New Life of Old Standard: Transition from One-Dimensional Version to 3D

Mikhail A. Ivanov, Andrey V. Starikovskiy

National Research Nuclear University “MEPhI” (Moscow Engineering Physics Institute)
Kashirskoe highway 31, 115409, Moscow, Russian Federation
maivanov@mephi.ru

Abstract
The trend of recent years has been the advent of 2D and 3D cryptographic transformations. Stand-ards that have appeared in the 21st century, specify algorithms based on the use of 2D and 3D transformations (AES, Kuznechik, Keccak, Stribog). In the article a 3D version of cryptographic transformation specified by GOST 28147-89 is suggested. The 3D GOST algorithm is characterized by the high degree of parallelism at the level of elementary operations. Increasing bit depth of the processed data blocks from 64 to 512 bits al-lows 3D GOST to be used for the synthesis of hash algorithms. Algorithm improvement agenda may be similar to the DOZEN family of algorithms.

Keywords: Block cipher, 2D transformation, 3D transformation, GOST, DOZEN

1 Introduction

Information security threats analysis and analysis of trends in IT development allows making an unambiguous conclusion about the constantly increasing role of cryptographic methods of information security. Thus, in some cases, cryptographic methods are the only possible mechanism to ensure information security.

The trend of recent years has been the advent of 2D and 3D cryptographic transformations. Standards that have appeared in the 21st century specify algorithms based on the use of 2D and 3D transformations (AES, Kuznechik, Keccak, Stribog algorithms). (Daemen 2016, GOST R 34.12-2015, Bertoni 2016, GOST R 34.11-2012)

A new standard GOST 34.12-2015 came into operation on the 1st of January, 2016. It specifies two cryptographic algorithms: a 128-bit Kuznechik algorithm and a 64-bit Magma algorithm. Moreover, the latter is a weakened version of the reputable cryptographic algorithm specified in GOST 28147-89 (further - old GOST). The article describes a 3D version of GOST 28147-89 (further - 3D GOST), which, authors dare to hope, will prolong even more the "lifetime" of the old GOST.

2 GOST 28147-89

Old GOST specified an iterative block cipher and modes of its use. Bit depth of a data block was equal to 64 bits, the number of rounds of transformation was 32. The cipher had the traditional round structure that is called a Feistel loop. The whole architecture in general is called a balanced Feistel network. Before the adoption of the AES standard old GOST could be rightly considered the simplest block cipher in the world. It is no accident, that one of the first articles describing the old GOST called "GOST is not simple... but very simple" (Vinokurov 1995).

Advantages of the old GOST:

- Simple and clear architecture;
- Effective implementation on the 32-bit platform;
- Huge, even excessive margin of safety;
- An original, two-stage design of the random number generator specified for counter mode.

3 3D GOST

So, the purpose of the proposed decision is a "life extension" of an overall very good cryptographic algorithm, which became obsolete, among other things due to a small bit depth of the processed data blocks.

The main features of the iterative block cryptographic algorithm 3D GOST are:

- representation of the input, output data units and all intermediate results of transformation as a cubic array of 8 by 8 by 8 bits (Fig 1, a.);
- introduction of the concept of Layer, conventionally represented in the form of a square array of 8 by 8 bits (Figure 1, b, c, d.);
- Implementation of the transformation operation (mixing) of the layer (MixLayer) in the form of n rounds of the old GOST (Fig 2), wherein n is an even number of rounds that is to ensure complete mixing and dispersion of information (for the old GOST $n \geq 6$);
- execution of three rounds of three-dimensional transformation respectively along the axes x, y, z (Figure 3);
- During the first round of transformations data block S is divided into 8 layers Sx0, Sx1, …, Sx7 along axis x; every layer Sxk , k = 0, 1, … , 7, conventionally represented in the form of a square array of 8 by 8 bits (Figure 1, b); afterwards it is subjected to MixLayer transformation, then the transformed layers are joined into a transformed block S;
- During the second round of transformations data block S is divided into 8 layers Sy0, Sy1, …, Sy7 along axis y; every layer Syk , k = 0, 1, … , 7, conventionally represented in the form of a square array of 8 by 8 bits (Figure 1, c); afterwards it is subjected to MixLayer transformation, then the transformed layers are joined into a transformed block S;
- During the third round of transformations data block S is divided into 8 layers Sz0, Sz1, …, Sz7 along axis z; every layer Szk, k = 0, 1, … , 7, conventionally represented in the form of a square array of 8 by 8 bits (Figure 1, d); afterwards it is subjected to MixLayer transformation, then the transformed layers are joined into a transformed block S.

