УДК 681.3.06

АЛГОРИТМ УСТРАНЕНИЯ СПЕКТРАЛЬНОЙ ЭКВИВАЛЕНТНОСТИ КОМПОНЕНТНЫХ БУЛЕВЫХ ФУНКЦИЙ S-БЛОКОВ КОНСТРУКЦИИ НИБЕРГ

СОКОЛОВ А. В., БАРАБАНОВ Н. А.

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

Аннотация. Исследовано явление спектральной эквивалентности компонентных булевых функций *S*-блоков подстановки конструкции Ниберг. Предложен эффективный алгоритм устранения спектральной эквивалентности, основанный на введении в каждую компонентную булеву функцию *S*-блока подстановки случайного модификатора. Анализ сгенерированных *S*-блоков подстановки на основе предложенного алгоритма подтвердил его эффективность и показал высокое криптографическое качество *S*-блоков подстановки

Ключевые слова: S-блок подстановки; булева функция; преобразование Уолша-Адамара; спектральная эквивалентность

Основным примитивом, определяющим криптографические свойства современных блочных алгоритмов шифрования является *S*-блок подстановки. В соответствии с принципами шифрования К. Шеннона задачей *S*-блока подстановки является конфузия, т. е. обеспечение сложной и нелинейной зависимости ключа и открытого текста [1].

Типичная конструкция современного *S*-блока подстановки состоит из дешифратора, шифратора и системы взаимосвязей между ними. Например, схематическое изображение *S*-блока подстановки для трехбитного ($k=3$) входного слова показано на рис. 1. Структура *S*-блока подстановки и его криптографические свойства полностью определяются кодирующей *Q*-последовательностью длины $N=2^k$, которая для приведенного примера имеет вид $\mathbf{Q} = \{5,0,4,2,6,1,7,3\}$.

В свою очередь для применения математического аппарата булевых функций для оценки

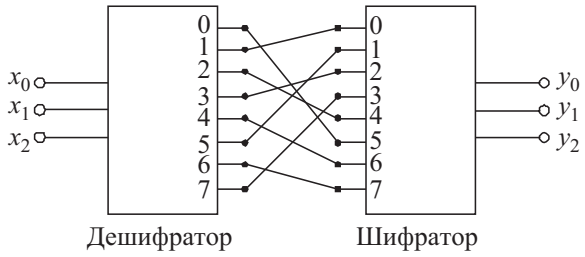

Рис. 1

криптографического качества *S*-блока подстановки кодирующая *Q*-последовательность раскладывается на множество из *k* компонентных булевых функций f_1, f_2, f_3, представленных в виде их таблиц истинности $\mathbf{F}^{(1)}, \mathbf{F}^{(2)}, \mathbf{F}^{(3)}$. Для данного примера таблицы истинности приведены в табл. 1.

Основными критериями, предъявляемыми к современным *S*-блокам подстановки, являются высокое расстояние нелинейности, в смысле расстояния до аффинного кода, низкий уровень корреляции между входными и вы-

Электронный вариант статьи: http://radio.kpi.ua/article/view/S0021347015050040