О подходах к построению низкоресурсных нелинейных преобразований

Д.Б. Фомин

27 сентября 2018

- $\mathbb{F}_{2^n}$ – конечное поле размерности 2^n.
- Подстановка (S-Box) S – нелинейное преобразование $S : \mathbb{F}_2^n \mapsto \mathbb{F}_2^n$.
- Крпитографические характеристики подстановок – мера, показывающая способность противостоять известным методам криптоанализа

Подстановки используются прои синтезе следующих криптографических функций:

- блочные шифры
- хэш-функции
- поточные шифры

Преобразование Уолша-Адамара

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:

$$W_S(a, b) = \sum_{x \in \mathbb{F}_{\mathbf{2}^n}} (-1)^{tr_{\mathbf{1}}^n(a \otimes x) + tr_{\mathbf{1}}^n(b \otimes S(x))},$$

где tr_1^n — функция след из поля $\mathbb{F}_{2^n}$ в поле $\mathbb{F}_2$.

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

δ-равномерность

Определим величину $\delta = \max\limits_{a \in \mathbb{F}_{2^n}/0, b} \delta_S(a, b)$, где

$$\delta_S(a, b) = \#\left\{x \in \mathbb{F}_{2^n} \,|S(x \oplus a) \oplus S(x) = b\right\}.$$

Тогда подстановку S будем называть δ-равномерным.

Одним из негласных правил создания низкоресурсного блочного шифра стало использование подстановок маленькой размерности

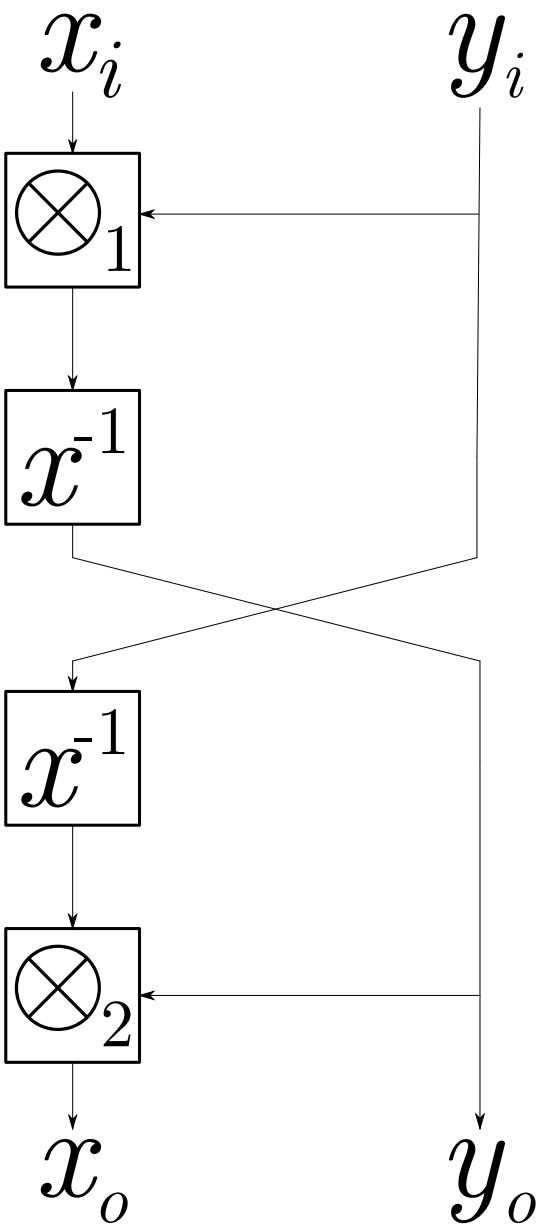
+ Хорошо исследованы (описаны криптографические характеристики каждой подстановки)
+ Требуют небольшого количества ресурсов при аппаратной реализации
+ Известны эффективные механизмы маскирования, позволяющие защититься от атак по побочным каналам утечки
– Криптографические свойства таких подстановок сильно уступают криптографическим характеристикам подстановок большей размерности

Одним из компромиссов является построение подстановок большей размерности с использованием нелинейных преобразований меньшей размерности:

- Сеть Фейстеля (CRYPTON v0.5, Zorro)
- Mysty-сети (Mysty, Kasumi, Fantomas)
- SPN-сети (Iceberg, Khazard, Crypton v1.0)
- Другие конструкции (Whirpool, BelT).

Есть достаточно много плюсов:

- возможность программной реализации с большими таблицами замен,
- возможность 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,
- показана возможность эффективного аппаратного маскирования.



1. Была представлена в 2017 году[1]
2. 8-ми битовая подстановка
3. $N_S = 108$, $\delta_S = 6$

[1] 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.

