О способе построения дифференциально 2δ-равномерных подстановок на $\mathbb{F}_{2^{2m}}$

Фомин Денис Бониславович
dfomin@hse.ru

Национальный исследовательский университет «Высшая школа экономики»

8 сентября 2021 г.

- Подстановка — биективная (n, n)-функция, биективное преобразование элементов $\mathbb{F}_2^n$
- $\mathbb{F}_2^n \sim \mathbb{F}_{2^n}$
- (n, m)-функция F является дифференциально δ_F равномерной, если

$$\delta_F = \max_{\substack{\alpha \in \mathbb{F}_2^n \setminus 0 \\ \beta \in \mathbb{F}_2^m}} \delta_F^{\alpha,\beta},$$

где $\delta_F^{\alpha,\beta} = |\{x \in \mathbb{F}_2^n \colon F(x \oplus \alpha) \oplus F(x) = \beta\}|$.

- Подстановки являются важной частью большого количества криптографических алгоритмов
- В настоящее время наиболее часто используются подстановки пространств $\mathbb{F}_2^n$, $n \in \{4, 8, 16\}$
- Стойкость криптографического алгоритма (в том числе) зависит от так называемых криптографических характеристик подстановок (нелинейность, дифференциальная δ-равномерность, алгебраическая степень и др.)
- Возможность эффективной программной/аппаратной реализации, применения алгоритмов маскирования, может зависеть от эксплуатационных характеристик подстановок

- Подстановки афинно-эквивалентные подстановке обращения и другим мономиальным подстановкам
- Подстановочные многочлены
- Модификация подстановки обращения

Подстановки построенные таким образом как правило имеют наилучшие из известных значений таких криптографических характеристик, как нелинейность, показатель дифференциальной δ-равномерности, алгебраическую степень.

В то же время имеют достаточно простую алгебраическую структуру (linear redundancy, показатель графовой алгебраической иммунности).

Для эффективной программной (bitslice) и аппаратной реализации требуется небольшое количество используемых битовых операций. Существуют разные подходы к построению таких подстановок [1]:

- Сеть Фейстеля
- Конструкция типа Misty
- Подстановки некоторых алгоритмов (Whirpool, CRYPTON, Robin, Fantomas)

Имеют показатель дифференциальной δ-равномерности равный 8, 10, 16.

[1] Canteaut, Anne, Duval, Sébastien and Leurent, Gaëtan. "Construction of Lightweight S-Boxes Using Feistel and MISTY Structures". 2015

Возможность порогового представления подстановки для маскирования, или использование маскирования случайными масками налагает ограничения на вид подстановок[2][3].

Имеют показатель дифференциальной δ-равномерности равный 8, 10, 16.

[2]Erik Boss and Vincent Grosso and etc. "Strong 8-bit Sboxes with Efficient Masking in Hardware". 2016

[3]Meyer, L., Varici, K. "More Constructions for strong 8-bit S-boxes with efficient masking in hardware". 2017

Определение

Пусть F — (n,m)-функция, $1 \le t \le \min(n,m)$, $x_1, y_1 \in \mathbb{F}_2^t$, $x_2 \in \mathbb{F}_2^{n-t}$, $y_2 \in \mathbb{F}_2^{m-t}$, $x = x_1 \| x_2 \in \mathbb{F}_2^n$, $y = y_1 \| y_2 \in \mathbb{F}_2^m$. Тогда если существуют функции $T\colon \mathbb{F}_2^t \times \mathbb{F}_2^{n-t} \to \mathbb{F}_2^t$, $U\colon \mathbb{F}_2^{n-t} \times \mathbb{F}_2^t \to \mathbb{F}_2^{m-t}$, что при фиксации x_2 произвольным значением $T(x_1, x_2)$ есть биекция по переменной x_1 и функция F представима в виде

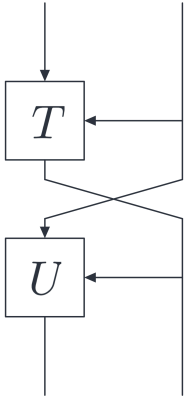
$$F(x) = F(x_1 \| x_2) = T(x_1, x_2) \| U\left(x_2, T(x_1, x_2)\right), \tag{1}$$

то такое представление функции F в виде (1) *будем называть TU-представлением.*

Известно, что в случае $m = n$ функция F является подстановкой, если функция $U(x_2, x_1)$ является подстановкой по x_2 при фиксации x_1.

