Statistical Hypotheses Testing for Random and Pseudorandom Generators Based on Statistical Estimators of Entropy

Uladzimir Palukha
Faculty of Applied Mathematics and Informatics;
Belarusian State University
Minsk, Belarus
palukha@bsu.by

Yuriy Kharin
Research Institute for Applied Problems of Mathematics and Informatics, Belarusian State University
Minsk, Belarus
kharin@bsu.by

***Abstract*—The topical information security problem of development of statistical tests for hypotheses on the discrete uniform distribution ("pure randomness") of output sequences produced by random or pseudorandom generators is considered. For Shannon, Rényi and Tsallis entropy functionals, the point statistical estimators based on the plug-in principle are constructed. The asymptotic probability distributions of constructed point estimators under the "pure randomness" hypothesis are found in the asymptotics, when the number of observed data is comparable with the number of parameters. Interval statistical estimators of considered information entropy functionals are constructed. On the base of interval estimators the decision rules for statistical hypotheses testing on "pure randomness" of observed discrete sequence are developed. The results of computer experiments are given.**

Keywords—Shannon, Rényi and Tsallis entropy, asymptotically normal probability distribution, statistical estimators, hypotheses testing, generators of random and pseudorandom sequences.

I. INTRODUCTION

Generators of random and pseudorandom sequences are the main structural elements of information security systems and play a central role in the construction of encryption schemes [1]. For example, generators are using to initialize parameters of digital signature systems and keys in encryption systems. The reliability of such systems depends on how the properties of generated sequence are close to the properties of "pure random" sequence [2]. To check the quality of generators in the sense of matching of probabilistic properties of their output sequences to probabilistic properties of "pure random" sequence statistical tests are used. The essence of the tests is as follows. The output sequence of the generator is observed and a null hypothesis H_* that the sequence is "pure random" is introduced. Some statistic, the probability distribution of which under the true null hypothesis H_* is known, is calculated. Based on the value of statistic, the hypothesis is either accepted or rejected. In this paper we propose to use estimators of the information entropy functionals as test statistics. The most common entropy functionals are the Shannon, Rényi and Tsallis entropy functionals, for point statistical estimators of which the asymptotic probability distributions under the true hypothesis H_* are found in this paper. The found probability distributions allow us to construct statistical tests and to apply them to analyze the output sequences of random and pseudorandom number generators.

II. MATHEMATICAL MODEL

Let a random variable $x = x(\omega) = \omega$ with the set of states $\Omega = \{\omega_1, \ldots, \omega_N\}$ and with the discrete probability distribution $p_k = P\{x = \omega_k\}, p_k \geq 0, \sum_{k=1}^{N} p_k = 1, k = 1, \ldots, N$, be defined on a probability space (Ω, F, P). We define the functional of generalized entropy according to [3]:

$$H_{h,w}^{\varphi_1,\varphi_2}(P) = h\left(\frac{\sum_{k=1}^{N} w_k \varphi_1(p_k)}{\sum_{k=1}^{N} w_k \varphi_2(p_k)}\right), \quad (1)$$

where $w_k > 0, k = 1, \ldots, N,$ is the weight of ω_k, φ_1: $[0, 1) \to \mathbb{R}$, φ_2: $[0, 1) \to \mathbb{R}$, h: $\mathbb{R} \to \mathbb{R}$, are given functions. There are different entropy functionals, for example, formulas of 23 functionals are given in [3]. Table 1 shows the most frequently used [3] particular cases of the generalized entropy functional (1), defined by the specification of the functions $h(\cdot)$, $\varphi_1(\cdot)$, $\varphi_2(\cdot)$, $\{w_k\}$, plugging into (1). It is worth to note that the Shannon entropy functional is the limiting case of the Rényi and Tsallis functionals for $r \to 1$ [4] and differs from them by the presence of some additional properties (for example, additivity [2]). Under the true hypothesis H_*, all three functionals reach their maximum value.

