Разработка эвристических методов построения подстановок с низкой дифф. равномерностью

Летняя школа-конференция «Криптография и информационная безопасность»

20 июля 2025 г.

Введение

- Актуальность симметричных шифров
- Важность нахождения S- и P-блоков с нужными качествами для обеспечения криптографической стойкости.

Основные определения

Определение

Для $n \in \mathbb{N}$, отображение вида $\mathbb{F}_2^n \to \mathbb{F}_2$, где $\mathbb{F}_2$ — поле из двух элементов, называется *булевой функцией*. Отображения вида $\mathbb{F}_2^n \to \mathbb{F}_2^m$, где $m \in \mathbb{N}$, называются *векторными булевыми функциями* (или (n, m)-*функциями*).

$(n, m)-$функцию $F(x_1, ..., x_n)$ можно задать m булевыми функциями от n переменных:

$$F(x_1, \dots, x_n) = (f_1(x_1 \dots x_n), \dots, f_m(x_1, \dots, x_n)).$$

Функции f_i называются *координатными функциями*, а произвольная ненулевая линейная комбинация координатных функций называется *компонентной функцией*.

Криптографические характеристики функций

Определение

Алгебраической степенью булевой функции называется степень ее полинома Жегалкина.

Определение

Нелинейностью булевой функции f от n переменных называется величина N_f, равная расстоянию Хэмминга от f до множества $\mathcal{A}_n$ всех аффинных функций от n переменных.

Определение

Алгебраической иммунностью $AI(f)$ функции f называется такое наименьшее число d, что существует аннулятор g степени d, не тождественно равный нулю, либо для функции f, либо для $f \oplus 1$

Криптографические характеристики функций

Криптографические характеристики булевых функций можно перенести на векторный случай

Определение

Минимальной алгебраической степенью векторной булевой функции называется наименьшая из алгебраических степеней ее компонентных функций.

Определение

Нелинейностью векторной булевой функции называется наименьшая из нелинейностей ее компонентных функций.

Определение

Алгебраической иммунностью векторной булевой функции называется наименьшая из алгебраических иммунностей ее компонентных функций.

Криптографические характеристики функций

Определение

Векторная булева (n, m)-функция f называется *дифференциально δ-равномерной*, если для любых $a \neq 0, b \in \mathbb{F}_2^n$ уравнение

$$f(x) + f(x + a) = b$$

имеет не более δ решений в $\mathbb{F}_2^n$. Наименьшее такое число δ называется *показателем дифференциальной равномерности*.

Определение

Отображение

$$f : \mathbb{F}_2^n \to \mathbb{F}_2^n$$

называется *APN-отображением*, если оно дифференциально 2-равномерно.

Комбинаторное описание дифференциальной равномерности

APN-отображения

$$F(x_1, ..., x_n) = (f_1(x), ..., f_n(x)) \quad f(x) = \sum_{i=0}^{n} a_i x^i$$

?

$$S(\mathbb{F}_{2^n})$$

Комбинаторное описание дифференциальной равномерности

Рассмотрим симметрическую группу $S(\Omega)$ на множестве Ω из n элементов.

- Расстоянием между подстановками $f, g \in S(\Omega)$ называется величина

$$d(f,g) = |\{x \in \Omega \mid f(x) \neq g(x)\}|$$

- Расстоянием между подгруппами $G, G' \leq S(\Omega)$ назовем

$$d(G,G') = \min_{\substack{g \in G \setminus \{e\} \\ g' \in G' \setminus \{e\}}} d(g,g')$$

Комбинаторное описание дифференциальной равномерности

- Далее будем рассматривать $\Omega = \mathbb{F}_{2^n}$
- Любой элемент поля $\alpha \in \mathbb{F}_{2^n}$ определяет биективное отображение

$$\begin{aligned} \tau_\alpha \colon \mathbb{F}_{2^n} &\to \mathbb{F}_{2^n} \\ x &\mapsto x + \alpha \end{aligned}$$

