ISSN 0735-2727, Radioelectronics and Communications Systems, 2017, Vol. 60, No. 12, pp. 538–544. © Allerton Press, Inc., 2017.
Original Russian Text © O.N. Zhdanov A.V. Sokolov, 2017, published in Izvestiya Vysshikh Uchebnykh Zavedenii, Radioelektronika, 2017, Vol. 60, No. 12, pp. 696–703.

Extending Nyberg Construction on Galois Fields of Odd Characteristic

O. N. Zhdanov[1] and A. V. Sokolov[2*]

[1]*Siberian State Aerospace University, Krasnoyarsk, Russia*
[2]*Odessa National Polytechnic University, Odessa, Ukraine*
**e-mail: radiosquid@gmail.com*

Received in final form October 1, 2017

Abstract—As is known, the Nyberg design *S*-boxes possess the cryptographic properties valuable for practical application. Up to date this construction has been considered only for fields of characteristic 2. This paper presents an extension of the Nyberg construction to the fields of odd characteristic. The notion of nonlinearity distance of *p*-function is introduced, and the affine ternary code is built. The Nyberg design *S*-boxes with field characteristic $p = 3$ for all lengths $N \le 243$ are built. The nonlinearity distances are calculated, and it is shown that with an increase of *S*-box length, these distances increase essentially faster as compared to the fields of characteristic $p = 2$.

DOI: 10.3103/S0735272717120032

URGENCY OF THE SUBJECT

Block symmetric cryptographic algorithms are among the primary tools for ensuring the information confidentiality. The blistering rise of the processing power of computers stipulates the need of enhancing the encryption strength of existing algorithms and developing the new ones. Many researchers and practitioners are engaged in this activity. The cryptoalgorithm stability in relation to most common types of cryptoanalysis is determined by the quality of replacement block, i.e. *S*-box. At present, it is generally accepted that the quality of substitution boxes is characterized by values of nonlinearity and avalanche effect [1, 2].

APPROACHES TO FORMATION OF SUBSTITUTION TABLES

In respect of the formation of substitution tables, we can single out two main approaches to the development of encryption algorithms.

The algorithm specified by Standard GOST 28147-90 [2] and recognized as highly robust that does not define the method of *S*-box generation is an example of the first approach. This algorithm implies the possibility of using different techniques for constructing substitution boxes. For example, the validated procedure of stepwise selection of Boolean functions that are components of substitution boxes was proposed in [3]. This procedure takes into account both the nonlinearity values of each of the functions forming the box and the nonlinearity of all possible nontrivial linear combinations of these functions. Note that in this case it is possible concurrently to solve the problem of enhancing the stability of linear and differential cryptoanalyses by using both the nonlinearity and dynamic distance as selection criteria [4–6]. The procedure of such stepwise selection is realized by software in relation the algorithm (GOST 28147-90) in [1].

The Rijndael algorithm also considered as robust [7] can represent the most peculiar example of the second approach. The substitution box in this algorithm is completely determined by an irreducible polynomial over the Galois field. The Rijndael algorithm employs the Nyberg construction [8] representing the mapping in the form of multiplicatively inverse elements of Galois field $GF(2^k)$:

$$y = x^{-1} \bmod [f(z), p],\ \ y, x \in GF(2^k), \tag{1}$$

in combination with affine transformation

REFERENCES

1. O. N. Zhdanov, *The Technique of Core Information Selection for Block Encryption Algorithm* [in Russian] (INFRA-M, Moscow, 2013).
2. A. V. Sokolov, *New Methods for Synthesis of Nonlinear Transformations of Modern Ciphers* [in Russian] (Lap Lambert Academic Publishing, Germany, 2015).
3. Standard GOST 28147-89. Data Processing Systems. Cryptographic Security. Cryptographic Transformation Algorithm (IPK Izdatel'stvo standartov, Moscow, 1996).
4. S. Mister, C. Adams, "Practical S-box design," *Proc. of Workshop in Selected Areas of Cryptography*, SAC'96, (1996), pp. 61-76. URI: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.40.7715&rep=rep1&type=pdf.
5. T. E. Medvedeva, "The S-boxes cryptography robustness assessment of GOST 28147-89 algorithm," *Reshetnevskie Chteniya*, 666 (2012). URI: http://disk.sibsau.ru/website/reshetnevsite/materials/2012_2.pdf.

6. T. A. Chalkin, "Development of the parameter selection technique for the algorithm of constructing S-boxes of the block cipher standard GOST 28147-89," *Proc. of III Int. Conf. on Pressing Security Problems of Information Technologies*, 2009, Sib. Gos. Aerokosmich. Un-t, Russia. Krasnoyarsk (2009).
7. FIPS 197. Advanced encryption standard, 2001. URI: http://csrc.nist.gov/publications/.
8. K. Nyberg, "Differentially uniform mappings for cryptography," *Advances in cryptology. Proc. of EUROCRYPT'93*, *Lecture Notes in Computer Science* **765**, 55 (1994). DOI: 10.1007/3-540-482 85-7_6.
9. M. I. Mazurkov and A. V. Sokolov, "Nonlinear transformations based on complete classes of isomorphic and automorphic representations of field GF(256)," *Radioelectron. Commun. Syst.* **56**, No. 11, 513 (2013). DOI: 10.3103/S0735272713110022.
10. M. I. Mazurkov and A. V. Sokolov, "Cryptographic properties of nonlinear transform of Rijndael cipher based on complete classes of irreducible polynomials," *Odes'kyi Politechnichnyi Universystet. Pratsi*, No. 2, 183 (2012). URI: http://pratsi.opu.ua/articles/show/864.
11. A. S. Ambrosimov, "Properties of bent functions of q-valued logic over finite fields," *Discrete Math. Appl.* **4**, No. 4, 341 (1994). DOI: 10.1515/dma.1994.4.4.341.
12. R. Lidl and H. Niederreiter, *Finite Fields*, 2nd ed. CUP, 1994.
13. Y.-S. Kim, J.-W. Jang, J.-S. No, T. Helleseth, "On p-ary bent functions defined on finite fields," *Mathematical Properties of Sequences and Other Combinatorial Structures*. The Springer International Series in Engineering and Computer Science, vol. 726 (Springer, Boston, MA, 2002), pp. 65–76. DOI: 10.1007/978-1-4615-0304-0_8.
14. O. N. Zhdanov, A. V. Sokolov, "Block symmetric cryptographic algorithm based on principles of variable block length and many-valued logic," *Far East J. Electronics Commun.* **16**, No. 3, 573 (2016). DOI: 10.17654/EC016030573.