ОБОЗРЕНИЕ
ПРИКЛАДНОЙ И ПРОМЫШЛЕННОЙ
Том 25 МАТЕМАТИКИ Выпуск 4
2018

Д. Б. Фомин (Москва, ТК-26). **О подходах к построению низкоресурсных нелинейных преобразований.**

Одним из негласных правил создания низкоресурсного блочного шифра стало использование подстановок маленькой размерности. Это обусловлено тем, что такие подстановки хорошо исследованы, требуют небольшого количества ресурсов при аппаратной реализации, и известны эффективные механизмы маскирования, позволяющие защититься от атак по побочным каналам утечки. В то же время, криптографические свойства таких подстановок уступают криптографическим характеристикам подстановок большей размерности.

Одним из компромиссов является построение подстановок больших размерностей с использованием нелинейных преобразований меньших размерностей (см. например [1]). При этом, для таких подстановок имеется возможность программной реализации с большими таблицами замен, программной реализации преобразования с меньшим количеством битовых преобразований (т.н. bitslice-реализации), возможность использования подстановок для легковесной криптографии с маленькими таблицами замен и небольшим количеством используемых ресурсов, а также показана возможность эффективного аппаратного маскирования [2].

Напомним некоторые необходимые определения, необходимые для изложения работы. Пусть $\mathbb{F}_{2^n}(\oplus,\otimes)$ конечное поле из 2^n элементов. Говоря подстановка размерности k будем подразумевать, что это подстановка на множестве элементов конечного поля $\mathbb{F}_{2^k}$.

Определение 1. Преобразованием Уолша–Адамара $W_S(a,b)$ нелинейной функции S для фиксированных значений $a \in \mathbb{F}_{2^n}$, $b \in \mathbb{F}_{2^m}$ определяется следующим образом: $W_S(a,b) = \sum_{x\in\mathbb{F}_{2^n}} (-1)^{tr_1^n(a\otimes x)+tr_1^n(b\otimes S(x))}$, где tr_1^n — функция след из поля $\mathbb{F}_{2^n}$ в поле $\mathbb{F}_2$.

Определение 2. Нелинейностью N_S преобразования S называется величина, определяемая следующим образом: $N_S = 2^{n-1} - \frac{1}{2}\max_{a,b\neq 0}|W_S(a,b)|$.

Определение 3. Определим величину $\delta = \max_{a\in\mathbb{F}_{2^n}/0,b}\delta_S(a,b)$, где $\delta_S(a,b) = \#\{x \in \mathbb{F}_{2^n} \,|S(x\oplus a)\oplus S(x) = b\}$. Тогда S будем называть δ-равномерным.

Особый интерес построения нелинейных преобразований большей размерности с использованием нелинейных преобразований меньшей размерности связан с тем, что, как показывают последние исследования такие подстановки обладают «хорошими» криптографическими свойствами. Например, единственная известная 2-равномерная подстановка размерности 6 в эквивалентном виде может быть представлена как комбинация небольшого количества подстановок размерности 3. Данный подход был обобщен и построен класс 4-равномерных подстановок размерности $2k$ для любого нечетного k. В последнее время с использованием подстановок размерности 4 построены подстановки размерности 8, которые обладают практически оптимальными криптографическими характеристиками.

В работе [3] впервые были приведены 6-равномерные подстановки размерности 8, имеющие нелинейность равную $N_S = 108$ и представляющиеся в виде комбинации подстановок размерности 4. Позже в работе [4] были рассмотрены некоторые новые

классы. Подстановки из работ [3, 4] можно обобщить следующим образом:

$$s_1(x_i, y_i) = y_o = \begin{cases} & \phi_1(y_i) \neq 0; \\ F_1(x_i, y_i), & \phi_1(y_i) \neq 0; \\ \widehat{\pi}_1(x_i), & \phi_1(y_i) = 0. \end{cases}$$
$$s_2(x_i, y_i) = x_o = \begin{cases} F_2(y_i, y_o), & \phi_2(y_o) \neq 0; \\ \widehat{\pi}_2(y_i), & \phi_2(y_o) = 0. \end{cases} \quad (1)$$

где $F_1(x_i, y_i) = \pi_1\left(\psi_1(x_i) \otimes \phi_1(y_i)\right)$, $F_2(y_i, y_o) = \pi_2\left(\psi_2(y_i) \otimes \phi_2(y_o)\right)$, π_i, $\widehat{\pi}_i$, ϕ_i, ψ_i, $i \in \{1, 2\}$ — подстановки.

Можно доказать следующие утверждения.

Утверждение 1. *Пусть* $s(x, y) = \begin{cases} \pi\left(\psi(x) \otimes \phi(y)\right), & \phi(y) \neq 0; \\ \widehat{\pi}(x), & \phi(y) = 0, \end{cases}$ *где* π, $\widehat{\pi}$, ϕ, ψ *— подстановки размерности* m. *Тогда преобразование Уолша–Адамара этой функции вычисляется по следующей формуле*:

$$W_{s(x,y)}(\alpha \| \beta, \gamma) = \begin{cases} W_{\pi(\psi(x) \otimes \phi(y))}(\alpha \| \beta, \gamma) + W_{\widehat{\pi}(x)}(\alpha, \gamma), & \alpha \neq 0; \\ W_{\pi(\psi(x) \otimes \phi(y))}(\alpha \| \beta, \gamma) - 2^m, & \alpha = 0, \gamma \neq 0; \\ W_{\pi(\psi(x) \otimes \phi(y))}(\alpha \| \beta, \gamma), & \alpha = 0, \gamma = 0. \end{cases} \quad (2)$$

Как видно из формулы (2), для того, чтобы функция s имела наибольшую нелинейность, необходимо, чтобы значение модуля преобразования Уолша–Адамара для функций $\pi_1\left(\psi_1(x_i) \otimes \phi_1(y_i)\right)$, $\widehat{\pi}_1(x_i)$, $\widehat{\pi}_2(y_i)$, а также композиции: $\pi_2\left(\psi_2(x_i) \otimes \phi_2(y_i)\right)$ были как можно меньше. Еще одним очевидным требованием является то, что $\pi_2\left(\psi_2(x_i) \otimes \phi_2(y_i)\right)$ и $\pi_1\left(\psi_1(x_i) \otimes \phi_1(y_i)\right)$ не должны быть линейно связаны.

