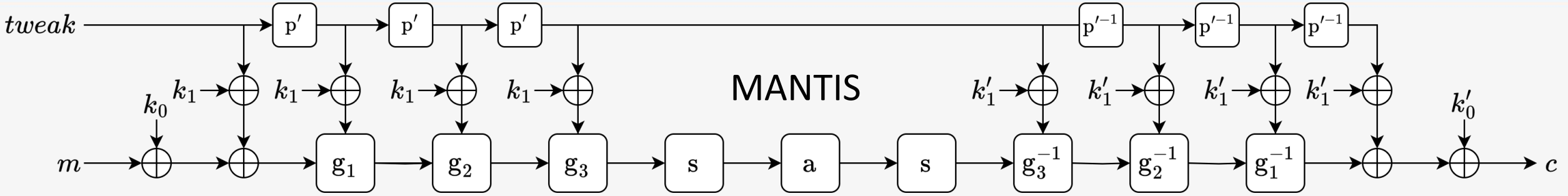
s — S-box,

h_i — побитовое сложение с i,

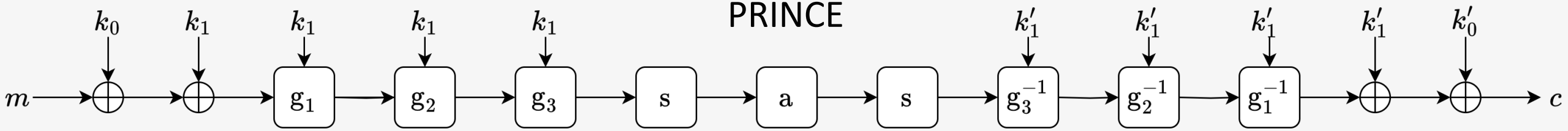
p — перестановка,

a — линейное преобразование, задающееся инволютивной матрицей.

Раундовая функция MANTIS и PRINCE

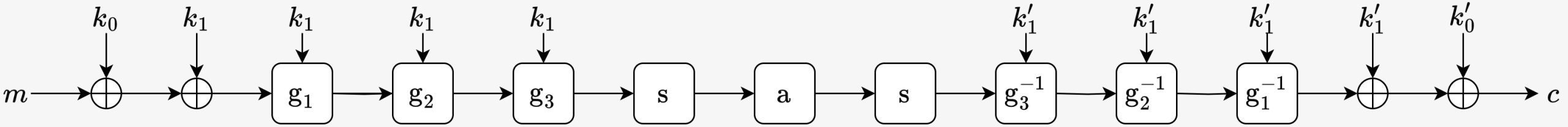


$$g_i(x) = a \circ p \circ h_{k_i} \circ h_{c_i} \circ s\ (x)$$



$$g_i(x) = h_{k_i} \circ h_{c_i} \circ p \circ a \circ s\ (x)$$

α-XSL-семейство алгоритмов блочного шифрования



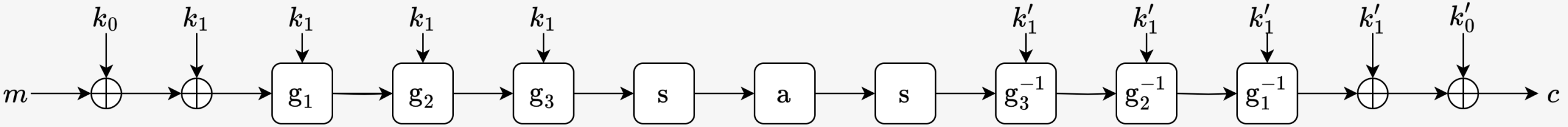
Открытый текст представим в виде d r-битных ячеек:

$$d = \delta^2, \delta \in \{4,5, \dots\}: m = m_0 || m_1 || \dots || m_{d-1},$$

$$m \in M_\delta\big(V_r(2)\big), \qquad m_i \in V_r(2), \qquad i \in \{0, \dots, \delta - 1\}$$

MANTIS и PRINCE — частные случаи при $d = 16,\ r = 4$.

