Секция 3

МАТЕМАТИЧЕСКИЕ МЕТОДЫ КРИПТОГРАФИИ

УДК 519.1 DOI 10.17223/2226308X/12/25

О ПЕРЕМЕШИВАЮЩИХ СВОЙСТВАХ НЕСТАЦИОНАРНОГО РЕГИСТРА СДВИГА

Я. Э. Авезова

Для регистра сдвига длины n, функция обратной связи которого зависит от двоичного знака управляющей последовательности (на каждом такте реализуется одно из двух регистровых преобразований), исследовано минимальное число γ тактов регистра, после которых достигнуто полное перемешивание, то есть существенная зависимость каждой координатной функции композиции преобразований от всех переменных. Эффект полного перемешивания оценен с помощью множества $\hat{\Gamma}$ перемешивающих n-вершинных орграфов регистровых преобразований, имеющих общий гамильтонов контур. Дана оценка экспонента $\exp\hat{\Gamma}$ примитивного множества $\hat{\Gamma}$, которая позволяет оценить снизу число γ:

$$\exp\hat{\Gamma} \leqslant 2n-2+\sum_{\alpha=0}^{1}\left(F(n-S(\varphi_\alpha))+d_\alpha+s^\alpha_{m(\alpha)}\right),$$

где $S(\varphi_\alpha)=\left\{s^\alpha_1,\ldots,s^\alpha_{m(\alpha)}\right\}$ — множество номеров существенных переменных функции обратной связи $\varphi_\alpha(x_0,\ldots,x_{n-1})$; $n-S(\varphi_\alpha)=\{n-s^\alpha_j : j=1,\ldots,m(\alpha)\}$; $d_\alpha=\text{НОД}\{n-S(\varphi_\alpha)\}$; $F(n-S(\varphi_\alpha))=d_\alpha\Phi((n-S(\varphi_\alpha))/d_\alpha)$; $\Phi((n-S(\varphi_\alpha))/d_\alpha)$ — число Фробениуса. Проведён вычислительный эксперимент при $n=6$ и 10 по вычислению точного значения γ с учётом управляющей последовательности. Установлено, что полное перемешивание возможно за число тактов, превышающее значение экспонента менее чем в 2 раза.

Ключевые слова: *гамильтонов контур, примитивность множества орграфов, экспонент орграфа, экспонент множества орграфов.*

Введение

Принцип перемешивания, описанный К. Шенноном [1], важен при построении криптографических систем, устойчивых к дифференциальному анализу и атакам, основанным на последовательном опробовании элементов ключа. Для хорошего перемешивания необходимо, чтобы преобразование было совершенным, т. е. чтобы каждая координатная функция существенно зависела от всех переменных [2]. Одним из способов построения совершенного преобразования является использование композиции нескольких преобразований, каждое из которых не является совершенным, но допускает относительно несложную реализацию.

Объектом исследования является нестационарный регистр сдвига (НРС) над пространством двоичных векторов V_n. Функция обратной связи НРС зависит от знака управляющей двоичной гаммы, за счёт чего на каждом такте реализуется одно из двух преобразований пространства V_n. Таким образом, за t тактов работы НРС реа-

лизуется композиция преобразований длины t. Актуальной задачей является оценка перемешивающих свойств НРС в зависимости от управляющей последовательности.

1. Определяющие свойства перемешивания с помощью композиции функций

Пусть $G = \{g_1, \ldots, g_p\}$ — множество преобразований пространства двоичных векторов V_n, где $p, n > 1$. Преобразованию $g_\tau \in G$ поставим в соответствие орграф $\Gamma(g_\tau)$, в котором пара вершин (i, j) является дугой, если и только если переменная x_i преобразования g_τ является существенной для координатной функции с номером j. Орграф $\Gamma(g_\tau)$ называется перемешивающим графом преобразования g_τ, $\tau = 1, \ldots, p$. Композиции функций $g(w) = g_{w_1} \ldots g_{w_s}$, где $g_{w_1}, \ldots, g_{w_s} \in G$, $s > 1$, соответствует перемешивающий граф $\Gamma(g(w)) = \Gamma(g_{w_1} \ldots g_{w_s})$. Преобразование $g(w)$ совершенное, если и только если $\Gamma(g(w))$ полный.