Утверждение 2. *Пусть фиксированы* $a_1, a_2, b_1, b_2 \in \mathbb{F}_{2^k}$, *тогда количество решений следующей системы уравнений* (*количество пар* $x, y \in \mathbb{F}_{2^k}$, *удовлетворяющих следующей системе уравнений*):

$$\begin{cases} s_1(x_i, y_i) \oplus s_1(x_i \oplus a_1, y_i \oplus a_2) = b_1 \\ s_2(x_i, y_i) \oplus s_2(x_i \oplus a_1, y_i \oplus a_2) = b_2 \end{cases}$$

больше либо равно:

1. $a_2 \neq 0$ *количества решений следующей системы уравнений*:

$$\begin{cases} \phi_1(y_i) \neq 0 \\ \phi_1(y_i \oplus a_2) \neq 0 \\ \phi_2(F_1(x_i, y_i)) \neq 0 \\ \phi_2(F_1(x_i \oplus a_1, y_i \oplus a_2)) \neq 0 \\ F_1(x_i, y_i) \oplus F_1(x_i \oplus a_1, y_i \oplus a_2) = b_1 \\ F_2(y_i, F_1(x_i, y_i)) \oplus F_2(y_i \oplus a_2, F_1(x_i \oplus a_1, y_i \oplus a_2)) = b_2 \end{cases} \quad (3)$$

2. $a_1 \neq 0$, $a_2 = 0$ *количества решений системы* (3) *плюс количества решений следующей системы уравнений*:

$$\begin{cases} \phi_1(y_i) = 0 \\ F_2(y_i, \widehat{\pi}_1(x_i)) \oplus F_2(y_i, \widehat{\pi}_1(x_i \oplus a_1)) = b_2 \end{cases} \quad (4)$$

Фактически, уравнения (3) задают ограничения на выбор возможных комбинаций функций $F_1(x_i, y_i)$ и $F_2(y_i, y_o)$. Уравнение (4) задает ограничение на выбор $\widehat{\pi}_1$ при

фиксированной функции $F_2(y_i, y_o)$. Аналогично системе (4) можно построить ограничение на выбор $\widehat{\pi}_2$ при фиксированной функции F_1.

С использованием вида подстановки (1), утверждения 1 и 2 можно построить 4-равномерные подстановки размерности 6, имеющие нелинейность 54.

Рассмотрим случай, когда $\pi_i,\ \phi_i,\ \psi_i,\ i \in \{1, 2\}$ — мономиальные подстановки поля F_{2^k}. В этом случае:

$$\begin{aligned} s_1(x_i, y_i) = y_o = \begin{cases} x_i^{\alpha} \otimes y_i^{\beta}, & y_i \neq 0; \\ \widehat{\pi}_1(x_i), & y_i = 0. \end{cases} \\ s_2(x_i, y_i) = x_o = \begin{cases} x_i^{\gamma} \otimes y_i^{\delta}, & y_o \neq 0; \\ \widehat{\pi}_2(y_i), & y_o = 0. \end{cases} \end{aligned} \tag{5}$$

Заметим, что уравнение (5) не всегда задает биективное преобразование. Рассмотрим случай $k = 4$. По малой теореме Ферма всего имеется 8 не равных между собой мономиальных подстановок поля F_{2^4}. Уравнение (3) позволяет ограничить количество $(\alpha, \beta, \gamma, \delta)$ в уравнении (5) с 8^4 до 768 так, что с использованием неотбракованных четверок $(\alpha, \beta, \gamma, \delta)$ при правильном выборе $\widehat{\pi}_i,\ i \in \overline{1, 2}$, получаются 6-равномерные подстановки, имеющие нелинейность 108. Заметим, что рассмотренные подстановки покрывают множество подстановок, рассмотренных в [3, 4].

СПИСОК ЛИТЕРАТУРЫ

1. *Canteaut A.*, *Duval S.*, *Leurent G.* Construction of Lightweight S-Boxes using Feistel and MISTY structures. IACR Cryptology ePrint Archive, 2015, http://eprint.iacr.org/2015/711.
2. *Boss E.*, *Grosso V.*, *Güneysu T.*, *Leander G.*, *Moradi A.*, *Schneider T.* Strong 8-bit Sboxes with efficient masking in hardware extended version. — J. Cryptographic Engineering, 2017, v. 7, is. 2, p. 149–165.
3. *Reynier Antonio de la Cruz Jiménez* Generation of 8-bit S-Boxes having almost optimal cryptographic properties using smaller 4-bit S-Boxes and finite field multiplication, 2017, www.cs.haifa.ac.il/ orrd/LC17/paper60.pdf.
4. *Fomin D. B.* New classes of 8-bit permutations based on a butterfly structure, 2018, CTCrypt'18.