α-XSL-семейство алгоритмов блочного шифрования



Раундовая функция $g_i(x) = h \circ l \circ s\,(x)$ или $g_i(x) = l \circ h \circ s\,(x)$,

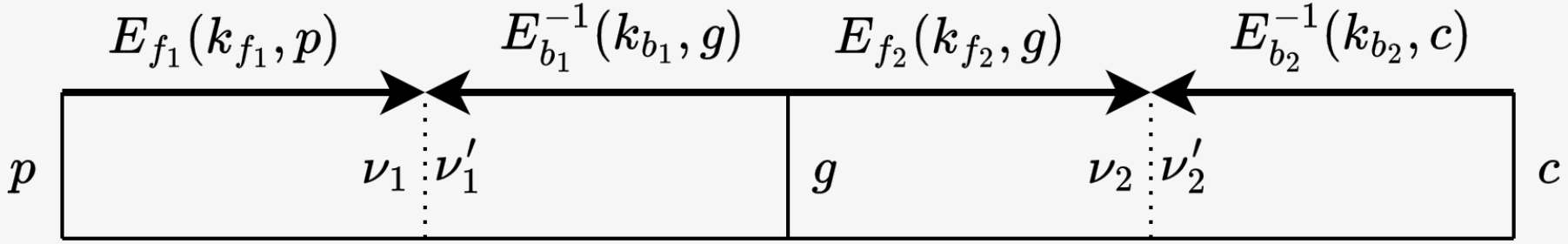
s — S-box,

h — побитовое сложение с раундовой константой и ключом,

l — линейное преобразование, задающееся инволютивной матрицей и перестановкой ячеек,

$l = a \circ p$ или $l = p \circ a$, где p — перестановка ячеек, a — инволютивная матрица.

Многомерный метод встречи посередине



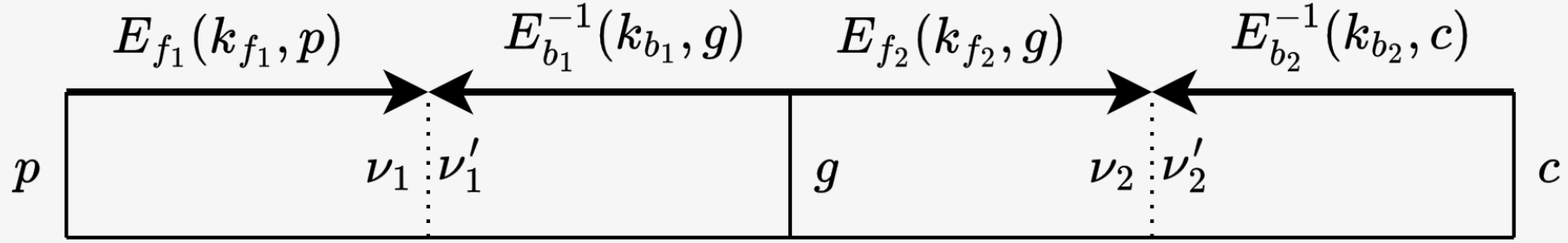
Впервые был предложен Бо Жу и Гуан Гоном в 2011 году применительно к низкоресурсному алгоритму блочного шифрования KATAN.

В 2016 году был предложен для атаки 8-раундового и 10-раундового алгоритма шифрования PRINCE.

Временная сложность:

$$2^{|k_{f_1}|} + 2^{|k_{b_n}|} + 2^{|g_1|} \cdot \left(2^{|k_{b_1}|} + 2^{|k_{f_2}|} + 2^{|g_2|} \cdot \left(2^{|k_{b_2}|} + 2^{|k_{f_3}|} + \cdots\right)\right).$$

Многомерный метод встречи посередине



Функция зашифрования $E_k(x) = E_{k_{b_2}} \circ E_{k_{f_2}} \circ E_{k_{b_1}} \circ E_{k_{f_1}}(x), \quad E_k(x): V_n(2) \to V_n(2).$

