СГЛАЖИВАЮЩИЕ СВОЙСТВА КЛЮЧЕЙ КОМБИНАЦИОННОГО УСТРОЙСТВА ВСЕВОЗМОЖНЫХ ПЕРЕСТАНОВОК

Кохновский С.И.

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Иванюк А.А. – д-р техн. наук, профессор

В работе рассмотрено функционирование устройства всевозможных перестановок при работе с *q*-ми векторами, а также свойства ключей устройства, полученные в процессе анализа сопоставления результатов работы ключей на бинарных и *q*-х векторах.

Широта сферы применения аппаратных шифраторов всем хорошо известна: от блочных шифров до составного компонента сложных вычислительных систем. Предметом исследования является спроектированное запутывающее устройство, задающее отображение множества входных сигналов *I* на множество выходных *O* в зависимости от используемого ключа. На вход комбинационной схемы подаются векторы $input = (i_1, i_2, \dots, i_n), input \in I$ и $key = (k_1, k_2, \dots, k_m), key \in K$, причём $k_i \in \{0,1\}, \forall i \in \overline{1,m}$. На выход схема возвращает вектор $output = (o_1, o_2, \dots, o_n), output \in O$ – перестановку входного вектора.

Введём расстояние по Хэммингу между векторами $input$ и $output$

$$D_H = d_{key}(input, output) = \sum_{i=1}^{n} |input_i - output_i|, \quad (1)$$

где $input_i \in \{0,1\}, \forall i \in \overline{1,n}$ и $output_i \in \{0,1\}, \forall i \in \overline{1,n}$.

А также среднее расстояние по Хэммингу

$$D_H^* = \frac{1}{n}\sum_{i=1}^{n} d_{key_i}(input, output), \quad (2)$$

причём $key_i \in K, \forall i \in \overline{1,m}$.

Расчёты D_H, а также D_H^* в зависимости от подаваемого вектора key приведены в работе [1].

Определим расстояние между *q*-ми векторами как

$$D_V = d'_{key}(input, output) = \sum_{i=1}^{n} |input_i - output_i|, \quad (3)$$

где $input_i = i, \forall i \in \overline{1,n}$; $output_i \in num, \forall i, num \in \overline{1,n}$.

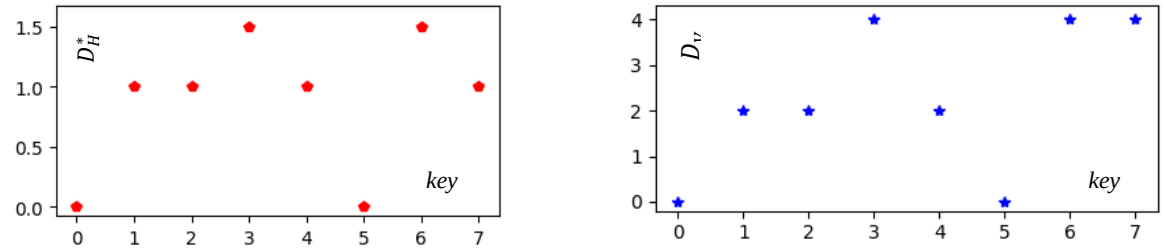
В таблице 1 приведён расчёт D_V для *q*-го вектора размерности $n = 3$.

Таблица 1 – Векторное расстояние для *q*-х векторов размерности 3

input	123	123	123	123	123	123	123	123
key	000	001	010	011	100	101	110	111
output	123	213	132	312	213	123	231	321
D_V	0	2	2	4	2	0	4	4

Введём понятие качества, определяющее, насколько хорошо ключ перемешивает, сглаживает *q*-й или случайный бинарный вектор. Пусть ключ key_i называется более качественным, чем ключ key_j, если $d_{key_i}(input, output) > d_{key_j}(input, output)$. Также будет определено понятие качества и для *q*-х векторов: key_i более качественный, чем key_j, если $d'_{key_i}(input, output) > d'_{key_j}(input, output)$.

На рисунке 1 приведён график зависимости D_H^* и D_V от всевозможных ключей для устройства размерности 3.



