References

[1] Kovalchuk, L., *Generalized Markov ciphers: evaluation of practical security against differential cryptanalysis.* Proc. 5-th All-Russian Sci. Conf. "Mathematics and Safety of Information Technologies" (MaBIT-06), MGU, Moscow, 25-27 Oct. 2006, 595–599.

[2] Kovalchuk, L., *Upper-bound estimation of the average probabilities of integer-valued differentials in the composition of key adder, substitution block, and shift operator.* Cybernetics and Systems Analysis **6**, 2010, 89–96.

[3] Kovalchuk, L., Kuchinska, N., *Upper-bound estimates for the average probabilities of integer differentials of round functions of certain block ciphers.* Cybernetics and Systems Analysis **3**, 2012, 42–51.

[1] Institute of Special Communication and Information Security, National Technical University of Ukraine "Kyiv Polytechnic Institute", Moskovska Str. 45/1, Kyiv 01011, Ukraine
E-mail address: lv_kov_crypto@mail.ru

[2] Institute of Special Communication and Information Security, National Technical University of Ukraine "Kyiv Polytechnic Institute", Moskovska Str. 45/1, Kyiv 01011, Ukraine
E-mail address: n.kuchinska@gmail.com

[3] Institute of Physics and Technology, National Technical University of Ukraine "Kyiv Polytechnic Institute", Peremohy Ave. 37, Kyiv 03056, Ukraine
E-mail address: victor.bezditny@gmail.com

ON STATISTICAL ESTIMATION OF MULTIVARIATE ENTROPY

U. Yu. Palukha[1], Yu. S. Kharin[2]

The problem of statistical estimation of Shannon entropy for n-words of random sequences is typical in cryptology, genetics and other applications [1, 2].

We have the sequence $x_1, \dots, x_T \in V = \{0, 1\}$, which is a stationary random sequence on the probability space (Ω, F, P). Let's consider the circular sequence of length $T + n - 1 : x_{T+1} = x_1, \dots, x_{T+n-1} = x_{n-1}$. We construct frequency estimator of $p_J(n) = P\{X_1^n = J_1^n\}$, where $J_1^n = (j_1, \dots, j_n) \in V_n$ is multiindex, and then build the entropy estimator by "plug-in" principle:

$$\hat{h}(n) = -\sum_{J \in V_n} \hat{p}_J(n) \ln \hat{p}_J(n).$$

Denote hypothesis $H_0 = \{\{x_t\} \text{ is "true random"}\} = \{p_{J_1^n} = 2^{-n}, J_1^n \in V_n\}$.

Theorem 1. *If $\{x_t\}$ satisfies hypothesis H_0, then*

$$E_{H_0}\{\hat{h}(n)\} = h_0(T,\ n) = \sum_{m=1}^{n} e^{-\frac{T}{2^m}} \sum_{k=1}^{\infty} \frac{T^k \ln(k+1)}{2^{mk} k!} (e^{-\frac{T}{2^m}} 2^k - 1).$$

Theorem 1 is useful for construction of statistical tests to evaluate performance of the random number generators' quality.

References

[1] Kharin, Yu. S. [et al.] Cryptology (in Russian). Minsk, BSU, 2013.

[2] Rukhin, A. L., *Approximate entropy for testing randomnesses.*
http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.45.6174&rep=rep1&type=pdf.

Belarusian State University, Nezavisimosti Ave. 4, Minsk 220030, Belarus
E-mail address: [1]palukha@bsu.by, [2]kharin@bsu.by

CLASSICAL AND MODERN CRYPTOGRAPHY

M. N. Savchuk

An overview of classical and modern methods of cryptography is presented. The following topics are discussed. Basic concepts of cryptographic methods of information security. The general scheme of secret communication in symmetric cryptography. Classical cryptography: permutation ciphers, substitution ciphers, Vernam cipher (one-time pad). The idea of cryptanalysis of classical ciphers. Mechanical and electromechanical ciphering machines. Beginning of modern cryptography. Types of cryptanalytic attacks. Theoretical and practical security. Basic concepts and statements Shannon's theory of secrecy communication systems. Classification of modern cryptosystems. Modern symmetric cryptography. Block ciphers, stream ciphers. Asymmetric cryptography. One-way functions. One-way functions with a trapdoor. Public-key cryptosystem. Asymmetric encryption scheme. Cryptosystem RSA. RSA digital signature. Cryptographic hash function. Cryptographic protocols. Quantum cryptography. The quantum computer. About security of asymmetric cryptography algorithms and protocols.

National Technical University of Ukraine "Kyiv Polytechnic Institute", Peremohy Ave. 37, Kyiv 03056, Ukraine
E-mail address: mikhail.savchuk@gmail.com