$p, c \in V_n(2)$ — открытый текст и шифртекст соответственно,

$\nu_1 = E_{k_{f_1}}(p), \qquad \nu_1' = E_{k_{b_1}}^{-1}(g),$

$\nu_2 = E_{k_{f_1}}(g), \qquad \nu_2' = E_{k_{b_2}}^{-1}(c),$

$g \in V_n(2)$ — перебираемое состояние посередине

Атака на 8-раундовые алгоритмы

x — состояние после трех раундов зашифрования,

$x' = \mathrm{s} \circ \mathrm{a} \circ s(x)$,

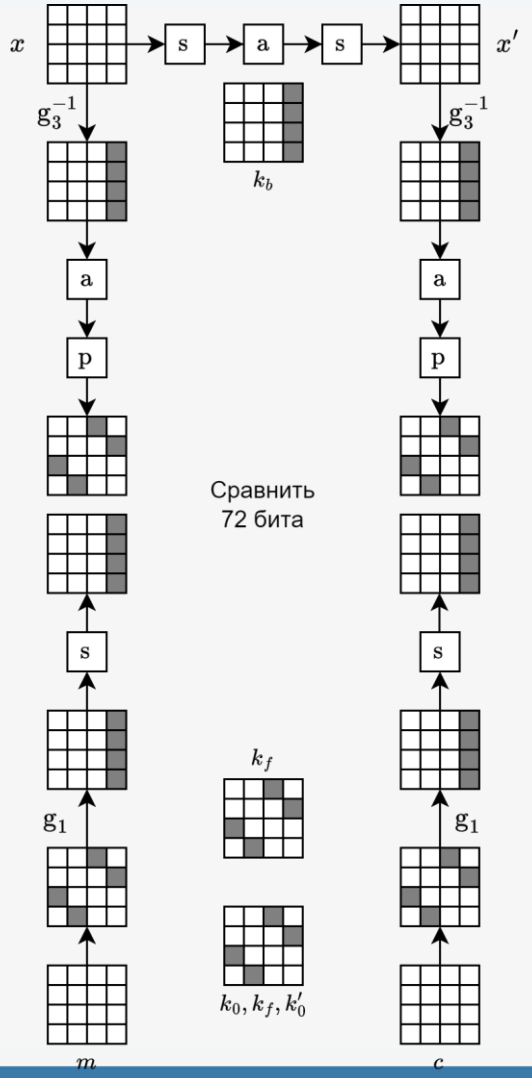
k_f — ключ, перебираемый со стороны открытого текста и шифртекста,

k_b — ключ, перебираемый со стороны x,

k_0 — ключ отбеливания,

Серые ячейки — не перебираемые ячейки,

Белые — перебираемые ячейки.



