МАТЕМАТИЧЕСКИЕ МЕТОДЫ КРИПТОГРАФИИ

DOI 10.17223/20710410/17/4

УДК 519.6

ОБ ОДНОМ ОБОБЩЕНИИ БЛОЧНЫХ ШИФРОВ ФЕЙСТЕЛЯ

А. М. Коренева*, В. М. Фомичев**

*Национальный исследовательский ядерный университет (*МИФИ*), г. Москва, Россия*

**Финансовый университет при Правительстве Российской Федерации, г. Москва, Россия*

E-mail: alisa.koreneva@gmail.com, fomichev@nm.ru

Исследованы блочные шифры на основе регистров сдвига, обобщающие шифры Фейстеля. Доказан критерий инволютивности алгоритмов шифрования из данного класса. С использованием теоретико-графового подхода исследованы перемешивающие свойства раундовой подстановки, даны верхние оценки диаметра и экспонента перемешивающего графа раундовой подстановки.

Ключевые слова: *блочный шифр Фейстеля, инволютивность алгоритма шифрования, перемешивающий граф (матрица) преобразования, диаметр графа, экспонент графа.*

Введение

Многие известные симметричные блочные шифры относятся к шифрам Фейстеля (DES-алгоритм, ГОСТ 28147-89 и др.). Отличительной особенностью этих шифров является то, что раундовая подстановка построена на основе преобразования регистра сдвига длины 2 над множеством двоичных векторов (описание алгоритма можно найти, например, в [1, с. 377]). Эта раундовая подстановка, зависящая от ключа, названа петлёй Фейстеля.

Идеи использования в блочных шифрах петли Фейстеля привлекательны до сих пор. Многочисленные исследования показали, что шифры Фейстеля позволяют обеспечить ряд хороших криптографических свойств, в том числе инволютивность алгоритма шифрования. На рубеже XX и XXI веков Национальный Институт стандартов и технологий США провел конкурс на разработку AES — нового криптографического стандарта, который с 2002 г. стал преемником DES. Среди кандидатов на AES было немало шифров, являющихся обобщениями шифра Фейстеля, например RC6, MARS, TWOFISH, LOKI и другие.

В данной работе разрабатывается идея построения симметричных блочных шифров на основе преобразований регистра сдвига произвольной длины. Увеличение длины базового регистра позволяет рассчитывать на улучшение некоторых характеристик шифра. Например, использование регистра сдвига большей длины дает возможность увеличить размер входного блока данных без существенного усложнения реализации функций, а также предоставляет больший выбор разработчику при построении раундовой функции, ключевого расписания и др. Возможны и другие улучшения криптографических свойств, впрочем, как и некоторые негативные изменения. Криптографические свойства симметричных блочных шифров, построенных на основе регистров сдвига длины больше 2, являются предметом исследований данной работы.

1. Инволютивность алгоритмов блочного шифрования регистрового типа

Ряд блочных шифров, в том числе шифры Фейстеля имеют инволютивный алгоритм шифрования [1, теоремы 17.1 и 17.2]. Инволютивность алгоритма шифрования является важным технологичным свойством шифрующих подстановок, так как зашифрование и расшифрование реализуются одним и тем же алгоритмом, изменяются лишь входные данные. Ключи зашифрования и расшифрования в инволютивном шифре Фейстеля обладают симметрией, точнее, они отличаются лишь взаимно обратным порядком использования раундовых ключей.

Рассмотрим обобщение шифров Фейстеля — класс итеративных симметричных блочных шифров на основе регистров сдвига длины $n > 2$ над множеством r-мерных двоичных векторов V_r, где n, r — натуральные. Определим условия на раундовую функцию, при которых алгоритм шифрования инволютивен.

Введём обозначения. Пусть q — ключ шифрования, h — количество раундов шифрования. Обозначим через $x(j) = [x_1(j), x_2(j), \ldots, x_n(j)]$ блок данных (состояние регистра) после j-го раунда шифрования, $j = 1, \ldots, h$, при $j = 0$ — входной блок данных, при $j = h$ — выходной блок данных. Вектор $x_i(j) \in V_r$ назовем i-м подблоком блока $x(j)$, $i = 1, \ldots, n$. Обозначим q_j раундовый ключ j-го раунда шифрования (двоичный вектор некоторой длины), $j = 1, \ldots, h$.

