УДК 681.3.06

АЛГОРИТМ СИНТЕЗА ЭКОНОМИЧНЫХ СХЕМ S-БЛОКОВ ПОДСТАНОВКИ НА ОСНОВЕ КЛЕТОЧНЫХ АВТОМАТОВ

МАЗУРКОВ М. И., СОКОЛОВ А. В.

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

Аннотация. Предложен алгоритм синтеза экономичных схем *S*-блоков подстановки на основе клеточных автоматов, которые удовлетворяют основным критериям криптографического качества. Найдены правила клеточных автоматов, позволяющие получить *S*-блоки подстановки, удовлетворяющие критерию максимального лавинного эффекта

Ключевые слова: клеточный автомат; S-блок подстановки; максимальный лавинный эффект

Вопросам конструирования криптографических биективных *S*-блоков подстановки, которые являются основными элементами современных блочных шифров, посвящено большое количество работ исследователей в области криптографии [1–3]. Современные методы конструирования высококачественных *S*-блоков подстановки подразумевают использование аппарата булевых функций для их описания [4]. Это позволяет достичь строго обоснованного уровня качества, которое определяется соответствием компонентных булевых функций конструируемого *S*-блока подстановки определенным критериям.

К таким критериям качества относятся высокая нелинейность, корреляционная независимость векторов выхода *S*-блока подстановки от его входа, строгий лавинный критерий, величина периодов возврата *S*-блока подстановки в исходное состояние. Однако, все чаще к требованиям конструируемых *S*-блоков подстановки относят критерий простоты их аппаратной или программной реализации [3]. Данное требование связано не только с концепцией энергоэффективности, но также с тем, что с ростом длины *S*-блока подстановки существенно улучшаются все его показатели криптографического качества [5]. Возможность реализовать *S*-блок подстановки большей длины при том же количестве аппаратных средств и энергоэффективности ведет к существенному улучшению характеристик криптоалгоритма, в котором такой *S*-блок подстановки применяется.

Так в случае использования криптографического *S*-блока подстановки, длина входного слова которого $k = 32$ бита, потребуется хранить в памяти криптографической системы кодирующую Q-последовательность, определяющую структуру *S*-блока подстановки, длины $N = 2^k = 2^{32} = 4294967296$. При этом, каждый элемент Q-последовательности представляет собой 32-разрядное число, т.е. необходимое для хранения *S*-блока подстановки количество памяти составит 4294967296 × 32 = = 137438953472 бит = 16 ГБ, что является весьма существенным объемом. При этом дальнейшее увеличение длины *S*-блока под-

DOI: 10.20535/S0021347016050034