МАТЕМАТИЧЕСКИЕ МЕТОДЫ КРИПТОГРАФИИ

УДК 519.7

ОБ ОЦЕНКЕ ЧИСЛА РАУНДОВ С НЕВОЗМОЖНЫМИ РАЗНОСТЯМИ В ОБОБЩЁННЫХ АЛГОРИТМАХ ШИФРОВАНИЯ ФЕЙСТЕЛЯ

М. А. Пудовкина, А. В. Токтарев

Национальный исследовательский ядерный университет «МИФИ», г. Москва, Россия

Исследуется семейство обобщённых алгоритмов шифрования Фейстеля. С использованием методов теории графов и теории чисел получены верхняя и нижняя оценки максимального числа раундов, для которого существуют невозможные разности для любого алгоритма блочного шифрования из семейства.

Ключевые слова: *обобщённый алгоритм шифрования Фейстеля, невозможная разность, число Фробениуса.*

DOI 10.17223/20710410/27/4

BOUNDS FOR THE NUMBER OF ROUNDS WITH IMPOSSIBLE DIFFERENCES IN GENERALIZED FEISTEL SCHEMES

M. A. Pudovkina, A. V. Toktarev

National Research Nuclear University MEPhI (Moscow Engineering Physics Institute), Moscow, Russia

E-mail: maricap@rambler.ru, toktarev@gmail.com

The class of ciphers described by a generalized Feistel scheme is considered. Some upper and lower bounds for the maximum number of rounds with impossible differences are provided. They do not depend on the type of Feistel scheme and on the number of nonlinear functions or blocks in the register.

Keywords: *block cipher, generalized Feistel scheme, impossible differential, differential probability.*

Введение

Обобщённые алгоритмы шифрования Фейстеля представляют естественное обобщение алгоритма шифрования Фейстеля [1, 2]. Они лежат в основе таких шифрсистем, как CAST-256, MARS, SMS4, CLEFIA, Piccolo, HIGHT и др. В основном обобщение осуществляется посредством увеличения числа ячеек регистра сдвига и выбором ячеек, содержимое которых меняется нелинейными функциями усложнения, зависящими от раундового ключа. При этом для обратимости раундовой функции не требуется обратимость нелинейных функций усложнения. Часто для построения функции усложнения используется SP-сеть. В последние годы стали предлагаться модификации

обобщённых алгоритмов шифрования Фейстеля, улучшающие их свойства рассеивания [3 – 5].

Пусть K — ключевое множество; V_n — n-мерное векторное пространство над $\mathrm{GF}(2)$; $g_k^{(r)}$ — раундовая функция зашифрования на ключе $k \in K$; $\oplus$ — бинарная операция покоординатного сложения в V_n. При атаке на l-раундовый n-битный алгоритм блочного шифрования один из этапов разностного метода и его обобщений состоит в нахождении для некоторого числа раундов r, $r \leqslant l$, элементов матрицы $\mathbf{p}^{(r)} = \left(p_{\lambda\lambda'}^{(r)}\right)$ вероятностей переходов ненулевых разностей n-битных блоков текста r-раундовой функции зашифрования, т. е.

$$p_{\lambda\lambda'}^{(r)} = 2^{-n}|K|^{-1}\left|\left\{(x,k) \in V_n \times K : g_k^{(r)}(x) \oplus g_k^{(r)}(x \oplus \lambda) = \lambda'\right\}\right|.$$

Матрица $\mathbf{p}^r$ также называется r-раундовой матрицей вероятностей переходов разностей. Как правило, в разностном методе ищется наибольшее r, при котором существуют $\lambda^{(0)}$, $\lambda^{(r)}$, такие, что $p_{\lambda^{(0)}\lambda^{(r)}}^{(r)} > 2^{-n}$, и при этом r находятся такие $\lambda^{(0)}, \lambda^{(r)}$, для которых $p_{\lambda^{(0)}\lambda^{(r)}}^{(r)}$ принимает максимальное значение. Так как найти точное значение элемента $p_{\lambda^{(0)}\lambda^{(r)}}^{(r)}$ часто не удаётся, приводится нижняя оценка $\widetilde{p}_{\lambda^{(0)}\lambda^{(r)}}^{(r)}$ для $p_{\lambda^{(0)}\lambda^{(r)}}^{(r)} > 2^{-n}$. Для марковских алгоритмов блочного шифрования [6], у которых раундовые функции реализуют одно и то же отображение на декартовом произведении множества n-битных блоков текста и множества раундовых ключей, величина $\widetilde{p}_{\lambda^{(0)}\lambda^{(r)}}^{(r)}$ находится с помощью разностной характеристики последовательности $\bar{\lambda} = \lambda^{(0)}, \lambda^{(1)}, \ldots, \lambda^{(r)}$ n-битных разностей промежуточных блоков текстов, у которой $p_{\lambda^{(i)}\lambda^{(i+1)}}^{(1)} > 0$ для каждого $i \in \{0, \ldots, r-1\}$, при этом полагают $\widetilde{p}_{(\lambda^{(0)}\lambda^{(r)})}^{(r)} = \prod_{i=0}^{(r-1)} p_{\lambda^{(i)}\lambda^{(i+1)}}^{(1)}$.

Для многих алгоритмов блочного шифрования существует такое число раундов $\widetilde{r}$, что матрица $\mathbf{p}^{(r)}$ не является положительной для каждого $r \in \{1, \ldots, \widetilde{r}\}$, т. е. среди элементов матрицы $\mathbf{p}^{(r)}$ есть нулевые. Например, при $r = 1$ такой матрицей является матрица $\mathbf{p}^{(1)}$ алгоритма шифрования Фейстеля.

Равенство $p_{\lambda\lambda'}^{(r)} = 0$ для некоторых ненулевых разностей $\lambda, \lambda' \in V_n$ означает, что ни при каком ключе шифрования $k \in K$ и блоке открытого текста $x \in V_n$ не выполняется равенство $g_k^{(r)}(x) \oplus g_k^{(r)}(x \oplus \lambda) = \lambda'$.

В этом случае пара λ, λ' называется r-раундовой невозможной разностью. Существование невозможной разности может позволить применить атаки различения, а также найти некоторые биты ключа шифрования или весь ключ с помощью метода невозможных разностей, первоначально предложенного в работе [7], а затем модифицированного в [8]. Часто рассматривается такая пара (Λ, Λ') r-раундовых невозможных множеств разностей, что каждая пара $(\lambda, \lambda') \in \Lambda \times \Lambda'$ является r-раундовой невозможной разностью.

При поиске невозможных разностей нередко применяется аналог разностной характеристики. В этом случае рассматривается такая последовательность множеств разностей $\bar{\Lambda} = \Lambda_0, \ldots, \Lambda_r$, что $\Lambda_0 \subset V_n$,

$$\Lambda_i = \{g_{k^{(i)}}(x) \oplus g_{k^{(i)}}(x \oplus \lambda) : (\lambda, x, k^{(i)}) \in \Lambda_{i-1} \times V_n \times K_i\}, i = 1, \ldots, r,$$

где K_i — множество раундовых ключей i-го раунда; $g_{k^{(i)}} : V_n \to V_n$ — раундовая функция на раундовом ключе $k^{(i)} \in K_i$. Если $\Lambda_r \neq V_n \setminus \{\bar{0}_n\}$, то пара $\Lambda_0, V_n \setminus (\Lambda_r \cup \{\bar{0}_n\})$ является r-раундовым невозможным множеством разностей, где $\bar{0}_n$ — нулевой n-мерный вектор.

