О разностных характеристиках обобщенного алгоритма шифрования Фейстеля 2-го типа

Пудовкина М.А.

Национальный исследовательский ядерный университет (МИФИ)

Невозможные и усеченные разности

- Невозможные (усечённые) разности и разностные характеристики с вероятностью 1.
- Невозможные разности – атака на Skipjack, 1999 г.

  Biham E. Biryukov A., Shamir A., Cryptanalysis of Skipjack Reduced to 31 Rounds Using Impossible Differentials. In: EUROCRYPT 1999, LNCS, v.2595.
- Невозможные разности используются для атак на AES (7-8 раундов), CLEFIA, CRYPTON, Camellia и т.д.
- *Теорема Амбросимова*. [Глу00] При случайном и равновероятном выборе подстановки h из множества $S(X)$ и при $|X|\to\infty$ вероятность 2-транзитивности множества $(Gh)^3$ стремиться к 1 равномерно по всем регулярным подгруппам $G<S(X)$.

Невозможные разности

- $X^{\times}$ есть $X \setminus 0$ или $X \setminus \vec{0}$;
- $p_{\varepsilon,\delta}(v) = 2^{-t} \cdot \left|\left\{\alpha \in V_t \mid (\alpha \oplus \varepsilon)^v \oplus \alpha^v = \delta\right\}\right|, v \in S(V_t), \varepsilon, \delta \in V_t$;

  $f_{(k_1,\ldots,k_j)}$ – функция зашифрования на ключах $k_1,\ldots,k_j$.

  Для $\delta, \varepsilon \in V_m^{\times}$ обозначим:

  (1) $\delta \xrightarrow{\;j\;} \varepsilon$,

  если $p_{\delta,\varepsilon}\left(f_{(k_1,\ldots,k_j)}\right) > 0$ при $k_1,\ldots,k_j \in_U V_m$;

  (2) $\delta \not\xrightarrow{\;j\;} \varepsilon$,

  если $p_{\delta,\varepsilon}\left(f_{(k_1,\ldots,k_j)}\right) = 0$ для всех $k_1,\ldots,k_j \in V_m$;

- Если $\delta \not\xrightarrow{\;j\;} \varepsilon$, то пара (δ,ε) называются j-раундовой *невозможной разность*.

5-раундовые невозможные структуры схемы Фейстеля

Утверждение (Р. Кнудсен). Пусть g_β – произвольная подстановка на V_m для любого $\beta \in V_m$. Тогда $(\alpha, 0) \not\xrightarrow{5} (0, \alpha)$ для любого $\alpha \in V_m^\times$.

Невозможные и 1-вероятные разности обобщённой схемы Фейстеля 2-го типа

- Шифрсистемы CAST-256, MARS, SMS4, CLEFIA, Piccolo, HIGHT, и др. – на основе обобщений схемы Фейстеля
  - *Алгоритм Фейстеля 1-го типа* [Sch88], [FeiNS75]

$$b_{k^{(i)}}(\alpha_{n-1},\ldots,\alpha_0)=\left(\alpha_{n-2}\oplus q^{(0)}_{k^{(i)}}(\alpha_{n-1}),\alpha_{n-3},\ldots,\alpha_0,\alpha_{n-1}\right).$$

Если $q_k^{(0)}$ биективна, то существует ([SunLHP00]) (n^2-1)-раундовая невозможная усечённая разность

$$(0,\ldots,0,V_m^{\times})\not\to(V_m^{\times},0,\ldots,0).$$

  - *Конструкция* [ChoCKY09]

$$b_{k^{(i)}}(\alpha_{n-1},\ldots,\alpha_0)=\left(\alpha_{n-2},\alpha_{n-3},\ldots,\alpha_0,\alpha_0\oplus\ldots\oplus\alpha_{n-2}\oplus q_{k^{(i)}}(\alpha_{n-1})\right).$$

Для любых $\varepsilon,\lambda\in V_m^{\times}$ существует ([WuZZZ09], [LiSLQ10]) (n^2+n-2)-раундовая невозможная разность

$$(\varepsilon,\underbrace{0,\ldots,0}_{n-1})\not\to(\lambda,\lambda,\underbrace{0,\ldots,0}_{n-2}).$$

- **Тенденция** – попытка улучшения перемешивающих и рассеивающих свойств шифрсистем на основе обобщённой схемы Фейстеля (например, [ZhaWZ09], [ShiIHMAS11], [SuzM10]).

- $h_{k_0}^{(0)}:V_m \to V_m, h_{k_1}^{(1)}:V_m \to V_m$– преобразования, зависящие от раундовых ключей k_1, k_0.
- $v_k : V_m^4 \to V_m^4$ – обобщённая схема Фейстеля 2-го типа

$$v_k : (\tilde{\alpha}_3, \tilde{\alpha}_2, \tilde{\alpha}_1, \tilde{\alpha}_0) \to \left(\tilde{\alpha}_3, \tilde{\alpha}_2 \oplus \left(\tilde{\alpha}_3 \right)^{h_{k_1}^{(1)}}, \tilde{\alpha}_1, \tilde{\alpha}_0 \oplus \left(\tilde{\alpha}_1 \right)^{h_{k_0}^{(0)}} \right).$$

- [ZhaWZ09] – раундовая функции $g_k : V_m^4 \to V_m^4$ на основе схемы Фейстеля 2-го типа и *максимально рассеивающей матрицы* a, где

$$g_k = v_k a,\ h_\kappa = h_\kappa^{(0)} = h_\kappa^{(1)} \text{ для всех } \kappa \in V_d\ ,$$

$$a = \begin{pmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 \end{pmatrix}.$$

- [ZhaWZ09] Алгоритм VGF2, $m = 64$, $d = 128$ с преобразованием

$$\tilde{\alpha}^{h_\kappa} = \left(\left(\tilde{\alpha} \oplus \kappa_0 \right)^{su} \oplus \kappa_1 \right)^s,$$

где $u -$ максимально рассеивающая матрица алгоритма Grindahl, $\kappa = (\kappa_1, \kappa_0) \in V_{64}^2$, $s = (s_7, \ldots, s_0)$, $s_i : V_8 \to V_8 - s$-бокс алгоритма AES, $i = 0, \ldots, 7$.