Раундовая подстановка φ_z блочного шифра при раундовом ключе z имеет вид

$$\varphi_z(x(j)) = (x_2(j), \ldots, x_n(j), \psi(x_2(j), \ldots, x_n(j), z) \oplus x_1(j)), j = 1, \ldots, h, \qquad (1)$$

где $\psi(y_2, \ldots, y_n, z)$ для $y_2, \ldots, y_n \in V_r$ есть функция усложнения шифра.

На рис. 1 представлена схема j-го раунда шифрования для блочного шифра на базе регистра сдвига длины n.

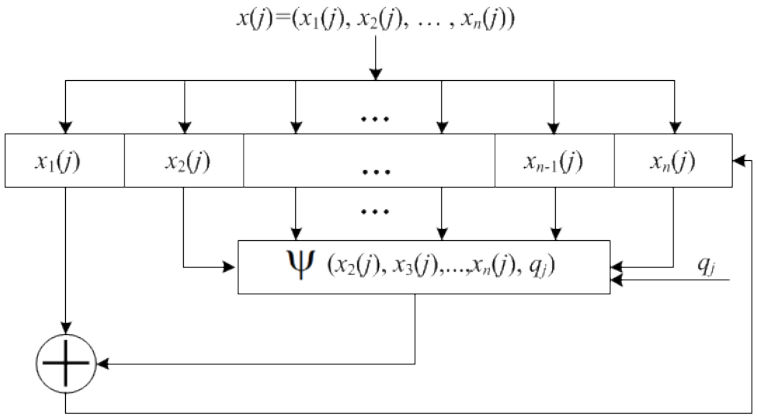

Рис. 1. Схема j-го раунда шифрования

Определим условия инволютивности данного блочного шифра. Обозначим через τ_n инволюцию степени $n > 1$ вида

$$\tau_n(y_1, \ldots, y_n) = (y_n, \ldots, y_1).$$

Для функции усложнения шифра $\psi(y_2, \ldots, y_n, z)$ при $n > 2$ имеем

$$\psi(\tau_{n-1}(y_2, \ldots, y_n), z) = \psi(y_n, \ldots, y_2, z).$$

Функцию усложнения $\psi(y_2, \ldots, y_n, z)$ назовем инвариантной относительно инволюции τ_{n-1}, если $\psi(y_2, \ldots, y_n, z) = \psi(y_n, \ldots, y_2, z)$. Очевидно следующее утверждение.

Лемма 1. Если функция $\psi(y_2, \ldots, y_n, z)$ инвариантна относительно инволюции τ_{n-1}, то переменная y_i является существенной тогда и только тогда, когда существенна переменная y_{n+2-i}, $i = 2, 3, \ldots, n$.

Лемма 2. При любой функции усложнения $\psi(y_2, \ldots, y_n, z)$, инвариантной относительно инволюции τ_{n-1}, для раундовой подстановки выполнено равенство

$$\varphi_z^{-1} = \tau_n \varphi_z \tau_n. \tag{2}$$

Доказательство. Докажем равносильное равенство $\tau_n \varphi_z \tau_n \varphi_z = e$. Для любых $y_1, \ldots, y_n$ и раундовой подстановки φ_z в соответствии с (1) выполнено

$$\varphi_z(y_1, \ldots, y_n) = (y_2, \ldots, y_n, y_1 \oplus \psi(y_2, \ldots, y_n, z)).$$

Применим инволюцию τ_n к $\varphi_z(y_1, \ldots, y_n)$:

$$\tau_n(\varphi_z(y_1, \ldots, y_n)) = (y_1 \oplus \psi(y_2, \ldots, y_n, z), y_n, \ldots, y_2).$$

Отсюда

$$\varphi_z(\tau_n(\varphi_z(y_1, \ldots, y_n))) = (y_n, \ldots, y_2, y_1 \oplus \psi(y_2, \ldots, y_n, z) \oplus \psi(y_n, \ldots, y_2, z)) = (y_n, \ldots, y_2, y_1),$$

так как $\psi(y_2, \ldots, y_n, z) \oplus \psi(y_n, \ldots, y_2, z) \equiv 0$. Тогда

$$\tau_n(\varphi_z(\tau_n(\varphi_z(y_1, \ldots, y_n)))) = \tau_n(y_n, \ldots, y_2, y_1) = (y_1, \ldots, y_n).$$

Лемма доказана. ■

Обратимость рассматриваемых алгоритмов шифрования на основе регистра сдвига длины $n > 2$ обеспечивается при любой функции усложнения, инвариантной относительно инволюции τ_{n-1}, с помощью применения после последнего раунда шифрования инволюции τ_n к блоку $x(h)$.

