Journal of Theoretical and Applied Information Technology
30th November 2016. Vol.93. No.2

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

STOCHASTIC METHOD OF DATA TRANSFORMATION RDOZEN+

IVANOV MIKHAIL, STARIKOVSKIY ANDREY, ROSLIY EVGENIY, POPOV ALEKSEY, MAKSUTOV ARTEM, KUSAKIN ILYA, KUTEPOV STANISLAV, BABALOVA IRINA

National Research Nuclear University MEPhI (Moscow Engineering Physics Institute)

Kashirskoe Highway 31, 115409, Moscow, Russian Federation

E-mail: msa@dozen.mephi.ru, avstarikovskij@mephi.ru

ABSTRACT

Analysis of information security threats and the trends in the development of computer technology allows to make an unambiguous conclusion about the increasing role of stochastic methods of information protection. The most promising method of protection, namely the method of introducing the unpredictability in the work of the funds and the objects protection is universal. It can be used in conjunction with any other method of protection automatically raising their quality. A special case of stochastic methods are cryptographic methods of information protection. The trend of recent years has been the advent of algorithms based on the use of 2D and 3D stochastic transformations. This article proposes a new algorithm of 3D stochastic data transformation, which is basically aimed for information security solutions. The algorithm is characterized by the high degree of parallelism at the level of elementary operations.

Keywords: *Cryptographic Primitives, 3D Transformation, Cube Architecture, Iterative Stochastic Transformation, MixState Transformation.*

1. INTRODUCTION

Information security threats analysis and analysis of trends in IT development allows making an unambiguous conclusion about the constantly increasing role of stochastic methods of information security. Methods are called stochastic if they are directly or indirectly based on the pseudo-random number generators (PRNG) [1-3]. As an example of a general stochastic method of information security (IS), a method of introducing uncertainty to the means and objects of information security implementation can be mentioned. The uncertainty can be inserted even in the result of the information protection algorithm [4-8].

Every problem of IS can be successfully solved by means of PRNG. Thus, in some cases, stochastic methods are the only possible mechanism to ensure information security from an active intruder. A special case of the stochastic methods are cryptographic methods of information security.

The term "stochastic" in the context of IS for the first time, apparently, was used by S.A. Osmolovsky when developing codes for detecting and correcting errors occurring during data transmission through communication channels [9-10]. The proposed stochastic codes have unique properties, we highlight two: ability to ensure the prescribed probability of correct information reception and ability (in addition to providing noise immunity) to solve the other two equally important tasks of IS: to ensure privacy and integrity of the transmitted information.

A stochastic 3D transformation algorithm DOZEN of Cube architecture aimed for implementation using hybrid (Heterogeneous) supercomputing technologies is proposed in [11-13]. The 3D transformations are characterized by the high degree of parallelism at the level of elementary operations. Building cryptographic primitives of pseudo-random numbers generation, hash, block and stream encryption is the field of application of nonlinear multiple stochastic transformations [11], [14-15]. The new transformation of the DOZEN family is discussed.

The article discusses the DOZEN + 3D transformation, essentially the 3D version of Kuznyechik algorithm [16]. There is a lack of the algorithm is its inefficient software implementation. The proposed solution to the problem is a new

Journal of Theoretical and Applied Information Technology
30th November 2016. Vol.93. No.2

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

algorithm of the DOZEN family, called RDOZEN +.

2. ADVANCED ENCRYPTION STANDARD

In 1997, the U.S. National Institute of Standards and Technology announced the launch of a program for the adoption of the new standard of cryptographic protection to replace the existing 1974 DES (data encryption standard) algorithm – the most popular cryptographic algorithms in the world at that time. DES is outdated in many respects: the key length, ease of implementation on modern processors, speed, ect., except for the most important one – resistance. Over 25 years of intensive analysis of the resistance there were found no methods to break it that were significantly different from the performance of exhaustive search in the keyword space. In October 2000, the contest was won by the Belgian algorithm Rijndael [17] as having the best combination of durability, performance, effectiveness of implementation, flexibility. Its low memory requirements makes it ideal for embedded systems. The cipher authors are Joan Daemen and Vincent Rijmen.

The interim results of changes carried out in the framework of the algorithm, called states. The states, i.e. all input data blocks, all intermediate results of the transformations, all the output data blocks, as well as round keys can be represented in the form of a square array of 4×4 bytes.