В данной работе рассматривается семейство обобщённых алгоритмов шифрования Фейстеля. В частности, это семейство включает в себя сбалансированные алгоритмы шифрования, предложенные в работах [1, 2, 5, 9, 10]. Приведены оценки сверху и снизу максимального числа раундов, для которого вероятность любой r-раундовой разности равна нулю для любого алгоритма шифрования из семейства. Предложен подход получения оценок для обобщённого алгоритма шифрования Фейстеля.

В п. 1 приводятся описания рассматриваемых семейств обобщённых алгоритмов шифрования Фейстеля. В п. 2 описаны свойства невозможных разностей и их применения к обобщённым алгоритмам шифрования Фейстеля. Пункт 3 посвящён теоретико-графовым свойствам обобщённых алгоритмов шифрования Фестеля. В п. 4 приведены верхние и нижние оценки максимального числа раундов, для которых существует l-раундовая невозможная разность. Доказательство оценок основано на теории числовых полугрупп.

1. Основные обозначения и определения

1.1. Обозначения

Пусть $\mathbb{N}$ — множество натуральных чисел; $\mathbb{N}_0 = \mathbb{N}\bigcup\{0\}$; $m, d, c \in \mathbb{N}$, $n = dm$; $c \in \{1, \ldots, m\}$; $B^\times = B\backslash\{0\}$ при $B \subseteq V_n$; $W = (A, A')$ — разбиение множества $\{1, \ldots, m\}$ на два подмножества A, A'; $W^{(m)}$ — множество всех упорядоченных разбиений множества $\{1, \ldots, m\}$ на два подмножества; $P(B)$ — множество всех подмножеств множества B; $S(B)$ — множество всех подстановок на B; $k = (k_1, \ldots, k_c) \in V_d^c$; $f_i : V_d^2 \to V_d$, $f_{i,k_i}(\alpha) = f_i(\alpha, k_i)$ для всех $\alpha \in V_d$, $i = 1, \ldots, c$;

$$F_d^{(c)} = \left\{(f_1, \ldots, f_c) : f_i : V_d^2 \to V_d, i = 1, \ldots, c\right\}.$$

Здесь d — число бит в ячейке регистра; m — длина регистра; n — длина блока шифрования; c — количество функций усложнения $f_1, \ldots, f_c$ на одном раунде; $k_1, \ldots, k_c$ — ключи, используемые в этих функциях шифрования.

1.2. Описание обобщённых алгоритмов шифрования Фейстеля

Кроме классического алгоритма шифрования Фейстеля (например, используемого в DES), существуют различные его модификации. Говоря об обобщённых алгоритмах шифрования Фейстеля, будем иметь в виду объединение большинства из них. Некоторые обобщения, например алгоритмы шифрования Фейстеля 1-го, 2-го и 3-го типов, представлены в работе [11]. Блочными шифрсистемами, построенными на основе обобщённых алгоритмов шифрования Фейстеля, являются Skipjack, BEAR/LION, BlowFish, Camelia, DEAL, DES, MARS, Twofish. Обобщённые алгоритмы шифрования Фейстеля с длиной регистра 4 отражены в работе [9]. На рис. 1 изображено 19 обобщённых алгоритмов шифрования Фейстеля с длиной регистра 4.

Приведём описание математической модели, включающей эти обобщения. Рассмотрим семейство алгоритмов шифрования Фейстеля, заданных следующими параметрами: натуральным числом c; разбиением $W = (A, A') \in W^{(m)}$; отображением $\chi : A' \to P(A)$; $f \in F_d^{(c)}$; биективными отображениями $\rho \in S(\{1, \ldots, m\})$, $\varphi : X(A') \to \{1, \ldots, c\}$, где $X(A') = \bigcup\limits_{i \in A', j \in \chi(i)} (i, j)$. Отметим, что для любого A' верно тождество $|X(A')| = c$.

Рассмотрим отображения $v_\rho, h_k \in S(V_d^m)$, определённые как

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

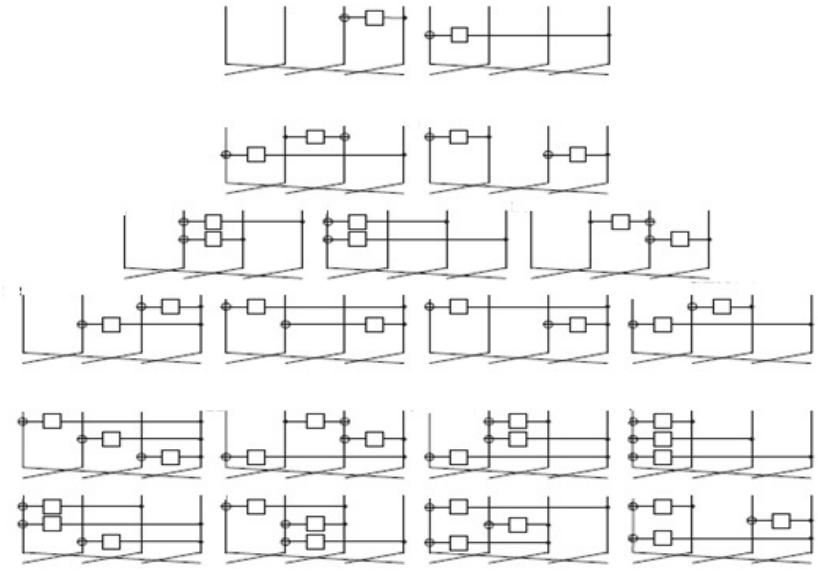

Рис. 1. Раундовые функции обобщённых алгоритмов шифрования Фейстеля с длиной регистра 4

где

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

Обобщённый алгоритм шифрования Фейстеля задаётся раундовой функцией $g_k \in S(V_d^m)$, где $g_k = v_\rho h_k$. Пусть $g_{k^{(r)}} \dots g_{k^{(1)}}$ — r-раундовая функция шифрования на ключе $k = (k^{(1)}, \dots, k^{(r)}) \in (V_d^c)^r$.

Семейство обобщённых алгоритмов шифрования Фейстеля с фиксированными параметрами $(W, \chi, \varphi, \rho)_c$ будем называть $(W, \chi, \varphi, \rho)_c$-семейством. Каждый алгоритм блочного шифрования из $(W, \chi, \varphi, \rho)_c$-семейства задан фиксированным набором функций $f \in F_d^{(c)}$ и называется $(W, \chi, \varphi, \rho, f)_c$-алгоритмом шифрования. Обозначим через $G_c(W, \chi, \varphi, \rho)$ множество всех $(W, \chi, \varphi, \rho, f)_c$-алгоритмов шифрования.

Будем писать $g \in G_c(W, \chi, \varphi, \rho)$, если g является раундовой функцией $(W, \chi, \varphi, \rho, f)_c$-алгоритма шифрования. Обозначение $g_{k^{(i)}}$ показывает зависимость g от конкретного раундового ключа $k^{(i)}$.