Теорема 1. Пусть функция усложнения $\psi(y_2, \ldots, y_n, z)$ инвариантна относительно инволюции τ_{n-1} и алгоритм шифрования состоит из h раундов и инволюции τ_n. Тогда алгоритм шифрования инволютивен и расшифрование отличается от зашифрования использованием раундовых ключей в обратном порядке.

Доказательство. В условиях теоремы подстановки зашифрования и расшифрования E_q и E_q^{-1} определяются формулами

$$E_q(x) = \tau_n \varphi_{q_h} \cdot \ldots \cdot \varphi_{q_1}(x); \tag{3}$$

$$E_q^{-1}(y) = \varphi_{q_1}^{-1} \cdot \ldots \cdot \varphi_{q_h}^{-1} \cdot \tau_n(y). \tag{4}$$

В равенстве (4) последовательно сделаем h раз замену подстановок $\varphi_{q_h}^{-1}, \ldots, \varphi_{q_1}^{-1}$ в соответствии с (2). Получим равенство $E_q^{-1}(y) = \tau_n \varphi_{q_1} \cdot \ldots \cdot \varphi_{q_h}(y)$. Сравнение его с (3) даёт утверждение теоремы. ■

2. Перемешивающие свойства алгоритма шифрования

Перемешивающие свойства преобразования f множества X^n, заданного системой координатных функций $\{f_1(x_1, \ldots, x_n), \ldots, f_n(x_1, \ldots, x_n)\}$, определяются системой множеств $\{S(f_1), \ldots, S(f_n)\}$, где $S(f_j)$ — множество номеров существенных переменных функции f_j, $j = 1, \ldots, n$. Считается, что наилучшее перемешивание достигается тогда,

когда каждая из координатных функций преобразования f зависит от всех переменных, то есть $S(f_j) = \{1, \ldots, n\}$, $j = 1, \ldots, n$. Аппаратная или программная реализация таких преобразований затруднена в связи с необходимостью реализации функций от большого числа переменных. Поэтому хорошее перемешивание часто достигается при итерациях (возведении в степень) преобразования с относительно слабыми перемешивающими свойствами. Показатель степени преобразования, при которой достигается хорошее перемешивание, является важной криптографической характеристикой. В частности, показатель степени раундовой подстановки, при которой достигается хорошее перемешивание, является определяющим для разработчика при выборе числа раундов шифрования блочного шифра.

Рассмотрим раундовую подстановку φ_z множества V_{nr}, определяемую равенством (1). Функцией обратной связи данного регистра является функция $\psi(x_2(j), \ldots, x_n(j), z) \oplus x_1(j)$. Подстановка φ_z задается системой булевых координатных функций $\{\varphi_1(x_1, x_2, \ldots, x_{nr}), \varphi_2(x_1, x_2, \ldots, x_{nr}), \ldots, \varphi_{nr}(x_1, x_2, \ldots, x_{nr})\}$ [1, теорема 5.1].

Для оценки перемешивающих свойств степеней подстановки φ_z при фиксированном ключе z используем теоретико-графовый подход. Обозначим $\Gamma(\varphi)$ перемешивающий nr-вершинный орграф подстановки φ_z, в котором пара (i, j) является дугой тогда и только тогда, когда $i \in S(\varphi_j)$, $i, j \in \{1, \ldots, nr\}$. Матрицу $M(\varphi)$ смежности вершин графа $\Gamma(\varphi)$ называют перемешивающей матрицей подстановки φ_z.

