УДК 004.056.55

ПРИМЕНЕНИЕ МАТЕМАТИЧЕСКОГО АППАРАТА КЛЕТОЧНЫХ АВТОМАТОВ ДЛЯ СИНТЕЗА КРИПТОГРАФИЧЕСКИХ *S*-БЛОКОВ ПОДСТАНОВКИ

А. В. Соколов

Одесский национальный политехнический университет
Украина, г. Одесса
radiosquid@gmail.com

В работе рассматривается возможность применения математического аппарата клеточных автоматов для синтеза S-блоков подстановки современных шифров. Показано, что применение клеточных автоматов позволяет строить S-блоки подстановки большой длины при минимальных затратах элементов памяти, а также соответствующие критерию максимального лавинного эффекта.

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

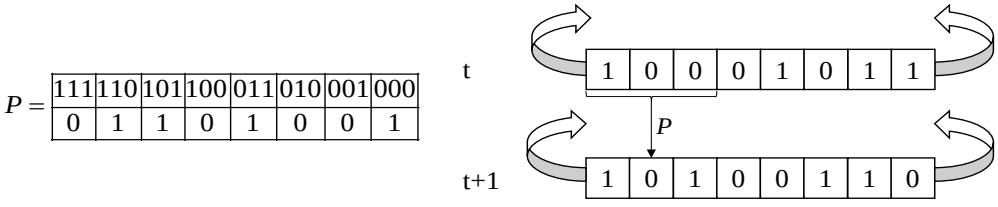
Базовым компонентом практически всех современных блочных шифров является криптографический *S*-блок подстановки, структура и криптографические свойства которого во многом определяют эффективность и быстродействие шифра в целом. Требования к криптографическим *S*-блокам подстановки в настоящее время состоят из двух частей: требования к криптографическому качеству, в которые входит высокая нелинейность, отсутствие корреляционной взаимосвязи между векторами выхода и входа, хороший лавинный эффект, а также возможность простой программной и аппаратной реализации. Наращиванию криптографического качества *S*-блоков подстановки посвящены многие современные исследования, например [1], тогда как вопрос конструирования экономичных *S*-блоков подстановки, особенно большой длины, остается исследованным недостаточно.

Целью настоящей работы является адаптация современного математического аппарата клеточных автоматов для синтеза больших криптографических *S*-блоков подстановки.

В соответствии с определением [2], криптографическим *S*-блоком подстановки называется конструкция, реализующая замену группы битов другой группой битов в соответствии с определенным правилом, которое обычно задается в виде кодирующей *Q*-последовательности. Последняя необходима для физической реализации *S*-блока подстановки и определяет его криптографические свойства.

Последние исследования показали, что иным способом задания криптографического описания *S*-блока подстановки является задание правила эволюции клеточного автомата, который полностью определяет структуру кодирующей *Q*-последовательности.

В простейшем случае одномерным клеточным автоматом называется дискретная структура, включающая в себя решетку ячеек памяти длиной l, такую, что для каждой ячейки определена окрестность из r ячеек, взаимодействующих по правилу P, определяющему переход ячеек из текущего состояние в новое с течением дискретного времени t [3]. Данную структуру несложно изобразить схематически, как показано на рисунке.



Схематическое представление работы клеточного автомата с течением дискретного времени t

В случае использования клеточного автомата для реализации криптографического *S*-блока подстановки исходное состояние клеточного автомата используется как вход *S*-блока подстановки,

тогда как на выход *S*-блока подстановки подается состояние решетки ячеек памяти по истечении τ тактов. В соответствии с определением клеточного автомата для его корректной работы требуется наличие лишь одного регистра, длины, равной длине входного слова *S*-блока подстановки, а также хранение последовательности, определяющей правило эволюции клеточного автомата. Длина правила эволюции определяется размером окрестности в соответствии с соотношением $L_P=2^{2r+1}$. Таким образом, при размере окрестности r=1 требуется всего 8 бит для хранения правила, которое гипотетически может определять *S*-блок подстановки с входным словом произвольной длины.