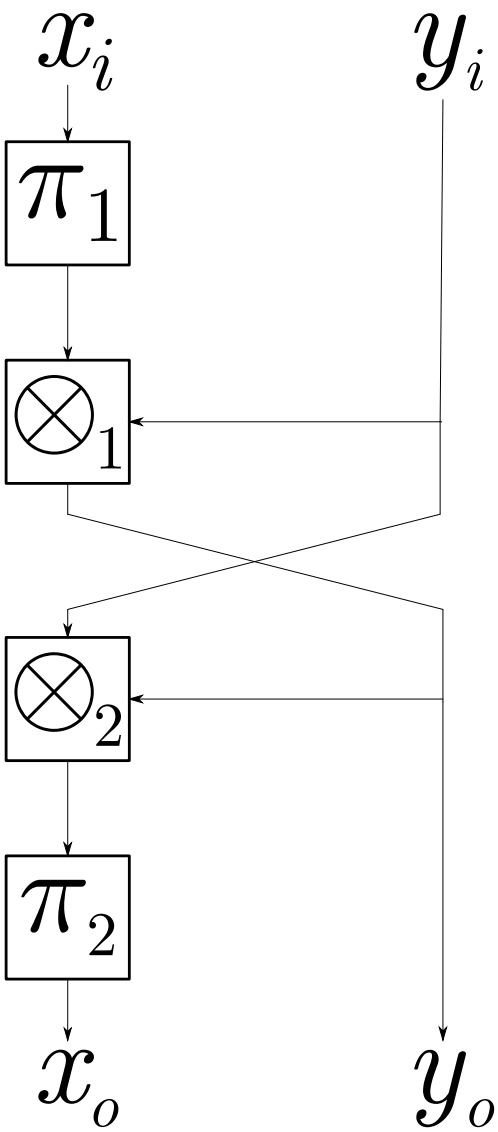


Рис.: Конструкция типа «A»

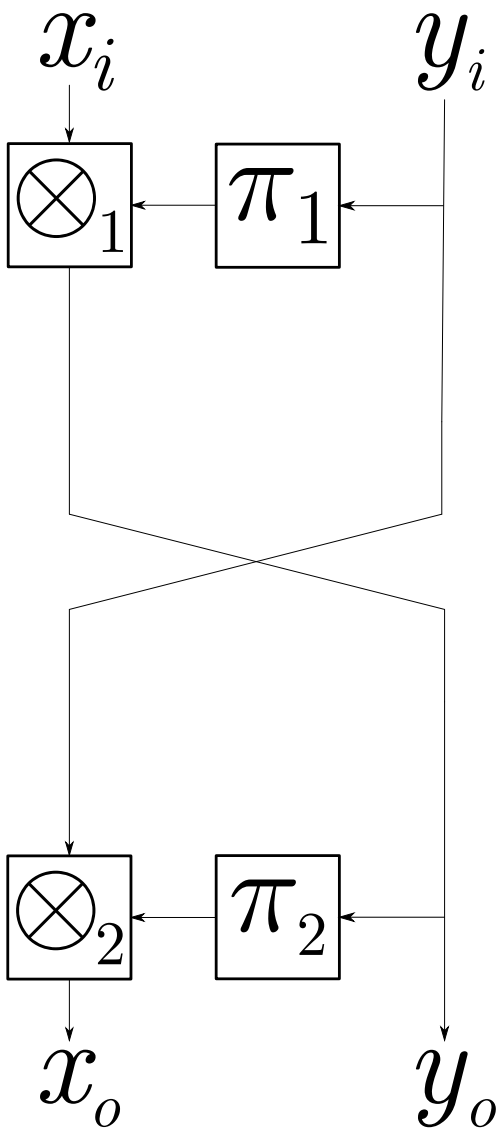


Рис.: Конструкция типа «B»

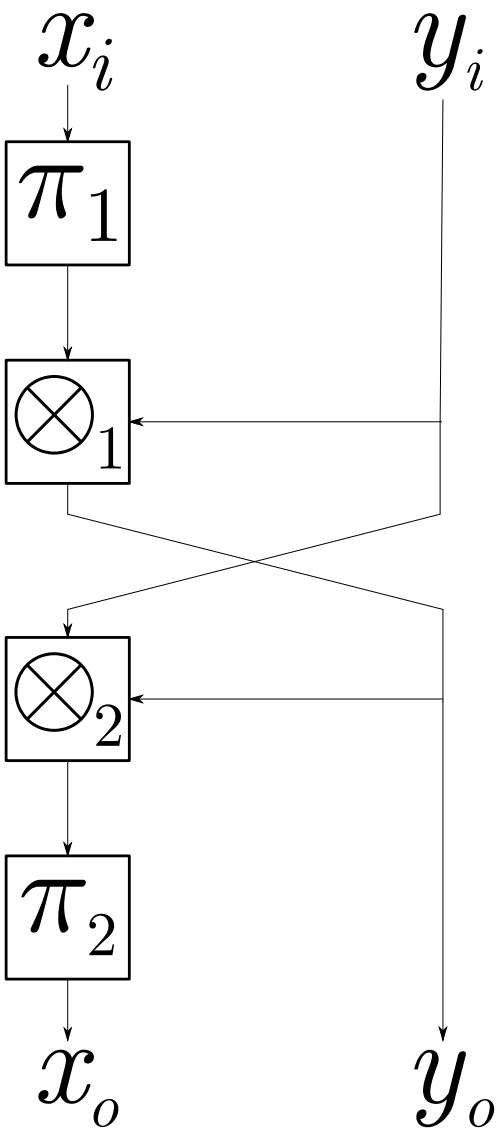


Рис.: Конструкция типа «A»

