УДК 621.3.06

ГЕНЕРАЦИЯ ПОДСТАНОВОК НА ОСНОВЕ ВЕКТОРНЫХ ФУНКЦИЙ

Александр Казимиров
Харьковский национальный университет радиоэлектроники

Анотация: **Приводится основное описание векторных булевых функций и рассматриваются критерии генерации подстановок в рамках данного математического аппарата. На основе анализа свойств векторных функций предлагается новый метод генерации долговременных ключей для шифра ГОСТ 28147-89.**
Summary: **It is provided a basic description for vectorial Boolean functions, and considered criteria for S-box selection in the framework. It is proposed a new method for the generation of long-term keys (S-boxes) based on vectorial Boolean functions for the GOST 28147-89 cipher.**
Ключові слова: ***векторные булевы функции, ГОСТ 28174, БСШ, ПСН***

Подстановки являются частью большинства симметричных преобразований и играют важную роль в обеспечении их надежности. Блочные симметричные шифры являются итерационными преобразованиями над блоком открытого текста, параметризованными ключевыми данными (раундовыми ключами). Каждый раундовый ключ вычисляется на основе ключа шифрования с применением функции разворачивания ключа.

Существует множество атак, которые должны учитываться при проектировании шифра. К ним можно отнести различные вариации дифференциальной атаки: бумеранговая, невыполнимых дифференциалов, на связанных ключах, усечённых дифференциалов, высоких порядков; линейный, алгебраический и интегральный криптоанализ и другие. Однако, как показывает практика, в конечном итоге в большинстве случаев основное внимание уделяется дифференциальному и линейному криптоанализу и, соответственно, выбору оптимальных подстановок с учётом данных типов атак.

Пусть n и m два натуральных числа. Функция $F:\mathcal{F}_2^n \mapsto \mathcal{F}_2^m$ называется (n,m)-функцией. Они используются в криптографии как нелинейные функции в псевдослучайных генераторах (потоковых шифрах) или как подстановки (S-блоки) обеспечивающие смешивание (confusion) в блочных шифрах. Любая (n,m)-функция F является δ-равномерной, если для любого $a \in \mathcal{F}_2^n \setminus \{0\}$ и $b \in \mathcal{F}_2^m$ уравнение $b = F(x) + F(x+a)$ имеет не более δ решений. Функция F называется почти совершенно нелинейной (ПСН) если $\delta = 2$. Нижняя граница δ равна 2^{n-m} и равна ей тогда и только тогда, когда F является совершенно нелинейной.

Известно несколько классов степенных ПСН функции: Голд (Gold), Касами (Kasami), Вэшл (Welch) и Нихо (Niho). Когда n четное, обратные функции являются дифференциально 4-распределёнными перестановками. Данный вид функций вместе с расширенным аффинным (РА) преобразованием, использовался при выборе подстановок в алгоритмах AES/Rijndael и «Лабиринт».

Исследование подстановок в виде векторных функций открывает огромные возможности. Например, позволяет находить целые классы функции со схожими свойствами, использование которых позволяет сократить время поиска оптимальной подстановки. В недавних работах были классифицированы все 4-битные перестановки с оптимальными показателями. Оптимальной считалась биективная подстановка с нелинейностью равной 8 и дифференциально 4-распределённая. Всего получилось 16 функций вплоть до РА-эквивалентности.

На основе этих данных можно генерировать долговременные ключи для шифра ГОСТ 28147. На первом шаге случайно выбираются 8 функций принадлежащих разным классам. На основе выбранных функций генерируются перестановки с использованием РА-эквивалентности и проверяются дополнительные свойства. Таким образом, получается быстрый и эффективный способ генерации долговременных ключей шифра ГОСТ 28147-89 с заданными свойствами.