Атака на 8-раундовые алгоритмы

Раундовая функция

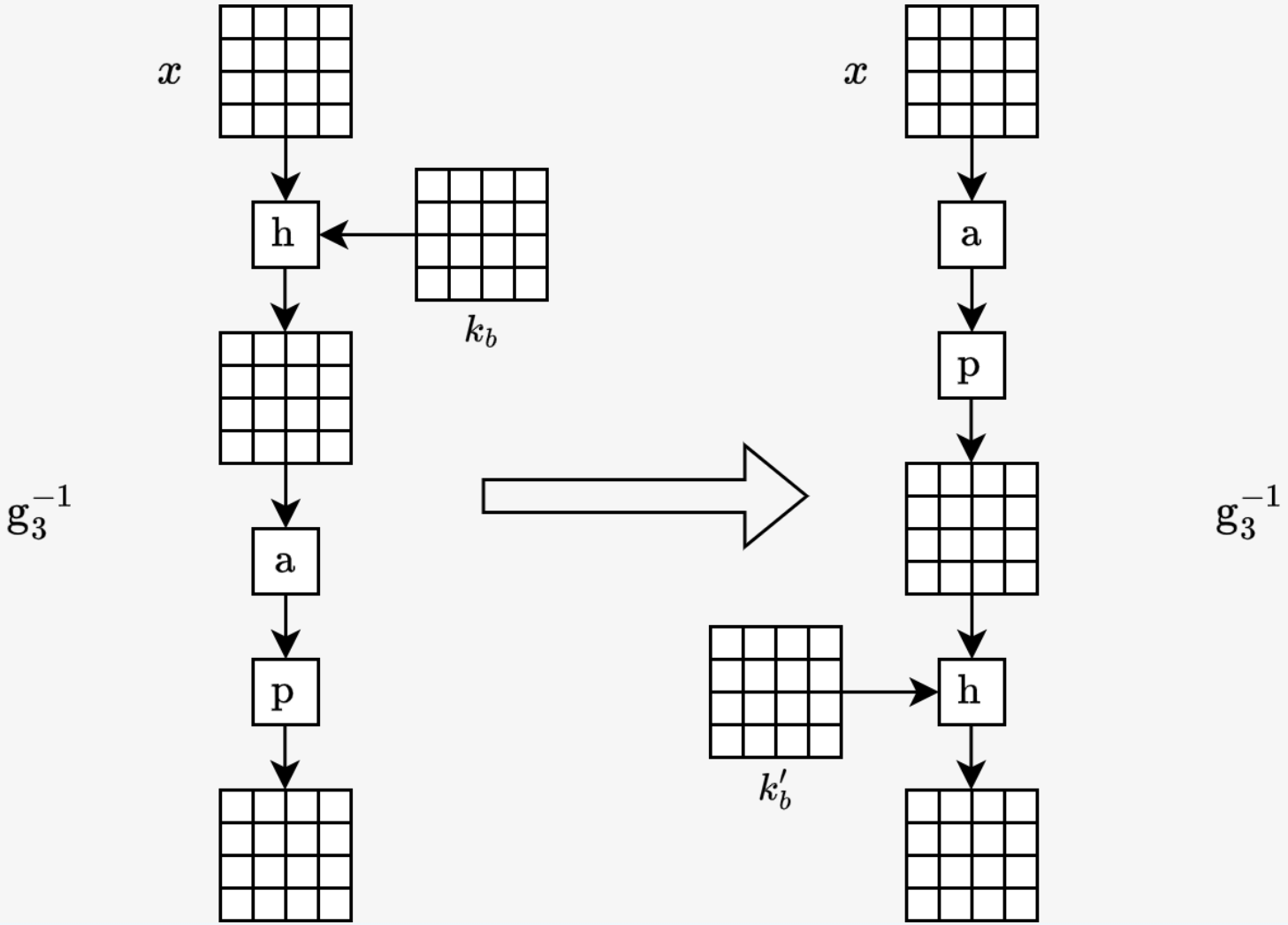
$$g_i = hls(\cdot).$$

Преобразуем ключ

