МАТЕМАТИЧЕСКИЕ ВОПРОСЫ КРИПТОГРАФИИ
2017 Т. 8 № 2 С. 97 – 116

УДК 519.719.2

Spectral-linear and spectral-differential methods for generating S-boxes having almost optimal cryptographic parameters

A. V. Menyachikhin

TVP Laboratories, Moscow

Получено 19.III.2016

Abstract. S-boxes are important parts of modern ciphers. To construct S-boxes having cryptographic parameters close to optimal is an unsolved problem at present time. In this paper some new methods for generating such S-boxes are introduced.

Keywords: S-box, substitution, involutory substitution, spectral-linear method, spectral-differential method, Kuznechik, BelT, Skipjack, Khazad-0, Khazad, Anubis

Спектрально-линейный и спектрально-дифференциальный методы построения S-боксов с близкими к оптимальным значениями криптографических параметров

А. В. Менячихин

Лаборатории ТВП, Москва

Аннотация. S-боксы являются важным элементом современных шифрсистем. Задача построения S-боксов с близкими к оптимальным значениями криптографических параметров в настоящее время не решена. В статье предлагается ряд новых методов построения таких S-боксов.

Ключевые слова: S-бокс, подстановка, инволютивная подстановка, спектрально-линейный метод, спектрально-дифференциальный метод, Кузнечик, BelT, Skipjack, Khazad-0, Khazad, Anubis

Citation: *Mathematical Aspects of Cryptography*, 2017, v. 8, № 2, pp. 97–116 (Russian)

References

[1] Agievich S. V., Afonenko A. A., “On the properties of exponential substitutions”, *Vesti NAN Belarusi*, **1** (2005), 106–112 (in Russian).

[2] Agievich S. V., Galinsky B. A., Mikulich N. D., Kharin U. S., “Algorithm of block encryption BelT” (in Russian), http://apmi.bsu.by/assets/files/agievich/BelT.pdf.

[3] Alekseychuk A., Kovalchuk L., Pal’chenko S., “Cryptographic parameters of s-boxes that characterize the security of GOST-like block ciphers against linear and differential cryptanalysis”, *Zakhist Inform.*, **2** (2007), 12–23 (in Ukrainian).

[4] Alekseychuk A., Kovalchuk L., “Upper bounds of maximum values of average differential and linear characteristic probabilities of Feistel cipher with adder modulo 2^m”, *Theory of Stochastic Processes*, **12 (28)**:1–2 (2006), 20–32.

[5] Barreto P., Rijmen V., “The ANUBIS block cipher”. In: “*NESSIE submission*”, 2000.

[6] Barreto P., Rijmen V., “The KHAZAD block cipher”. In: “*NESSIE submission*”, 2000.

[7] Biham E., Biryukov A., Shamir A,, “Cryptanalysis of Skipjack reduced to 31 rounds using impossible differentials,”. In: “*EUROCRYPT’99*”, Lect. Notes Comput. Sci., **1592**, 1999, 12–23.

[8] Bugrov A. D., “Piecewise affine substitution of finite fields”, *Prikl. Diskr. Matem.*, **4(30)** (2015), 5–23 (in Russian).

[9] Blondeau C., Gerard B., “Links between theoretical and effective differential probabilities: experiments on PRESENT”. In: “*In: ECRYPT II Workshop on Tools for Cryptanalysis*”, 2010, https://eprint.iacr.org/2010/261.pdf.

[10] Bogdanov A., Knudsen L. R., Leander G., Paar C., Poschmann A., Robshaw M. J. B., Seurin Y., Vikkelsoe C., “PRESENT: An ultra-lightweight block cipher”. In: “*CHES 2007*”, Lect. Notes Comput. Sci., **4727**, 2007, 450–466.

[11] Carlet C., Ding C., “Nonlinearities of S-boxes”, *Finite Fields Appl.*, **13** (2007), 121-135.

[12] Chabaud F., Vaudenay S., “Links between differential and linear cryptanalysis”. In: “*EUROCRYPT*”, Lect. Notes Comput. Sci., **950**, 1994, 356–365.

[13] Daemen J., Rijmen V., “Probability distributions of correlations and differentials in block ciphers”, *J. Math. Crypt.*, **1** (2007), 221–242.

[14] Daemen J., Rijmen V., *The Design of Rinjdael: AES — The Advanced Encryption Standard*, Heidelberg etc.: Springer, 2002.

[15] Dygin D. M., Lavrikov I. V., Marshalko G. B., Rudsky V. I., Trifonov D. I., Shishkin V. A., “On a new Russian Encryption Standard”, *Mathematical Aspects of Cryptography*, **6**:2 (2015), 29–34.

[16] Evans A., *Orthomorphism Graphs of Groups*, Lect. Notes Math., **1535**, Heidelberg etc.: Springer-Verlag, 1992, 116 pp.

[17] Gluhov M. M., “On the matrices of transitions of differences when using some modular groups”, *Mathematical Aspects of Cryptography*, **4**:4 (2013), 27–47 (in Russian).

[18] Gluhov M. M., “On a method of construction of orthogonal quasigroups systems by means of groups”, *Mathematical Aspects of Cryptography*, **2**:4 (2011), 5–24 (in Russian).

[19] Goldberg D., *Genetic Algorithms in Search, Optimization and Machine Learning*, Readings, MA: Addsion-Wesley, 1985, 432 c.