TABLE I. BASIC ENTROPY FUNCTIONALS

Type	Formula	$h(x)$	$\varphi_1(x)$	$\varphi_2(x)$	w_k
Shannon entropy	$H(P) = -\sum_{k=1}^{N} p_k \ln p_k$	x	$-x\ln x$	x	$w \equiv 1$
Rényi entropy	$H_r(P) = \frac{1}{1-r}\ln\left(\sum_{k=1}^{N} p_k^r\right)$	$\frac{\ln x}{1-r}$	x^r	x	$w \equiv 1$
Tsallis entropy	$S_r(P) = \frac{1}{r-1}\left(1-\sum_{k=1}^{N} p_k^r\right)$	$\frac{x-1}{1-r}$	x^r	x	$w \equiv 1$

A common approach to statistical estimation of entropy is the construction of frequency estimators of the states

probabilities and the substitution of the obtained estimates in the entropy functional instead of the true values of probabilities. In this paper, we propose a method for constructing statistical estimators of Shannon, Rényi and Tsallis entropy. Also we give the probabilistic properties of the obtained estimators in the asymptotics, which is more often encountered in practice, and means that the number of observables is comparable with the number of parameters being evaluated. Using the point estimators, interval statistical estimators of entropy are constructed. Based on the interval statistical estimators the decision rules for statistical testing of hypothesis about the closeness of the observed output sequence to the "pure random" sequence are developed.

III. Construction of Statistical Estimators for Entropy

A. Frequency Estimators of Probabilities

Let there be a random sequence of length n, from the probability distribution $\{p_k\}$. We construct the frequency estimators of the probability distribution $\{p_k: k = 1, \ldots, N\}$:

$$\hat{p}_k = \frac{v_k}{n}, \quad v_k = \sum_{t=1}^{n} I\{x_t = \omega_k\} \in \square \quad \square$$
$$I\{x_t = \omega_k\} = \begin{cases} 1, & x_t = \omega_k; \\ 0, & x_t \neq \omega_k. \end{cases} \tag{2}$$

As it had been already mentioned in the introduction, we introduce the hypothesis H_* = {{x_t} is "pure random" sequence} = {{x_t} are independent identically distributed random variables, $p_k = 1 / N$, $k = 1, \ldots, N$}, and the general alternative $\overline{H_*}$.

Following [5], we will assume that the series scheme holds. In this case, the vector $(v_1, \ldots, v_N)^T$, composed of the frequencies v_k from (2), has the multinomial probability distribution Mul(n, N, $p_1, \ldots, p_N$), and each of the components has the binomial probability distribution $Bi(n, p_k)$. Consider the asymptotics:

$$n, N \to \infty, \; n / N \to \lambda, \; 0 < \lambda < \infty, \tag{3}$$

which differs from the classical one ($n \to \infty$, $N < \infty$) in that the duration of observation n and the number of values N grow synchronously. In the asymptotics (3), the probability distribution of the statistics $\{v_k\}$ is approximated by the Poisson distribution $\Pi(\lambda_k)$ with the parameter $\lambda_k = np_k$. Under the true hypothesis H_*, all elementary probabilities are equal: $p_k = 1 / N$, $k = 1, \ldots, N$, therefore, all frequencies $\{v_k\}$ have the same Poisson distribution parameter $\lambda = n / N$.

The theorem on the asymptotically normal distribution of statistics that are functions of the frequencies v_k is proved in [5]. It can be briefly reformulated as follows. Let $f(\cdot)$: $\mathbb{N}_0 \to \mathbb{R}$ be a function; $Z = \sum_{k=1}^{N} f(v_k)$, where v_k, $k = 1, \ldots, N$ are frequencies with the joint multinomial distribution, approximated by the Poisson distribution in the asymptotics (3). Then, under certain regularity conditions, the statistic Z has the asymptotically normal distribution $\mathrm{L}\left\{\frac{Z-\mu}{\sigma}\right\} \to N_1(0,1)$:

$$\mu = \sum_{k=1}^{N} E\{f(v_k)\}, \tag{4}$$

$$\sigma^2 = \sum_{k=1}^{N} \mathrm{var}\{f(v_k)\} - \left(\sum_{k=1}^{N} \mathrm{cov}\{v_k, f(v_k)\}\right)^2 \Big/ n, \tag{5}$$