The direct E AES-128 conversion consists of the addition of the initial round key (9 rounds) the final round. In the final round, there is no column mixing operation. The purpose of this decision is to minimize the differences in direct and inverse transformation, respectively, E and D. The round keys are generated from the original key using KeyExpansion procedure.

The new architecture which is built using the E conversion is called Square. Two rounds of transformation ensure complete diffusion and confusion of information. Even slight changes in the non-linear function input leads to unpredictable changes in the output (in average, half of the bits changes).

The square architecture opened new and interesting area of symmetric encryption algorithms. In 2002 after adaption of the AES, the mass emergence of 2D and 3D cryptographic algorithms took place.

3. PAGE LAYOUT DOZEN+ TRANSFORMATION

Consider the 3D DOZEN+ transformation essentially a modified version of the 3D Kuznyechik algorithm [16].

The DOZEN+ transformation sequence for a block M of data, 512 bits size (4 × 4 × 4 × 8), having the structure shown in Fig. 1a, where $a_{x,\,y,\,z}$, $x = 0, 1, 2, 3$, $y = 0, 1, 2, 3$, $z = 0, 1, 2, 3$, are bites, is as follows:

- add (XOR) round key K_0 to the data block;
- the first round (*MixLayersX* transformation): divide the resulting data block into Layers S_{x0}, S_{x1}, S_{x2}, S_{x3} along the x-axis (Fig. 1b); conduct a two-dimensional stochastic transformation (*MixLayer*) of layers S_{x0}, S_{x1}, S_{x2}, S_{x3} by performing sixteen (number of bytes) *SubBytes* operations, *MixState* operation and *AddRoundSubKey* operation for each layer S_{xj};
- the second round (*MixLayersY* transformation): divide the resulting data block into Layers S_{y0}, S_{y1}, S_{y2}, S_{y3} along the y-axis; conduct a two-dimensional stochastic transformation *(MixLayer)* of layers S_{y0}, S_{y1}, S_{y2}, S_{y3} by performing sixteen (number of bytes) *SubBytes* operations, *MixState* operation and *AddRoundSubKey* operation for each layer S_{yj};
- third round (*MixLayersZ* transformation): divide the resulting data block into Layers S_{z0}, S_{z1}, S_{z2}, S_{z3} along the z-axis; conduct a two-dimensional stochastic transformation (*MixLayer*r) of layers S_{z0}, S_{z1}, S_{z2}, S_{z3} by performing sixteen (number of bytes) SubBytes operations, *MixState* operation and *AddRoundSubKey* operation for each layer S_{zj};

The round keys K_0, K_1, K_2, K_3 are generated from initial key K using the *KeyExpansion* procedure.

Thus, the sequence of the 3D nonlinear multilayer transformation DOZEN+ has the form shown in Fig.2a and is defined as follows:

$$S = M;\ C = DOZEN+(M) = MixLayersZ(K_3, MixLayersY(K_2, MixLayersX(K_1, (S \oplus K_0))));$$

$$MixLayersX(K_1, S) =$$
$$= MixLayer(K_{13}, S_{x3}) \parallel MixLayer(K_{12}, S_{x2}) \parallel MixLayer(K_{11}, S_{x1}) \parallel MixLayer(K_{10}, S_{x0});$$

$$MixLayersY(K_2, S) =$$
$$= MixLayer(K_{23}, S_{y3}) \parallel MixLayer(K_{22}, S_{y2}) \parallel MixLayer(K_{21}, S_{y1}) \parallel MixLayer(K_{20}, S_{y0});$$

$$MixLayersZ(K_3, S) =$$

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

$$= MixLayer(K_{33}, S_{z3}) \| MixLayer(K_{32}, S_{z2}) \| MixLayer(K_{31}, S_{z1}) \| MixLayer(K_{30}, S_{x0});$$

$$MixLayer(K_{ij}, S_{mj}) = = AddRoundSubKey(K_{ij}, (MixState(SubBytes(S_{mj})))) = MixState(SubBytes(S_{mj})) \oplus K_{ij};$$

$$| M | = | S | = | K_i | = 512, | S_{mj} | = | K_{ij} | = 128; i = 0, 1, 2, 3; j = 0, 1, 2, 3; m = x, y, z;$$