Для нижнего крайнего справа семейства, изображённого на рис. 1, параметры $(W, \chi, \varphi, \rho)_c$-семейства следующие:

$$g_k : (\alpha_1, \alpha_2, \alpha_3, \alpha_4) \mapsto (\alpha_2, \alpha_3 \oplus f_{1,k_1}(\alpha_4), \alpha_4, \alpha_1 \oplus f_{2,k_2}(\alpha_2) \oplus f_{3,k_3}(\alpha_4)),$$

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

Заметим, что многие обобщённые алгоритмы шифрования Фейстеля основаны на описанной конструкции и ρ^{-1} часто совпадает с циклом $(1, 2, \dots, m)$. Для обобщённых алгоритмов шифрования Фейстеля 1-го типа [12, 13] получаем

$$g_k : (\alpha_1, \dots, \alpha_m) \mapsto (\alpha_2 \oplus f_{1,k_1}(\alpha_1), \alpha_3, \dots, \alpha_m, \alpha_1),$$

где $c = 1$; $A' = \{2\}$; $A = \{1, \ldots, m\} \backslash \{2\}$; $\chi(2) = \{1\}$; $\varphi(2, 1) = 1$ и $\rho^{-1} = (1, 2, \ldots, m)$. Для обобщённых алгоритмов шифрования Фейстеля 2-го типа [11] и чётного числа m получаем

$$g_k : (\alpha_1, \ldots, \alpha_m) \mapsto (\alpha_2 \oplus f_{1,k_1}(\alpha_1), \alpha_3, \alpha_4 \oplus f_{2,k_2}(\alpha_3), \alpha_5, \ldots, \alpha_m, \alpha_1),$$

где $c = m/2$; $A' = \{2i : i \in \{1, \ldots, m/2\}\}$; $A = \{1, \ldots, m\} \backslash A'$; $\chi(2i) = \varphi(2i, i-1) = \{i\}$, $i \in \{1, \ldots, m/2\}$, и $\rho^{-1} = (1, 2, \ldots, m)$. В работе [9] приведены различные классификации обобщённых алгоритмов шифрования Фейстеля для параметров $m = 4$ и $\rho^{-1} = (1, 2, 3, 4)$.

Отметим, что перестановка ρ^{-1} может не совпадать с циклом $(1, 2, \ldots, m)$. Такие перестановки рассмотрены в работах [4, 5]. Например, $\rho^{-1} = (1, 3, 5, 7)(2, 8, 6, 4)$ используется в блочной шифрсистеме Piccolo [4].

2. Невозможные усечённые разности

Существование невозможной разности для r раундов обобщённого алгоритма шифрования Фейстеля означает возможность применения метода невозможных разностей. Для анализа стойкости алгоритма важно оценивать максимальное число раундов, для которого существуют невозможные разности.

Рассмотрим произвольное $(W, \chi, \varphi, \rho)_c$-семейство. Пусть $\alpha^{(0)}$ — n-битный открытый текст, δ — ненулевая n-битная разность. Для $\delta \in V_n^\times$ оценим верхнюю и нижнюю границы числа раундов $r = r_{W,\chi,\varphi,\rho}(\delta)$, удовлетворяющего следующим условиям:

1) для любых $g \in G_c(W, \chi, \varphi, \rho)$, $(k^{(1)}, \ldots, k^{(r)}) \in (V_d^c)^r$, $\alpha^{(0)} \in V_n$ и некоторого $\delta' \in V_n^\times$ выполняется неравенство $g_{k^{(r)}} \ldots g_{k^{(1)}}(\alpha^{(0)}) \oplus g_{k^{(r)}} \ldots g_{k^{(1)}}(\delta \oplus \alpha^{(0)}) \neq \delta'$;
2) для любого $\delta' \in V_n^\times$ существуют $\alpha^{(0)} \in V_n$, $g \in G_c(W, \chi, \varphi, \rho)$, $(k^{(1)}, \ldots, k^{(r+1)}) \in \in (V_d^c)^{r+1}$, удовлетворяющие равенству

$$g_{k^{(r+1)}} \ldots g_{k^{(1)}}(\alpha^{(0)}) \oplus g_{k^{(r+1)}} \ldots g_{k^{(1)}}(\delta \oplus \alpha^{(0)}) = \delta'.$$

Пусть $r_{W,\chi,\varphi,\rho} = \max\{r_{W,\chi,\varphi,\rho}(\delta) : \delta \in V_n^\times\}$ и l — такое произвольное натуральное число, что $l > r_{W,\chi,\varphi,\rho}$. Тогда $r_{W,\chi,\varphi,\rho}$ — максимальное число раундов, для которого не существует невозможной разности для любого l-раундового $(W, \chi, \varphi, \rho, f)_c$-алгоритма шифрования. Другими словами, все элементы его разностной матрицы ненулевые.

Отметим, что если алгоритм шифрования Фейстеля не имеет невозможных разностей на раунде с номером r, то он не имеет невозможных разностей на любом раунде больше r. Действительно, пусть алгоритм шифрования не имеет невозможных разностей на r раундах, а на $(r+1)$-м раунде разность $\alpha \in V_n^\times$ имеет парную невозможную $\beta \in V_n^\times$. Зашифруем два открытых текста с разностью α на ключе $k \in V_d^c$; пусть при этом выходной разностью первого раунда будет $\beta' \in V_n^\times$. Тогда в силу того, что на r раундах невозможных разностей нет, существуют ключи на r раундах шифрования, переводящие блоки с разностью β' в блоки с разностью β. Значит, существуют ключи на $r+1$ раундах шифрования, переводящие блоки с разностью α в блоки с разностью β. Получено противоречие — значит, на $(r+1)$-м раунде также отсутствуют невозможные разности.

Некоторые $(W, \chi, \varphi, \rho)_c$-семейства имеют невозможные разности для любого числа раундов $l \in \mathbb{N}$. Это означает, что для каждого $l \in \mathbb{N}$ существует такая пара $(\delta, \delta') \in \in \left(V_d^\times\right)^2$, что $g_{k^{(l)}} \ldots g_{k^{(1)}}(\alpha^{(0)}) \oplus g_{k^{(l)}} \ldots g_{k^{(1)}}(\delta \oplus \alpha^{(0)}) \neq \delta'$ для любых $g \in G_c(W, \chi, \varphi, \rho)$, $(k^{(1)}, \ldots, k^{(l)}) \in (V_d^c)^l$, $\alpha^{(0)} \in V_n$. В этом случае положим, что $r_{W,\chi,\varphi,\rho} = \infty$. Если $r_{W,\chi,\varphi,\rho}$

конечно, то после некоторого (конечного) числа раундов $(W, \chi, \varphi, \rho)_c$-семейство не имеет невозможных разностей.

Для специального типа обобщённых алгоритмов шифрования Фейстеля в работах [14, 15] для параметра $r_{W,\chi,\varphi,\rho}$ получены различные оценки.

Для получения верхней и нижней оценок параметра $r_{W,\chi,\varphi,\rho}$ используется аддитивная коммутативная полугруппа $(D, \oplus)$, заданная на множестве $D = \{\gamma, \Delta, \tilde{0}\}$. Похожее множество, состоящее из пяти элементов, использовано в [5] для классификации разностей в ячейках регистра обобщённого алгоритма шифрования Фейстеля. Полугруппа $(D, \oplus)$ определена следующим образом:

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

Для произвольных векторов $\alpha_1 = \left(\alpha_1^{(1)}, \ldots, \alpha_1^{(m)}\right)$, $\alpha_2 = \left(\alpha_2^{(1)}, \ldots, \alpha_2^{(m)}\right)$ из V_d^m обозначим $\alpha_1 \to \alpha_2$, если существуют такие раундовый ключ $k \in V_d^c$ и открытые тексты $x_1, x_2 \in V_d^m$, что $\alpha_1 = x_1 \oplus x_2$, $\alpha_2 = g_k(x_1) \oplus g_k(x_2)$.

Приведём пример, иллюстрирующий построение невозможных усеченных разностей на основе введёной полугруппы. Рассмотрим обобщённый алгоритм шифрования Фейстеля, заданный как $g_k : (\alpha_1, \alpha_2, \alpha_3, \alpha_4) \mapsto (\alpha_2, \alpha_3 \oplus f_{1,k}(\alpha_4), \alpha_4, \alpha_1)$.