$$k_b^1 = l(k_b).$$

Новая раундовая функция

$$g_i = lhs(\cdot).$$



Атака на 8-раундовые алгоритмы

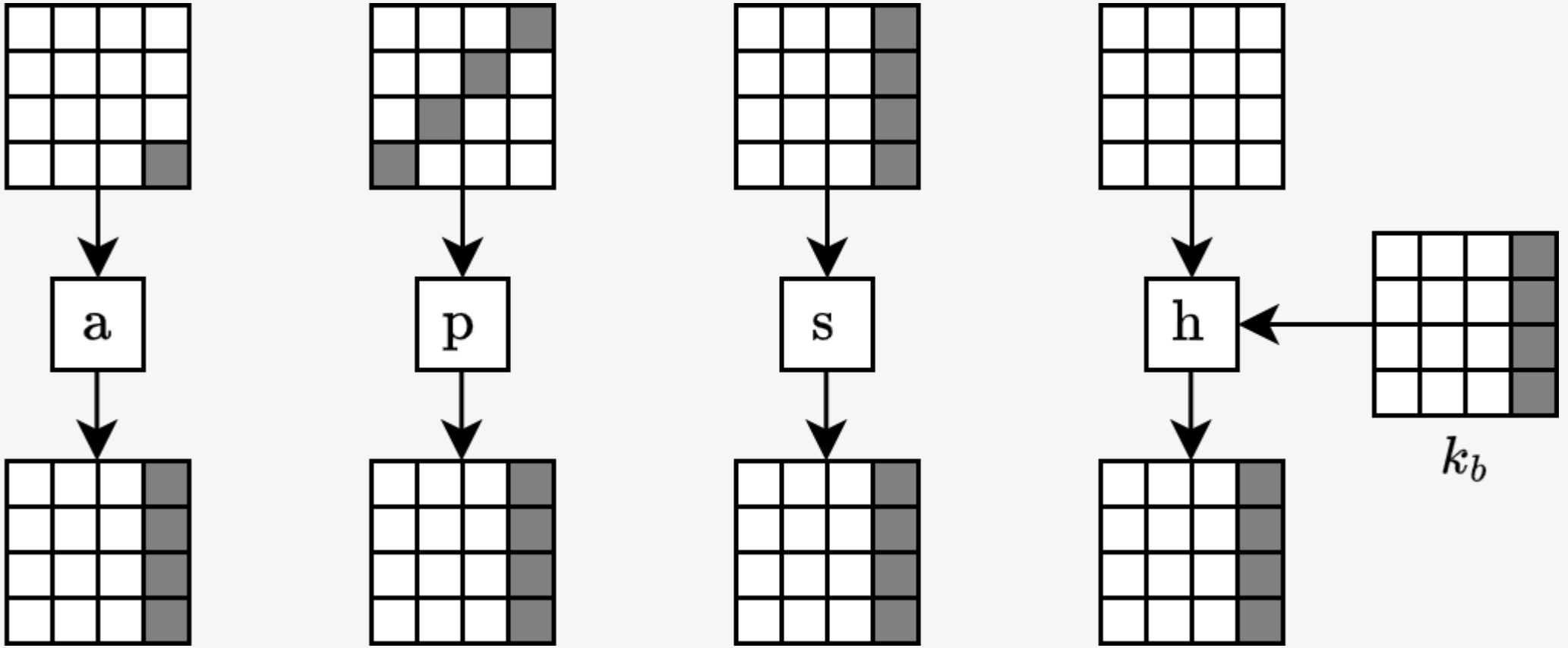


Иллюстрация атаки

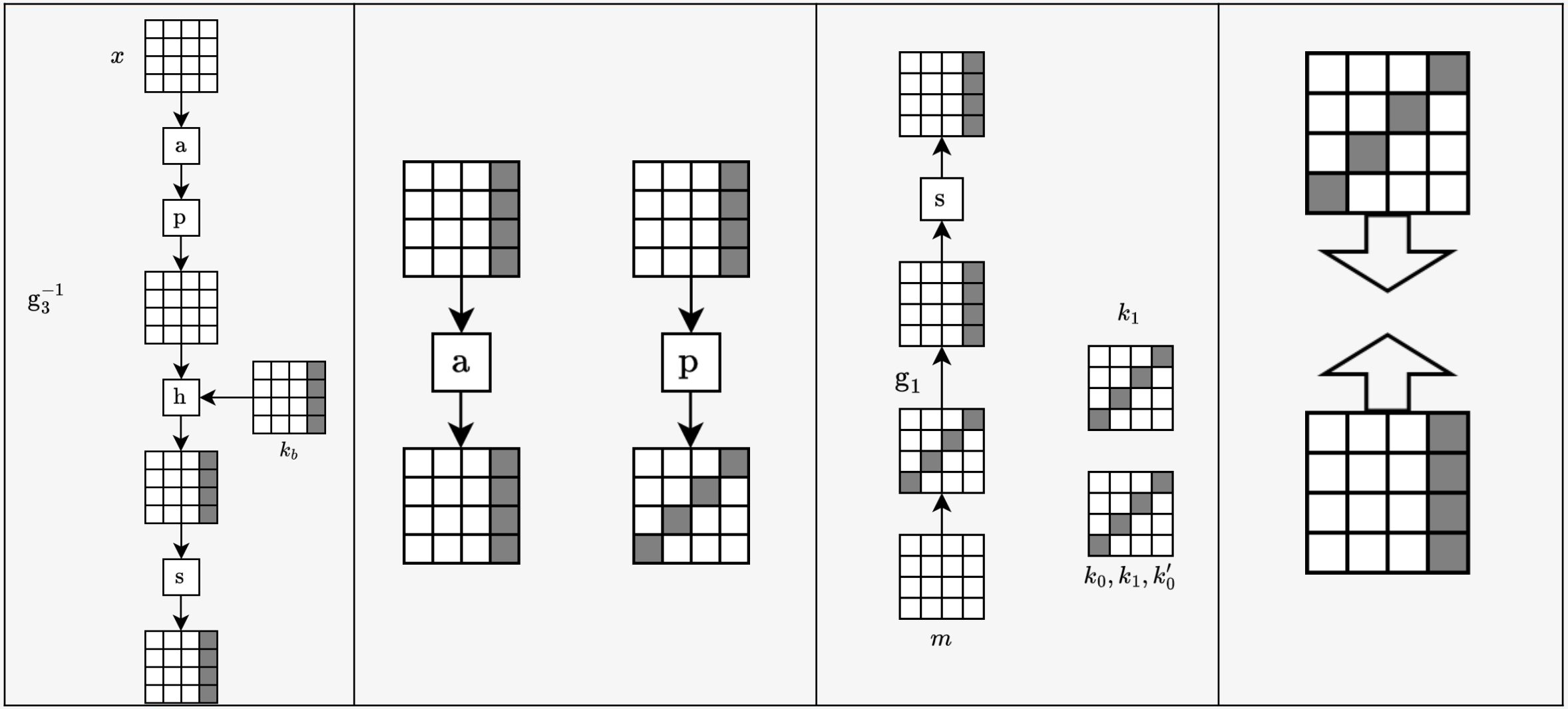
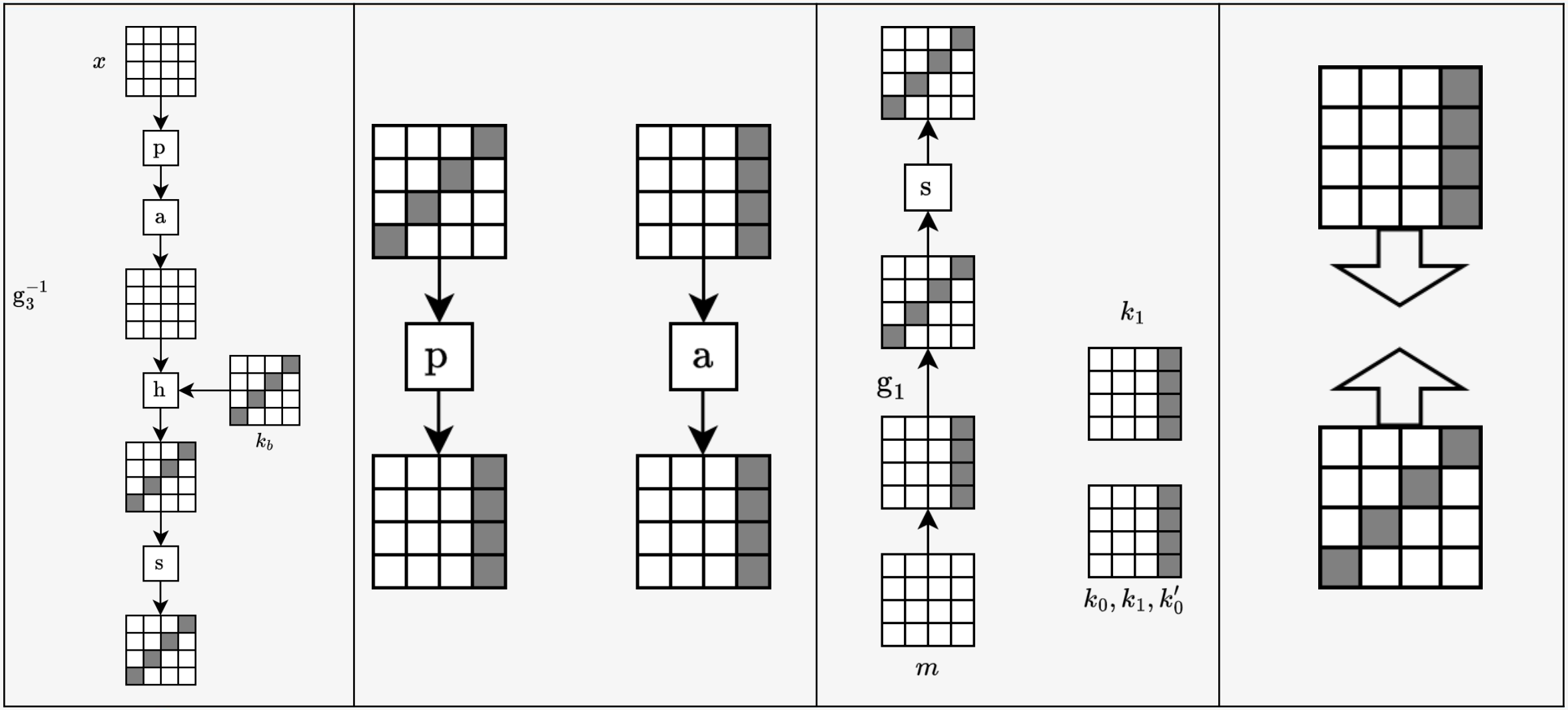