$$K_i = K_{i3} \| K_{i2} \| K_{i1} \| K_{i0}, S = S_{x3} \| S_{x2} \| S_{x1} \| S_{x0} = S_{y3} \| S_{y2} \| S_{y1} \| S_{y0} = S_{z3} \| S_{z2} \| S_{z1} \| S_{z0};$$

where M is data input block, S is the state of the algorithm; K_i are round keys, *SubBytes* is the byte-substitution transformation of the layer state S_{mj}; *Mix-State* is the shuffle transformation of the layer state S_{mj}; *MixLayersX* is the layer-based transformation along the x-axis; S_{x3}, S_{x2}, S_{x1}, S_{x0} are the layers of the state along the x-axis; *MixLayersY* is the layer-based transformation along the y-axis; S_{y3}, S_{y2}, S_{y1}, S_{y0} are the layers of the state along the y-axis; *MixLayersZ* is the layer-based transformation along the z-axis; S_{z3}, S_{z2}, S_{z1}, S_{z0} are the layers of the state along the z-axis.

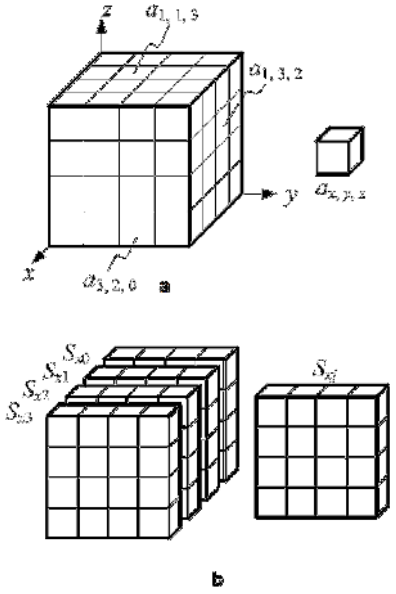

Figure 1: 3D data stochastic transformation algorithms: a – the format of the data block (state) and round keys K_i, b – state division into layers along the x-axis.

Let Q be the state of the layer: $| Q | = 128$, $Q = (Q_{16} \ldots Q_1)$, $Q_i \in GF(2^8)$, $i = 1, \ldots, 16$. Nonlinear transformation SubBytes (layer state byte substitution) is defined as follows:

$$SubBytes(Q) = SubBytes(Q_{16} \| \ldots \| Q_1) = SubByte(Q_{16}) \| \ldots \| SubByte(Q_1),$$

where $SubByte(Q_i)$ is bite Qi substitution transformation. Linear stochastic transformation MixState (mixing layer state) on the basis of PRNG operating in $GF(2^8)$ and designed according to the concept of Galois, is determined by the following expressions:

$$MixState(Q) = = R^{16}(Q) = R^{16}(Q_{16} \| \ldots \| Q_1) = (a_{16}Q_1 \| Q_{16} + a_{15}Q_1 \| \ldots \| Q_2 + a_1Q_1)^{16} = QT^{16},$$

where all operations are conducted in the field $GF(2^8)$, $a_i \in GF(2^8)$are the coefficients of the characteristic polynomial $\varphi(x) = a_{16}x^{16} + a_{15}x^{15} + a_{14}x^{14} + \ldots + a_2x^2 + a_1x - 1$, which is primitive over the field $GF(2^8)$, T is the square matrix of the order 16 × 16, like:

$$\begin{pmatrix} 0 & 1 & 0 & \ldots & 0 & 0 \\ 0 & 0 & 1 & \ldots & 0 & 0 \\ 0 & 0 & 0 & \ldots & 0 & 0 \\ \ldots & \ldots & \ldots & & \ldots & \ldots \\ 0 & 0 & 0 & \ldots & 1 & 0 \\ 0 & 0 & 0 & \ldots & 0 & 1 \\ a_{16} & a_{15} & a_{14} & \ldots & a_2 & a_1 \end{pmatrix}.$$

The equation of the basic linear transformation R (multiplication of the state of the layer Q by T) is like:

$$\begin{cases} Q_j = Q_{j+1} + a_jQ_1, j = 1, \ldots, 15, \\ Q_{16} = a_{16}Q_1. \end{cases}$$

4. DOZEN+ TRANSFORMATION

The RDOZEN+ transformation sequence for a block M of data, 512 bits size (4 × 4 × 4 × 8), having the structure shown in Fig. 1a, is as follows:

- add (XOR) round key K_0 to the state ($S = M$);
- the first round (*MixLayersX* transformation): divide the state into Layers S_{x0}, S_{x1}, S_{x2}, S_{x3} along the x-axis (Fig. 1,b); conduct a two-dimensional stochastic transformation (*MixLayer*) of layers S_{x0}, S_{x1}, S_{x2}, S_{x3} by performing sixteen (number of bytes) *SubByte* operations, *MixState* operation and *AddRoundSubKey* operation for each layer S_{xj};
- preparations for the second round: repositioning of state bytes by executing the RandPermBytes transformation and forming thereby a new "pseudocube", i.e. the new data block, 512 bits size (4 × 4 × 4 × 8) having the structure shown in Fig. 1, but with a different division into columns, rows and layers;
- the second round (entirely similar to the first);
- preparations for the third round – forming a new "pseudocube" with a different division into columns, rows and layers;

Journal of Theoretical and Applied Information Technology
30th November 2016. Vol.93. No.2

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

- the third round (entirely similar to the first and the second);

The round keys K_0, K_1, K_2, K_3 and shuffling keys k_1 и k_2 are generated from initial key K using the *KeyExpansion* procedure.

Thus, the sequence of the 3D nonlinear multilayer transformation RDOZEN+ has the form shown in Fig. 2b and is defined as follows:

$$S = M;\ C = RDOZEN+(M) =$$
$$= MLX(K_3,\ RPBytes(k_2,\ (MLX(K_2,\ RPBytes(k_1,$$
$$(MLX(K_1,(S \oplus K_0)))))));$$

$$MixLayersX(K_i,\ S) =$$
$$= MixLayer(K_{i3},\ S_{x3}) \parallel MixLayer(K_{i2},\ S_{x2}) \parallel$$
$$MixLayer(K_{i1},\ S_{x1}) \parallel MixLayer(K_{i0},\ S_{x0});$$
$$MixLayer(K_{ij},\ S_{xj}) =$$
$$= ARSKey(K_{xj},\ (MixState(SubBytes(S_{xj})))) =$$
$$MixState(SubBytes(S_{xj})) \oplus K_{ij};$$

where *MLX* is a *MixLayersX* transformation, *ARSKey* is a *AddRoundSubKey* transformation, *RPBytes* is a *RandPermBytes* transformation.

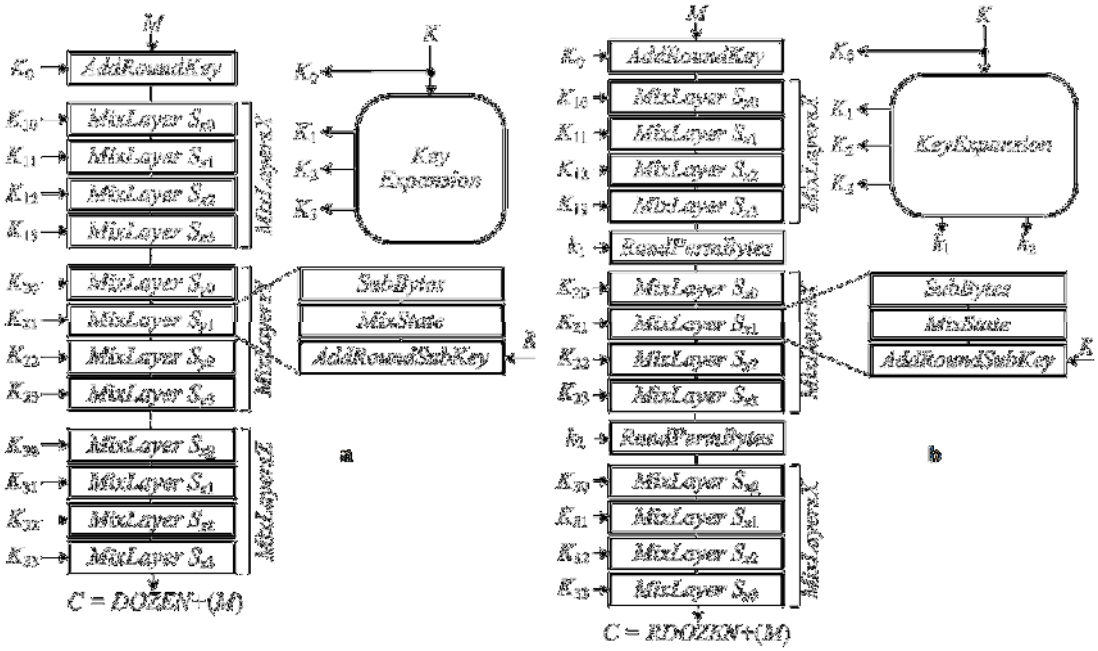

Figure 2: 3D data stochastic transformation algorithms: a – the sequence of transformations in DOZEN+ algorithm, b – the sequence of transformations in RDOZEN+ algorithm.