Пусть $\hat{\Gamma} = \{\Gamma_1, \ldots, \Gamma_p\}$ — множество орграфов, где $\Gamma_\tau = \Gamma(g_\tau)$, $\tau = 1, \ldots, p$. Тогда порождённая множеством $\hat{\Gamma}$ полугруппа имеет вид $\langle\hat{\Gamma}\rangle = \{\Gamma(w)\colon w \in N_p^*\}$, где $\Gamma(w) = \Gamma_{w_1} \ldots \Gamma_{w_s}$ при $w = w_1 \ldots w_s$; N_p^* — множество всех слов в алфавите $\{1, \ldots, p\}$; умножение орграфов определяется как умножение бинарных отношений. Множество $\hat{\Gamma}$ называется примитивным, если полугруппа $\langle\hat{\Gamma}\rangle$ содержит полный орграф. Наименьшая длина произведения, соответствующего полному орграфу, называется экспонентом множества $\hat{\Gamma}$ и обозначается $\exp\hat{\Gamma}$. Известно [2], что орграф $\Gamma(g(w))$ является частью орграфа $\Gamma(w)$. Следовательно, если орграф $\Gamma(w)$ не полный, то преобразование $g(w)$ не является совершенным.

Таким образом, примитивность множества $\hat{\Gamma}$ является необходимым условием существования совершенной композиции преобразований из множества G. Если найден экспонент примитивного множества $\hat{\Gamma}$, то исключена необходимость проверять совершенность любой композиции, длина которой меньше $\exp\hat{\Gamma}$.

2. Перемешивающие свойства НРС

Нестационарным регистром левого сдвига над V_n с обратной связью $\varphi(x_0, \ldots, x_{n-1}, \alpha)$ назовём отображение $g\colon V_{n+1} \to V_n$, если

$$g(x_0, \ldots, x_{n-1}, \alpha) = (x_1, \ldots, x_{n-1}, \varphi(x_0, \ldots, x_{n-1}, \alpha)),$$

где α — случайный или псевдослучайный двоичный знак управления; $\varphi(x_0, \ldots, x_{n-1}, \alpha) = (\alpha\oplus 1)\varphi_0(x_0, \ldots, x_{n-1}) \oplus \alpha\varphi_1(x_0, \ldots, x_{n-1})$; φ_0 и φ_1 — различные булевы функции от переменных $x_0, \ldots, x_{n-1}$.

Схема функционирования НРС представлена на рис. 1. Управляющую двоичную последовательность обозначим $\{\alpha_k\}$. В зависимости от знака гаммы α_k на k-м такте работы регистра сдвига реализуется одно преобразование из множества преобразований $\{g_0, g_1\}$, где $g_\alpha(x_0, \ldots, x_{n-1})$ — преобразование V_n, реализуемое регистром сдвига с функцией обратной связи $\varphi_\alpha(x_0, \ldots, x_{n-1})$, $\alpha \in \{0, 1\}$.

Перемешивающие свойства НРС моделируются множеством перемешивающих орграфов $\hat{\Gamma} = \{\Gamma(g_0), \Gamma(g_1)\}$, длины контуров которых определяются ячейками съёма регистра. Обозначим $S(\varphi_\alpha) = \left\{s_1^\alpha, \ldots, s_{m(\alpha)}^\alpha\right\}$ множество номеров существенных переменных функции $\varphi_\alpha(x_0, \ldots, x_{n-1})$, где $0 = s_1^\alpha < \ldots < s_{m(\alpha)}^\alpha \leqslant n-1$; $n - S(\varphi_\alpha) = \{n - s_j^\alpha\colon j = 1, \ldots, m(\alpha)\}$.