Приведём 14-раундовую усеченную разность:

$$(\tilde{0}, \tilde{0}, \gamma, \tilde{0}) \to (\tilde{0}, \gamma, \tilde{0}, \tilde{0}) \to (\gamma, \tilde{0}, \tilde{0}, \tilde{0}) \to (\tilde{0}, \tilde{0}, \tilde{0}, \gamma) \to (\tilde{0}, \Delta, \gamma, \tilde{0}) \to$$
$$\to (\Delta, \gamma, \tilde{0}, \tilde{0}) \to (\gamma, \tilde{0}, \tilde{0}, \ \Delta) \to (\tilde{0}, \Delta, \Delta, \gamma) \to (\Delta, \Delta, \gamma, \tilde{0}) \to (\Delta, \gamma, \tilde{0}, \Delta) \to$$
$$\to (\Delta, \gamma, \Delta, \Delta) \to (\gamma, \Delta, \Delta, \Delta) \to (\Delta, \Delta, \Delta, \gamma) \to (\Delta, \Delta, \gamma, \Delta) \to (\Delta, \Delta, \Delta, \Delta).$$

Очевидно, что максимальное число раундов, для которого существует невозможная разность, зависит от входной разности. Покажем, что максимальное число раундов достигается, если у входной разности существует ненулевая координата.

Рассмотрим $(W, \chi, \varphi, \rho)_c$-семейство, s — номер раунда, x_1, x_2 — md-битные открытые тексты, $x_i = \left(x_i^{(1)}, \ldots, x_i^{(m)}\right) \in V_d^m$, где $i \in \{1, 2\}$. Обозначим

$$x_i^{(s)} = \left(x_i^{(1,s)}, \ldots, x_i^{(m,s)}\right) = g_{k^{(s)}} g_{k^{(s-1)}} \ldots g_{k^{(1)}} \left(x_i^{(1)}, \ldots, x_i^{(m)}\right),$$

где $x_i^{(s)}$ — шифртекст после s раундов шифрования; $k^{(1)}, \ldots, k^{(s)}$ — раундовые ключи из V_d^c. Пусть E — множество всех отображений из V_d^2 в V_d.

Определим отображение $\lambda : V_d^m \times V_d^m \times \mathbb{N} \to D^m$, где $\lambda(x_1, x_2, s) = \left(l^{(1,s)}, \ldots, l^{(m,s)}\right)$;

$$l^{(i,s)} = \begin{cases} \tilde{0}, & \text{если } \forall k^{(1)}, \ldots, k^{(s)} \in V_d^c, \varepsilon_1, \ldots, \varepsilon_c \in E \left(x_1^{(i,s)} = x_2^{(i,s)}\right), \\ \gamma, & \text{если } \forall k^{(1)}, \ldots, k^{(s)} \in V_d^c, \varepsilon_1, \ldots, \varepsilon_c \in E \left(x_1^{(i,s)} \neq x_2^{(i,s)}\right), \\ \Delta, & \text{если } \forall z \in V_d^c \, \exists k^{(1)}, \ldots, k^{(s)} \in V_d^c, \varepsilon_1, \ldots, \varepsilon_c \in E \left(x_1^{(i,s)} \oplus x_2^{(i,s)} = z\right). \end{cases}$$

Отметим, что $\lambda(x_1, x_2, s)$ определяет усечённую разность s-го раунда. Пусть

$$\Theta_{x_1,x_2,s} = \left\{i \in \{1, \ldots, m\} : l^{(i,s)} \in \left\{\tilde{0}, \gamma\right\}\right\},$$
$$\Psi_{x_1,x_2,s} = \left\{i \in \{1, \ldots, m\} : l^{(i,s)} = \Delta\right\},$$
$$\Upsilon_{x_1,x_2,s} = \left\{i \in \{1, \ldots, m\} : l^{(i,s)} \neq \tilde{0}\right\}.$$

Следующая лемма отражает важный факт об упомянутых выше множествах.

Зафиксируем произвольные числа $i \in \{1, \ldots, m\}$, $s \in \mathbb{N}$ и ненулевой вектор $\alpha \in V_d$.

Лемма 1. Пусть x_1, x_2, y_1, y_2 — такие md-битные тесты, что

$$x_1 \oplus x_2 = \left(0, \ldots, 0, \underbrace{\alpha}_{i}, 0, \ldots, 0\right) \in V_d^m, \quad y_1 \oplus y_2 = (\beta_1, \beta_2, \ldots, \beta_m) \in V_d^m,$$

где β_{j_1}, β_{j_2} — ненулевые d-битные векторы для некоторых $j_1, j_2 \in \{1, \ldots, m\}$, $j_1 \neq j_2$. Тогда имеют место включения $\Upsilon_{x_1,x_2,s} \subseteq \Upsilon_{y_1,y_2,s}$, $\Theta_{y_1,y_2,s} \subseteq \Theta_{x_1,x_2,s}$, $\Psi_{x_1,x_2,s} \subseteq \Psi_{y_1,y_2,s}$.

Доказательство. Проводится по индукции относительно числа s и числа ненулевых элементов среди $\beta_1, \ldots, \beta_m$ и представляет собой перебор всевозможных вариантов и проверку условия включения. ■

Утверждение 1. Пусть $i \in \{1, \ldots, m\}$ и векторы

$$\delta = (\bar{0}_d, \ldots, \bar{0}_d, \delta_i, \bar{0}_d, \ldots, \bar{0}_d), \quad \delta' = (\delta'_1, \delta'_2, \ldots, \delta'_{m-1}, \delta'_m)$$

таковы, что $\delta_i \neq \bar{0}_d$, $\delta'_{j_1} \neq \bar{0}_d$, $\delta'_{j_2} \neq \bar{0}_d$ для некоторых $j_1, j_2 \in \{1, \ldots, m\}$, $j_1 \neq j_2$. Тогда $r_{W,\chi,\varphi,\rho}(\delta') \leqslant r_{W,\chi,\varphi,\rho}(\delta)$ для любого $(W, \chi, \varphi, \rho)_c$-семейства.

Доказательство. Пусть $r_1 = r_{W,\chi,\varphi,\rho}(\delta) + 1$, $r_2 = r_{W,\chi,\varphi,\rho}(\delta')$, $x_2 = x_1 \oplus \delta'$. Из леммы 1 следует, что $|\Theta_{x_1,x_2,r_1}| = 0$, но $|\Theta_{x_1,x_2,r_2}| > 0$. Таким образом, $r_{W,\chi,\varphi,\rho}(\delta) + 1 > r_{W,\chi,\varphi,\rho}(\delta')$. Отсюда $r_{W,\chi,\varphi,\rho}(\delta) \geqslant r_{W,\chi,\varphi,\rho}(\delta')$. ■

Утверждение 2. Пусть $i \in \{1, \ldots, m\}$, $\alpha \in V_d^\times$ и $\delta = \left(0, \ldots, 0, \underbrace{\alpha}_{i}, 0, \ldots, 0\right) \in V_d^m$.

Тогда для любого $(W, \chi, \varphi, \rho)_c$-семейства справедливо равенство $r_{W,\chi,\varphi,\rho} = r_{W,\chi,\varphi,\rho}(\delta)$.

Таким образом, для нахождения нижней границы параметра $r_{W,\chi,\varphi,\rho}$ следует рассматривать только разности с ровно одной ненулевой координатой.

3. Представление обобщённого алгоритма шифрования Фейстеля в виде орграфа

Для заданного $(W, \chi, \varphi, \rho)_c$-семейства рассмотрим ориентированный помеченный граф $\Gamma_{W,\chi,\varphi,\rho} = (X, Y)$ с множествами вершин X и дуг Y. Между вершинами орграфа $\Gamma_{W,\chi,\varphi,\rho}$ и ячейками регистров обобщённого алгоритма шифрования Фейстеля существует взаимно однозначное соответствие. Каждая вершина имеет такой же номер, как соответствующая ячейка регистра. Вершины с номерами i и j соединены дугой, если значение регистровой ячейки с номером j зависит от значения в регистровой ячейке с номером i после одного раунда зашифрования, другими словами, если верно одно из следующих условий:

1) $\rho(i) = j$;
2) $i \in A$ и существует $l \in A'$, такое, что $i \in \chi(l)$, $\rho(l) = j$.

