Tokareva, N.; **Gorodilova, A.**; **Agievich, S.**; **Idrisova, V.**; **Kolomeec, N.**; **Kutsenko, A.**; **Oblaukhov, A.**; **Shushuev, G.**

Mathematical methods in solutions of the problems presented at the third international students' olympiad in cryptography. (English) Zbl 07311617

Prikl. Diskretn. Mat. 2018, No. 40, 34-58 (2018).

Summary: The mathematical problems, presented at the Third International Students' Olympiad in Cryptography NSUCRYPTO'2016, and their solutions are considered. They are related to the construction of algebraic immune vectorial Boolean functions and big Fermat numbers, the secrete sharing schemes and pseudorandom binary sequences, biometric cryptosystems and the blockchain technology, etc. Two open problems in mathematical cryptography are also discussed and a solution for one of them proposed by a participant during the Olympiad is described. It was the first time in the Olympiad history. The problem is the following: construct $F\colon \mathbb{F}_2^5 \to \mathbb{F}_2^5$ with maximum possible component algebraic immunity 3 or prove that it does not exist. Alexey Udovenko from University of Luxembourg has found such a function.

MSC:

94A60 Cryptography
97D50 Teaching mathematical problem solving and heuristic strategies

Keywords:

cryptography; ciphers; Boolean functions; biometry; blockchain; olympiad; NSUCRYPTO

Full Text: DOI MNR

References:

[1] Agievich S., Gorodilova A., Kolomeec N., et al., "Problems, solutions and experience of the first international student"s Olympiad in cryptography.", Prikladnaya Diskretnaya Matematika, 2015, no. 3, 41-62

[2] Agievich S., Gorodilova A., Idrisova V., et al., "Mathematical problems of the second international student"s Olympiad in cryptography", Cryptologia, 41:6 (2017), 534-565

[3] Geut K., Kirienko K., Sadkov P., et al., "On explicit constructions for solving the problem 'A secret sharing' ", Prikladnaya Diskretnaya Matematika. Prilozhenie, 2017, no. 10, 68-70 (in Russian)

[4] Rathgeb C., Uhl C., "A survey on biometric cryptosystems and cancelable biometrics", EURASIP J. Inform. Security, 2011 (2011), 3

[5] Diffie W., Van Oorschot P. C., Wiener M. J., "Authentication and authenticated key exchanges", Designs, Codes and Cryptography, 2:2 (1992), 107-125

[6] Daemen J., Rijmen V., The Design of Rijndael: AES - the Advanced Encryption Standard, Springer Verlag, 2002 · Zbl 1065.94005

[7] Nakamoto S., Bitcoin: a peer-to-peer electronic cash system, Available at

[8] Carlet C., "On the algebraic immunities and higher order nonlinearities of vectorial Boolean Functions", Proc. NATO Advanced Research Workshop ACPTECC (Veliko Tarnovo, Bulgaria, October 6-9, 2008), IOS Press, Amsterdam, 2009, 104-116