[20] *GOST R 34.12-2015. Information technology. Cryptographic protection of information. Block ciphers*, Moscow : Standartinform, 2015 (in Russian).

[21] *GOST R 34.11-2012. Information technology. Cryptographic protection of information. Hash function*, Moscow : Standartinform, 2012 (in Russian).

[22] Izbenko Y., Kovtun V., Kuznetsov A., "The design of Boolean functions by modified hill climbing method", *IEEE Computer Soc.* (2009), 356–361.

[23] Jacobson Jr. M., Huber K., *The MAGENTA Block Cipher Algorithm*, NIST AES Proposal, 1998, http://edipermadi.files.wordpress.com/2008/09/magenta-spec.pdf.

[24] Kazymyrov O. V., Kazymyrova V. N., Oliynykov R. V., "A method for generation of high-nonlinear S-boxes based on gradient descent", *Mathematical Aspects of Cryptography*, **5**:2 (2014), 71–78.

[25] Knuth D., *Art of Computer Programming, Volume 2: Seminumerical Algorithms*, 3rd ed. : Addison-Wesley Professional, 1997.

[26] Leander G., Poschmann A., "On the classification of 4-bit s-boxes", Lect. Notes Comput. Sci., **4547**, 2007, 159–176.

[27] Malyshev F. M., "Doubly transitive XSL-families of permutations", *Mathematical aspects of cryptography*, **1**:2 (2010), 93–103 (in Russian).

[28] Malyshev F. M., "The duality of difference and linear methods in cryptography", *Mathematical aspects of cryptography*, **5**:3 (2014), 35–47 (in Russian).

[29] Matsumoto M., Nishimura T., "Mersenne Twister: a 623-dimensionally equidistributed uniform pseudo-random generator", *ACM Trans. Modeling and Computer Simul. (TOMACS)*, **8**:1 (1998), 3–30.

[30] Millan W., Clark A., Dawson E., "Smart hill climbing finds better Boolean functions", Lect. Notes Comput. Sci., **1334**, 1997, 149–158.

[31] Millan W., "How to improve the nonlinearity of bijective S-boxes", Lect. Notes Comput. Sci., **1438**, 1998, 181–192.

[32] Nyberg K., "On the construction of highly nonlinear permutations". In: "*EUROCRYPT'92*", Lect. Notes Comput. Sci., 1992, 92–98.

[33] Nyberg K., "Perfect nonlinear S-boxes". In: "*EUROCRYPT'91*", Lect. Notes Comput. Sci., 1991, 378–386.

[34] Nyberg K., Knudsen L., "Provable security against differential cryptanalysis", *J. Cryptology*, **8**:1 (1992), 27–37.

[35] Pichkur A. B., "Description of the set of permutations represented as a product of two permutations with fixed number of mobile points", *Mathematical Aspects of Cryptography*, **3**:2, (2012), 79–95 (in Russian).

[36] Pichkur A. B., "Description of the set of permutations represented as a product of two permutations with fixed number of mobile points. II", *Mathematical Aspects of Cryptography*, **4**:1 (2013), 87–109 (in Russian).

[37] Pieprzyk J., "Non-linearity of exponent permutations". In: "*EUROCRYPT'89*", Lect. Notes Comput. Sci., **434**, 1990, 81–92.

[38] Pogorelov B. A., "Substitution groups. Part 1 (the review over 1981-95)", Trudy po Diskretnoi Matematike, **2**, 1998, 237–281 (in Russian).

[39] Pogorelov B. A., Pudovkina M. A., “On the distance from permutations to the union of all imprimitive groups with identical parameters of imprimitivity systems”, *Discrete Math. Appl.*, **24**:3 (2014), 163–173.

[40] Sachkov V. N., “Combinatorial properties of differentially 2-uniform substitutions”, *Mathematical Aspects of Cryptography*, **6**:1 (2015), 159–179 (in Russian).

[41] Sachkov V. N., “Random mapping with fixed elements”, *Mathematical Aspects of Cryptography*, **2**:2 (2011), 95-118 (in Russian).

[42] Shemyakina O. V., “On the estimation of the characteristics of partitions of various algebraic structures”. In: *“Inf. security of Russian regions (ISRR-2011)*”, St-Pb.: SPOISU, 2011, 137 (in Russian).

[43] *Skipjack and KEA Algorithm Specifications, Version 2.0.*, 1998, http://csrc.nist.gov/encryption/skipjack-kea/htm.

[44] *STB 34.101.31-2011. Information technologies. Information security. Cryptographic algorithms of enciphering and continuity test*, Minsk: Gosstandart, 2011 (in Russian).

[45] Tokareva N. N., “Quadratic approximations of the special type for the 4-bit permutations in S-boxes”, *Prikl. Diskr. Matem.*, **1** (2008), 50–54 (in Russian).

[46] Tokareva N. N., “On quadratic approximations in block ciphers”, *Probl. Inf. Transmiss.*, **44**:3 (2008), 266–286.

[47] Trishin A. E., “The nonlinearity index for a piecewise-linear substitution of the additive group of the field”, *Prikl. Diskr. Matem.*, **4(30)** (2015), 32–42 (in Russian).

[48] Trishin A. E., “The method of constructing orthogonal Latin squares on the basis of substitution binomials of finite fields”, *Obozr. prikl. i prom. matem.*, **15**:4 (2008), 764–765 (in Russian).