Если выполнено первое условие, то дуга не имеет метки; иначе дуга помечена меткой Ф.

Приведём пример орграфа, соответствующего некоторому обобщённому алгоритму шифрования Фейстеля. Рассмотрим обобщённый алгоритма шифрования Фейстеля вида $g_k : (\alpha_1, \alpha_2, \alpha_3, \alpha_4) \mapsto (\alpha_2, \alpha_3 \oplus f_{1,k}(\alpha_4), \alpha_4, \alpha_1)$. Он принадлежит $(W, \chi, \varphi, \rho)_c$-семейству с параметрами

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

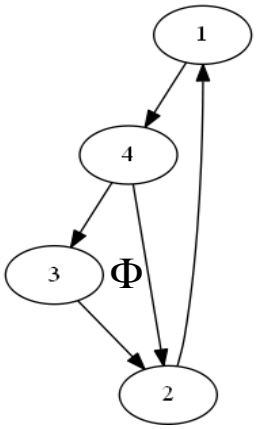

Рис. 2. Орграф обобщённого алгоритма шифрования Фейстеля

Соответствующий орграф представлен на рис. 2.

Напомним некоторые определения из теории графов. Маршрут в графе (орграфе) из вершины i в вершину j — это последовательность вершин и рёбер (дуг), инцидентных двум соседним вершинам; путь — это ориентированный маршрут; длина пути — количество дуг в нём; замкнутый путь — это путь, у которого первая и последняя вершины совпадают; простой путь — это путь без повторяющихся вершин; орцепь — путь без повторяющихся дуг; простая орцепь — орцепь без повторяющихся вершин; контур — замкнутая орцепь; простой контур — контур без повторяющихся вершин. Максимальный кратчайший путь между вершинами орграфа Γ называется диаметром и обозначается $\mathrm{d}(\Gamma)$. Примитивным орграфом называется такой сильносвязный орграф, что наибольший общий делитель длин всех его простых контуров равен 1. Для произвольного замкнутого пути w через $\mathrm{len}(w)$ обозначим его длину.

4. Числовые полугруппы с порождающими элементами и оценки

Пусть M — полугруппа с элементами из $\mathbb{N}_0$, замкнутая относительно операции сложения. Числовую полугруппу, порождённую элементами $d_1, \ldots, d_v \in \mathbb{N}$, определим как $M = \langle d_1, \ldots, d_v \rangle = \left\{ \sum\limits_{i=1}^{v} n_i d_i : n_i \in \mathbb{N}_0 \right\}$. Наибольшее целое число, которое не принадлежит числовой полугруппе M, называется числом Фробениуса полугруппы M.

Пусть U — множество всех числовых полугрупп, $g(S)$ — число Фробениуса полугруппы $S \in U$.

4.1. Построение множества порождающих элементов числовой полугруппы для каждой вершины примитивного орграфа $\Gamma_{W,\chi,\varphi,\rho}$

Оценки максимального числа раундов $r_{W,\chi,\varphi,\rho}$, для которого существуют невозможные разности для любого алгоритма шифрования Фейстеля из $(W, \chi, \varphi, \rho)_c$-семейства, получены с использованием максимального числа Фробениуса числовых полугрупп, соответствующих вершинам орграфа $\Gamma_{W,\chi,\varphi,\rho}$ обобщённого алгоритма шифрования Фейстеля.

Алгоритм состоит из двух шагов. На первом шаге для каждой вершины орграфа $\Gamma_{W,\chi,\varphi,\rho}$ находятся порождающие элементы соответствующей ей полугруппы. На втором шаге определяются числа Фробениуса для найденных числовых полугрупп. Затем выбирается максимальное из полученных чисел Фробениуса.

Пусть V — множество номеров вершин орграфа $\Gamma_{W,\chi,\varphi,\rho}$; C_i — множество его простых контуров, содержащих вершину с номером $i \in V$.

Для любой вершины с номером $i \in \{1, \ldots, m\}$ и простого контура $w \in C_i$ через $C_{i,w}$ обозначим множество простых контуров, принадлежащих целиком какому-либо маршруту с началом в вершине i и второй вершиной, принадлежащей контуру w.

Алгоритм 1. Алгоритм нахождения максимального числа Фробениуса

Вход: орграф $\Gamma_{W,\chi,\varphi,\rho}$

Выход: $g_{\max}$; множества $G(i,w)$, $G(i,w,d)$ для всех вершин $i \in \{1,\ldots,m\}$ и контуров $w \in C_i$, $d \in C_{i,w}$

1: **Для** каждой вершины $i \in V$

2: Найти все простые контуры из C_i.

3: **Для** каждого простого контура $w \in C_i$

4: $s := w$, $C_{i,w} := \{w\}$, $G(i,w,w) := \{\mathrm{len}(w)\}$.

5: **Для** каждой вершины j, принадлежащей контуру s (за исключением вершины i)

6: Найти все простые контуры (исключая s), которые содержат вершину j, но не содержат вершину i, и поместить их в множество C'_j.

7: Если $C'_j \neq \varnothing$, то добавить все элементы множества C'_j в $C_{i,w}$.
Вычислить множество

$$G(i,w,s') = \bigcup_{d \in G_{i,w,s}} \left\{ d + \sum_{s \in C'_j} m_i \cdot \mathrm{len}(s) : 0 \leqslant m_i < d \right\}.$$

8: **Для** каждого простого контура $s' \in C'_j$ положить $s := s'$ и повторить шаги 5–7.

9: Вычислить множество $G(i,w) = \bigcup\limits_{d \in C_{i,w}} G(i,w,d)$.

10: **Для** каждой вершины с номером $i \in V$ вычислить число Фробениуса полугруппы $\left\langle \bigcup\limits_{w \in C_i} G(i,w) \right\rangle$.

11: Найти максимальное из чисел Фробениуса, вычисленных на шаге 10, и обозначить его $g_{\max}$.

Приведём пример нахождения $g_{\max}$ для обобщённого алгоритма шифрования Фейстеля с раундовой функцией $g_k : (\alpha_1, \alpha_2, \alpha_3, \alpha_4) \mapsto (\alpha_2, \alpha_3, \alpha_4, \alpha_1 \oplus f_{1,k}(\alpha_4))$, которая принадлежит $(W, \chi, \varphi, \rho)_c$-семейству с параметрами $W = (A, A')$, $A = \{2,3,4\}$, $A' = \{1\}$), $\chi(1) = \{4\}$, $\varphi(1,4) = 1$, $\rho = (1,4,3,2)$. Соответствующий орграф представлен на рис. 3.

Прокомментируем работу алгоритма. Заметим, что орграф на рис. 3 содержит два простых контура. Первый из них (w_1) содержит все вершины из множества $\{1,2,3,4\}$; второй (w_2) — одну вершину 4. Приведём шаги работы алгоритма.

1–2. $C_1 = C_2 = C_3 = \{w_1\}$, $C_4 = \{w_1, w_2\}$.

3. Для каждой вершины $i \in \{1,2,3\}$ и контура w_1 применим шаги 4–9 и получим $C_{1,w_1} = C_{2,w_1} = C_{3,w_1} = \{w_2\}$, $G(1,w_1) = G(2,w_1) = G(3,w_1) = \{4,5,6,7\}$.
Для вершины 4 и циклов w_1, w_2 применим шаги 4–9 и получим $C_{4,w_1} = \varnothing$, $C_{4,w_2} = \varnothing$, $G(4,w_1) = \{4\}$, $G(4,w_2) = \{1\}$.