Если орграф $\Gamma(\varphi)$ не является полным (матрица $M(\varphi)$ не положительна, то есть содержит нулевые элементы), то подстановка φ_z реализует неполное перемешивание, иначе говоря, φ_z не является совершенной. Если матрица $(M(\varphi))^m$ не положительна, то подстановка $(\varphi_z)^m$ реализует неполное перемешивание, $m \geqslant 1$ [1, следствие 2 теоремы 10.3].

Необходимым условием хорошего перемешивания с использованием степеней подстановки φ_z является примитивность орграфа $\Gamma(\varphi)$, что равнозначно сильной связности орграфа [1, следствие 1 теоремы 10.3] и наличию в нем простых циклов длины $l_1, \ldots, l_k$, где $k > 1$ и НОД$(l_1, \ldots, l_k) = 1$ [2, с. 393]. Степень преобразования, при которой достигается хорошее перемешивание, оценивается снизу экспонентом орграфа $\Gamma(\varphi)$ (экспонентом матрицы $M(\varphi)$).

Исследуем условия хорошего перемешивания входных блоков с помощью раундовой подстановки φ_z множества V_{nr} данных блочных шифров. Построим перемешивающую матрицу $M(\varphi)$ размера $nr \times nr$ в соответствии с равенством (1). Матрица $M(\varphi)$, разбитая на n^2 блоков размера $r \times r$, изображена в таблице.

Перемешивающая матрица $M(\varphi)$ раундовой подстановки φ_z

Переменные	$\varphi_1 \ldots \varphi_r$	$\varphi_{r+1} \ldots \varphi_{2r}$	...	$\varphi_{(n-2)r+1} \ldots \varphi_{(n-1)r}$	$\varphi_{(n-1)r+1} \ldots \varphi_{nr}$
x_1 ... x_r	0	0	...	0	E
x_{r+1} ... x_{2r}	E	0	...	0	ψ_1
x_{2r+1} ... x_{3r}	0	E	...	0	ψ_2
...	...	...	...	...	...
$x_{(n-1)r+1}$ ... x_{nr}	0	0	...	E	ψ_r

Символом 0 обозначены блоки, состоящие из нулей, символом E — единичные матрицы. Блок ψ_j показывает зависимость координатных функций $\varphi_{(n-1)r+1}, \ldots, \varphi_{nr}$ (обратной связи регистра) от переменных $x_{(j-1)r+1}, \ldots, x_{jr}$, $j = 2, \ldots, n$.

Для функции усложнения $\psi(y_2, \ldots, y_n, z)$ определим r-вершинный граф Γ_ψ: пара (v, w) образует дугу тогда и только тогда, когда функция $\varphi_{(n-1)r+w}$ зависит существенно хотя бы от одной из переменных множества $\{x_v, x_{r+v}, \ldots, x_{(n-1)r+v}\}$. То есть

граф Γ_ψ получается из графа $\Gamma(\varphi)$ отождествлением n вершин, соответствующих одинаковым координатам r-мерных векторов. Обозначим через Γ_0 граф $\Gamma(\varphi)$ для функции $\psi(y_2,\ldots,y_n,z)\equiv 0$.

Теорема 2. Перемешивающий граф $\Gamma(\varphi)$ сильно связен тогда и только тогда, когда сильно связен граф Γ_ψ.

Доказательство. Граф Γ_0 состоит из r независимых циклов длины n (рис. 2). Обозначим эти циклы $C_1,\ldots,C_r$.

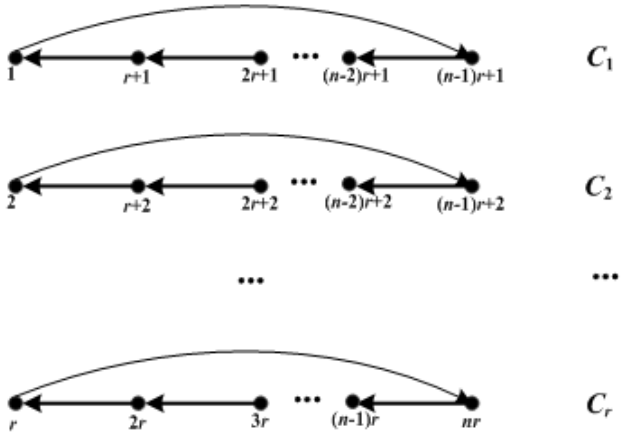

Рис. 2. Граф Γ_0

Множества вершин графов Γ_0 и $\Gamma(\varphi)$ совпадают, и Γ_0 является частью графа $\Gamma(\varphi)$. Значит, если вершины i,j графа $\Gamma(\varphi)$ принадлежат одному циклу, то каждая из них достижима из другой.