Иллюстрация атаки



Атака на 8-раундовые алгоритмы

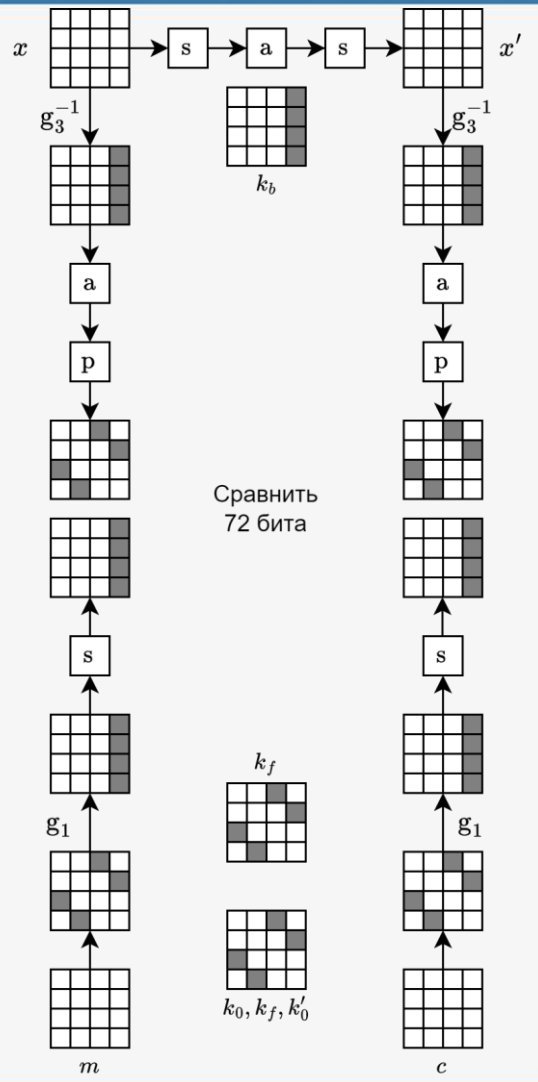
$\mathcal{T}$ — пустая таблица
для $k_c \in \mathrm{C}(k_f, k_b)$:
  для $k_w \in B(k_0)$:
    для $k_s \in \left(B(k_f) \setminus C(k_f, k_b)\right)$:
      $v_1 \leftarrow sg_{k_f} h_{k_f} h\_k_0(p)$
      $v_2 \leftarrow sg_{k_f} h'_{k_f} h_{k_0}{}'(c)$
      $\mathcal{T} \leftarrow \{(v_1, v_2) : (k_w, k_s)\}$
  для $x \in \mathbb{F}_2^{dr}$:
    $x' \leftarrow (s \circ a \circ s)(x)$
    для $k_m \in \left(B(k_b) \setminus C(k_f, k_b)\right)$:
      $v'_1 \leftarrow ag_{k_b}^{-1}(x)$
      $v'_2 \leftarrow ag_{k_b}^{-1}(x')$
      если $\exists (k_w, k_s) : (k_w, k_s) = \mathcal{T}[(v'_1, v'_2)]$
        если биты (k_w, k_s, k_m, k_c) совпадают:
          если верно для другой пары (p', c'):
            вернуть (k_w, k_s, k_m, k_c)

$C(k, k')$ — множество общих бит k и k',

$B(k)$ — множество перебираемых бит k.