Consider the example of a high-speed implementation of a byte-swap operation (Fig. 3), similar to that used in stream cipher RC4 [12], [18]. Let k_i be the i-th byte of the transformation key k, S_i be the i-th state byte (interim calculation result before performing the PermBytes operation), then the sequence of shuffle can be described as follows:

Initialize the variable j: $j = 0$;

For each $i = 0, 1, \ldots, 63$

calculate $j = (j + S_i + k_i) \bmod 64$;

state bytes rearrangement: $S_i \leftrightarrow S_j$.

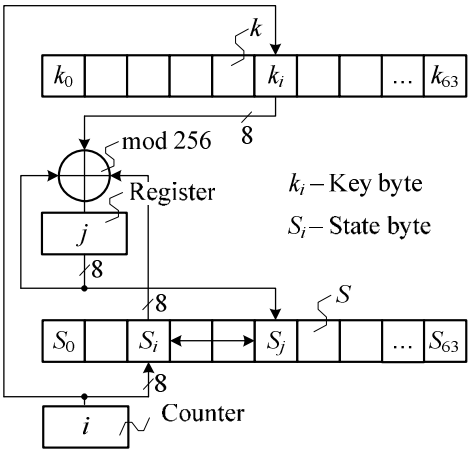

Figure 3: Scheme of the state S bytes rearrangement

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

4. CONCLUSION

The high degree of parallelism at the level of elementary transformations is characteristic for the proposed algorithm RDOZEN+ due to the possibility of parallel execution of MixLayer operations. Thus, the use of CUDA technology [19-20] allows to significantly simplify the process of software development. In the transformation RDOZEN + via eliminating transitions from MixLayer transformation performed along the axis x to MixLayer transformation performed along the axis y, and then to MixLayer transformation performed along the axis z, performance of the algorithm in its software implementation improves, since instead of layers shuffling transformations sequentially along the axes x, y, z, layers transformation of the same type is performed three times along the axis x, an operation of forming a new state by repositioning its bytes is performed in between. The RDOZEN+ algorithm is an evolution of the DOZEN+ algorithm, which, in its turn, is a 3D version of the Kuznyechik algorithm specified in the new Russian encryption standard [16]. The transformation MixState RDOZEN + built on the basis of the PRNG functioning on the Galois scheme provides better information diffusion and confusion than a similar transformation *L* of the Kuznyechik cipher, built on the PRNG, functioning on the basis of the Fibonacci pattern. For cycle in the PRNG built on the Galois scheme, the status of all registers PRNG changes (with corresponding choice of the characteristic polynomial), rather than one that receives a signal Feedback, as in the case of PRNG functioning on the basis of the Fibonacci pattern.

Testing RDOZEN + algorithm by the NIST technique [21-22] showed the statistical security of it.

ACKNOWLEDGMENT

The publication is prepared in accordance with the scientific research under the Agreement between the Federal State Autonomous Educational Institution of Higher Education "National Research Nuclear University MEPhI" and the Ministry of Education and Science № 14.578.21.0117 on 27.10.2015. The unique identifier for the applied scientific research (project) is RFMEFI57815X0117.

REFRENCES:

[1] O. Goldreich, Modern Cryptography, Probabilistic Proofs and Pseudorandomness, vol. 17 of Algorithms and Combinatorics. Berlin: Springer-Verlag, 1999.

[2] O. Goldreich, A Primer on Pseudorandom Generators, vol. 55 of University Lecture Series. Providence, RI: American Mathematical Society, 2010.

[3] Toby Prescott. Random Number Generation Using AES. Date Views 30.10.2016 http://www.atmel.com/Images/article_random_number.pdf.