where $N_1(0, 1)$ is the standard one-dimensional normal probability distribution with zero mathematical expectation and variance that equals one, $E\{\xi\}$ and $\mathrm{var}\{\xi\}$, respectively, the mathematical expectation and the variance of the random variable ξ, $\mathrm{cov}\{\xi, \eta\}$ is the covariance of the random variables ξ and η. Under the true hypothesis H_*, the relations (4) and (5) are transformed respectively:

$$\mu = \sum_{k=1}^{N} E\{f(v_k)\} = NE\{f(v)\},$$

$$\sigma^2 = N \,\mathrm{var}\{f(v)\} - N^2 \,\mathrm{cov}^2\{v, f(v)\}/n =$$
$$= N\left(\mathrm{var}\{f(v)\} - \mathrm{cov}^2\{v, f(v)\}/\lambda\right).$$

To apply the results from [5] to the proof of the probabilistic properties of statistical estimators of entropy, it is necessary to express the estimators of the entropy functionals in the terms of frequencies.

B. Statistical Estimation of Shannon Entropy

We take $f(v) = v\ln v$ as a function f. The statistical estimator of Shannon entropy $\hat{H}(n, N)$ is linearly expressed in terms of $Z = \sum_{k=1}^{N} v_k \ln v_k$ [6]:

$$\hat{H} = \hat{H}(n, N) = -\sum_{k=1}^{N} \hat{p}_k \ln \hat{p}_k = -\sum_{k=1}^{N} \frac{v_k}{n} \ln \frac{v_k}{n} = \ln n - \frac{1}{n} Z. \tag{6}$$

The theorem on the asymptotic probability distribution of the statistic (6) is proved by the first author in [7].

Theorem 1. *In the asymptotics* (3)*, the statistic* (6) *with the true hypothesis* H_* *has the asymptotically normal distribution* $\mathrm{L}\left\{\frac{\hat{H}-\mu_H}{\sigma_H}\right\} \to N_1(0,1)$:

978-1-5090-5689-7/17/$31.00 ©2017 IEEE

$$\mu_H = \ln n - e^{-\lambda} \sum_{k=1}^{+\infty} \frac{\ln(k+1)\lambda^k}{k!}, \quad (7)$$

$$\sigma_H^2 = \frac{e^{-\lambda}}{n} \sum_{k=1}^{+\infty} \frac{(k+1)\lambda^k}{k!} \ln^2(k+1) - \frac{e^{-2\lambda}}{N} \left(\sum_{k=1}^{+\infty} \frac{\ln(k+1)\lambda^k}{k!} \right)^2 - \frac{e^{-2\lambda}}{n} \left(\sum_{k=1}^{+\infty} \ln(k+1) \frac{\lambda^k}{k!} (k+1-\lambda) \right)^2. \quad (8)$$

The behavior of the mathematical expectation of the Shannon entropy estimator of a binary sequence, which is divided into fragments of length s (they are called s-grams; in this case $N = 2^s$), is considered in [8].

Knowing the asymptotic probability distribution of the point estimator (6) allows us to construct the interval estimator for the Shannon entropy:

with probability that equals $1 - \varepsilon$, the entropy estimate

$$\hat{H}(P) \in (H_-, H_+), \quad H_\pm = \mu_H \pm \sigma_H \Phi^{-1}\left(1 - \frac{\varepsilon}{2}\right), \quad (9)$$

where $\Phi(\cdot)$ is the cumulative distribution function of the standard normal distribution.

The disadvantage of the constructed point estimator is the presence of a bias, as it's demonstrated in [8]. Therefore we consider the construction of the statistical estimators for the Rényi and Tsallis entropy functionals.

