# ВВЕДЕНИЕЕЕЕЕ

ВВЕДЕНИЕ

# Комбинаторное описание дифференциальной равномерности

APN-отображения

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

?

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

# Комбинаторное описание дифференциальной равномерности

Рассмотрим симметрическую группу $S(\Omega)$ на множестве $\Omega$ 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

### Утверждение

Пусть разложение в произведение независимых циклов $f, g \in S(\Omega)$ имеет вид:

$$f = (x_1, y_1)...(x_s, y_s)\tau_1...\tau_k,$$

$$g = (x_1, y_1)...(x_s, y_s)\sigma_1...\sigma_l,$$

где $\tau_i, \sigma_j$ различные транспозиции.
Тогда

$$d(f, g) = n - 2s - |fix(f) \cap fix(g)|,$$

где

$$fix(\pi) = \{x \in \Omega \mid \pi(x) = x\}.$$

# 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 $\delta$-равномерной $\iff d(G, T) = 2^n - \delta$

# Комбинаторное описание дифференциальной равномерности

**Утверждение**

Пусть $G \cong T$ и $d(G, T) = \alpha$. Тогда если $\pi$ - транспозиция, то

$$\alpha + 4 \geq d(\pi^{-1} \cdot G \cdot \pi, T) \geq \alpha - 4$$

Т.е. дифференциальная равномерность не может изменится более чем на 4 при умножении на транспозицию. [1]

---

[1] Yu, Y., Wang, M., Li, Y.: Constructing Differentially 4 Uniform Permutations from Known Ones. Chin. J. Electron. 22(3), 495–499 (2013)

# 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 $\Delta(G) \overset{\text{def}}{:=} \{D(g) \mid g \in G\}$.

**Утверждение**

Дифференциальная равномерность подстановки $\pi$ равна

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

Сложность вычисления $\delta$ 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 $\sigma_s, \sigma_r$ (если они там есть) и добавлением $\sigma'_s, \sigma'_r$ (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.

ВЫЧИСЛИТЕЛЬНЫЕ ЭКСПЕРИМЕНТЫ

# Направления дальнейшего исследования

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

Спасибо за внимание!