Об аппаратной реализации одного класса байтовых подстановок

Д. Б. Фомин, Д. И. Трифонов

12 сентября 2019

- Подстановки являются неотъемлемой частью большого класса криптографических функций
- К подстановкам предъявляются требования, позволяющие гарантировать невозможность применимости известных методов криптографического анализа
- Помимо криптографических требований, также предъявляются требования и к реализации подстановок

Существуют следующие подходы к построению подстановок:

- Переборный (случайный поиск, полное опробование)
- Эвристический
- Алгебраический (степенные подстановки, экспоненциальные подстановки, подстановки, задаваемые подстановочными многочленами)
- Модификация существующих подстановок
- Алгоритмический (задаваемые блок-схемой)

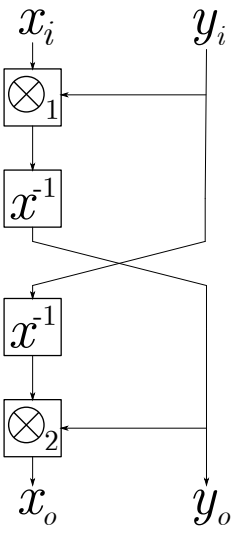
Построение подстановок больших размерностей с использованием преобразований меньших размерностей имеет следующие плюсы:

- программной реализации с большими таблицами замен;
- программной реализации с меньшим количеством битовых преобразований (bitslice-реализации, защита от атак по времени выполнения);
- использования подстановок для низкоресурсной реализации на ПЛИС и СБИС;
- эффективного аппаратного маскирования.

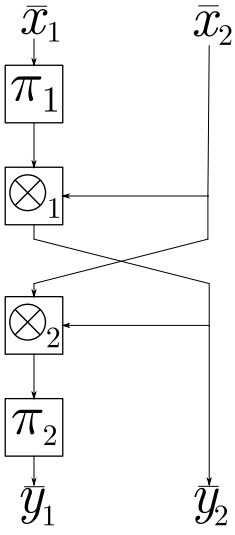
НО!

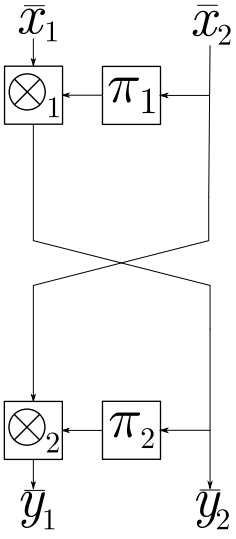
Как правило, такие подстановки обладают далекими от оптимальных криптографическими характеристиками.

Новые классы подстановок

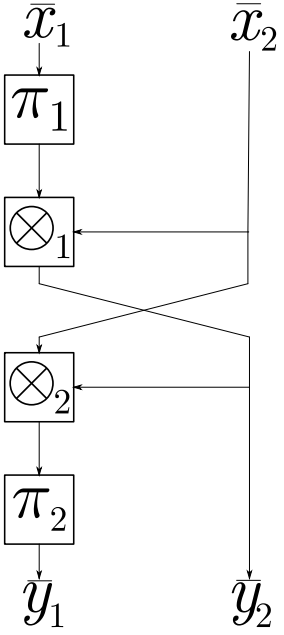


De la Cruz Jimenez R. A. Generation of 8-bit S-Boxes Having Almost Optimal Cryptographic Properties Using Smaller 4-bit S-Boxes and Finite Field Multiplication.





Denis Fomin. New classes of 8-bit permutations based on a butterfly structure



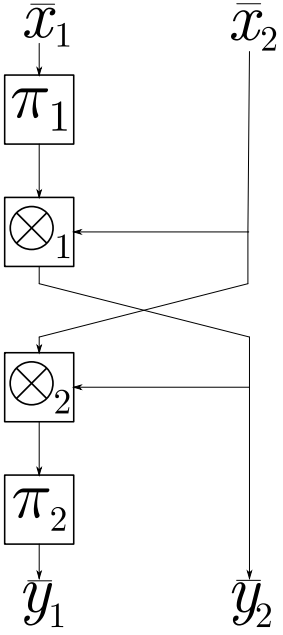
Определение

Пусть $\bar{x}_1, \bar{x}_2 \in V_4$, π_1, π_2, $\widehat{\pi}_1$, $\widehat{\pi}_2$ *– биективные преобразования пространства* V_4.
Подстановку $F_A : V_8 \times V_8 \to \mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$, *определяемую уравнениями*