Известно достаточно много примеров подстановок, обладающих высокими криптографическими характеристиками и имеющих TU-представление:

- подстановка, CCZ-эквивалентная подстановке Диллона;
- подстановка, линейно эквивалентная подстановке алгоритмов ГОСТ Р 34.11-2012 и «Кузнечик» (ГОСТ Р 34.12-2018);
- подстановки из работ [4][5]



[4]Reynier Antonio de la Cruz Jiménez "On some methods for constructing almost optimal S-Boxes and their resilience against side-channel attacks".2018

[5]D. B. Fomin, "New classes of 8-bit permutations based on a butterfly structure". 2019

Для $a \in \mathbb{F}_2^{n-t}$ обозначим:

- $\delta_{T,a}$ — показатель дифференциальной δ-равномерности подстановки, которую задаёт функция $T(x_1, x_2)$ при фиксации $x_2 = a$;
- $\Delta_{T,a}^{\alpha_1,\alpha_2,\beta_1}$ — количество решений уравнения

$$T(x_1, a) + T(x_1 + \alpha_1, a + \alpha_2) = \beta_1,\ \alpha_1, \beta_1 \in \mathbb{F}_2^{n-t}, \alpha_2 \in \mathbb{F}_2^t \setminus \{\mathbf{0}\}.$$

Теорема

Пусть у функции F имеется TU-представление (1). *Тогда показатель дифференциальной δ-равномерности функции F меньше либо равен значения*

$$2^t \cdot \max_{a \in \mathbb{F}_2^t} \left\{ \delta_{T,a}, \max_{\substack{\alpha_1,\beta_1 \in \mathbb{F}_2^{n-t}, \\ \alpha_2 \in \mathbb{F}_2^t \setminus \{\mathbf{0}\}}} \Delta_{T,a}^{\alpha_1,\alpha_2,\beta_1} \right\}.$$

Следствие

Пусть в условиях теоремы 1 $t = 1$ и $\delta_{T,a} \leq \delta$ для всех $a \in \mathbb{F}_2$. Тогда функция F, имеющая TU-представление (1)*, не более чем дифференциально 2δ-равномерна тогда и только тогда, когда* $\max\limits_{\alpha_1,\beta_1 \in \mathbb{F}_2^{n-1}} \Delta_{T,0}^{\alpha_1,1,\beta_1} \leq \delta$.

Задача построения дифференциально 2δ-равномерных подстановок сводится к поиску двух подстановок $\pi_0, \pi_1 \in \mathbb{S}\left(\mathbb{F}_2^{n-1}\right)$, таких, что количество решений уравнений

$$\pi_0(x) + \pi_1(x + \alpha_1) = \beta_1 \tag{2}$$

при всевозможных значениях $\alpha_1, \beta_1 \in \mathbb{F}_2^{n-1}$ не больше 2.

Теорема

Пусть $x_1 \in \mathbb{F}_{2^{n-1}}$, *n чётное*, $n > 6$, $x_2 \in \mathbb{F}_2$, f — *произвольная булева функция от* $n-1$ *переменной*, $c \in \mathbb{F}_{2^{n-1}} \setminus \{\mathbf{0}, \mathbf{1}\}$,

$$T\colon \mathbb{F}_{2^{n-1}} \times \mathbb{F}_2 \to \mathbb{F}_{2^{n-1}}, \quad T(x_1, x_2) = x_1^{-1} \cdot c^{x_2},$$
$$U\colon \mathbb{F}_2 \times \mathbb{F}_{2^{n-1}} \to \mathbb{F}_2, \quad U(x_2, x_1) = f(x_1) + x_2.$$

Тогда формула (1) *задаёт подстановку F, при этом*

1. *если* $\mathrm{tr}(c) = \mathrm{tr}\left(c^{-1}\right) = 1$, *то* $\delta_F = 4$;
2. *иначе* $\delta_F = 6$.

Результат п. 1 теоремы доказан в [6], однако предложенное следствие позволяет проводить доказательство с более общих позиций.

