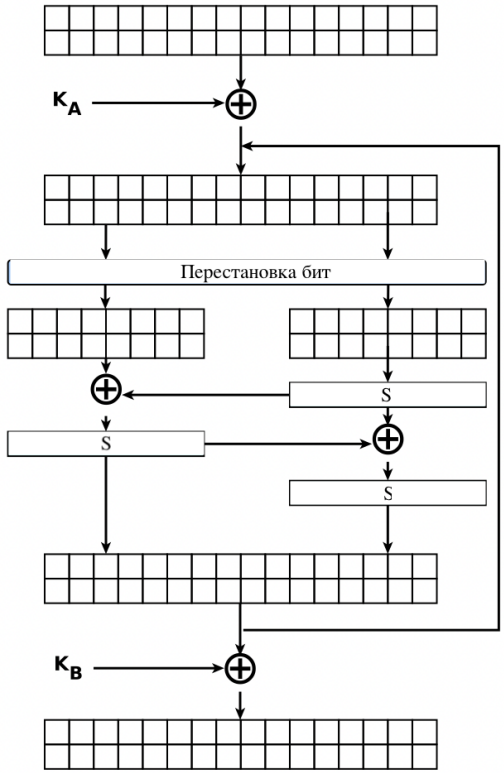
Об одном обобщении Flex-подобных алгоритмов блочного шифрования и его алгебраических свойствах

Исполнитель: А.М. Смирнов
Научный руководитель: д. ф.-м. н. М.А. Пудовкина

НИЯУ МИФИ

Москва, 2025

Алгоритм блочного шифрования FlexAEAD



- Один раунд функции зашифрования представлен на рисунке.
- Предложен в 2019 году.
- Длины блоков — 64, 128, 256 бит. Длина ключа — 128 и 256 бит. Число раундов — 15, 18 и 21.

Обзор существующих работ по анализу алгоритма FlexAEAD

1. SEichlseder, M., Kales, D., Schofnegger, M.: Forgery Attacks on FlexAE and FlexAEAD. Cryptology ePrint Archive, Report 2019/679 (2019), https://eprint.iacr.org/2019/679
Предложена атака с использованием подхода классического разностного анализа на 5 раундов Flex-64, 6 раундов Flex-128, 7 раундов Flex-256.

2. Mostafizar R., Dhiman S. and Gotman P. Cryptoanalysys of FLEX-AEAD // Cryptology ePrint Archive, Paper 2019/539 URL: https://eprint.iacr.org/2019/539.
Предложена атака различения на 4 раунда Flex-64, 7 раундов Flex-128, 8 раундов Flex-256 с использованием подхода «йо-йо».

Алгоритм блочного шифрования FlexAEAD

- $V_n(2^m)$ — n-мерное векторное пространство над $\mathbb{F}_{2^m}$
- Раундовая функция $g_k : V_n(2^m) \to V_n(2^m)$,

$$g_k = sqhq^{-1}v_k,$$

$$q : \alpha \to \alpha', \ , \alpha \in V_{n\times m}(2), \alpha' \in V_n(2^m),$$

$$\alpha'_i = 2^{m-1}\cdot\alpha_{1+m(i-1)}+...+2\cdot\alpha_{m-1+m(i-1)}+\alpha_{m+m(i-1)}, \alpha = (\alpha_1, ..., \alpha_n),$$

$$\alpha' = (\alpha'_1, ..., \alpha'_{n\times m}), i = 1, ..., n.$$

$$v_k : \alpha \to \alpha \oplus k, \ k, \alpha = (\alpha_1, \alpha_2, ..., \alpha_n) \in V_n(2^m)$$

Алгоритм блочного шифрования FlexAEAD

$$s : \alpha \to (\pi(\alpha_1 \oplus \pi(\alpha_{n/2+1})), \pi(\alpha_2 \oplus \pi(\alpha_{n/2+2})), ...,$$

$$\pi(\alpha_{n/2} \oplus \pi(\alpha_n)), \pi(\pi(\alpha_1 \oplus \pi(\alpha_{n/2+1})) \oplus \pi(\alpha_{n/2+1})), ...,$$

$$\pi(\pi(\alpha_{n/2} \oplus \pi(\alpha_n)) \oplus \pi(\alpha_n))), \alpha = (\alpha_1, \alpha_2, ..., \alpha_n) \in V_n(2^m)$$

$$\pi \in S(\mathbb{F}_{2^m}),$$

$h : V_{n\times m}(2) \to V_{n\times m}(2)$ — линейное отображение,

определяемое перестановочной матрицей.

