ISSN 0735-2727, Radioelectronics and Communications Systems, 2016, Vol. 59, No. 5, pp. 212–220. © Allerton Press, Inc., 2016.
Original Russian Text © M.I. Mazurkov, A.V. Sokolov, 2016, published in Izv. Vyssh. Uchebn. Zaved., Radioelektron., 2016, Vol. 59, No. 5, pp. 27–37.

Algorithm for Synthesis of Efficient S-Boxes Based on Cellular Automata

M. I. Mazurkov and A. V. Sokolov*
Odessa National Polytechnic University, Odessa, Ukraine
**e-mail: radiosquid@gmail.com*
Received in final form October 24, 2015

Abstract—A method for synthesis of efficient schemes of *S*-boxes based on cellular automata satisfying the main criteria of cryptographic quality has been proposed. The cellular automata rules making it possible to obtain *S*-boxes satisfying the criterion of maximum avalanche effect were found.

DOI: 10.3103/S0735272716050034

Cryptographic bijective *S*-boxes are main components of all modern block ciphers, and a large number of research papers in the field of cryptography are devoted to the issues of designing such *S*-boxes [1–3]. Modern design methods of high-quality *S*-boxes imply their description by the Boolean function apparatus [4] making it possible to attain a rigorously substantiated level of quality that is determined by the component Boolean functions of the *S*-box under construction complying with specific criteria.

Such quality criteria include high nonlinearity, correlation independence of vectors of *S*-box output on its input, strict avalanche criterion, and the value of *S*-box reset time. However, the simplicity criterion of the hardware or software implementation of *S*-box under construction is increasingly frequently referred to the requirements of designed *S*-boxes [3]. This requirement is related not only with the energy efficiency concept, but also with the fact that with the rise of the *S*-box length, all its indicators of cryptographic quality significantly improve [5]. The possibility of implementing *S*-box of larger length with the same amount of hardware and the same energy efficiency leads to a significant improvement of characteristics of the cryptoalgorithm, where such *S*-box is applied.

Hence, the use of cryptographic *S*-box with the input word length equal to $k = 32$ bits involves the need of storing in the cryptographic system memory the coding *Q*-sequence determining the *S*-box structure of length $N = 2^k = 2^{32} = 4294967296$. In this case, each element of the *Q*-sequence represents a 32-bit number, i.e., the memory volume required for storing the *S*-box amounts to $4294967296 \times 32 = 137438953472$ bits = 16 GByte (GB), which is a fairly significant volume. Further rise of the *S*-box length occurring in modern cryptographic systems results in the exponential growth of the amount of memory needed for storing the *Q*-sequence.

Therefore, the development of new schemes for implementing *S*-boxes of large length is a topical problem. At present, an approach for construction of efficient *S*-boxes based on peculiarities of the Nyberg design [6] and also the approach based on noise-like signals representing De Bruijn sequences [3] are available. Nevertheless, both approaches are effective only at small values of *S*-box length *N*. A new approach to formation of *S*-boxes based on the mathematical apparatus of cellular automata proposed and substantiated in [7] is more promising and versatile.

However, a significant disadvantage of *S*-boxes designed in [7] is their nonbijectivity that leads to difficulties in determining the inverse transformation and prevents the practical use of efficient schemes of *S*-boxes based on cellular automata.

The purpose of this study is to develop a method for synthesis of bijective efficient schemes of cryptographic *S*-boxes based on the apparatus of cellular automata.

Let us consider a cryptographic *S*-box, the structure and properties of which are fully specified by the coding *Q*-sequence [3, 4] of length $N = 16$

$$Q = \{5,2,15,10,6,13,7,4,14,0,1,3,12,8,9,11\}. \quad (1)$$