УДК 681.3.06

МАЗУРКОВ М. И., СОКОЛОВ А. В.

НЕЛИНЕЙНЫЕ S-БЛОКИ ПОДСТАНОВКИ НА ОСНОВЕ КОМПОЗИЦИОННЫХ КОДОВ СТЕПЕННЫХ ВЫЧЕТОВ

Одесский национальный политехнический университет,
Украина, Одесса, 65044, пр. Шевченко 1

Аннотация. На основе композиционных кодов степенных вычетов предложен способ построения новых конструкций нелинейных *S*-блоков подстановки длины $N = 256$ и объема $|S| = 8{,}6248 \times 10^{13}$. Синтезированные конструкции обладают хорошими криптографическими свойствами, существенно дополняют и расширяют класс конструкций Ниберга шифра Rijndael а также обеспечивают возможность их применения в качестве долговременного ключа

Ключевые слова: криптографический шифр; нелинейный S-блок; метод синтеза; коды степенных вычетов; поле Галуа

Коды степенных вычетов широко используются для построения нормальных, композиционных и больших систем дискретных частотных сигналов с большой базой и заданными структурными, дистанционными и корреляционными свойствами [1]. Вместе с тем, вопросы построения нелинейных *S*-блоков подстановки на основе композиционных кодов степенных вычетов исследованы в литературе недостаточно полно [2].

Целью настоящей статьи является разработка способа построения нелинейных *S*-блоков подстановки на основе композиционных кодов степенных вычетов с хорошими криптографическими свойствами, применительно к шифру Rijndael/AES.

Вне зависимости от выбранной архитектуры блочного симметричного шифра, будь то сеть Фейстеля или SP-сеть, основным компонентом, определяющим устойчивость криптопреобразования к основным видам атак криптоанализа, является надежность нелинейного *S*-блока подстановки шифра, производящего отображение группы входных битов x_i в группу выходных битов y_i в соответствии с правилом кодирующей *Q*-последовательности, которая полностью определяет структуру и криптографические свойства *S*-блока подстановки.

Пусть, например, задана кодирующая *Q*-последовательность

$$Q_1 = \{0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15\}, \quad (1)$$

что соответствует отсутствию подстановки, т.е. прямому отображению входных битов *S*-блока подстановки в выходные: $y_i = x_i$. Очевидно, что подобный *S*-блок подстановки не обладает криптостойкостью. Тем не менее, кодирующая *Q*-последовательность (1) не содержит в себе повторяющихся элементов: операция подстановки, выполненная с помощью данного *S*-блока подстановки является полностью обратимой. Такой *S*-блок подстановки называется биективным [2], и может служить основой для построения криптографически

Электронный вариант статьи: http://radio.kpi.ua/article/view/S0021347013090045