Орграф $\Gamma(g_\alpha)$ имеет множество простых контуров $\hat{C}(\varphi_\alpha) = \{C_1(\varphi_\alpha), \ldots, C_{m(\alpha)}(\varphi_\alpha)\}$, где $C_j(\varphi_\alpha) = (n-1, \ldots, s_j^\alpha + 1, s_j^\alpha)$ — контур длины $n - s_j^\alpha$, $j = 1, \ldots, m(\alpha)$. В каж-

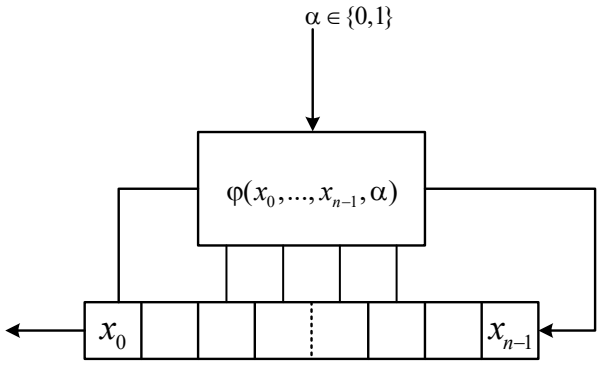

Рис. 1. Нестационарный регистр левого сдвига

дом орграфе множества $\hat{\Gamma}$ есть гамильтонов контур $(n-1,\dots,0)$. Согласно критерию примитивности множества орграфов с общим гамильтоновым контуром [3, теорема 4], множество $\hat{\Gamma}$ примитивное, если и только если орграф $U^{(2)}$ примитивный, где $U^{(2)}$ суть объединение орграфов $\Gamma(g_0)\cup\Gamma(g_1)$ с отождествлением кратных дуг. Поскольку $n-S(\varphi_\alpha)$ — множество длин простых контуров $\Gamma(g_\alpha)$, то орграф $U^{(2)}$ примитивный, если и только если НОД$\{n-(S(\varphi_0)\cup S(\varphi_1))\}=1$. Для экспонента примитивного множества справедлива оценка, которая следует из [3, теорема 4]:

$$\exp\hat{\Gamma}\leqslant 2n-2+\sum_{\alpha=0}^{1}\left(F(n-S(\varphi_\alpha))+d_\alpha+s^\alpha_{m(\alpha)}\right). \tag{1}$$

Здесь $d_\alpha=$ НОД$\{n-s^\alpha_j\colon j=1,\dots,m(\alpha)\}$; $F(n-S(\varphi_\alpha))=d_\alpha\Phi((n-S(\varphi_\alpha))/d_\alpha)$; $\Phi((n-S(\varphi_\alpha))/d_\alpha)$ — число Фробениуса; $(n-S(\varphi_\alpha))/d_\alpha=\{(n-s^\alpha_j)/d_\alpha\colon j=1,\dots,m(\alpha)\}$.

3. Экспериментальное исследование перемешивающих свойств НРС

Обозначим: $g_{\alpha_k}=g(x_0,\dots,x_{n-1},\alpha_k)$ — преобразование множества V_n, реализуемое НРС при знаке управляющей гаммы α_k; $g(\alpha,t)=g_{\alpha_t}\dots g_{\alpha_1}$ — композиция преобразований, реализуемая за t тактов при управляющей последовательности $\alpha=\{\alpha_k\}$, $\alpha_k\in\{0,1\}$, $k=1,2,\dots$; $\{f_0^{g(\alpha,t)},\dots,f_{n-1}^{g(\alpha,t)}\}$ — система координатных функций преобразования $g(\alpha,t)$; $S(f_j^{g(\alpha,t)})$ — множество номеров существенных переменных координатной функции $f_j^{g(\alpha,t)}$, $j=0,\dots,n-1$.

В соответствии с определением [2], $i\in S(f_j^{g(\alpha,t)})$, если найдутся такие векторы $(\beta_0,\dots,\beta_{i-1},0,\beta_{i+1},\dots,\beta_{n-1}),(\beta_0,\dots,\beta_{i-1},1,\beta_{i+1},\dots,\beta_{n-1})\in V_n$, что

$$f_j^{g(\alpha,t)}(\beta_0,\dots,\beta_{i-1},0,\beta_{i+1},\dots,\beta_{n-1})\neq f_j^{g(\alpha,t)}(\beta_0,\dots,\beta_{i-1},1,\beta_{i+1},\dots,\beta_{n-1}).$$