- Функция зашифрования t-раундового алгоритма блочного шифрования FlexAEAD $\tilde{g}$ задается равенством

$$\tilde{g}(\alpha, k_1, k_2) = g_{k_1,k_2}(\alpha) = v_{k_2}(g_{0_n})^{t-1} g_{k_1}(\alpha).$$

r-обобщение Flex-подобных алгоритмов блочного шифрования

Раундовая функция $g_k : V_n(2^m) \to V_n(2^m)$,

$$g_k = s^{(r)} q h q^{-1} v_k,$$

$$s^{(0)} = s,$$

$$s^{(r)} : \alpha \to (\pi(s^{(r-1)}(\alpha)_1 \oplus \pi(s^{(r-1)}(\alpha)_{n/2+1})), \pi(s^{(r-1)}(\alpha)_2 \oplus$$

$$\oplus \pi(s^{(r-1)}(\alpha)_{n/2+2})), ..., \pi(s^{(r-1)}(\alpha)_{n/2} \oplus \pi(s^{(r-1)}(\alpha)_n)),$$

$$\pi(\pi(s^{(r-1)}(\alpha)_1 \oplus \pi(s^{(r-1)}(\alpha)_{n/2+1})) \oplus \pi(s^{(r-1)}(\alpha)_{n/2+1})), ...,$$

$$\pi(\pi(s^{(r-1)}(\alpha)_{n/2} \oplus \pi(s^{(r-1)}(\alpha)_n)) \oplus \pi(s^{(r-1)}(\alpha)_n))),$$

$$\alpha = (\alpha_1, \alpha_2, ..., \alpha_n) \in V_n(2^m).$$

r-обобщение Flex-подобных алгоритмов блочного шифрования

Утверждение 1

Нелинейное преобразование $s^{(r)} : V_n(2^m) \to V_n(2^m)$ биективно.

Утверждение 2

Пусть $\alpha \in V_n(2^m)$, $\alpha = (0, \alpha_2, ..., \alpha_n)$, $\pi \in S(\mathbb{F}_{2^m})$, $\pi(\alpha_{n/2+1}) = 0$ и в разложении подстановки π на независимые циклы существует транспозиция вида $(0, \alpha_{n/2+1})$. Тогда $(s^{(r)}(\alpha))_1 = \alpha_{n/2+1}$ для любого $r \in \mathbb{N}_0$.

r-обобщение Flex-подобных алгоритмов блочного шифрования

Утверждение 3

Пусть $\alpha \in V_n(2^m)$, для всех $i \in 1, ..., n/2$ разность

$$(s^{(l)}(\alpha))_i \oplus \pi((s^{(l)}(\alpha))_{i+n/2})$$

принимает различные ненулевые значения, а подстановка π имеет цикловую структура вида $[m_1, m_2, ..., m_q]$, $m^{(e)} = \max\{m_1, m_2, ..., m_q\}$, $0 \leq l \leq r$. Тогда

$$r \leq (m^{(e)} - 2 + \sum_{i=1, m_i \neq m^{(e)}}^{t} (m_i - 1))^n.$$

r-обобщение Flex-подобных алгоритмов блочного шифрования

Рассмотрим группу подстановок $G^{(r)} = \langle s^{(0)}, ..., s^{(r)} \rangle$, действующую на множестве $V_n(2^m)$.