- Множество таких отображений $T = \{\tau_\alpha \mid \alpha \in \mathbb{F}_{2^n}\}$ образует подгруппу симметрической группы $S(\mathbb{F}_{2^n})$

Комбинаторное описание дифференциальной равномерности

В работе использовалась следующая комбинаторная характеризация дифференциальной равномерности:

Утверждение

Пусть $f \in S(\mathbb{F}_{2^n})$, T – группа сдвигов, определенная выше, а

$$G = f^{-1} \cdot T \cdot f = \{f^{-1} \cdot t \cdot f | t \in T\}.$$

Тогда подстановка f является дифференциально δ-равномерной $\iff d(G, T) = 2^n - \delta$

Комбинаторное описание дифференциальной равномерности

тут будет пример

Комбинаторное описание дифференциальной равномерности

Тут аккуратно сформулировать цели и задачи проекта

Алгоритм вычисления дифференциальной равномерности после умножения на транспозицию

- Рассмотрим $\pi \in S(\mathbb{F}_{2^n})$ и $G = \pi^{-1} \cdot T \cdot \pi$.
- Пусть $N = |\mathbb{F}_{2^n}|$, $G = \{g_1, \ldots, g_{N-1}\}$, $T = \{t_1, \ldots, t_{N-1}\}$.
- Каждый элемент t_i раскладывается в произведение независимых транспозиций $t_i = \tau_1^i \ldots \tau_{\frac{N}{2}}^i$.
- Зафиксируем некоторый элемент $g = \sigma_1 \ldots \sigma_{\frac{N}{2}} \in G$.
- Определим множество $I(t_i, g) \overset{\text{def}}{:=} t_i \cap g$.

Утверждение

Сложность построения множества $I(t_i, g)$ равна $O(N)$ и $d(t_i, g) = N - 2|I(t_i, g)|$

Алгоритм вычисления дифференциальной равномерности после умножения на транспозицию

- Определим

$$I(g) \overset{\text{def}}{:=} \{I(t_i, g) \mid t_i \in T\},$$

$$D(g) \overset{\text{def}}{:=} (I(g), \max_{i \in I(g)} \{2 \cdot |i|\})$$

Утверждение

Сложность построения $D(g)$ равна $O(N^2)$.

Алгоритм вычисления дифференциальной равномерности после умножения на транспозицию

- Определим множество $\Delta(G) \stackrel{\text{def}}{:=} \{D(g) \mid g \in G\}$.

Утверждение

Дифференциальная равномерность подстановки π равна

$$\delta = \max_{(d_1, d_2) \in \Delta(G)} \{d_2\}.$$

Сложность вычисления δ равна $O(N^3)$.

Сложность классического алгоритма $O(N^2)$...

Алгоритм вычисления дифференциальной равномерности после умножения на транспозицию

Пусть $I(t_i, g)$ уже построено и $\sigma = (\alpha\beta)$ – некоторая транспозиция. Тогда вычислить $I(t_i, \sigma^{-1}g\sigma)$ можно следующим образом:

- Если $\sigma = \sigma_i$, то $I(t_i, g) = I(t_i, \sigma^{-1}g\sigma)$
- Пусть $\sigma \neq \sigma_i$. Тогда $\exists \sigma_s = (\alpha, \alpha'), \sigma_r = (\beta, \beta')$ в разложении g. Тогда

$$\sigma^{-1}g\sigma = \sigma_1 ... \sigma'_s ... \sigma'_r ... \sigma_{\frac{N}{2}}, \text{ где } \sigma'_s = (\beta, \alpha'), \sigma'_r = (\alpha, \beta').$$

Таким образом $I(t_i, \sigma^{-1}g\sigma)$ получается из $I(t_i, g)$ удалением σ_s, σ_r (если они там есть) и добавлением σ'_s, σ'_r (при условии, что они есть в разложении t_i)

Утверждение

Сложность вычисления $I(t_i, \sigma^{-1}g\sigma)$ по известному $I(t_i, g)$ равна $O(1)$.