10. Получим

$$\left\langle \bigcup_{d \in C_1} G(1,d) \right\rangle = \left\langle \bigcup_{d \in C_2} G(2,d) \right\rangle = \left\langle \bigcup_{d \in C_3} G(3,d) \right\rangle = \langle 4,5,6,7 \rangle, \left\langle \bigcup_{d \in C_4} G(4,d) \right\rangle = \langle 1,4 \rangle.$$

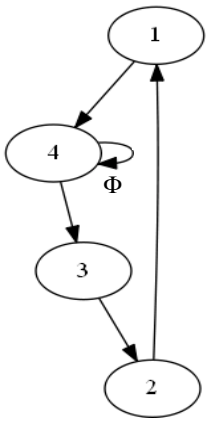

Рис. 3. Орграф обобщённого алгоритма шифрования Фейстеля

Числа Фробениуса полученных числовых полугрупп:

$$g(\langle 4,5,6,7\rangle)=3,\quad g(\langle 1,4\rangle)=0.$$

11. $g_{\max}=3$.

4.2. Оценки максимального числа раундов $r_{W,\chi,\varphi,\rho}$

Приведём необходимое и достаточное условие конечности параметра $r_{W,\chi,\varphi,\rho}$. Для этого сформулируем и докажем ряд лемм и утверждение. Для формулировок нам потребуются следующие обозначения.

Пусть r — номер раунда и $\alpha=\left(\alpha^{(1)},\ldots,\alpha^{(m)}\right)\in V_d^m$. Зададим такое отображение $\theta: V_d\to D$, что для любой d-битной разности δ имеет место

$$\theta(\delta)=\begin{cases}\gamma, & \text{если } \delta\neq\bar{0}_d,\\ \tilde{0}, & \text{если } \delta=\bar{0}_d.\end{cases}$$

Для входной разности $\alpha=\left(\alpha^{(1)},\ldots,\alpha^{(m)}\right)\in V_d^m$ зададим отображение $\xi: V_d^m\times\mathbb{N}\to$ $\to D^m$ как

$$\xi(\alpha,r)=(t_1,\ldots,t_m)=\begin{cases}\lambda(\alpha,\bar{0}_{md},r), & \text{если } r>0,\\ \left(\theta\left(\alpha^{(1)}\right),\ldots,\theta\left(\alpha^{(m)}\right)\right), & \text{если } r=0.\end{cases}$$

Рассмотрим ориентированный помеченный орграф $\Gamma_{W,\chi,\varphi,\rho,\alpha,r}=(V,R,\upsilon)$, соответствующий $(W,\chi,\varphi,\rho)_c$-семейству, где $V=\{v_1,\ldots,v_m\}$ — упорядоченное и пронумерованное множество вершин; R — множество дуг. Отображение $\upsilon: V\to D$ задаёт соответствие множеств вершин и меток и действует на V как $\upsilon(v_i)=t_i$. Заметим, что любой орграф $\Gamma_{W,\chi,\varphi,\rho,\alpha,r}$ имеет те же множества вершин и дуг, что и орграф $\Gamma_{W,\chi,\varphi,\rho}$, но метки его вершин зависят от параметров α и r.

Лемма 2. Для любых таких чисел $s,v\in\mathbb{N}$, $d_1,\ldots,d_v\in\mathbb{N}$, что $(s,d_1,\ldots,d_v)=1$, и числовой полугруппы $M=\langle d_1,\ldots,d_v\rangle$ положим

$$G(s,d_1,\ldots,d_v)=\left\{s+\sum_{i=1}^{v}m_id_i:0\leqslant m_i<s\right\},\quad I(M,s)=\left\{s+\sum_{i=1}^{v}n_id_i:n_i\in\mathbb{N}\right\}\bigcup\{0\}.$$

Тогда $I(M,s)=\langle G(s,d_1,\ldots,d_v)\rangle$.

Доказательство. Любой элемент из $I(M,s)$ может быть представлен как

$$s + d_1u_1 + \ldots + d_vu_v,$$

где $u_1, \ldots, u_v \in \mathbb{N}_0$. Рассмотрим два случая:

1) $u_1 = \ldots = u_v = 0$;

2) существует такое натуральное число j, что $1 \leqslant j \leqslant v$ и $u_j \neq 0$.

Пусть $u_1 = \ldots = u_v = 0$. Тогда $I(M,s) = \{s, 0\}$ и имеет место включение $I(M,s) \subseteq$ $\subseteq G(s, d_1, \ldots, d_v)$.

Пусть существует такое число $j \in \{1, \ldots, v\}$, что $u_j \neq 0$. Положим $\{m_1, \ldots, m_r\} =$ $= \{u_j : 0 < u_j < s, j \in \{1, \ldots, v\}\}$, а соответствующие коэффициенты из $\{d_1, \ldots, d_v\}$ обозначим как $d_m^{(1)}, \ldots, d_m^{(r)}$. Аналогично положим

$$\{h_1, \ldots, h_w\} = \{u_j : u_j \geqslant s, j \in \{1, \ldots, v\}\},$$

а соответствующие коэффициенты из $\{d_1, \ldots, d_v\}$ обозначим $d_h^{(1)}, \ldots, d_h^{(r)}$. Ясно, что каждое число из $\{h_1, \ldots, h_w\}$ представимо как $h_i = k_i s + m_h^{(i)}$, где $k_i > 0$; $0 \leqslant m_h^{(i)} < s$ для любого $i \in \{1, \ldots, w\}$. Таким образом,

$$\begin{aligned} s + d_1u_1 + \ldots + d_vu_v &= s + \sum_{i=1}^{r} d_m^{(i)} m_i + \sum_{i=1}^{w} d_h^{(i)} h_i = \\ &= s + \sum_{i=1}^{r} d_m^{(i)} m_i + \sum_{i=1}^{w} \left(s + d_h^{(i)} m_h^{(i)} \right) + \sum_{i=1}^{w} (k_i - 1)s. \end{aligned}$$

Значит, $I(M,s) \subseteq \langle G(s, d_1, \ldots, d_v) \rangle$. Доказательство включения $\langle G(s, d_1, \ldots, d_v) \rangle \subseteq$ $\subseteq I(M,s)$ очевидно. ■

Имеет место следующая

Лемма 3. Длина замкнутого пути w представима в виде суммы длин простых контуров (не обязательно различных), все дуги и вершины которых принадлежат этому пути.

Лемма 4. Для любых $i \in \{1, \ldots, m\}$, простого контура w, проходящего через вершину с номером i, простого контура $d \in C_{i,w}$ и $g \in G(i, w, d)$ существует замкнутый путь длины g с началом и концом в вершине с номером i, где множества $C_{i,w}$ и $G(i, w, d)$ — результаты работы алгоритма 1.

Доказательство. Для любых простых контуров w, d и вершины i, принадлежащей контуру w, множество $G(i, w, d)$ образовано путём последовательного обхода простых контуров, начиная с вершины i. Значит, для любого $g \in G(i, w, d)$ существует такая последовательность простых контуров w,s_1, …, s_k, d, что существует замкнутый маршрут с началом в вершине i, содержащий только эти контуры (возможно, многократно). ■

Лемма 5. Пусть орграф $\Gamma_{W,\chi,\varphi,\rho}$ примитивен и $\alpha = \left(0, \ldots, 0, \underbrace{\alpha^{(i)}}_{i}, 0, \ldots, 0\right) \in V_d^m$. Тогда в орграфе $\Gamma_{W,\chi,\rho,\alpha,r}$ метка вершины i не равна $\tilde{0}$ тогда и только тогда, когда $r \in \left\langle \bigcup\limits_{d \in C_i} G(i,d) \right\rangle$, где множество $G(i,d)$ — выход алгоритма 1.