$$\bar{y}_1 = \begin{cases} \pi_2\left(\left(\bar{x}_2\right)^2 \cdot \pi_1\left(\bar{x}_1\right)\right), & \bar{x}_1 \neq 0; \\ \widehat{\pi}_2\left(\bar{x}_2\right), & \bar{x}_1 = 0. \end{cases}$$

$$\bar{y}_2 = \begin{cases} \pi_1\left(\bar{x}_1\right) \cdot \bar{x}_2, & \bar{x}_2 \neq 0; \\ \widehat{\pi}_1\left(\bar{x}_1\right), & \bar{x}_2 = 0. \end{cases}$$

будем называть подстановкой типа «A».



При подходящем выборе подстановок π_1, π_2, $\widehat{\pi}_1$, $\widehat{\pi}_2$ подстановка типа «A» задает 6-равномерную подстановку, имеющую нелинейность 108, алгебраическую степень 7, графовую алгебраическую иммунность равную 3

Будем рассматривать эффективность аппаратной реализации подстановок

- на ПЛИС, оцениваем задействованные ресурсы, например, количество ячеек памяти и таблиц замены, реализующих булевы функции от 6 переменных (LUT)
- на СБИС, оцениваем количеством условных вентилей (GE)

Для корректности сравнения рассмотрим три варианта реализации 8-битовой подстановки типа «A»:

- реализация «в лоб», с помощью которой можно реализовать произвольное отображение $V_8 \to V_8$;
- реализация произвольного отображения $V_8 \to V_8$ с использованием координатных функций, которое позволяет существенно сократить используемые ресурсы;
- реализация подстановки типа «A».

- В случае реализации произвольного отображения $V_8 \to V_8$ «в лоб» происходит запись таблицы значений преобразования в память.
- Будем использовать память типа BRAM.
- Для реализации произвольного отображения $V_8 \to V_8$ в табличном виде необходимо 65 558 GE

LUT рассматриваемых ПЛИС реализуют произвольную булеву функцию от 6 переменных.

Рассмотрим отображение $f : V_8 \to V_8$, а также функции $f_i,\ i = 1, 2, 3, 4, f_i : V_8 \to V_8$, которые существенным образом зависят лишь от 6 переменных, причём

$$f(x_1, x_2, x_3, \ldots, x_8) = \begin{cases} f_1(0, 0, x_3, \ldots, x_8), & \text{если } x_1 = 0, x_2 = 0; \\ f_2(0, 1, x_3, \ldots, x_8), & \text{если } x_1 = 0, x_2 = 1; \\ f_3(1, 0, x_3, \ldots, x_8), & \text{если } x_1 = 1, x_2 = 0; \\ f_4(1, 1, x_3, \ldots, x_8), & \text{если } x_1 = 1, x_2 = 1. \end{cases}$$

- Для реализации каждой функции f_i, $i = 1, 2, 3, 4$, необходимо 6 LUT (ровно по одному LUT для реализации каждой из шести координатных функций).
- Для реализации мультиплексора (т. е. функции выбора выходной функции) необходимо ещё 8 LUT.
- Суммарное количество LUT, необходимых для данной реализации функции f, равно 40.
- Для реализации отображения $f : V_8 \to V_8$ потребовалось 812 GE (примерно в 80 раз меньше)

- Для реализации подстановки типа «A» требуется реализовать (не более, чем) четыре подстановки на двоичных векторах длины 4, две операции сравнения, две операции сложения и два мультиплексора
- Для реализации подстановки типа «A» конструкции на ПЛИС необходимо 19 LUT
- Это более чем в два раза меньше по сравнению с реализацией 8-битовой подстановки с использованием координатных функций
- Для реализации на СБИС необходимо лишь 147 GE (в 5,5 раз меньше, чем вторым способом)

Выводы

- Подстановки типа «A» могут быть использованы при синтезе стойких низкоресурсных примитивов
- Требуется меньше операций при программной bitslice-реализации

Спасибо за внимание

Вопросы?