[4] M. Bellare and P. Rogaway. Optimal asymmetric encryption. In, R. Rueppel editor, Advances in Cryptology - Eurocrypt'94, Lecture Notes in Computer Science, volume 950, pages 92--111. Springer Verlag, 1994.

[5] M. Bellare, S. Goldwasser, and D. Micciancio, "Pseudo-Random" number generation within cryptographic algorithms: The DDS case, in CRYPTO, vol. 1294 of Lecture Notes in Computer Science, (B. S. K. Jr., ed.), pp. 277–291, Springer, 1997.

[6] S. Goldwasser and S. Micali, "Probabilistic Encryption," Journal of Computer and System Sciences, vol. 28, pp. 270–299, April 1984.

[7] RSAES-OAEP Encryption Scheme. RSA Security Inc., 2000.

[8] Johannes Boeck, RSA-PSS – Provable secure RSA Signatures and their Implementation http://rsapss.hboeck.de/ May 4, 2011.

[9] Osmolovsky, S.A., 1991. Stochastic Methods of Data Transmission. Moscow: Radio i Svyaz.

[10] Osmolovsky, S.A., 2003. Stochastic Methods of Information Defense. Moscow: Radio i Svyaz.

[11] Three-Dimensional Pseudo-Random Number Generator for Implementating in Hybrid Computer Systems. M. A. Ivanov, N. P. Vasilyev, I. V. Chugunkov et. al. // Vestnik NRNU MEPhI, 2012, Vol. 1, № 2.

[12] Ivanov, M.A. and I.V. Chugunkov, 2012.Cryptographic Methods of Information Defense in the Computer Systems and Networks: Teaching Guide. Moscow: National Research Nuclear University MEPhI.

[13] Three-Dimensional Data Stochastic Transformation Algorithms for Hybrid Supercomputer Implementation / Ivanov M.A., Spiridonov A.A., Chugunkov I.V., et. al. – Proceedings of 17th IEEE Mediterranean

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Electrotechnical Conference (MELECON), 2014, Beirut, Lebanon, pp. 451 – 457.

[14] Nakahara, Jorge Jr. 3D: A Three-Dimensional Block Cipher. Date Views 07.06.2016 infoscience.epfl.ch/record/128649/files/Nak08.pdf

[15] Keccak sponge function family. Main document. Guido Bertoni, Joan Daemen, Michael Peeters, Gilles Van Assche. Date Views 07.06.2016 keccak.noekeon.org/Keccak-main-2.1.pdf

[16] GOST R 34.12─ 2015. Informacionnaja tehnologija. KRIPTOGRAFIChESKAJa ZAShhITA INFORMACII. Blochnye shifry. – Moskva, Standartinform, 2015. (ГОСТ Р 34.12─ 2015. Информационная технология. КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ. Блочные шифры. – Москва, Стандартинформ, 2015.)

[17] Daemen, Joan, Vincent Rijmen. AES Proposal: Rijndael. Date Views 07.06.2016 citeseerx.ist.psu.edu/viewdoc/download;jsessionid=53629D362985331263F38DB3A1667573?doi=10.1.1.36.640&rep=rep1&type=pdf

[18] William Stallings, THE RC4 STREAM ENCRYPTION ALGORITHM Date Views 30.10.2016 vanila47.com/PDFs/Cryptography/RC4%20Stream%20Cipher/Tutorials/THE%20RC4%20STREAM%20ENCRYPTION%20ALGORITHM.pdf

[19] Боресков А.В., Харламов А.А. Основы работы с технологией CUDA. М.:ДМК Пресс, 2011.

[20] CUDA Zone. [Электронный ресурс] : URL http://developer.nvidia.com/category/zone/cuda-zone

[21] A. Rukhin, J. Soto, J. Nechvatal, M. Smid, E. Barker, S. Leigh, M. Levenson, M. Vangel, D. Banks, A. Heckert, J. Dray, and S. Vo, A statistical test suite for random and pseudorandom number generators for cryptographic applications. NIST Special Publications 800-22. Revision 1.a. April, 2010.

[22] Reducing of Memory Usage in Statistical Research into Pseudorandom Number Generators by Validation Tests. Chugunkov I.V., Kutepov S.V., Shustova L.I. et. al. Proceedings of The Radio-Electronic Devices and Systems for the Infocommunication Technologies (REDS-2013), Moscow, Russia, May 22-23, 2013, pp.148-152.