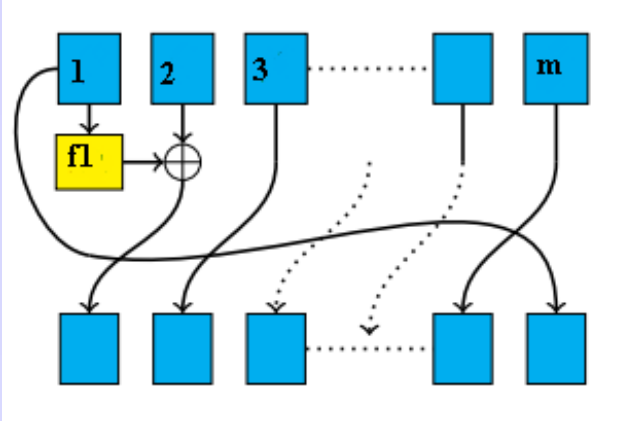
Кафедра 42
Криптология и дискретная математика
Тел. 324-7334; факс. 323-9137; e-mail: kaf42@mail.ru.

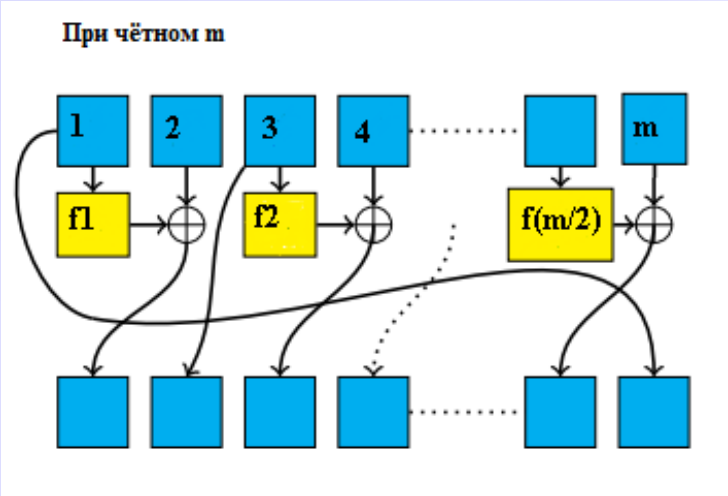
О геометрических свойствах обобщённых алгоритмов шифрования Фейстеля

Пудовкина М.А., Токтарёв А.В.