Использование небольших значений r приводят к низкому уровню криптографического качества *S*-блока подстановки. Установлено, что практически наиболее привлекательным является значение $r=1$, позволяющее получить *S*-блоки подстановки, соответствующие основным критериям криптографического качества, и требующими для своей реализации хранения правила длины $L_P=2^{2\cdot2+1}=32$. Так, при длине *S*-блока подстановки $L_S=256$ выигрыш составляет $\gamma=256\cdot8/32=64$ раза. Нетрудно видеть, что коэффициент γ стремительно растет с увеличением L_S.

Количество таких существующих в природе правил составляет, соответственно, $J=2^{L_P}=2^{32}$, из которых выделены 37 правил, приводящих к формированию клеточным автоматом биективных *S*-блоков подстановки, т. е. таких, в кодирующей *Q*-последовательности которых отсутствуют повторяющиеся элементы. Свойство биективности позволяет формировать полностью обратимые преобразования, что является существенным с криптографической точки зрения. Два правила P={851955; 805359615}, представленные в виде своих десятичных эквивалентов, позволяют конструировать *S*-блоки подстановки, допускающие существование матриц аффинного преобразования, приводящих к максимальному лавинному эффекту с использованием алгоритма [4].

Отметим основные результаты проведенных исследований:

— впервые найдены все правила эволюции клеточных автоматов с окрестностью $r=2$, приводящие к формированию биективных криптографических *S*-блоков подстановки;

— теория синтеза *S*-блоков подстановки, соответствующих критерию максимального лавинного эффекта, получила дальнейшее развитие, в рамках чего были найдены два правила эволюции клеточных автоматов, позволяющие осуществлять синтез матриц аффинного преобразования, приводящих S-блок подстановки к максимальному лавинному эффекту;

— оценен выигрыш в реализации криптографических *S*-блоков подстановки на основе клеточных автоматов по сравнению с классической реализацией на основе *Q*-последовательности.

Таким образом, использование математического аппарата клеточных автоматов в задачах синтеза *S*-блоков подстановки современных шифров является перспективным и позволяет получить значительный выигрыш при их программной реализации.

ИСПОЛЬЗОВАННЫЕ ИСТОЧНИКИ

1. Nyberg K. Differentially uniform mappings for cryptography. In Advances in cryptology / K. Nyberg. — Pr. of EUROCRYPT’93. — Berlin, Heidelberg, New York, 1994. — Lect. Notes in Comp. Sprin.-Verlag. — P.55 — 65.

2. Скляр, Б. Цифровая связь. Теоретические основы и практическое применение. — Москва: Издательский дом "Вильямс". — 2003. — 1104 с.

3. Szaban M. Cryptographically Strong S-Boxes Based on Cellular Automata / M. Szaban, F. Seredynski. — Polnad, Krakow: Lecture Notes in Computer Science, 2008. — Vol. 5191, P. 478—485.

4. Chandrasekharappa, T.G.S. S-boxes generated using Affine Transformation giving Maximum Avalanche Effect / T.G.S. Chandrasekharappa, K.V. Prema, Kumara Shama // Internation Journal of Computer Science and Engineering. — Manipal Institute of Technology, India. — Vol. 3(N 9). — 2011. — P. 3185—3193.

———————

A. V. Sokolov

Using the mathematical apparatus of cellular automata for the synthesis of cryptographic S-boxes.

This paper considers the possibility of using the mathematical apparatus of cellular automata for synthesis of S-boxes for modern ciphers. It is shown that the application of cellular automata allows to build the S-boxes of great length with a minimum amounts of storage elements, as well as satisfying the criterion of maximum avalanche effect.

Keywords: *cryptographic S-box, cellular automaton, maximum avalanche effect.*