Заметим, что при любой функции усложнения ψ граф Γ_ψ получается из графа $\Gamma(\varphi)$ отождествлением вершин, принадлежащих одному и тому же циклу. Тогда, учитывая взаимную достижимость вершин одного цикла, в графе $\Gamma(\varphi)$ любая вершина w, принадлежащая циклу C_j, достижима из любой вершины v, принадлежащей циклу C_i при $i\neq j$, где $i,j\in\{1,\ldots,r\}$, тогда и только тогда, когда вершина j достижима из вершины i в графе Γ_ψ. Следовательно, $\Gamma(\varphi)$ сильно связен тогда и только тогда, когда сильно связен r-вершинный граф Γ_ψ. ■

Теорема 3. Если граф Γ_ψ сильносвязный и $\operatorname{diam}\Gamma_\psi\leqslant d$, то

1) $\operatorname{diam}\Gamma(\varphi)\leqslant(n-1)\min\{d,r-1\}+n$;
2) если граф $\Gamma(\varphi)$ примитивный и алгоритм блочного шифрования инволютивен, то $\operatorname{diam}\Gamma(\varphi)\leqslant n/2\cdot\min\{d,r-1\}+n$;
3) если граф $\Gamma(\varphi)$ примитивный, то $\exp\Gamma(\varphi)\leqslant n^2r+nr-2n$.

Доказательство.

1) Обозначим длину кратчайшего пути в графе $\Gamma(\varphi)$ из i в j через $l_{i,j}$. Диаметр орграфа $\Gamma(\varphi)$ — это максимум $l_{i,j}$ (по всем $i,j\in\{1,\ldots,nr\}$).

Если вершины i,j принадлежат одному циклу графа Γ_0, то $l_{i,j}\leqslant n$.

Пусть вершины i,j принадлежат циклам C_v и C_w графа Γ_0, где $v\neq w$. Так как граф Γ_ψ сильно связный и $\operatorname{diam}\Gamma_\psi\leqslant d$, то в Γ_ψ имеется простой путь $(b_0,b_1,\ldots,b_l)$ из v в w длины l, где $v=b_0$, $w=b_l$, $l\leqslant d$ и $l\leqslant r-1$, так как $v\neq w$. Без ущерба для общности положим, что $i,b_0\in C_1$, $b_1\in C_2$, …, $b_l,j\in C_{l+1}$. Тогда из определения графа Γ_ψ следует, что в графе $\Gamma(\varphi)$ при некоторых $j_1,j_2,\ldots,j_l\in\{1,\ldots,n-1\}$

имеются дуги $(j_1r+1,(n-1)r+2),(j_2r+2,(n-1)r+3),\ldots,(j_lr+l,(n-1)r+l+1)$. Значит, путь из i в j в графе $\Gamma(\varphi)$ можно составить как последовательность путей $(u_0,\delta_1,u_1,\delta_2,\ldots,u_{l-1},\delta_l,u_l)$, где δ_k есть дуга $(j_kr+k,(n-1)r+k+1)$ при $k=1,\ldots,l$, путь u_0 есть путь длины не более $n-1$ из i в j_1r+1 (часть цикла C_1), путь u_{k-1} есть путь длины не более $n-2$ из $(n-1)r+k$ в j_kr+k (часть цикла C_k) при $k=2,\ldots,l$ и путь u_l есть путь длины не более $n-1$ из $(n-1)r+l+1$ в j (часть цикла C_{l+1}). Следовательно, при любых $i,j\in\{1,\ldots,nr\}$ длина данного пути из i в j в графе $\Gamma(\varphi)$ не превышает $l+2(n-1)+(l-1)(n-2)=nl+n-l$. В силу произвольности рассмотренных i,j получим $\operatorname{diam}\Gamma(\varphi)\leqslant nl+n-l$, где $l\leqslant\min\{d,r-1\}$. Следовательно, $\operatorname{diam}\Gamma(\varphi)\leqslant(n-1)\min\{d,r-1\}+n$.