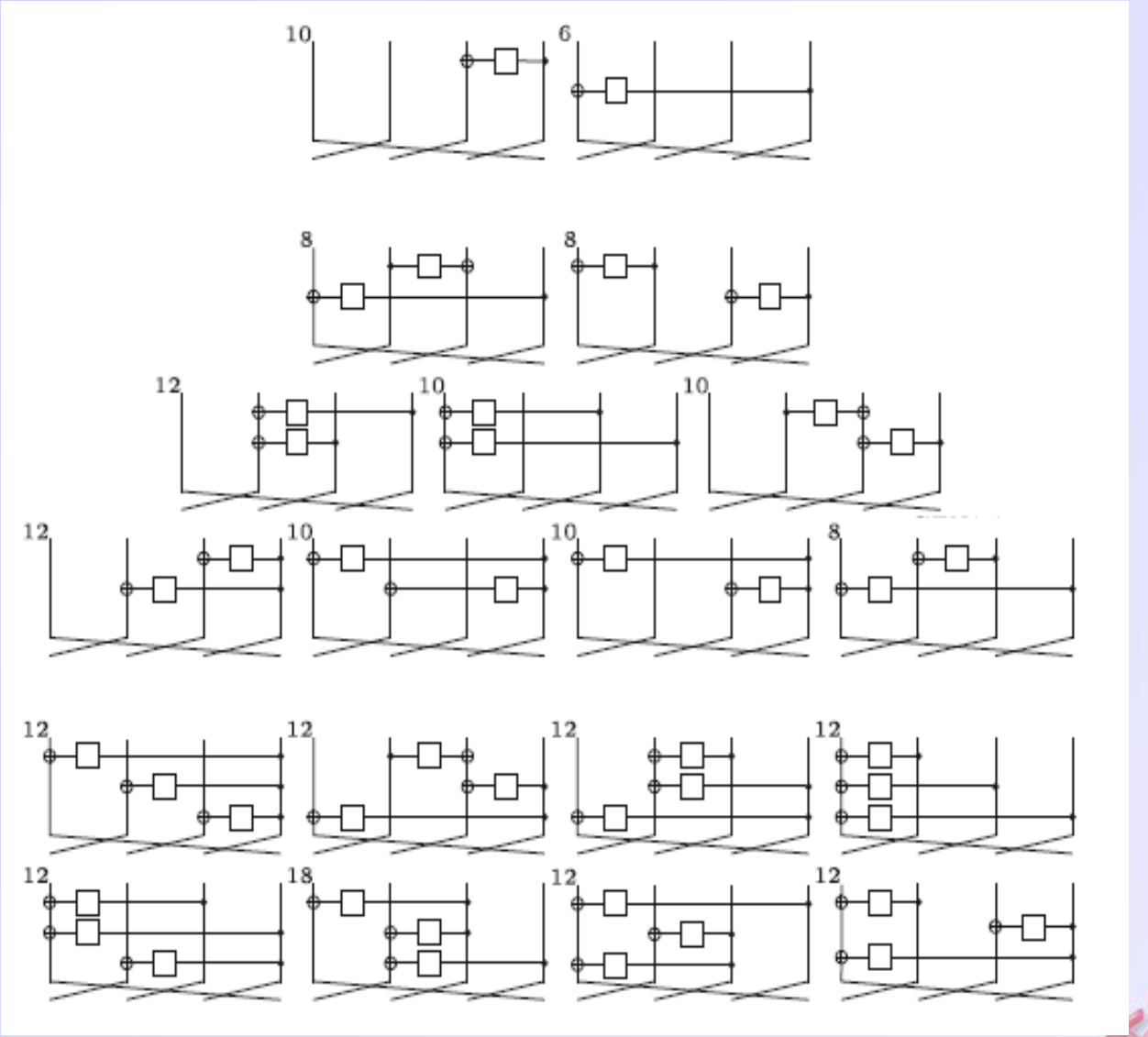
1-ого рода: *Schnorr C.P.*, On the construction of random number generators and random function generators, 1988;
Feistel H., Notz W., Smith J.L., Some cryptographic techniques for machine-to-machine data communications, 1975:



2-ого рода: *Zheng, Y., Matsumoto, T., Imai, H.*, On the Construction of Block Ciphers Provably Secure and Not Relying on Any Unproved Hypotheses, 1989:



Bogdanov A., Shibutani K., Generalized Feistel networks revisited, 2012 :



$n = d \cdot m; c \in \{1,\ldots,m\}$; $\mathrm{A} = A, A'$ – разбиение множества $\{1,\ldots,m\}$ на два подмножества A, A'.

$P(B)$ – множество всех подмножеств множества B.

$$\chi : A' \to P(A),\ \mathrm{X}(A') = \bigcup_{i \in A'} \chi(i), \varphi : \mathrm{X}(A') \to \{1,\ldots,c\}, \rho \in S(\{1,\ldots,m\}).$$

$$v_\rho : (\alpha_1,\ldots,\alpha_m) \mapsto \alpha_{\rho^{-1}(1)},\ldots,\alpha_{\rho^{-1}(m)}\ ,\ h_k : (\alpha_1,\ldots,\alpha_m) \mapsto (\alpha'_1,\ldots,\alpha'_m).$$

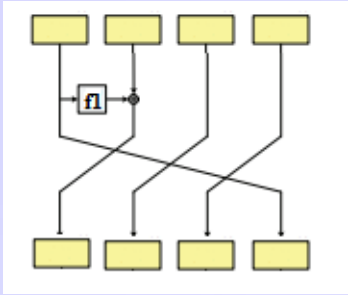
$$\alpha'_i = \begin{cases} \alpha_i, & \text{если } i \in A, \\ \alpha_i \oplus \sum\limits_{j \in \chi(i)} \oplus f_{\varphi(j),k_{\varphi(j)}}(\alpha_j), & \text{если } i \in A'. \end{cases}$$

$$g_k \in S(V_d^m), \text{ где } g_k = h_k \circ v_\rho.$$

Семейство обобщённых алгоритмов шифрования Фейстеля с фиксированным набором $(\mathrm{A}, \chi, \varphi, \rho)_c$ назовём $(\mathrm{A}, \chi, \varphi, \rho)_c$ – семейством.