C. Statistical Estimation of Rényi and Tsallis Entropy

We consider the Rényi and Tsallis entropy functionals with a parameter $r \in \{2, 3, \ldots\}$. As it can be seen from the Table 1, functionals have a common function $\varphi_1(x) = x^r$. The argument of the function is the probability p_k. It's also seen that the Rényi and Tsallis entropies are functions of the quantity

$$P_r(P) = \sum_{k=1}^{N} p_k^r . \quad (10)$$

Consequently, the problem of the statistical estimation of the quantity $P_r(P)$ arises.

It's known [9] that the statistical estimator for (10) $\hat{P}_r(P) = \sum_{k=1}^{N} \hat{p}_k^r = \sum_{k=1}^{N} \left(\frac{\nu_k}{n} \right)^r$, constructed by the plug-in principle, is biased. To construct an asymptotically unbiased estimator, we define the r^{th} descending factorial of x:

$$x^{\underline{r}} = x(x-1)\ldots 1) = \frac{x!}{(x-r)!} = \sum_{i=0}^{r} s(r,i) x^i, \quad (11)$$

where $s(r, i)$ is the Stirling number of the first kind [10]; by definition, for $x < r$ it is assumed $x^{\underline{r}} ::= 0$. The asymptotically unbiased and consistent statistical estimator for the quantity (10), which is based on (11), is proposed in [9]:

$$\tilde{\imath}_{r\backslash -,} \quad \underbrace{\sum_{k=1}^{N} \frac{\nu_k^{\underline{r}}}{n^r}}. \quad (12)$$

Assuming that $f_r(v) = v^{\underline{r}}$,

$$Z_r = \sum_{k=1}^{N} f_r(\nu_k) = \sum_{k=1}^{N} \nu_k^{\underline{r}} = n^r \tilde{\imath}_{r\backslash -,}. \quad (13)$$

We have the following lemma [11] on the probability distribution of statistic (13).

Lemma. *In the asymptotics* (3)*, the statistic* (13) *with the true hypothesis H_* has the asymptotically normal distribution* $\mathrm{L}\left\{ \frac{Z_r - \mu_r}{\sigma_r} \right\} \to N_1(0,1)$ *:*

$$\mu_r = N\lambda^r = n\lambda^{r-1},$$

$$\sigma_r^2 = N\lambda^r \left(\sum_{i=1}^{r} s(r,i) \sum_{j=0}^{i-1} C_i^j r^{i-j} \sum_{k=1}^{j} S(j,k)\lambda^k - r^2\lambda^{r-1} + r! \right) = n\lambda^{r-1} \left(\sum_{i=1}^{r} s(r,i) \sum_{j=0}^{i-1} C_i^j r^{i-j} \sum_{k=1}^{j} S(j,k)\lambda^k - r^2\lambda^{r-1} + r! \right),$$

where $S(j, k)$ is the Stirling number of the second kind [10].

Corollary 1. *For $r = 2$, the following expressions for the parameters of the asymptotically normal probability distribution of the random variable Z_2 take place:*

$$\mu_2 = n\lambda, \ \sigma_2^2 = 2n\lambda.$$

The statistical estimators of Rényi and Tsallis entropy are expressed in terms of Z_r [11]:

$$\hat{H}_r(n, N) = \frac{1}{1-r} \ln\left(\sum_{k=1}^{N} \frac{\nu_k^{\underline{r}}}{n^r} \right) = \ln n + \frac{1}{r-1} \left(\ln n - \ln Z_{n,r} \right), \quad (14)$$

$$\hat{S}_r(n, N) = \frac{1}{r-1} \left(1 - \sum_{k=1}^{N} \frac{\nu_k^{\underline{r}}}{n^r} \right) = \frac{1}{r-1} \left(1 - \frac{Z_{n,r}}{n^r} \right). \quad (15)$$

The theorems on the asymptotic probability distribution of statistical estimators of Rényi and Tsallis entropy, which are based on [5], are proved by the authors [11] and allow us to

construct the interval estimators. We also give corollaries of the theorems for the most commonly used particular case $r = 2$.