Утверждение 4

Пусть $\pi \in S(\mathbb{F}_{2^m})$ и уравнение

$$\pi^2(x) \oplus \pi(x) \oplus x = 0 \tag{1}$$

имеет единственное решение относительно $x \in \mathbb{F}_{2^m}$. Тогда группа $G^{(r)}$, действующая на множестве $V_n(2^m)$, интранзитивна при произвольных значениях $n, m > 1$, $r \geq 0$.

r-обобщение Flex-подобных алгоритмов блочного шифрования

Утверждение 5

Пусть $\pi \in S(\mathbb{F}_{2^m})$. Тогда число подстановок π, удовлетворяющих условию (1), равно $2 \cdot (2^m - 1)!$.

Рассмотрим группу подстановок $G_k'^{(r)} = \langle s_k^{(0)}, ..., s_k^{(r)} \rangle$, где $s_k^{(i)} = s^{(i)} v_k$, $k \in V_n(2^m)$, $i = 0, 1, .., r$, действующую на множестве $V_n(2^m)$.

Утверждение 6

Пусть $\pi \in S(\mathbb{F}_{2^m})$. Тогда группа $G_k'^{(r)}$, действующая на множестве $V_n(2^m)$, является транзитивной при произвольных значениях $n, m > 1$, $r \geq 0$.

Утверждение 7

Пусть $\pi \in S(\mathbb{F}_{2^m})$ удовлетворяет условию (1). Тогда группа $G_k'^{(r)}$,действующая на множестве $V_n(2^m)$, является импримитивной.

Модель предлагаемой атаки на r-обобщение Flex-подобных алгоритмов блочного шифрования

- Для произвольного $\alpha = (\alpha_1, \alpha_2, ..., \alpha_n) \in V_n(2^m)$ определим отображение $w : V_n(2^m) \to V_n(2)$:

$$w^{(i)}(\alpha) = I(\alpha_i \neq 0),\ w(\alpha) = (w^{(1)}(\alpha), w^{(2)}(\alpha), ..., w^{(n)}(\alpha))$$

- Для произвольных

$$\alpha = (\alpha_1, ..., \alpha_n) \in V_n(2^m), \beta = (\beta_1, ..., \beta_n) \in V_n(2^m),$$

$$\theta = (\theta_1, ..., \theta_n) \in V_n(2)$$

и каждого $i \in \{1, ..., n\}$ определим отображение $\rho_\theta^{(i)} : V_n(2^m)^2 \to \mathbb{F}_2$,

$$\rho_\theta^{(i)}(\alpha, \beta) = \begin{cases} \beta_i, \text{ если } \theta_i = 1, \\ \alpha_i, \text{ если } \theta_i = 0, \end{cases}$$

Модель предлагаемой атаки на r-обобщение Flex-подобных алгоритмов блочного шифрования

- Пусть $I = \{1, 2, ..., n\}$, $f : V_n(2^m) \to V_n(2^m)$, $f = (f_1, f_2, ..., f_n)$, $f_i : V_n(2^m) \to \mathbb{F}_{2^m}$.
- $V(f_i)$ — множество номеров существенных переменных в f_i, $s \in S(I)$, $t_i = s(i)$, $i \in I$.
- Отношение $\mathcal{R}_f$ на множестве I координат вектора $\alpha = (\alpha_1, ..., \alpha_n)$ определяется следующим образом: $(i, j) \in \mathcal{R}_f$, если существуют f_{t_1}, ..., f_{t_n}, удовлетворяющие условиям:
  1) существуют такие $k, l \in I$, что $i \in V(f_{t_k})$, $j \in V(f_{t_l})$, если $k \neq l$;
  2) выполнено неравенство
  $V(f_{t_k}) \cup V(f_{t_l}) \subseteq \{1, ..., n/4, n/2 + 1, ..., 3n/4\}$ либо
  $V(f_{t_k}) \cup V(f_{t_l}) \subseteq \{n/4 + 1, ..., n/2, 3n/4 + 1, ..., n\}$.

Замечание

Существует ровно два различных класса эквивалентности $[i]_{\mathcal{R}_{g^{t/2}}}$, $[j]_{\mathcal{R}_{g^{t/2}}}$ над $g^{t/2}$.

