Не сохраняющие меру Т-функции

Сопин Валерий Валерьевич

Студент

Факультет ВМК МГУ имени М. В. Ломоносова, Москва, Россия

E-mail: `VvS@myself.com`

Т-функция, как важный класс криптографических примитивов, изучались Анашиным [1] [2], а также Климовым и Шамиром [3]. **Т-функция** — это такое отображение n-бит входного слова в n-бит выходного слова, что каждый i-тый бит выходного слова зависит только от 0,1, ..., i бит входного слова. Все логические и большинство арифметических операций по модулю 2^n, $n \in \mathbb{N}$, а также их композиции, являются Т-функциями.

Существуют множество методов построения транзитивных Т-функций (последнее означает, наибольший возможный период и биективность соответственно), исчерпывающий список может быть найден в работе [1]. Транзитивные Т-функции основные кандидаты по замене РСЛОС в генерации ключей, так как обладают многими важными криптографическими свойствами: высокая линейная сложность, равномерное распределение подслов и многое другое.

Задача описания транзитивных Т-функция была решена благодаря p-адическому анализу, так как **Т-функция** — это 1-Липшицево (эквивалентно **совместимости** [1]) отображение в 2-адической метрике, а ее транзитивность эквивалентена эргодичности.

Но псевдослучайные генераторы, вообще говоря, не предполагают биективность и представляют особый интерес, так как не сохраняется однозначность начального состояния. Получение критерия того, что граф, соответствующий 1-Липшицеву отображению, по всем модулям натуральной степени двойки слабо связен (цикл с хвостами) является основной целью данной доклада.

Графом Т-функции $f(x) : \mathbb{Z}_2 \mapsto \mathbb{Z}_2$ **по модулю** 2^n, $n \in \mathbb{N}$, назовем ориентированный граф, вершинами которого являются точки $0, \ldots, 2^n - 1$, две вершины y, z связаны дугой, если $f(y) \equiv z \bmod 2^n$.

Теорема 1. *Слабо связный граф по модулю* 2^n, $\forall n \in \mathbb{N}$, *Т-функции имеет единственный цикл. Граф эргодической Т-функции* $f : \mathbb{Z}_2 \mapsto \mathbb{Z}_2$ *по модулю* 2^n, $\forall n \in \mathbb{N}$, *является слабо связным.*

Через $\delta_i(m)$ обозначим координатную функцию, возвращающую i-ый разряд в 2-адическом представлении числа m.

Любое 1-Липшицево отображение имеет вид

$$f(x) = b_0\chi(0,\ x) + \sum_{k=1}^{\infty} 2^{\lfloor \log_2 k \rfloor} b_k \chi(k,\ x),\ b_k \in \mathbb{Z}_2\ [1].$$

Теорема 2. *1-Липшицево, не сохраняющее меру, слабо связное по модулю 2^j с циклом длиной не меньше 4 отображение*

$$f(x) = b_0\chi(0,\ x) + \sum_{k=1}^{\infty} 2^{\lfloor log_2 k \rfloor} b_k \chi(k,\ x),\ b_k \in \mathbb{Z}_2 : \mathbb{Z}_2 \mapsto \mathbb{Z}_2,$$

слабо связно по модулю 2^n, $\forall n \in \mathbb{N}$, если и только если для каждого $n > j$ выполняется одно из условий

1)

$$\exists k \in \Phi_n(\Omega_{n-1}) : b_k \equiv 0\ mod\ 2, \tag{1}$$

2)

если цикл сохранил длину на предыдущей шаге, то

$$\delta_{n-1}\Big(\sum_{k \in \Omega_{n-1}} f(k)\Big) = 1, \tag{2}$$

иначе

$$\sum_{k \in \Phi_n(\Omega_{n-1})} b_k \equiv 0\ mod\ 4, \tag{3}$$

где $\Phi_n(\Omega_{n-1}) = \{2^{n-1} \le k < 2^n :\ k\ mod\ 2^{\max\limits_{i \in \Omega_{n-1}} (ord_2\ i)+1} \in \Omega_{n-1}\}$, Ω_n = *элементы цикла* f *по модулю* 2^n, *если цикл сохранил длину,* $\Omega_n = \Omega_{n-1}$ *иначе.* Ω_j = *элементы цикла* f *по модулю* 2^j.

Литература

1. Anashin A., Khrennikov A. Applied algebraic dynamics // de Gruyter Expositions in Mathematics, Berlin, 2009.

2. Anashin A., Khrennikov A., Yurova E. T -Funtions Revisited: New Criteria for Bijectiv-ity/Transitivity // Designs, Codes and Cryptography, 2012.

3. Klimov A., Shamir A. Cryptographic applications of T-functions, Selected areas in cryptography // Lecture Notes in Comput. Sci., 3006, Springer, 2004, P. 248–261.