Семейство $FG_l^{(4)}\left(h^{(0)},h^{(1)},\mathbf{a}\right)$ с раундовой функцией $g_k = v_k a$, $k \in V_d^2$, где

- $\mathbf{a} \in GL_4(2)$,
- $h^{(0)}: V_m \times V_d \to V_m$, $h^{(1)}: V_m \times V_d \to V_m$,

$$h^{(i)}(\alpha,k) = \alpha^{h_\kappa^{(i)}},\ \kappa \in V_d,\ \alpha \in V_m,\ i = 0,1.$$

- $A_1 = \left\{\mathbf{a}_1,\mathbf{a}_3\right\}$, $A_2 = \left\{\mathbf{a}_2,\mathbf{a}_4\right\}$ с циркулянтными максимально рассеивающими (4×4)-матрицы

$$\mathbf{a}_1 = \begin{pmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 \end{pmatrix}, \mathbf{a}_2 = \begin{pmatrix} 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 \end{pmatrix},$$

$$\mathbf{a}_3 = \begin{pmatrix} 1 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 \end{pmatrix}, \mathbf{a}_4 = \begin{pmatrix} 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 \end{pmatrix},$$

$$W^{(1)}(\varepsilon,\theta)=\left\{\left(\alpha_3,\alpha_2,\alpha_1,\alpha_0\right)\in V_m^4 \mid \alpha_3=\varepsilon,\alpha_2\oplus\alpha_1=\theta\right\},\ \varepsilon,\theta\in V_m.$$

Утверждение 1. *Если* $l\in\mathbb{N}$, $\left(k^{(1)},\ldots,k^{(l)}\right)\in V_d^l$, $\mathbf{a}\in A_1$, *то*

1) для любого вектора $(\beta,\gamma)\in\left(V_m^2\right)^{\times}$ *существует такой вектор* $\left(\beta'',\gamma''\right)\in V_m^2$, *что*

$$\left(\tilde{0},\beta,\beta,\gamma\right)\xrightarrow{g_{k^{(1)}}\cdots g_{k^{(l)}},1}\begin{cases}\left(\tilde{0},\beta'',\beta'',\gamma''\right), & l \text{ чётно},\\ \left(\beta'',\gamma'',\tilde{0},\beta''\right), & l \text{ нечётно},\end{cases}$$

2) для любого вектора $(\delta,\lambda)\in\left(V_m^2\right)^{\times}$ *существует такой вектор* $\left(\delta'',\lambda''\right)\in V_m^2$, *что*

$$\left(\delta,\lambda,\tilde{0},\delta\right)\xrightarrow{g_{k(1)}\cdots g_{k(l)},1}\begin{cases}\left(\tilde{0},\delta'',\delta'',\lambda''\right), & l \text{ нечётно},\\ \left(\delta'',\lambda'',\tilde{0},\delta''\right), & l \text{ чётно},\end{cases}$$

3) $W^{(1)}(\tilde{0},\tilde{0})\xrightarrow{g_{k(1)}\cdots g_{k(l)},1}W^{(1)}(\tilde{0},\tilde{0})$,

4) $W^{(1)}(\tilde{0},\tilde{0})\xrightarrow{g_{k(1)}\cdots g_{k(l)},0}W^{(1)}(\sigma,\sigma')$ *для любого вектора* $(\sigma,\sigma')\in\left(V_m^2\right)^{\times}$.

$$W^{(2)}(\varepsilon)=\left\{(\alpha_3,\alpha_2,\alpha_1,\alpha_0)\in V_m^4 \mid \alpha_3\oplus\alpha_1=\varepsilon\right\},\ \ \varepsilon,\theta\in V_m.$$

Утверждение 2. Если $l\in\mathbb{N}$, $\left(k^{(1)},\ldots,k^{(l)}\right)\in V_d^l$, $\mathbf{a}\in A_2$, $\varepsilon\in V_m$, *то:*

1) *для любого вектора* $(\beta,\gamma,\theta)\in\left(V_m^3\right)^{\times}$ *существует такой вектор* $(\beta',\gamma',\theta')\in\left(V_m^3\right)^{\times}$, *что*

$$\left(\beta,\gamma,\beta\oplus\varepsilon,\theta\right)\xrightarrow{g_{k^{(1)}}\cdots g_{k^{(l)}},1}\left(\beta',\gamma',\beta'\oplus\varepsilon,\theta'\right);$$

2) $W^{(2)}(\varepsilon)\xrightarrow{g_{k^{(1)}}\cdots g_{k^{(l)}},1}W^{(2)}(\varepsilon)$;

3) $W^{(2)}(\varepsilon)\xrightarrow{g_{k^{(1)}}\cdots g_{k^{(l)}},0}W^{(2)}(\varepsilon')$ *для любых* $\varepsilon\in V_m$, $\varepsilon'\in V_m\setminus\{\varepsilon\}$.

Спасибо за внимание!