Модель предлагаемой атаки на r-обобщение Flex-подобных алгоритмов блочного шифрования

Лемма 1

Пусть $\alpha^{(0)}, \alpha^{(1)}, \beta^{(0)}, \beta^{(1)}$ – произвольные элементы векторного пространства $V_n(2^m)$, $\tilde{s}$ — фиксированная подстановка из $S(V_n(2^m))$, действующая биективно и на множестве классов эквивалентности $[i_1]_{\mathcal{R}_{g^{r/2}}}$, ...,$[i_k]_{\mathcal{R}_{g^{t/2}}}$ на $g^{t/2}$ независимо. Более того, $\beta^{(0)} = v_{k_2}\tilde{s}\tilde{h}\tilde{s}\tilde{h}v_{k_1}(\alpha^{(0)})$, $\beta^{(1)} = v_{k_2}\tilde{s}\tilde{h}\tilde{s}\tilde{h}v_{k_1}(\alpha^{(1)})$, $\theta = (\theta_1, ..., \theta_n)$,

$$\theta_i = \begin{cases} 1, \text{ если } i \in [i_l]_{\mathcal{R}_{g^{t/2}}} \text{ для некоторого } 1 \leq l \leq k, \\ 0, \text{ иначе,} \end{cases}$$

$\beta'^{(0)} = \rho_\theta(\beta^{(0)}, \beta^{(1)})$, $\beta'^{(1)} = \rho_\theta(\beta^{(1)}, \beta^{(0)})$.
Тогда

$$w((v_{k_2}\tilde{s}\tilde{h}\tilde{s}\tilde{h}v_{k_1})^{-1}(\beta'^{(0)}) \oplus (v_{k_2}\tilde{s}\tilde{h}\tilde{s}\tilde{h}v_{k_1})^{-1}(\beta'^{(1)})) = w(\alpha'^{(0)} \oplus \alpha'^{(1)}) =$$

$$= w(\alpha^{(0)} \oplus \alpha^{(1)}).$$

Модель предлагаемой атаки на r-обобщение Flex-подобных алгоритмов блочного шифрования. Общая идея

- Рассмотрим подстановку $\tilde{s} : V_n(2^m) \to V_n(2^m)$, имеющую вид:

$$\tilde{s} = (s^{(r)}h)^{(t/2-1)}s^{(r)}.$$

- Для выбранных текстов $\gamma^{(0)}$, $\gamma^{(1)}$, удовлетворяющих условию $w(\gamma^{(0)} \oplus \gamma^{(1)}) = (1, 0, ..., 0)$, вычислить $\alpha^{(0)} = qh^{-1}q^{-1}(\gamma^{(0)})$, $\alpha^{(1)} = qh^{-1}q^{-1}(\gamma^{(1)})$. Проверить условие из Леммы 1.
- Для атаки требуется 4 пары открытый текст —шифртекст.
- Трудоемкость атаки — одна операция зашифрования.
- Надежность атаки — $\frac{2^{nm}-2^{nm/2}}{2^{nm}}$.

Эксперимент

Таблица: Результаты проведенного эксперимента

Текст $\gamma^{(0)}$	Текст $\gamma^{(1)}$	Результат
(12,0,13,0,15,0,1,0)	(1,0,0,0,0,0,0,0)	1
(12,0,13,0,15,0,1,0)	(0,0,1,0,0,0,0,0)	1
(12,0,13,0,15,0,1,0)	(0,0,0,0,0,0,1,0)	1
(1,0,1,0,1,0,1,0)	(0,0,0,0,0,0,0,0)	1
(1,0,2,0,3,0,5,0)	(0,0,1,0,0,0,1,0)	1
(1,0,1,0,2,0,1,0)	(1,0,0,0,0,0,1,0)	1
(121,0,17,0,12,0,1,0)	(234,0,26,0,27,0,0,0)	1
(95,0,232,0,11,0,1,0)	(110,0,2,0,7,0,1,0)	1

Вопросы???