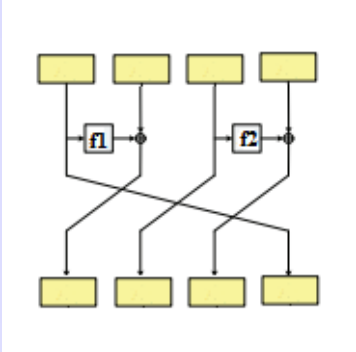
$$g_k : (\alpha_1, \alpha_2, \alpha_3, \alpha_4) \mapsto (\alpha_2 \oplus f_{1,k}(\alpha_1), \alpha_3, \alpha_4, \alpha_1)$$

$$A = \{1,3,4\},\ A' = \{2\},\ \chi(2) = \{1\},\ \mathrm{X}(A') = \{1\},\ \rho \in (1,4,3,2), \varphi(1) = 1.$$



$$g_k : (\alpha_1, \alpha_2, \alpha_3, \alpha_4) \mapsto (\alpha_2 \oplus f_{1,k_1}(\alpha_1), \alpha_3, \alpha_4 \oplus f_{2,k_2}(\alpha_3), \alpha_1)$$

$$A = \{1,3\},\ A' = \{2,4\}, \chi(2) = \{1\}, \chi(4) = \{3\},\ \mathrm{X}(A') = \{1,3\},\ \rho \in (1,4,3,2),$$
$$\varphi(1) = 1, \varphi(3) = 2.$$



Невозможные разности для семейства алгоритмов шифрования Фейстеля

Пусть $G_c(\mathrm{A},\chi,\varphi,\rho)$ – множество всех $(\mathrm{A},\chi,\varphi,\rho,f)_c$ – алгоритмов.

Невозможная разность $\delta \overset{r}{\not\longrightarrow} \delta'$, если

$$\forall\ g \in G_c(\mathrm{A},\chi,\varphi,\rho),\ (k^{(1)},\ldots,k^{(r)}) \in (V_d^c)^r, \alpha \in {V_d}^m$$

$$\alpha^{g_{k^{(1)}}\cdots g_{k^{(r)}}} \oplus (\delta \oplus \alpha)^{g_{k^{(1)}}\cdots g_{k^{(r)}}} \neq \delta'$$

$\delta \overset{r}{\longrightarrow} \delta'$, если $\exists\ g \in G_c(\mathrm{A},\chi,\varphi,\rho),\ (k^{(1)},\ldots,k^{(r)}) \in (V_d^c)^r,$ $\alpha \in {V_d}^m$

$$\alpha^{g_{k^{(1)}}\cdots g_{k^{(r)}}} \oplus (\delta \oplus \alpha)^{g_{k^{(1)}}\cdots g_{k^{(r)}}} = \delta'.$$

$r = r_{\mathrm{A},\chi,\varphi,\rho}(\delta)$ если $\forall\ \delta' \in (V_d^m)^{\times}$: $\delta \not\xrightarrow{r} \delta'$ и $\exists\, \delta' \in (V_d^m)^{\times}$: $\delta \xrightarrow{r+1} \delta'$

$$r_{\mathrm{A},\chi,\varphi,\rho} = \max\{r_{\mathrm{A},\chi,\varphi,\rho}(\delta) \mid \delta \in (V_d^m)^{\times}\}.$$

$r_{\mathrm{A},\chi,\varphi,\rho}$ – такое наибольшее число раундов, что для любого $l > r_{\mathrm{A},\chi,\varphi,\rho}$ не существует невозможных разностей у некоторого l-раундового $(\mathrm{A},\chi,\varphi,\rho,f)_c$ – алгоритма, т.е. все элементы его разностной матрицы ненулевые.

