On criteria and methods for generating optimal S-boxes

Yerzhan Seitkulov*, Ruslan Ospanov, Banu Yergaliyeva,

Kuandyk Niyazaliyev

Institute of Information Security and Cryptology, Gumilyov Eurasian National University. Kazakhstan

**Corresponding author's e-mail: erj@mail.ru*

Abstract

In this paper, we consider criteria and methods for generating optimal S-boxes. The current issue is the analysis of the existing criteria for S-boxes and a reasonable choice of the necessary set of criteria for specific cryptographic algorithms or classes of cryptographic algorithms; search and develop theoretically based effective practical methods for obtaining optimal S-boxes that provide high indicators of security in symmetric cryptographic algorithms. The analysis of the criteria and methods will make it possible to build the most efficient algorithm for generating optimal S-boxes.

Keywords: Information security, Cryptography, S-box

1 Introduction

S-boxes (substitution block, s-box, substitution box) are one of the main components that determine the nonlinearity of the encryption transformation and the level of security of modern symmetric cryptographic algorithms. When designing many symmetric block encryption algorithms, S-blocks are often chosen for the purpose of implementing confusion in the cipher. Thus, the cryptographic security of ciphers strongly depends on the cryptographic properties of S-boxes. S-boxes are substitutions that map an n-bit input block to an m-bit output block. Widely used in block ciphers and the most interesting subclass of substitutions are bijective (also called permutations). To protect cryptographic algorithms from various types of attacks, S-boxes must meet a number of criteria. Due to the large number of existing criteria, their inconsistency or partial interdependence, it is problematic to form an S-box that has all the known specified properties. Therefore, in practice, S-boxes are used that meet the main criteria essential for a particular symmetric algorithm. Such S-boxes are usually called optimal.

2 Criteria

The optimal S-box criteria can be set for an entire class of cryptographic algorithms, as well as set for a single cryptographic primitive. When selecting replacement tables for new ciphers, the main criteria are non-linearity and differential uniformity. Differential uniformity is an indicator of resistance against differential attack. For example, for 8-bit substitutions, the optimal values of differential uniformity are no more than 8. Non-linearity is an indicator of resistance against a linear attack. The optimal values for 8-bit substitutions are at least 100. Algebraic degree and algebraic immunity are indicators of resistance against algebraic attacks. In the case of 8-bit substitutions, the optimal values of the algebraic degree are at least 7, and the maximum value of the algebraic immunity is 3 for 441 equations. And in the case of substitutions of 4 in 4 bits, the criterion of algebraic immunity does not play a big role, since they can be described by a system of equations of the second degree. But at the same time, it cannot be equal to 1. Another criterion is the absence of cycles of length 1, i.e. fixed points. There are many other criteria. Most of the criteria have not yet been proven to be necessary. Many of them are not applicable to block ciphers, but at the same time they are used in stream ciphers. The properties of S-boxes of DES and GOST 28147 block ciphers are not relevant today. Modern criteria are focused on protection against existing types of cryptanalysis: linear, algebraic, and various variations of differential. Another criterion is related to whether substitutions belong to different equivalence classes of vector Boolean functions. This criterion is only applicable if the algorithm uses more than one non-linear replacement node. Many studies show that there are probably no perfect S-boxes. Therefore, the concept of optimal S-box was introduced, the criteria of which are determined for a specific cryptographic algorithm or class of cryptographic algorithms) and are optimal from the point of view of protection against existing types of attacks.

Generating optimal S-boxes is a time-consuming task. Existing methods for obtaining S-boxes can be divided into three main areas: algebraic constructions, pseudorandom generation, and a heuristic approach.

In the first approach, S-boxes are designed according to some proven mathematical relations and principles. The most well-known representatives of this approach are bijective (n × n) S-boxes (permutations) based on inversion in a finite field GF (2n). They are the best S-boxes found

and at the same time optimal with respect to most of the desired criteria. For example, an S-box in AES is an S-box that has high algebraic degree - 7, high nonlinearity - 112, low autocorrelation - 32, and low differential uniformity – 4. In [1], we propose a construction based on a linear fractional transformation and a permutation function. In [2], we consider a method for designing S-boxes based on the use of cubic polynomial mappings. In [3], we synthesize (8 × 8) S-boxes based on the projective general linear group PGL(2, GF(28)) over the Galois field GF(28). There are many other algebraic methods for generating substitutions, for example, [4], [5]. Although such S-boxes are often preferred because of their excellent cryptographic properties, there are some problems related to their simple algebraic structure and possible future vulnerability to algebraic attacks. In addition, the number of these S-boxes is small, and they are all affine equivalent.

The second approach consists in constructing S-boxes from a table of random numbers and then checking its correspondence. This approach is doomed to failure from the very beginning, since most of the cryptographic criteria you are looking for often contradict each other, which significantly reduces the number of S-boxes that are good for all criteria, and reduces the probability of selecting good S-boxes.