2) Вернёмся к рассмотрению кратчайшего пути $(u_0,\delta_1,u_1,\delta_2,\ldots,u_{l-1},\delta_l,u_l)$ в графе $\Gamma(\varphi)$ из i в j длины $l_{i,j}$. Если алгоритм шифрования инволютивен, то в соответствии с леммой 1 в графе $\Gamma(\varphi)$ при некоторых $j_1,\ldots,j_l\in\{1,\ldots,n-1\}$ имеются пары дуг $(j_1r+1,(n-1)r+2)$ и $((n-j_1)r+1,(n-1)r+2),\ldots,(j_lr+l,(n-1)r+l+1)$ и $((n-j_l)r+l,(n-1)r+l+1)$. Тогда уточним определения элементов пути. Здесь u_0 есть путь из i в a_1 (часть цикла C_1), где a_1 — ближайшая из двух вершин j_1r+1 и $(n-j_1)r+1$ к вершине i. Путь u_{k-1} есть при $k=2,\ldots,l$ путь из $(n-1)r+k$ в a_k (часть цикла C_k), где a_k — ближайшая из двух вершин j_kr+k и $(n-j_k)r+k$ к вершине $(n-1)r+k$. И u_l есть путь из $(n-1)r+l+1$ в j (часть цикла C_{l+1}). Соответственно δ_k есть дуга $(a_k,(n-1)r+k+1)$ при $k=1,\ldots,l$.

Следовательно (см. рис. 2), длина пути u_0 не превышает $\lfloor n/2\rfloor$, длины путей $u_1,\ldots,u_{l-1}$ не превышают $\lfloor n/2\rfloor-1$ и длина пути u_l не превышает $n-1$. Отсюда

$$l_{i,j}\leqslant l+n/2+(l-1)(n/2-1)+n-1=nl/2+n,$$

где $l\leqslant\min\{d,r-1\}$. Тогда $\operatorname{diam}\Gamma(\varphi)\leqslant nl/2+n$ в силу произвольности рассмотренных i,j.

3) Известно [2, с. 227], что если λ — длина самого короткого цикла сильно связного примитивного m-вершинного графа Γ, то $\exp\Gamma\leqslant m+\lambda(m-2)$. В nr-вершинном графе $\Gamma(\varphi)$ длина самого короткого цикла не превышает n в силу наличия циклов $C_1,\ldots,C_r$. Следовательно, $\exp\Gamma(\varphi)\leqslant nr+n(nr-2)$. ■

Теорема 4. Сильносвязный граф $\Gamma(\varphi)$ примитивен, если выполнено любое из следующих условий:

1) координатная функция φ_m зависит существенно от переменной x_m при некотором $m\in\{(n-1)r+1,(n-1)r+2,\ldots,nr\}$, в этом случае $\exp\Gamma(\varphi)\leqslant 2nr-2$;

2) алгоритм шифрования инволютивен и при некоторых $m\in\{(n-1)r+1,(n-1)r+2,\ldots,nr\}$ и $\mu\in\{1,\ldots,r\}$ координатная функция φ_m зависит существенно от переменной $x_{jr+\mu}$, где $n-2j=1$, в этом случае $\exp\Gamma(\varphi)\leqslant(ln/2)^2+n(r-l)-1$, где l — длина кратчайшего цикла графа Γ_ψ, проходящего через дугу (μ,m).

Доказательство.

1) Из существенной зависимости функции φ_m от переменной x_m следует наличие петли в вершине m графа $\Gamma(\varphi)$. Петля является простым циклом длины 1. Тогда в сильносвязном графе $\Gamma(\varphi)$ имеются простые циклы длины 1 и $l>1$, где НОД $(1,l)=1$. Следовательно, граф $\Gamma(\varphi)$ примитивен и [2, с. 227] $\exp\Gamma(\varphi)\leqslant 2nr-2$.

2) Без ущерба для общности положим $m=(n-1)r+1$, тогда по условию в графе Γ_ψ имеется дуга $(\mu,1)$ и в графе $\Gamma(\varphi)$ имеется дуга $(jr+\mu,(n-1)r+1)$ при $j=(n-1)/2$.