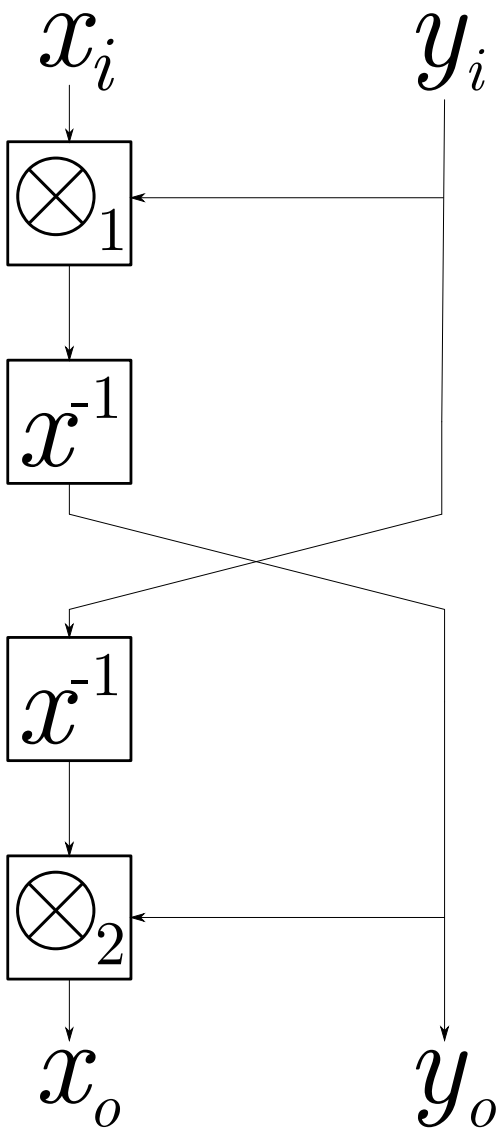


Рис.: Конструкция Антонио де ла Круза

Рассмотренные подстановки можно обобщить следующим образом:

$$s_1(x_i, y_i) = y_o = \begin{cases} F_1(x_i, y_i), & \phi_1(y_i) \neq 0; \\ \widehat{\pi}_1(x_i), & \phi_1(y_i) = 0. \end{cases}$$

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

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.

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:

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

Следствия утверждения 1

- 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: $\pi_2\left(\psi_2(y_i) \otimes \phi_2(y_o)\right)$ были как можно меньше
- $\pi_2\left(\psi_2(y_i) \otimes \phi_2(y_o)\right)$ и $\pi_1\left(\psi_1(x_i) \otimes \phi_1(y_i)\right)$ не должны быть линейно связаны

Утверждение 1

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:

$$\begin{cases} F_1(x_i, y_i) \oplus F_1(x_i \oplus a_1, y_i \oplus a_2) = b_1 \\ F_2(y_i, F_1(x_i, y_i)) \oplus F_2(y_i \oplus a_2, F_1(x_i \oplus a_1, y_i \oplus a_2)) = b_2 \end{cases} \quad (1)$$

   при $\phi_1(y_i) \neq 0$, $\phi_1(y_i \oplus a_2) \neq 0$, $\phi_2(F_1(x_i, y_i)) \neq 0$, $\phi_2(F_1(x_i \oplus a_1, y_i \oplus a_2)) \neq 0$.

2. $a_1 \neq 0$, $a_2 = 0$ количества решений системы (1) плюс количества решений следующей системы уравнений:

$$\begin{cases} \phi_1(y_i) = 0 \\ F_2(y_i, \widehat{\pi}_1(x_i)) \oplus F_2(y_i, \widehat{\pi}_1(x_i \oplus a_1)) = b_2 \end{cases} \quad (2)$$

- 4-равномерные подстановки размерности 6, имеющие нелинейность 54
- В случае, когда π_i, ϕ_i, ψ_i, $i \in \{1, 2\}$ — мономиальные подстановки поля $\mathbb{F}_{2^4}$:

$$s_1(x_i, y_i) = y_o = \begin{cases} x_i^{\alpha} \otimes y_i^{\beta}, & y_i \neq 0; \\ \widehat{\pi}_1(x_i), & y_i = 0. \end{cases}$$

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

удалось построить 768 классов, содержащих 6-равномерные подстановки, имеющие нелинейность 108

Спасибо за внимание

Вопросы?