

УДК 681.3.06

## НЕЛИНЕЙНЫЕ S-БЛОКИ КОНСТРУКЦИИ НИБЕРГ С МАКСИМАЛЬНЫМ ЛАВИННЫМ ЭФФЕКТОМ

МАЗУРКОВ М. И., СОКОЛОВ А. В.

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

**Аннотация.** Построен полный класс неприводимых полиномов  $f(z)$  восьмой степени над всеми изоморфными представлениями поля  $GF(256)$ . Найдено множество оптимальных пар  $\{f(z), A\}$ , где  $A$  — невырожденная матрица аффинного преобразования, что позволило существенно увеличить число  $S$ -блоков конструкции Ниберг, оптимальных по критерию максимального лавинного эффекта

**Ключевые слова:**  $S$ -блок; конструкция Ниберг; аффинное преобразование; критерий максимального лавинного эффекта

Ключевым этапом разработки любого современного симметричного алгоритма шифрования является построение криптографически качественного нелинейного преобразования —  $S$ -блока, свойства которого определяют устойчивость шифра к атакам линейного, корреляционного и дифференциального криптоанализа.

В последнее время усиленное внимание уделяется вопросам синтеза нелинейных  $S$ -блоков конструкции, предложенной К. Ниберг [1], удовлетворяющих критерию максимального лавинного эффекта [2], применительно к шифру Rijndael/AES [3].

Нелинейные  $S$ -блоки конструкции Ниберг, отвечающие максимальному лавинному критерию, синтезируются путем выбора подходящей пары: вида неприводимого полинома  $f(z)$  степени  $\deg f(z) = 8$  и вида матрицы аффинного преобразования  $y = Ax + b$ . При этом в [2] применялись неприводимые над полем  $GF(2^8)$  полиномы восьмой степени, число которых  $|f_2^8| = 30$ .

Целью настоящей статьи является построение нелинейных  $S$ -блоков конструкции Ниберг, удовлетворяющих критерию максимального лавинного эффекта на основе полного класса неприводимых полиномов над всеми изоморфными представлениями поля  $GF(256)$ , применительно к шифру Rijndael/AES.

Для полноты изложения материала статьи приведем сущность метода построения  $S$ -блоков, удовлетворяющих критерию максимального лавинного эффекта [2].

Пусть  $X = [x_i]_{i=0,255}$  — последовательность возрастающих чисел от 0 до 255. Конструкция Ниберг отображает каждый элемент  $x_i$  в мультипликативно обратный элемент  $y_i$  по правилу

$$y_i \equiv x_i^{-1} \bmod (f(z), 2), \quad i = \overline{0, 255}, \quad (1)$$

где в качестве  $f(z)$  выбран неприводимый полином  $f(z) = z^8 + z^6 + z^3 + z^2 + 1$ ;  $\bmod (f(z), 2)$  — взятие по двойному модулю.