[6] Claude Carlet, Deng Tang, Xiaohu Tang, Qunying Liao, "New Construction of Differentially 4-Uniform Bijections". 2014

Теорема

Пусть $x_1 \in \mathbb{F}_{2^{n-1}}$, n *чётное,* $n > 6$, $x_2 \in \mathbb{F}_2$, f *— произвольная булева функция от* $n-1$ *переменной,* $c \in \mathbb{F}_{2^{n-1}} \setminus \{\mathbf{0}, \mathbf{1}\}$,

$$T\colon \mathbb{F}_2^{n-1} \times \mathbb{F}_2 \to \mathbb{F}_2^{n-1}, \quad T(x_1, x_2) = x_1^3 \cdot c^{x_2},$$
$$U\colon \mathbb{F}_2 \times \mathbb{F}_{2^{n-1}} \to \mathbb{F}_2, \quad U(x_2, x_1) = f(x_1) + x_2.$$

Тогда формула (1) *задаёт подстановку* F, *при этом* $\delta_F = 6$.

Напомним, что две (n, m)-функции g и f называются расширенно аффинно-эквивалентными, если существуют аффинные подстановки a и b пространств $\mathbb{F}_2^n$ и $\mathbb{F}_2^m$ соответственно и аффинная (n, m)-функция c, что $f(x) = (b \circ g \circ a)(x) + c(x)$.

Утверждение

Пусть $x_1 \in \mathbb{F}_{2^{n-1}}$, n чётное, $n > 6$, $x_2 \in \mathbb{F}_2$, f — произвольная булева функция от $n-1$ переменной, $a, b \in \mathbb{F}_{2^{n-1}}$,

$$T\colon \mathbb{F}_2^{n-1} \times \mathbb{F}_2 \to \mathbb{F}_2^{n-1}, \quad T(x_1, 0) = x_1^3,\ T(x_1, 1) = x_1^3 + a \cdot x_1^2 + b \cdot x_1,$$
$$U\colon \mathbb{F}_2 \times \mathbb{F}_2^{n-1} \to \mathbb{F}_2, \quad U(x_2, x_1) = f(x_1) + x_2.$$

Тогда существуют $\alpha_1, \beta_1 \in \mathbb{F}_{2^{n-1}}$, такие, что количество решений уравнения $T(x_1 + \alpha_1, 0) + T(x_1, 1) = \beta_1$ равно 2^{n-1}, либо $T(x_1, 1)$ не является подстановкой.

Утверждение

Пусть $x_1 \in \mathbb{F}_{2^{n-1}}$, *n чётное,* $n > 6$, $x_2 \in \mathbb{F}_2$, f *— произвольная булева функция от* $n-1$ *переменной,*

$$T\colon \mathbb{F}_{2^{n-1}} \times \mathbb{F}_2 \to \mathbb{F}_{2^{n-1}}, \quad T(x_1, 0) = x_1^3,\ T(x_1, 1) = x_1^{-1},$$
$$U\colon \mathbb{F}_2^1 \times \mathbb{F}_2^{n-1} \to \mathbb{F}_2, \quad U(x_2, x_1) = f(x_1) + x_2.$$

Тогда формула (1) *задаёт подстановку* F, *при этом* $\delta_F = 8$.

Утверждение

Пусть $t = 2$, $x_1 \in \mathbb{F}_2^{n-t}$, $x_2 \in \mathbb{F}_2^t$. *Тогда существуют такие* c_{x_2}, $x_2 \in \mathbb{F}_{2^2}$, $c_{x_2'} \neq c_{x_2''}$ *при* $x_2' \neq x_2''$, *что подстановка* F, *задаваемая формулой* (1), *дифференциально 8-равномерна, где*

$T\colon \mathbb{F}_2^{n-t} \times \mathbb{F}_2^t \to \mathbb{F}_2^{n-1}$, $T(x_1, x_2) = x_1^{-1} \cdot c_{x_2}$,

$U\colon \mathbb{F}_2^t \times \mathbb{F}_2^{n-t} \to \mathbb{F}_2^t$, *при фиксации произвольного* x_1 *функция* $U(x_2, x_1)$ *является подстановкой по переменной* x_2.

Спасибо за внимание!

Вопросы?