Доказательство. Опишем процесс образования орграфа $\Gamma_{W,\chi,\rho,\alpha,r+1}$ из орграфа $\Gamma_{W,\chi,\rho,\alpha,r}$.

Зафиксируем вершину с номером j. Рассмотрим все дуги (пусть их число равно $t \in \{1,\dots,m\}$) с концом в вершине j. Пусть номера вершин, являющихся началом этих дуг, образуют множество $U = \{u_1,\dots,u_t\}$ и в графе $\Gamma_{W,\chi,\rho,\alpha,r}$ каждая вершина из множества U с номером u_k, $1 \leqslant k \leqslant t$, помечена меткой $v_k \in D$. Тогда метка вершины j в графе $\Gamma_{W,\chi,\rho,\alpha,r+1}$ равна $\bigoplus\limits_{i=1}^{t} v_i$. Значит, в орграфе $\Gamma_{W,\chi,\rho,\alpha,r}$ метка вершины i не равна $\tilde{0}$ тогда и только тогда, когда r — длина замкнутого пути, проходящего через вершину i. Рассмотрим такой произвольный замкнутый путь w, что вершина i находится только в начале и конце этого пути.

Из лемм 2 и 3 следует, что длина любого замкнутого пути, проходящего через вершину i, принадлежит множеству $P = \left\langle \bigcup\limits_{d \in C_i} G(i,d) \right\rangle$.

Рассмотрим произвольный элемент p множества P. Пусть он образован генераторами $g_1, \dots, g_k$. Докажем, что существует замкнутый путь длины p с началом и концом в вершине i. Доказательство проведём индукцией по числу k.

Пусть $k = 1$. Ясно, что $g_1 \in G(i,w)$ для некоторого простого контура w, проходящего через вершину i. Из алгоритма 1 следует, что $g_1 \in G(i,w,d)$ для некоторого простого контура $d \in C_{i,w}$. Из леммы 4 следует, что существует замкнутый путь длины g_1 с началом и концом в вершине i.

Пусть утверждение верно для k генераторов $g_1, \dots, g_k$. Докажем для $k+1$.

В силу леммы 4 существует замкнутый путь с началом и концом в вершине i длины g_{k+1}. Отсюда, учитывая предположение индукции и примитивность графа $\Gamma_{W,\chi,\rho,\alpha,r}$, получаем справедливость индуктивного перехода для $k+1$.

Утверждение леммы 5 напрямую следует из доказанного факта и леммы 4. ■

Утверждение 3. Для любого $(W,\chi,\varphi,\rho)_c$-семейства число $r_{W,\chi,\varphi,\rho}$ конечно тогда и только тогда, когда орграф $\Gamma_{W,\chi,\varphi,\rho}$ примитивен.

Доказательство. Пусть орграф $\Gamma_{W,\chi,\rho,\alpha,r}$ импримитивен. Рассмотрим входную разность

$$\alpha = \left(0,\dots,0,\ \underbrace{\alpha^{(i)}}_{i},0,\dots,0\right) \in V_d^m.$$

Если орграф $\Gamma_{W,\chi,\rho,\alpha,r}$ не является сильносвязным, то существуют по крайне мере два таких несвязных подграфа Γ_1 и Γ_2, что вершина i принадлежит множеству вершин подграфа Γ_1.

Метки всех вершин графа Γ_2 равны $\tilde{0}$. Очевидно, что невозможные разности существуют для любого r. Отсюда $r_{W,\chi,\varphi,\rho}$ бесконечно.

Если орграф $\Gamma_{W,\chi,\rho,\alpha,r}$ сильно связен, но наибольший общий делитель длин всех простых контуров равен $t > 1$, то все графы $\Gamma_{W,\chi,\rho,\alpha,tq+1}$, $q \in \mathbb{N}$, имеют метку $\tilde{0}$ у вершины i. Число таких графов бесконечно. Таким образом, $r_{W,\chi,\varphi,\rho}$ бесконечно.

Если орграф $\Gamma_{W,\chi,\rho,\alpha,r}$ примитивен, то из леммы 5 следует, что $r_{W,\chi,\varphi,\rho}$ конечно. ■

Отметим, что если параметр $r_{W,\chi,\varphi,\rho}$ бесконечен, то все алгоритмы шифрования Фейстеля из $(W,\chi,\varphi,\rho)_c$-семейства не являются стойкими к методу невозможных разностей.

Пусть $p_{\max}$ — длина максимального простого контура в орграфе $\Gamma_{W,\chi,\varphi,\rho}$. В следующем утверждении приведены нижняя и верхняя оценки конечного числа $r_{W,\chi,\varphi,\rho}$. Это основной результат работы.

Утверждение 4. Для любого $(W,\chi,\varphi,\rho)_c$-семейства с примитивным орграфом $\Gamma_{W,\chi,\varphi,\rho}$ справедливы неравенства

$$\max\left(g_{\max},\mathrm{d}\left(\Gamma_{W,\chi,\varphi,\rho}\right)\right)\leqslant r_{W,\chi,\varphi,\rho}\leqslant g_{\max}+\mathrm{d}\left(\Gamma_{W,\chi,\varphi,\rho}\right)+p_{\max}.$$

Доказательство. Используем утверждение 1 и рассмотрим входную разность

$$\alpha=\left(0,\ldots,0,\underbrace{\alpha^{(i)}}_{i},0,\ldots,0\right)\in V_d^m.$$

Пусть $r=\max\left(g_{\max},\mathrm{d}\left(\Gamma_{W,\chi,\varphi,\rho}\right)\right)$. Из определения диаметра орграфа, числа Фробениуса и леммы 4 получаем, что орграф $\Gamma_{W,\chi,\rho,\alpha,r}$ содержит по крайней мере одну вершину с меткой не равной Δ. Отсюда $\max\left(g_{\max},\mathrm{d}\left(\Gamma_{W,\chi,\varphi,\rho}\right)\right)\leqslant r_{W,\chi,\varphi,\rho}$.

Пусть $r=g_{\max}+\mathrm{d}\left(\Gamma_{W,\chi,\varphi,\rho}\right)$. Очевидно, что все метки орграфа $\Gamma_{W,\chi,\rho,\alpha,r}$ принадлежат множеству $\{\Delta,\gamma\}$.

Пусть $l=r+p_{\max}$. Из равенств $\gamma\oplus\gamma=\Delta$, $\gamma\oplus\Delta=\Delta$, $\Delta\oplus\Delta=\Delta$ следует, что метки всех вершин в орграфе $\Gamma_{W,\chi,\rho,\alpha,l}$ равны Δ. Таким образом, $r_{W,\chi,\varphi,\rho}\leqslant g_{\max}+\mathrm{d}\left(\Gamma_{W,\chi,\varphi,\rho}\right)+$ $+\,p_{\max}$. ■

Используя результаты утверждения 4, приведём пример нахождения оценок сверху и снизу величины $r_{W,\chi,\varphi,\rho}$ для обобщённых алгоритмов шифрования Фейстеля 1-го типа. Рассмотрим такое $(W,\chi,\varphi,\rho)_c$-семейство, что $|A|=\{1,\ldots,m\}\setminus\{j\}$, $|A'|=\{j\}$ для некоторых $i,j\in\{1,\ldots,m\}$, $\chi\left(j\right)=i$. Ясно, что орграф $\Gamma_{W,\chi,\varphi,\rho}$, соответствующий семейству, есть объединение двух простых контуров и состоит из m вершин; он показан на рис. 4.