Аддитивная коммутативная полугруппа

В работе *Suzaki T., Minematsu K.*, Improving the generalized Feistel, 2012 используется полугруппа $(D,\oplus)$, заданная на множестве $D=\{\gamma,\Delta,\tilde{0}\}$ следующим образом:

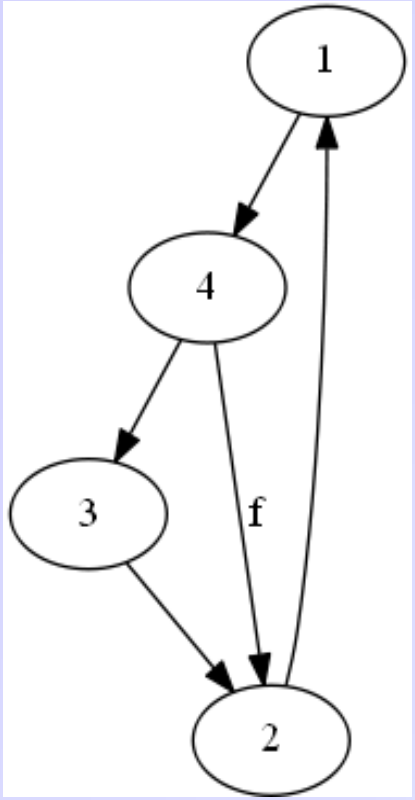
$\oplus$	γ	Δ	$\tilde{0}$
γ	Δ	Δ	γ
Δ	Δ	Δ	Δ
$\tilde{0}$	γ	Δ	$\tilde{0}$

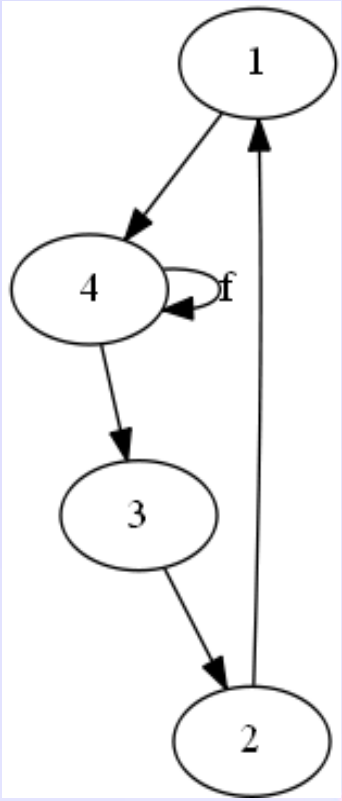
$$g_k:(\alpha_1,\alpha_2,\alpha_3,\alpha_4)\mapsto(\alpha_2,\alpha_3\oplus f_{1,k}(\alpha_4),\alpha_4,\alpha_1)$$

$$(0,0,\gamma,0)\to(0,\gamma,0,0)\to(\gamma,0,0,0)\to(0,0,0,\gamma)\to$$
$$\to(0,\Delta,\gamma,0)\to(\Delta,\gamma,0,0)\to(\gamma,0,0,\Delta)\to$$
$$\to(0,\Delta,\Delta,\gamma)\to(\Delta,\Delta,\gamma,0)\to(\Delta,\gamma,\Delta,\Delta)\to$$
$$\to(\gamma,\Delta,\Delta,\Delta)\to(\Delta,\Delta,\Delta,\gamma)\to(\Delta,\Delta,\Delta,\Delta)$$

- $\Gamma_{A,\chi,\varphi,\rho}$ – ориентированный помеченный граф для семейства $(A,\chi,\varphi,\rho)_c$.
- Граф примитивен, если наибольший общий делитель длин всех его простых контуров равен единице.