Theorem 2. *In the asymptotics* (3)*, the statistic* (14) *is a consistent estimator of Rényi entropy and, under the true hypothesis* H_**, has the asymptotically normal distribution*: $\mathrm{L}\left\{\frac{H_r - \mu_{H,r}}{\sigma_{H,r}}\right\} \to N_1(0,1)$,

$$\mu_{H,r} = \ln N, \tag{16}$$

$$\sigma^2_{H,r} = \frac{\sum_{i=1}^{r} s(r,i) \sum_{j=0}^{i-1} C_i^j r^{i-j} \sum_{k=1}^{j} S(j,k) \lambda^k - r^2 \lambda^{r-1} + r!}{(r-1)^2 n \lambda^{r-1}}. \tag{17}$$

Corollary 2. *For* $r = 2$*, the variance of the estimator* (14) *is*

$$\sigma^2_{H,2} = \frac{2}{n\lambda}.$$

Note that $p_k = 1 / N$, $k = 1, \ldots, N$ with the true hypothesis H_*, therefore the value of the Rényi entropy equals $H_r(P) = \frac{1}{1-r} \ln\left(\sum_{k=1}^{N} p_k^r\right) = \frac{1}{1-r} \ln\left(\sum_{k=1}^{N} \frac{1}{N^r}\right) = \ln N$, that is equal to (16).

Knowing the asymptotic distribution of the consistent point estimator (14) allows us to construct the interval estimator for Rényi entropy:

with probability that equals $1 - \varepsilon$, the entropy

$$H_r(P) \in (H_-, H_+),\ H_\pm = \mu_{H,r} \pm \sigma_{H,r} \Phi^{-1}\left(1 - \frac{\varepsilon}{2}\right). \tag{18}$$

Theorem 3. *In the asymptotics* (3)*, the statistic* (15) *is a consistent asymptotically unbiased estimator of Tsallis entropy and, under the true hypothesis* H_**, has the asymptotically normal distribution* $\mathrm{L}\left\{\frac{S_r - \mu_{S,r}}{\sigma_{S,r}}\right\} \to N_1(0,1)$:

$$\mu_{S,r} = \frac{1}{r-1}\left(1 - \frac{1}{N^{r-1}}\right), \tag{19}$$

$$\sigma^2_{S,r} = \frac{\lambda^{r-1}}{(r-1)^2 n^{2r-1}}\left(\sum_{i=1}^{r} s(r,i) \sum_{j=1}^{i-1} C_i^j r^{i-j} \sum_{k=1}^{j} S(j,k) \lambda^k - r^2 \lambda^{r-1} + r!\right). \tag{20}$$

Corollary 3. *For* $r = 2$*, the mathematical expectation and the variance of statistic* (15) *are respectively:*

$$\mu_{S,2} = 1 - \frac{1}{N},\ \sigma^2_{S,2} = \frac{2}{Nn^2}.$$

Knowing the asymptotic distribution of the consistent point estimator (15) allows us to construct the interval estimator for Tsallis entropy:

with probability that equals $1 - \varepsilon$, the entropy

$$S_r(P) \in (S_-, S_+),\ S_\pm = \mu_{S,r} \pm \sigma_{S,r} \Phi^{-1}\left(1 - \frac{\varepsilon}{2}\right). \tag{21}$$

IV. Testing of "Pure Randomness" by Entropy Estimators

The obtained interval estimators (9), (18) and (21) allow us to construct the decision rule for testing hypotheses about whether the observed generator's output sequence is "pure random" sequence: H_* and $\overline{H_*}$. Let $\varepsilon \in (0, 1)$ be a given significance level. We introduce the notation: $\hat{h}$ is the statistical estimate of the Shannon (6), Rényi (14) or Tsallis (15) entropy, μ_h is the asymptotic expectation of the statistical estimator of Shannon (7), Rényi (16) or Tsallis (19) entropy, σ_h^2 is the asymptotic variance of the statistical estimator of Shannon (8), Rényi (17) or Tsallis (20) entropy under the true hypothesis H_*. We compute the statistic $\hat{h}$ for the observed sequence. The decision rule based on statistic $\hat{h}$ has the form:

$$\begin{cases} H_*, & \text{if } t_- < \hat{h} < t_+; \\ \overline{H_*}, & \text{else;} \end{cases} \quad t_\pm = \mu_h \pm \sigma_h \Phi^{-1}\left(1 - \frac{\varepsilon}{2}\right). \tag{22}$$

If we accept the hypothesis H_*, it can be concluded that, at the significance level ε, the analyzed process is indistinguishable from the "pure random" sequence with respect to its entropic properties on the base of the observed output sequence with the length no longer than n.

