Чередник Игорь Владимирович

Использование бинарных функциональных сетей при построении кратно транзитивных множеств блочных преобразований

Данная работа инспирирована традиционными блочными шифрсистемами, в основе которых лежит конструкция сети Фейстеля или ее обобщения. Целью исследования является разработка теоретических основ одного из обобщений сетей Фейстеля, которое позволяет строить кратно транзитивные блочные шифрсистемы, заведомо стойкие к разностному методу криптоанализа.

Пусть Ω — произвольное конечное множество, $\mathcal{B}(\Omega)$ — множество всех бинарных операций, определенных на Ω, $\{x_1, \ldots, x_n\}$ — множество переменных и $*$ — общий символ бинарной операции. Произвольная формула $w(x_1, \ldots, x_n)$ в алфавите $\{x_1, \ldots, x_n, *\}$ при сопоставлении символу $*$ конкретной бинарной операции $F \in \mathcal{B}(\Omega)$ реализует функцию $w^F \colon \Omega^n \to \Omega$, а набор формул $(w_1, \ldots, w_m)$ реализует отображение $(w_1^F, \ldots, w_m^F) \colon \Omega^n \to \Omega^m$. При проведении анализа криптографических узлов переработки информации часто возникает задача исследования семейств отображений вида

$$\{(w_1^F, \ldots, w_m^F) \,:\, F \in \mathcal{K}\}, \quad \mathcal{K} \subset \mathcal{B}(\Omega). \tag{1}$$

Так, например, в некоторых случаях наличие запретов в совместных распределениях нескольких отображений из класса (1) позволяет идентифицировать начальные состояния и часть постоянных параметров изучаемых узлов.

Один из способов построения произвольного набора формул $(w_1, \ldots, w_m)$ состоит в последовательном преобразовании набора переменных $(x_1, \ldots, x_n)$. Каждая последовательность преобразований набора переменных $(x_1, \ldots, x_n)$ в набор формул $(w_1, \ldots, w_m)$ допускает наглядное представление в виде подходящей бинарной функциональной сети Σ, у которой степень захода каждой вершины не превосходит 2. При этом удобно говорить, что сеть Σ описывает преобразование набора переменных $(x_1, \ldots, x_n)$ в набор формул $(w_1, \ldots, w_m)$, а при выборе бинарной операции $F \in \mathcal{B}(\Omega)$ реализует отображение $\Sigma^F = (w_1^F, \ldots, w_m^F)$.

Предметом исследований являются классы блочных преобразований

$$\{\Sigma^F \ : \ F \in \mathcal{K}\},$$

которые реализуются произвольной фиксированной бинарной функциональной сетью Σ постоянной ширины, а в качестве параметрического множества бинарных операций $\mathcal{K}$ используются следующие семейства бинарных операций:

- $\mathcal{Q}(\Omega)$ — все бинарные операции обратимые по обеим переменным (бинарные квазигруппы);
- $\mathcal{B}^*(\Omega)$ — все бинарные операции обратимые по правой переменной.

Полученные результаты:

1. Описано строение $\mathcal{K}$-биективных сетей — бинарных функциональных сетей постоянной ширины, которые определяют биективное преобразование при выборе любой бинарной операции из множества $\mathcal{K}$.
2. Разработан эффективный метод проверки кратной транзитивности класса блочных преобразований $\{\Sigma^F \ : \ F \in \mathcal{K}\}$, определяемых произвольной $\mathcal{K}$-биективной сетью Σ.
3. Предложены и строго обоснованы алгоритмы построения $\mathcal{K}$-биективных сетей, для которых соответствующие классы блочных преобразований обладают требуемой кратной транзитивностью.
4. Построены практически значимые классы $\mathcal{K}$-биективных сетей с небольшим количеством вершин, для которых соответствующие классы блочных преобразований обладают требуемой кратной транзитивностью.