Если алгоритм шифрования инволютивен, то в силу леммы 1 функция φ_m зависит существенно и от $x_{jr+\mu}$, и от $x_{(n-j)r+\mu}$, то есть в $\Gamma(\varphi)$ имеется дуга $((n-j)r+\mu, (n-1)r+1)$ при $j=(n-1)/2$.

Рассмотрим в сильносвязном графе Γ_ψ кратчайший простой цикл C_ψ, проходящий через дугу $(\mu, 1)$. Без ущерба для общности можно считать, что $C_\psi = (\mu, 1, \ldots, l-1)$, где l — длина цикла C_ψ. Тогда в графе $\Gamma(\varphi)$ имеется цикл C, проходящий через дугу $(jr+\mu, (n-1)r+1)$ и составленный при некоторых $j_1, \ldots, j_{l-1} \in \{1, \ldots, n-1\}$ как последовательность путей $(u_1, \delta_1, \ldots, u_l, \delta_l)$. Здесь u_k — путь (часть цикла C_k) из $(n-1)r+k$ в a_k, где a_k — ближайшая из двух вершин $j_k r+k$ и $(n-j_k)r+k$ к вершине $(n-1)r+k$, $k=1, \ldots, l-1$; u_l есть путь (часть цикла C_μ) из $(n-1)r+\mu$ в a_μ, где a_μ — ближайшая из двух вершин $jr+\mu$ и $(n-j)r+\mu$ к вершине $(n-1)r+\mu$. Соответственно δ_k при $k=1, \ldots, l-2$ есть дуга $(a_k, (n-1)r+k+1)$, δ_{l-1} есть дуга $(a_{l-1}, (n-1)r+\mu)$ и δ_l есть дуга $(a_\mu, (n-1)r+1)$. Следовательно (см. рис. 2), длина пути u_k не превышает $n/2-1$, $k=1, \ldots, l$, и длина цикла C не превышает $nl/2$.

Вместе с тем в графе $\Gamma(\varphi)$ имеется цикл C', полученный из цикла C заменой пути u_l на путь из вершины $(n-1)r+\mu$ в b и заменой дуги $(a_\mu, (n-1)r+1)$ на дугу $(b, (n-1)r+1)$, где b — более удалённая (от вершины $(n-1)r+\mu$) из двух вершин $jr+\mu$ и $(n-j)r+\mu$. При $n-2j=1$ вершины a_μ и b являются соседними на цикле C', поэтому длина цикла C' превышает длину цикла C на 1.

Итак, в графе $\Gamma(\varphi)$ имеются простые циклы C и C' взаимно простых длин λ и $\lambda+1$, где $\lambda \leqslant nl/2$, и порядок пересечения множеств вершин циклов C и C' равен λ. Следовательно, сильносвязный граф $\Gamma(\varphi)$ примитивен и верна оценка для экспонента графа $\Gamma(\varphi)$ [3, теорема 1$б$] $\exp\Gamma(\varphi) \leqslant (ln/2)^2 + n(r-l) - 1$. ■

Выводы

Сформулирован критерий инволютивности алгоритма блочного шифрования, основанного на регистре сдвига длины n над множеством двоичных r-мерных векторов (обобщение шифров Фейстеля). Исследованы свойства nr-вершинного перемешивающего графа $\Gamma(\varphi)$ раундовой подстановки φ, а именно:

1) показано, что граф $\Gamma(\varphi)$ сильно связен тогда и только тогда, когда сильно связен r-вершинный граф Γ_ψ, полученный из $\Gamma(\varphi)$ отождествлением вершин, соответствующих одинаковым координатам r-мерных векторов;
2) получены достаточные условия примитивности графа $\Gamma(\varphi)$;
3) получены оценки диаметра и экспонента графа $\Gamma(\varphi)$ в различных условиях.

ЛИТЕРАТУРА

1. *Фомичёв В. М.* Методы дискретной математики в криптологии. М.: ДИАЛОГ-МИФИ, 2010. 424 с.
2. *Сачков В. Н., Тараканов В. Е.* Комбинаторика неотрицательных матриц. М.: ТВП, 2000. 448 с.
3. *Фомичев В. М.* Оценки экспонентов примитивных графов // Прикладная дискретная математика. 2011. № 2(12). С. 101–112.