(а) (б)

Рисунок 1 – Расстояние Хэмминга для бинарного вектора (а), векторное расстояние для q-го вектора (б), $n = 3$

Далее для большей иллюстративности будем рассматривать свойства устройства размерности $n = 4$. Пусть ключ j будет качественным, если $d_{key_j}(input, output) > (\max_{i=\overline{1,m}} d_{key_i}(input, output))/2$. Аналогично ключ j – качественный, когда $d'_{key_j}(input, output) > (\max_{i=\overline{1,m}} d'_{key_i}(input, output))/2$, тогда на рисунке 2 (график D_V масштабирован) наглядно отображено, что если ключ является качественным относительно D_V, то он также будет являться качественным относительно D_H^*.

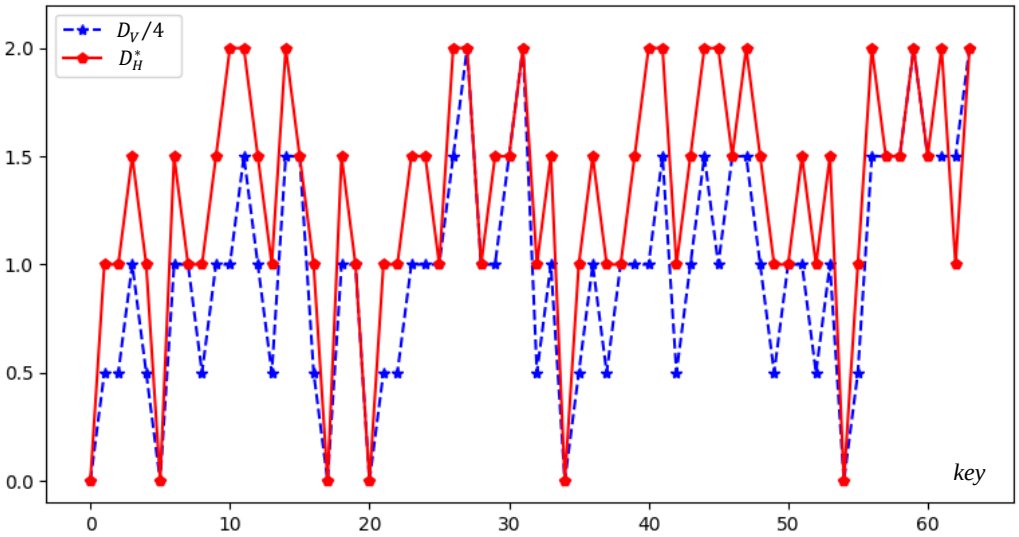


Рисунок 2 – Расстояние по Хэммингу для бинарного вектора D_H^*, векторное расстояние для q-го вектора, уменьшенное в 4 раза ($D_V/4$) для любого ключа устройства размерности $n = 4$

Причём если назвать каждое из значений 0, 0.5, 1, 1.5, 2 группой и в этом порядке присвоить им номера, то верно утверждение, что $|D_V/4 - D_H^*| \leq 1, \forall key \in K$. Это утверждение можно обобщить и на большие размерности. Тогда нормировочный коэффициент может быть рассчитан как максимум из векторных расстояний, разделённый на максимум из средних расстояний по Хэммингу, а константа в правой части неравенства может быть вычислена как $\max\left(d_{key_i}(input, output)\right)/2, i = \overline{1,m}$ для всевозможных векторов $input$.

В результате анализа значений D_H^* и D_V, полученных на различных размерностях устройства, были сделаны следующие выводы:

- Средние значения расстояний по Хэммингу для бинарных векторов и значения векторного расстояния q-х векторов в зависимости от подаваемого ключа находятся в зависимости друг от друга.
- Для быстрой проверки качества ключа возможно рассчитать векторное расстояние D_V для определённого ключа. Если ключ окажется качественным, то его можно принимать за качественный и для бинарных векторов.

Список использованных источников:

1. Кохновский, С. И. Оценка ключей комбинационного устройства всевозможных перестановок [Электронный ресурс] / С. И. Кохновский, А. А. Иванюк // Информационные технологии и системы 2020 (ИТС 2020) : материалы междунар. науч. конф. – Минск : БГУИР, 2020. – 220 с. – С. 105–106. – Режим доступа : https://its.bsuir.by/m/12_130111_1_147692.pdf. – Дата доступа : 05.04.2021.