The advantage of the developed approach in comparison with other statistical tests is that we can specify different dimensions of the alphabet. For example, if we deal with a binary sequence, we can form s-grams from each s neighboring bits, thereby obtaining an alphabet of dimension 2^s. Applying the decision rule for different values of s, we can improve the decision rule: we assume that the sequence is "pure random" if the proportion of rejections of the hypothesis H_* does not exceed a given significance level. In addition, the dependence of the entropy estimate on the length of the fragment s can also be used to analyze the presence of dependencies in the observed sequence.

 978-1-5090-5689-7/17/$31.00 ©2017 IEEE

V. The Results of Computer Experiments

The developed decision rule (22) with the significance level $\varepsilon = 0.05$ was used to analyze the output binary sequence of a real physical binary random sequence generator [12] $\{y_\tau\}$, $\tau = 1, \ldots, T$, with a length of $T = 125 \cdot 2^{25}$ bits. The output sequence was "cut" into non-overlapping consecutive fragments of length s (s-grams): $X^{(t)} = (X_j^{(t)}) = (y_{(t-1)s+1}, \ldots \quad \{0,1\}^s$, $t = 1, \ldots, n = [T / s]$. From the resulting s-grams, a new sequence $\{x_t\}$ with the dimension of alphabet equals $N = 2^s$ was formed by the rule $x_t = \sum_{j=1}^{s} 2^{j-1} X_j^{(t)} + 1$. The entropy estimates were calculated by the algorithms from [13].

Fig. 1 shows the values of the deviation of Shannon entropy estimate (6) from the mathematical expectation (7) divided by the confidence interval boundaries: $\frac{H - \mu_H}{\sigma_H \Phi^{-1}(1-\varepsilon/2)}$, depending on $s \in \{5, \ldots, 24\}$. Fig. 2 shows the values of the deviation of Rényi entropy estimate (14) at $r = 2$ from the mathematical expectation (16) divided by the confidence interval boundaries: $\frac{H_r - \mu_{H,r}}{\sigma_{H,r} \Phi^{-1}(1-\varepsilon/2)}$, depending on $s \in \{2, \ldots, 30\}$. If the value does not fall into the confidence bandwith $(-1; 1)$, it means that the statistic does not match the confidence interval and the hypothesis H_* is rejected. As can be seen from Fig. 1, at many values of the order s the hypothesis H_* is rejected, which indicates that the output sequence of the generator is differ from the "pure random" sequence. Therefore, as can be seen from Fig. 2, at values $s \le 25$ the output sequence of the generator is consistent with the "pure random" sequence by the value of Rényi entropy estimate.

The decision rules based on the estimators of Shannon and Rényi entropy have given different results. This means that these tests should be applied in a complex: one test can reveal deviations from the "pure random" sequence that another test has not revealed.

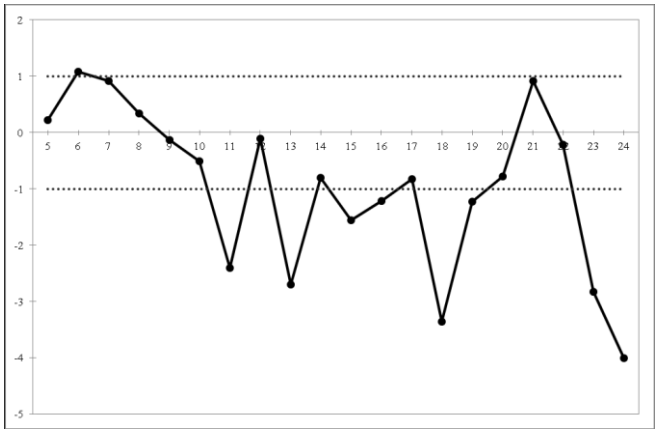

Figure 1. Deviation of Shannon entropy estimate from its expectation for $s \in \{5, \ldots, 24\}$.