The third approach involves iterative improvement of an S-box or a whole set of S-boxes with respect to one or more properties. Unlike algebraic constructions, heuristic methods are able to create large sets of S-boxes, since they use direct search methods. Most often, the cryptographic properties of S-boxes obtained using heuristic algorithms are not as good as those of algebraically constructed S-boxes. However, in recent years, the difference between these properties has become increasingly indistinguishable. The latter is achieved using some specific heuristic methods, such as the method of search by hill climbing, the method of simulated annealing, genetic algorithms, or various combinations of them. Although most of the methods described give good results for constructing bijective S-boxes based on only one of the main criteria, this becomes much more complex when both non-linearity and differential uniformity must be considered simultaneously.

A known method for generating highly nonlinear S-boxes based on gradient descent [6] requires the sequential application of several criteria for each generated substitution. In [7], an improvement of this method is presented by selecting the appropriate order of criteria application, which reduces the required computing power for generating S-boxes. In [8], we propose a heuristic method for generating large sets of (n × n) bijective S-boxes with a good combination of target properties, such as high nonlinearity, high algebraic degree, low differential uniformity, and low autocorrelation, based on the use of a specific artificial immune algorithm in combination with a modification of the hill climbing method for S-boxes. In [9], the prospects for further research in order to improve heuristic methods for the synthesis of random S-boxes are substantiated. In [10], a generalized methodology for designing and testing S-boxes for symmetric ciphers is described. This methodology includes the application of three well-established tests that should be used to design or test each S-box. The study also shows that at least some mathematical methods for designing S-boxes, while safe, are no more secure than non-mathematical methods, but are more computationally intensive

3 Conclusion

Thus, the current issue is the analysis of the existing criteria for S-boxes and a reasonable choice of the necessary set of criteria for specific cryptographic algorithms or classes of cryptographic algorithms; search and develop theoretically based effective practical methods for obtaining optimal S-boxes that provide high indicators of security in symmetric cryptographic algorithms. The analysis of the criteria and methods will make it possible to build the most efficient algorithm for generating optimal S-boxes.

4 Support information.

This work was carried out with the financial support of the Ministry of Education and Science grant funding, No. AP09258274.

References

[1] Nizam Chew L.C., Ismail E.S. *S-box Construction Based on Linear Fractional Transformation and Permutation Function*. Symmetry 2020, 12, 826.

[2] Zahid A.H., Arshad M.J. *An Innovative Design of Substitution-Boxes Using Cubic Polynomial Mapping*. Symmetry 2019, 11, 437.

[3] Altaleb A., Saeed M.S., Hussain I., Aslam M. *An algorithm for the construction of substitution box for block ciphers based on projective general linear group*. AIP Advances. 2017, 7, 035116

[4] Hussain S., Jamal S. S., Shah T., Hussain I. A *Power Associative Loop Structure for the Construction of Non-Linear Components of Block Cipher*. IEEE Access, vol. **8**, pp. *123492-123506*, 2020

[5] Gao W., Idrees B., Zafar S., Rashid T. *Construction of Nonlinear Component of Block Cipher by Action of Modular Group PSL(2, Z) on Projective Line* PL(GF(28)). IEEE Access, vol. **8**, pp. **136736-136749**, 2020

[6] Kazymyrov O.V. *Methods and tools of generating nonlinear replacement nodes for symmetric cryptoalgorithms.* Dissertation for the degree of Candidate of Technical Sciences, specialty 05.13.21-information security systems. Kharkiv National University of Radioelectronics, Kharkiv, 2013. *(in Russian)*

[7] Rodinko M., Oliynykov R., Gorbenko Y. *Optimization of the high nonlinear s-boxes generation method. Tatra Mountains Mathematical Publications,* Mathematical Institute, Slovak Academy of Sciences, Bratislava, 2017, Volume **70**: Issue **1**, pp. **93-105**.

[8] Ivanov G., Nikolov N., Nikova S. *Cryptographically Strong S-Boxes Generated by Modified Immune Algorithm*. In: Pasalic E., Knudsen L. (eds) Cryptography and Information Security in the Balkans. BalkanCryptSec 2015. Lecture Notes in Computer Science, vol **9540**. Springer, Cham. 2016, pp **31-42**.

[9] Gorbenko I., Kuznetsov A., Gorbenko Y., Pushkar'ov A., Kotukh Y., Kuznetsova K. *Random S-Boxes Generation Methods for Symmetric Cryptography*. 2019 IEEE 2nd Ukraine Conference on Electrical and Computer Engineering (UKRCON), Lviv, Ukraine, 2019, pp. **947-950**.

[10] Easttom C. A *generalized methodology for designing non-linear elements in symmetric cryptographic primitives.* 2018 IEEE 8th Annual Computing and Communication Workshop and Conference (CCWC), Las Vegas, NV, 2018, pp. **444-449**.