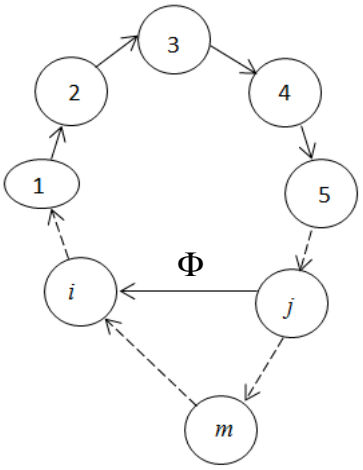

Рис. 4. Орграф обобщённого алгоритма шифрования Фейстеля 1-го типа

Из рис. 4 видно, что $\mathrm{d}(\Gamma_{W,\chi,\varphi,\rho})=m-1$. По теореме Сильвестра [16] имеем

$$g\left(\langle m+o\left(i,j\right),m\rangle\right)=\left(m+o\left(i,j\right)\right)m-o\left(i,j\right)-2m.$$

Здесь $o(i,j)$ — длина простого контура с началом в вершине i, проходящего через вершину j и содержащего дугу с меткой Ф.

Длина максимального простого контура равна m. Очевидно, что $g\left(\langle m + o\left(i,j\right), m\rangle\right)$ максимально, если $o\left(i,j\right) = m - 1$. В этом случае получаем

$$g_{\max} = g\left(\langle 2m-1, m\rangle\right) = 2m^2 - 4m + 1,$$
$$2m^2 - 4m + 1 \leqslant r_{W,\chi,\varphi,\rho} \leqslant 2m^2 - 4m + 1 + m - 1 + m = 2m\left(m-1\right).$$

В таблице приведены сравнительные характеристики оценок числа раундов для конкретных шифров и заявленного разработчиками числа раундов.

Алгоритм шифрования	Оценка снизу	Оценка сверху	Заявленное число раундов
CAST-256	3	10	48
RC-6	2	10	20
MARS	9	13	32

ЛИТЕРАТУРА

1. *Nyberg K.* Generlized Feistel networks // ASIACRYPT'1996. LNCS. 1996. V. 1163. P. 91–104.
2. *Schneier B. and Kelsey J.* Unbalanced Feistel networks and block cipher design // FSE'2005. LNCS. 2005. V. 3557. P. 121–144.
3. *Zhang L., Wu W., and Zhang L.* Proposition of two cipher structures // Inscrypt'2009. LNCS. 2010. V. 6151. P. 215–229.
4. *Shibutani K., Isobe T., Hiwatari H., et al.* Piccolo: an ultra-lightweight blockcipher // CHES'2011. LNCS. 2011. V. 6917. P. 342–357.
5. *Suzaki T. and Minematsu K.* Improving the generalized Feistel // FSE'2010. LNCS. 2010. V. 6147. P. 19–39.
6. *Lai X., Massey J. L., and Murphy S.* Markov ciphers and differential cryptanalysis // EuroCrypt'91. LNCS. 1991. V. 547. P. 17–38.
7. *Knudsen L. R.* DEAL — a 128-bit block cipher. Technical report 151. Department of Informatics, University of Bergen, Norway, February 1998.
8. *Biham E., Biryukov A., and Shamir A.* Cryptanalysis of Skipjack reduced to 31 rounds using impossible differentials // EUROCRYPT'99. LNCS. 1999. V. 1592. P. 12–23.
9. *Bogdanov A. and Shibutani K.* Generalized Feistel networks revisited // Designs, Codes and Cryptography. 2012. V. 66. P. 75–79.
10. *Li R., Sun B., Li C., and Qu L.* Cryptanalysis of a generalized unbalanced Feistel network structure // ACISP'2010. LNCS. 2010. V. 6168. P. 1–18.
11. *Zheng Y., Matsumoto T., and Imai H.* On the construction of block ciphers provably secure and not relying on any unproved hypotheses // CRYPTO'1989. LNCS. 1989. V. 435. P. 461–480.
12. *Schnorr C. P.* On the construction of random number generators and random function generators // EUROCRYPT'88. LNCS. 1988. V. 330. P. 225–232.
13. *Feistel H., Notz W., and Smith J. L.* Some cryptographic techniques for machine-to-machine data communications // Proc. IEEE. 1975. V. 63. No. 11. P. 1545–1554.
14. *Luo Y., Wu Z., Lai X., and Gong G.* A unified method for finding impossible differentials of block cipher structures // Inform. Sci. 2014. V. 263. P. 211–220.
15. *Kim J., Hong S., and Lim J.* Impossible differential cryptanalysis using matrix method // Discr. Math. 2010. V. 310. P. 988–1002.
16. *Sylvester J. J.* Problem 7382 // Math. Quest. From Educat. Times. 1884. V. 37. P. 26.

REFERENCES

1. *Nyberg K.* Generlized Feistel networks. ASIACRYPT'1996, LNCS, 1996, vol. 1163, pp. 91–104.
2. *Schneier B. and Kelsey J.* Unbalanced Feistel networks and block cipher design. FSE'2005, LNCS, 2005, vol. 3557, pp. 121–144.
3. *Zhang L., Wu W., and Zhang L.* Proposition of two cipher structures. Inscrypt'2009, LNCS, 2010, vol. 6151, pp. 215–229.
4. *Shibutani K., Isobe T., Hiwatari H., et al.* Piccolo: an ultra-lightweight blockcipher. CHES'2011, LNCS, 2011, vol. 6917, pp. 342–357.
5. *Suzaki T. and Minematsu K.* Improving the generalized Feistel. FSE'2010, LNCS, 2010, vol. 6147, pp. 19–39.
6. *Lai X., Massey J. L., and Murphy S.* Markov ciphers and differential cryptanalysis. EuroCrypt'91, LNCS, 1991, vol. 547, pp. 17–38.
7. *Knudsen L. R.* DEAL — a 128-bit block cipher. Technical report 151. Department of Informatics, University of Bergen, Norway, February 1998.
8. *Biham E., Biryukov A., and Shamir A.* Cryptanalysis of Skipjack reduced to 31 rounds using impossible differentials. EUROCRYPT'99, LNCS, 1999, vol. 1592, pp. 12–23.
9. *Bogdanov A. and Shibutani K.* Generalized Feistel networks revisited. Designs, Codes and Cryptography, 2012, vol. 66, pp. 75–79.
10. *Li R., Sun B., Li C., and Qu L.* Cryptanalysis of a generalized unbalanced Feistel network structure. ACISP'2010, LNCS, 2010, vol. 6168, pp. 1–18.
11. *Zheng Y., Matsumoto T., and Imai H.* On the construction of block ciphers provably secure and not relying on any unproved hypotheses. CRYPTO'1989, LNCS, 1989, vol. 435, pp. 461–480.
12. *Schnorr C. P.* On the construction of random number generators and random function generators. EUROCRYPT'88, LNCS, 1988, vol. 330, pp. 225–232.
13. *Feistel H., Notz W., and Smith J. L.* Some cryptographic techniques for machine-to-machine data communications. Proc. IEEE, 1975, vol. 63, no. 11, pp. 1545–1554.
14. *Luo Y., Wu Z., Lai X., and Gong G.* A unified method for finding impossible differentials of block cipher structures. Inform. Sci., 2014, vol. 263, pp. 211–220.
15. *Kim J., Hong S., and Lim J.* Impossible differential cryptanalysis using matrix method. Discr. Math., 2010, vol. 310, pp. 988–1002.
16. *Sylvester J. J.* Problem 7382 // Math. Quest. From Educat. Times, 1884, vol. 37, p. 26.