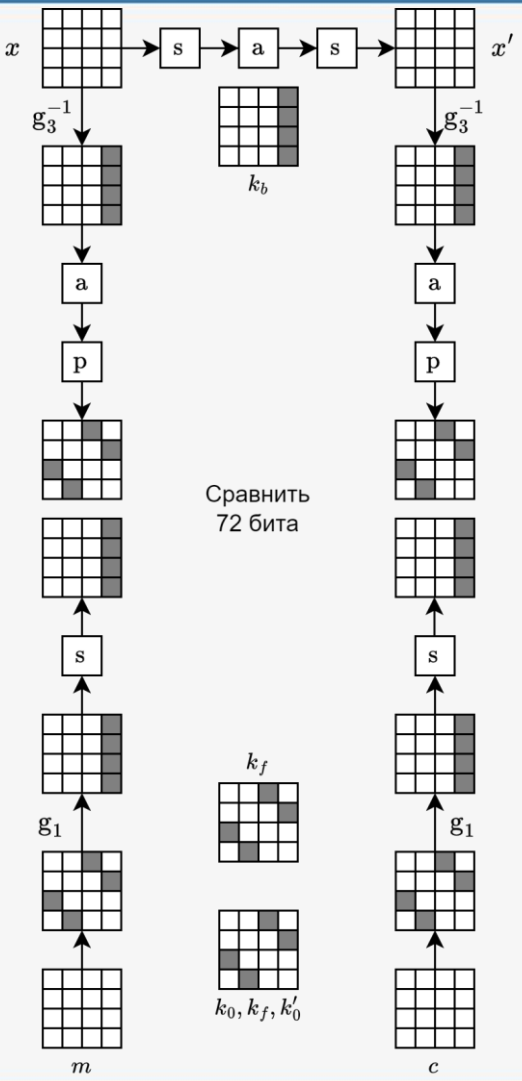
Атака на 8-раундовые алгоритмы

$\mathcal{T}$ — пустая таблица
для $k_c \in \mathrm{C}(k_f, k_b)$:
  для $k_w \in B(k_0)$:
    для $k_s \in \left(B(k_f) \setminus C(k_f, k_b)\right)$:
      $v_1 \leftarrow sg_{k_f} h_{k_f} h\_k_0(p)$
      $v_2 \leftarrow sg_{k_f} h'_{k_f} h_{k_0}{}'(c)$
      $\mathcal{T} \leftarrow \{(v_1, v_2): (k_w, k_s)\}$
  для $x \in \mathbb{F}_2^{dr}$:
    $x' \leftarrow (s \circ a \circ s)(x)$
    для $k_m \in \left(B(k_b) \setminus C(k_f, k_b)\right)$:
      $v'_1 \leftarrow ag_{k_b}^{-1}(x)$
      $v'_2 \leftarrow ag_{k_b}^{-1}(x')$
      если $\exists (k_w, k_s): (k_w, k_s) = \mathcal{T}[(v'_1, v'_2)]$
        если биты (k_w, k_s, k_m, k_c) совпадают:
          если верно для другой пары (p', c'):
            вернуть (k_w, k_s, k_m, k_c)



Временная сложность атаки

d	r	Временная сложность атаки	Временная сложность полного перебора	Необходимый объем памяти
16	4	$2^{110.8}$	2^{128}	От 2^{64} до 2^{68} ячеек памяти по 72 бит
16	8	$2^{221.8}$	2^{256}	От 2^{128} до 2^{136} ячеек памяти по 144 бит
64	4	$2^{477.9}$	2^{512}	От 2^{256} до 2^{324} ячеек памяти по 392 бит
d	r	$2^{r(2d-\sqrt{d})}\left(2d+d-\sqrt{d}\right)\frac{1}{d}\cdot\frac{1}{8}$	2^{2rd}	От $2^{r\left(d-\sqrt{d}+\frac{1}{2}d-\sqrt{d}\right)}$ до $2^{r\left(d-\sqrt{d}+\frac{1}{2}d-\sqrt{d}+1\right)}$ ячеек памяти по $2r\left(d-2\sqrt{d}+1\right)$ бит



Атака на PRINCE и MANTIS

	MANTIS	PRINCE
Временная сложность	$2^{110.8}$ функций зашифрования	$2^{110.8}$ функций зашифрования
Необходимый объем памяти	2^{67} ячеек памяти по 72 бита	2^{65} ячеек памяти по 72 бита
Необходимый объем материала	2 пары открытый текст / шифртекст	2 пары открытый текст / шифртекст

Заключение

- Предложено XSL-семейство алгоритмов блочного шифрования с α-отражением.
- Разработана атака на 8-раундовые алгоритмы семейства.
- Впервые применена атака на MANTIS.
- Результаты для PRINCE совпадают с ранее известными [1].

1. Rasoolzadeh Shahram, Raddum H˚avard. Cryptanalysis of PRINCE with Minimal Data. 2016. 01. С. 109–126.

Спасибо за внимание!