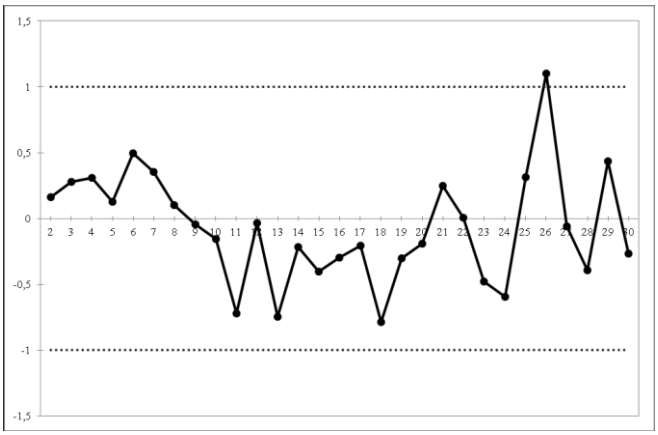

Figure 2. Deviation of Rényi entropy estimate from its expectation for $s \in \{2, \ldots, 30\}$

References

[1] O. Goldreich, "Foundations of Cryptography: Basic Tools". Cambridge: University Press, 2004.

[2] Yu. S. Kharin, S. V. Agievich, D. V. Vasilyev, and G. V. Matveev, "Cryptology" [in Russian]. Minsk: BSU, 2013.

[3] M. D. Esteban and D. Morales, "A summary on entropy statistics", in Kybernetika, 1995, vol. 31, no. 4, pp. 337–346.

[4] P. A. Bromiley, N. A. Thacker, and E. Bouhova-Thacker, "Shannon Entropy, Renyi Entropy, and Information". Available at http://www.tina-vision.net/docs/memos/2004-004.pdf.

[5] L. Holst, "Asymptotic normality and efficiency for certain goodness-of-fit tests", in Biometrika, 1972, vol. 59, no. 1, pp. 137–145.

[6] U. Yu. Palukha, "The probability properties of the multivariate entropy estimator in information security tasks" [in Russian], in Proceedings of the XVII Young Scientists Republican Scientific and Practical Conference, Brest, 2015, Part 1. Brest: BrSU, 2015, pp. 57–59.

[7] U. Yu. Palukha, "Statistical tests based on entropy estimates for checking the hypotheses of the uniform distribution of a random sequence" [in Russian], in Proceedings of the National Academy of Sciences of Belarus: Physics and Mathematics Series, 2017, no. 1, pp. 79–88.

[8] U. Yu. Palukha and Yu. S. Kharin, "Entropy characteristics of binary sequences in cryptography" [in Russian], in Proceedings of the XX Scientific and Practical Conference "Complex Information Protection", Minsk, 2015. Minsk: RIHE, 2015, pp. 99–102.

[9] J. Acharya, A. Orlitsky, A. T. Suresh, and H. Tyagi, "Estimating Renyi Entropy of Discrete Distributions". Available at http://arxiv.org/pdf/1408.1000v3.pdf.

[10] A. Yu Envin, "Discrete mathematics: lecture notes" [in Russian]. Cheliabinsk: YuUrGU, 1998.

[11] Yu. S. Kharin and U. Yu. Palukha, "Statistical estimates of Rényi and Tsallis entropy and their use for testing the hypotheses of "pure randomness"" [in Russian], in Proceedings of the National Academy of Sciences of Belarus: Physics and Mathematics Series, 2016, no. 2, pp 37–47.

[12] speedtest-500MB.bin. Available at http://qrng.physik.hu-berlin.de/files/speedtest-500MB.bin.

[13] U. Yu. Palukha and Yu. S. Kharin, "Calculating of the entropy functionals statistical estimates of binary sequences" [in Russian], in Proceedings of the CSIST'2016. Minsk: BSU, 2016, pp. 472–476.