Секция «Дискретная математика и математическая кибернетика»

Вычислительно эффективные логарифмически сжимающие функции над кольцом вычетов по модулю труднофакторизуемого числа

Научный руководитель – Бабенко Людмила Климентьевна

Трепачева Алина Викторовна
Выпускник (магистр)
Южный федеральный университет, Институт математики, механики и компьютерных наук им. И.И. Воровича, Ростов-на-Дону, Россия
E-mail: alina1989malina@ya.ru

Обозначим как $Im(f(x))$ образ функции $f(x)$, для множества S будем обозначать его мощность как $|S|$, также будем использовать $\mathbb{Z}_n$ для обозначения кольца вычетов по модулю труднофакторизуемого числа n ($n = p \cdot q$, p, q - большие простые числа).

Определение 1. Назовем функцию от одной переменной $f(x)$, действующую на кольце вычетов $\mathbb{Z}_n$ *σ-логарифмически сжимающей*, если для всех $x \in \mathbb{Z}_n$ выполняется

$$|Im(f(x))| < \sigma \log_2 n \ ,$$

т.е. количество элементов в её образе не превышает двоичный логарифм от общего количества элементов $\mathbb{Z}_n$ домноженный на σ.

Определение 2. Назовем функцию от одной переменной $f(x)$, действующую на кольце вычетов $\mathbb{Z}_n$ *Ω-вероятностно σ-логарифмически сжимающей* ($\Omega, \sigma \in \mathbb{R}, 0 \leq \Omega \leq 1$), если существует такое подмножество S элементов $\mathbb{Z}_n$, $|S| > \Omega \cdot m$ что

$$|Im(f(S))| < \sigma \log_2 n \ .$$

Определение 3. Эффективно вычислимая функция $f(x) : \mathbb{Z}_n \mapsto \mathbb{Z}_n$ – это такая функция, которую можно вычислить за число операций $+, \cdot$ кольца $\mathbb{Z}_n$, логарифмичное от его размеров.

Функции из определений 1-3 имеют большое значение для криптографии: в частности для алгебраически гомоморфных криптосистем использующих для обоснования криптостойкости задачу факторизации чисел эти функции позволяют свести атаку по шифртекстам к атакам на основе известного открытого текста. В самом деле, если $m \in \mathbb{Z}_n$ – 'открытый текст' , информация для зашифрования; $Enc(m)$ – 'шифртекст' , зашифрованная информация. то поскольку для алгебраически гомоморфной криптосистемы сумма и произведение шифртекстов после расшифрования дают,соответсвенно, сумму и произведение соответсвующих открытых текстов, становится возможным вычислять любые полиномиальные функции над шифртекстами. Однако, криптоаналитик может не зная исходного открытого текста соответствующего шифртексту, применить к этому шифртексту *σ-логарифмически сжимающую* функцию и получить шифртекст, про который он знает, что количество возможных вариантов того, каким может быть соответствующий открытый текст ограничено и доступно для полного перебора за небольшое время.

В докладе рассмотрены различные способы построения эффективно вычислимых σ-логарифмически сжимающих и Ω-вероятностно σ-логарифмически сжимающих функций.