$(\alpha_1,\alpha_2,\alpha_3,\alpha_4)\mapsto(\alpha_2,\alpha_3\oplus f_{1,k}(\alpha_4),\alpha_4,\alpha_1)$ $(\alpha_1,\alpha_2,\alpha_3,\alpha_4)\mapsto(\alpha_2,\alpha_3,\alpha_4,\alpha_1\oplus f_{1,k}(\alpha_4))$





Необходимое и достаточное условие существования конечного числа раундов для невозможных разностей семейства

Некоторые $(\mathrm{A},\chi,\varphi,\rho)_c$-семейства для любого числа раундов имеют невозможные разности, в этом случае будем полагать $r_{\mathrm{A},\chi,\varphi,\rho}=\infty$, иначе будем говорить что $r_{\mathrm{A},\chi,\varphi,\rho}$ конечно.

Утверждение 1. $r_{\mathrm{A},\chi,\varphi,\rho}$ *конечно тогда и только тогда когда орграф* $\Gamma_{\mathrm{A},\chi,\varphi,\rho}$ *примитивен.*

Если орграф $\Gamma_{\mathrm{A},\chi,\varphi,\rho}$ не является примитивным, то $(\mathrm{A},\chi,\varphi,\rho)_c$ –семейство для любого числа раундов $l\in\mathbb{N}$ имеет невозможные разности.

- Пусть M – числовая полугруппа, т.е. полугруппа из $\mathbb{N}_0$, замкнутая по сложению.
- Числовую полугруппу, порождённую набором натуральных чисел $d_1,\ldots,d_v \in \mathbb{N}$, обозначим в виде:

$$M = < d_1,\ldots,d_v > = \left\{ \sum_{i=1}^{v} n_i d_i \mid n_i \in \mathbb{N} \right\}.$$

- Пусть U – множество всех числовых полугрупп. Тогда $q : U \to \mathbb{N}$ функция для заданной числовой полугруппы, определяющая число Фробениуса, т.е. наибольшее целое неотрицательное число, не принадлежащее ей.

Оценка для максимального числа раундов

$d(\Gamma_{A,\chi,\varphi,\rho})$ – диаметр графа $\Gamma_{A,\chi,\varphi,\rho}$,

p_{max} – длина максимального простого контура графа $\Gamma_{A,\chi,\varphi,\rho}$.

Утверждение 2. *Для любого семейства* $(A,\chi,\varphi,\rho)_c$ *граф* $\Gamma_{A,\chi,\varphi,\rho}$ *которого примитивен справедливы оценки:*

$$\max(q_{max}, d(\Gamma_{A,\chi,\varphi,\rho})) \le r_{A,\chi,\varphi,\rho} \le q_{\max} + d(\Gamma_{A,\chi,\varphi,\rho}) + p_{max}$$

Пример 1

$$(\alpha_1, \alpha_2, \alpha_3, \alpha_4) \mapsto (\alpha_2, \alpha_3 \oplus f_{1,k}(\alpha_4), \alpha_4, \alpha_1)$$

Полугруппа для вершины «3» с максимальным числом Фробениуса: $< 4, 7, 13, 10 >$

$$q_{max} = 9, \quad d(\Gamma_{A,\chi,\varphi,\rho}) = 3, \quad p_{max} = 4$$

$$\max(q_{max}, d(\Gamma_{A,\chi,\varphi,\rho})) = 9$$

$$q_{\max} + d(\Gamma_{A,\chi,\varphi,\rho}) + p_{max} = 9 + 3 + 4 = 16$$

$$9 \le r_{A,\chi,\varphi,\rho} \le 16$$

Реальное значение 11 раундов

Пример 2

$$(\alpha_1, \alpha_2, \alpha_3, \alpha_4) \mapsto (\alpha_2, \alpha_3, \alpha_4, \alpha_1 \oplus f_{1,k}(\alpha_4))$$

Полугруппа для вершин «1,3,2» с максимальным числом Фробениуса $< 4,5,6,7 >$

$$q_{max} = 3,\ d(\Gamma_{A,\chi,\varphi,\rho}) = 3,\ p_{max} = 4$$

$$\max(q_{max}, d(\Gamma_{A,\chi,\varphi,\rho})) = 3$$

$$q_{\max} + d(\Gamma_{A,\chi,\varphi,\rho}) + p_{max} = 3+3+4 = 10$$

$$3 \le r_{A,\chi,\varphi,\rho} \le 10$$

Реальное значение 6 раундов

Спасибо за внимание !