Приведём алгоритм проверки условия $i\in S(f_j^{g(\alpha,t)})$. Для заданной управляющей последовательности α и всех возможных начальных состояний регистра (векторов V_n в лексикографическом порядке) вычислим значение преобразования $g(\alpha,t)$, т. е. составим таблицы значений координатных функций $f_0^{g(\alpha,t)},\dots,f_{n-1}^{g(\alpha,t)}$. Далее для функции $f_j^{g(\alpha,t)}$ и переменной x_i, $i,j=0,\dots,n-1$:

1) вычислим величины $c=2^i$, $l=2^{n-i}$;
2) разделим столбец значений функции $f_j^{g(\alpha,t)}$ на c равных отрезков длины l: $(f_1,\dots,f_c)$, $f_1,\dots,f_c\in V_l$;

3) каждый из полученных на предыдущем шаге отрезков разделим на две половины: $f_b = (f_b^{(1)}, f_b^{(2)}) \in V_{l/2} \times V_{l/2}$, тогда если $f_b^{(1)} = f_b^{(2)}$ для всех $b = 1, \ldots, c$, то $i \notin S(f_j^{g(\alpha,t)})$, иначе $i \in S(f_j^{g(\alpha,t)})$.

Для исследования перемешивающих свойств отображения НРС при различных значениях его параметров проведён вычислительный эксперимент. Реализована компьютерная программа, которая позволяет вычислить результат t тактов при управляющей последовательности $\alpha = \{\alpha_k\}$, $k = 1, \ldots, t$, и проверить совершенность преобразования $g(\alpha, t)$, используя вышеописанный алгоритм. Минимальное число тактов работы НРС, после которых каждая координатная функция существенно зависит от всех переменных, обозначим γ. В таблице для $n = 6$ и 10 приведены управляющие последовательности, при которых получены минимальные значения γ, близкие к точным значениям экспонента множества $\hat{\Gamma}$. Запись α^m означает конкатенацию m символов α, $\alpha \in \{0, 1\}$.

n	φ_0	φ_1	Оценка (1) $\exp\hat{\Gamma}$	Значение $\exp\hat{\Gamma}$	γ	$\alpha_1 \ldots \alpha_\gamma$
6	$x_0 \oplus x_3$	$x_0 \oplus x_2x_4$	17	11	18	$0^6 1^6 0^3 1^3$
10	$x_0 \oplus x_5$	$x_0 \oplus x_2 \oplus x_4 \oplus x_6x_8$	31	17	30	$0^{10} 1^{10} 0^5 1^5$
		$x_0 \oplus x_2x_4x_8$	31	19	30	$0^{10} 1^{10} 0^5 1^5$
		$x_0 \oplus x_2x_4x_6$	33	19	34	$0^{10} 1^{14} 0^5 1^5$

Выводы

Функциям обратной связи $\varphi_0(x_0, \ldots, x_{n-1})$ и $\varphi_1(x_0, \ldots, x_{n-1})$, рассмотренным в ходе вычислительного эксперимента, соответствуют непримитивные перемешивающие орграфы $\Gamma(g_0)$, $\Gamma(g_1)$. Однако множество орграфов $\hat{\Gamma} = \{\Gamma(g_0), \Gamma(g_1)\}$ примитивное, согласно критерию примитивности множества орграфов с общим гамильтоновым контуром. Вычислительный эксперимент показал, что в этом случае композиция преобразований из множества $\{g_0, g_1\}$ может быть совершенной. Наименьшее число тактов, начиная с которого композиция преобразований совершенная, при псевдослучайной управляющей последовательности превосходит точное значение экспонента множества $\hat{\Gamma}$. Показано, что при определённых начальных знаках управляющей последовательности возможно получить полное перемешивание входных данных за число тактов, которое превосходит точное значение экспонента менее чем в 2 раза.

ЛИТЕРАТУРА

1. *Shannon C. E.* Communication theory of secrecy systems // Bell System Technical J. 1949. V. 28. P. 656–715.
2. *Фомичев В. М., Мельников Д. А.* Криптографические методы защиты информации. В 2 ч. Ч. 1. Математические аспекты. М.: Юрайт, 2016. 209 с.
3. *Авезова Я. Э.* Свойства примитивных множеств ориентированных графов с общим множеством контуров // Прикладная дискретная математика. 2019. № 43, С. 101–114.