Алгоритм вычисления дифференциальной равномерности после умножения на транспозицию

Для вычисления множества $D(\sigma^{-1} g \sigma)$ по $D(g) = (I(g), d)$ нужно:

- Если $\sigma = \sigma_i$, то $D(g)$ не изменится
- Найти сдвиги $t(\sigma_s), t(\sigma_r), t(\sigma'_s), t(\sigma'_r)$ и пересчитать $I(t(\sigma_s), g)$, $I(t(\sigma_r), g$ $I(t(\sigma'_s), g)$, $I(t(\sigma'_r), g)$
- Обновить максимальное значение d.

Утверждение

Сложность вычисления $D(\sigma^{-1} g \sigma)$ по известному $D(g)$ равна $O(1)$.

Утверждение

Сложность вычисления $\Delta(\sigma^{-1} G \sigma)$ по известному $\Delta(G)$ равна $O(N)$.

Подходы к построению подстановок с низкой дифф. равномерностью

Наиболее удачные подходы:

- Полный перебор транспозиций.
- Перебор образующих транспозиций.
- Перебор транспозиций, образованных элементами пересечения.

“Комбинированный” подход

После многочисленных экспериментов оказалось, что лучше всего справляется с задачей уменьшения дифференциальной равномерности “комбинированный” подход, который состоит из поочерёдного применения подходов с перебором образующих транспозиций и с перебором транспозиций, образованных элементами пересечения. Такой “комбинированный” подход позволяет стабильно снижать дифференциальную равномерность S-блока размерности 8 до значения 6.

Используя построенные алгоритмы, проводились вычислительные эксперименты. Была построена подстановка на $\mathbb{F}_{2^8}$:

π=(1,17,29,209,85,91,54,34,95,157,255,147,128,25,23,75,113,72,87,156,204,102,130,227,121,44,19,151,

137,123,243,237,165,61,27,183,142,88,70,191,163,170,99,20,103,146,166,139,111,182,31,59,154,116,150,

160,196,7,205,48,21,241,153,112,178,189,93,198,253,201,3,225,5,172,155,242,175,176,184,108,122,28,190,

77,194,42,132,129,148,52,79,131,152,246,05,186,109,219,248,134,9,35,217,211,64,149,249,222,164,226,30,

41,74,229,117,254,221,199,145,15,81,218,247,212,51,47,119,144,200,159,60,181,173,65,4,8,236,104,208,43,

71,233,136,50,115,207,140,63,107,6,86,214,203,216,223,101,228,49,67,239,114,138,83,53,13,124,180,96,234,

22,231,210,16,26,125,82,100,206,18,94,24,169,106,69,202,126,11,141,12,250,133,193,33,251,92,98,174,185,

252,90,158,197,188,118,127,80,57,215,135,45,56,162,10,195,36,62,177,245,213,58,110,192,2,40,167,168,143,

38,66,187,39,240,68,220,32,120,76,55,97,161,235,46,37,14,78,89,73,238,171,232,230,179,84,224,244,0).

Результаты

Таблица: Таблица 1

	π_{AES}	$\pi_{Kuznechik}$	$\pi_{Jimenez}$ [1]	π
Дифференциальная равномерность	4	8	6	6
Нелинейность	112	100	104	100
Минимальная алгебраическая степень	7	7	7	7
Алгебраическая иммунность	4	4	4	4

[1] R. A. de la Cruz Jimenez, "Constructing 8-bit permutations, 8-bit involutions and 8-bit orthomorphisms with almost optimal cryptographic parameters", Матем. вопр. криптогр., 12:3 (2021), 89–124

Направления дальнейшего исследования

- Придумать и опробовать новые эвристики.
- Переписать код на более “быстрый” язык.
- Использовать более мощный компьютер для перебора.

Спасибо за внимание!