

УДК 681.3.06

МЕТОД СИНТЕЗА S-БЛОКОВ ПО КРИТЕРИЮ НУЛЕВОЙ КОРРЕЛЯЦИИ МЕЖДУ ВЫХОДНЫМИ И ВХОДНЫМИ ВЕКТОРАМИ ДАННЫХ И СТРОГОМУ ЛАВИННОМУ КРИТЕРИЮ

МАЗУРКОВ М. И., СОКОЛОВ А. В.

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

Аннотация. Предложен конструктивный метод синтеза корреляционно иммунных S-блоков длины $N = 256$, удовлетворяющих строгому лавинному критерию. Найдены его свойства а также оценки количества оптимальных S-блоков, которые могут быть получены с его помощью. Предложен регулярный метод размножения полученных оптимальных S-блоков

Ключевые слова: S-блок; корреляционный иммунитет; матрица коэффициентов корреляции; строгий лавинный критерий

Криптографический S-блок является основным компонентом практически всех современных симметричных шифров, который обуславливает его лавинный эффект, корреляционную связь векторов выхода y_j и входа x_j , а также нелинейность. Вопросы синтеза криптографически качественных S-блоков, нашли свое отражение во многих работах [1–6], где в качестве основы для их синтеза выбран тот или иной критерий. Однако для построения новых высокоскоростных криптоалгоритмов интерес представляют такие S-блоки, которые соответствуют одновременно нескольким критериям криптографического качества и таким образом позволяют эффективно противостоять одновременно нескольким видам атак криптоанализа.

Одними из наиболее существенных с практической точки зрения критериями качества S-блоков является критерий независимости векторов выхода S-блока y_j от векторов его входа x_j , известный также как корреляци-

онный иммунитет [1], а также строгий лавинный критерий [2]. Корреляционно иммунным называется такой S-блок длины $N = 2^k$, каждая компонентная булева функция F_j , $j = 1, k$, которого обладает корреляционным иммунитетом первого или более высокого порядка $m \geq 1$, что справедливо тогда и только тогда, когда ее спектральные коэффициенты Уолша-Адамара

$$W(\omega) = F_j A(n) = \sum_{i=0}^{n-1} F_j(i) (-1)^{\langle i, \omega \rangle} = 0, \\ \forall \omega, \text{ wt}(\omega) = m, \quad (1)$$

где $A(n)$ — матрица Уолша-Адамара порядка $n = N^2$, $N = 2^m$; $\text{wt}(\cdot)$ — вес Хэмминга; $\langle i, \omega \rangle$ — скалярное произведение по bmod2 коэффициентов двоичного представления десятичных чисел, которые запишем в виде $(i)_{10} = (i_{s-1}, i_{s-2}, \dots, i_0)_2$ и, соответственно, $(\omega)_{10} = (\omega_{s-1}, \omega_{s-2}, \dots, \omega_0)_2$, тогда