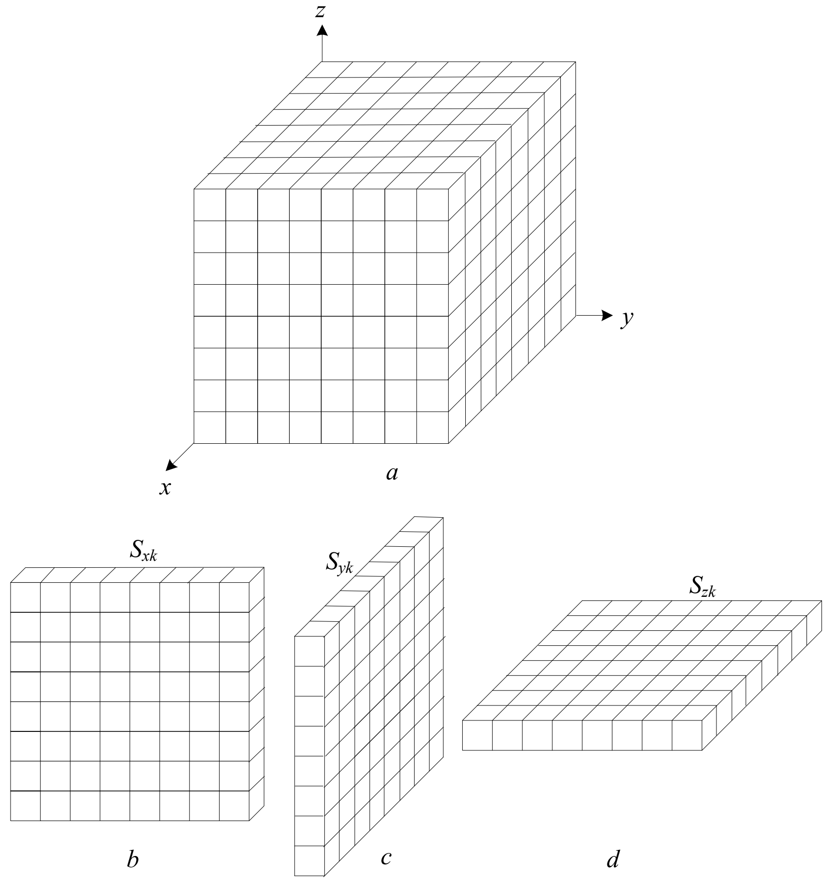

Figure 1: 3D GOST transformation: *a* – data block (cryptographic algorithm state), *b* – layer S_{xk} , *c* – layer S_{yk} , *d* – layerS_{zk}, $k = 0, 1, …, 7$.

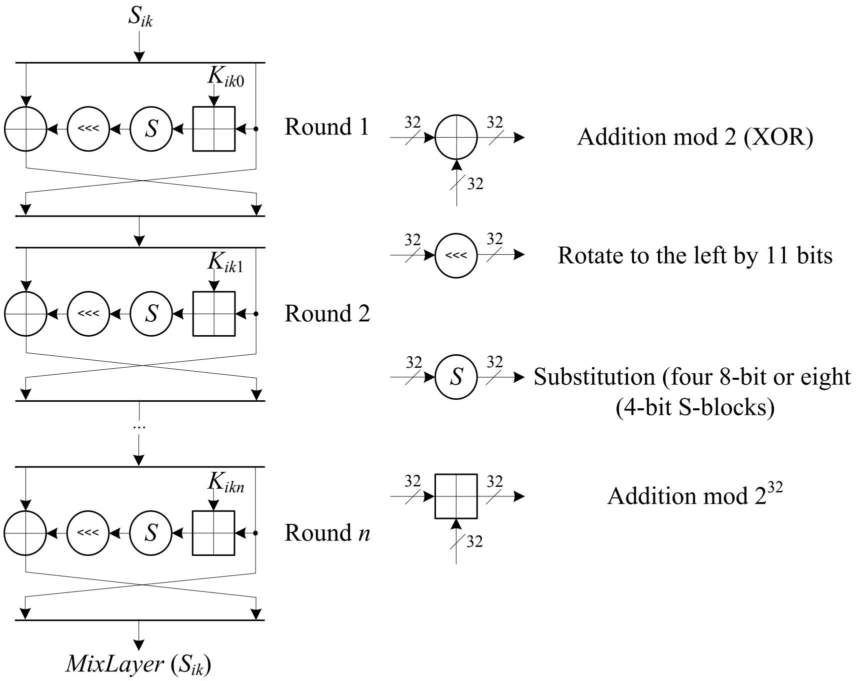

Figure 2: Mixing layer transformation MixState

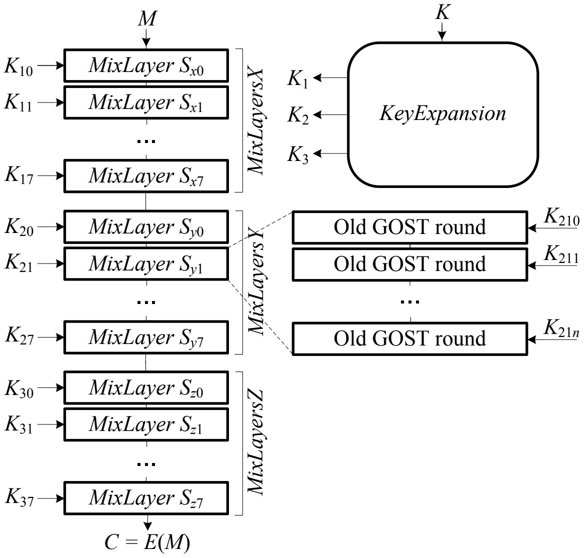

Figure 3: Sequence of 3D GOST transformation execution

3D GOST transformation sequence is shown in Fig. 3. Select a secret table of substitutionss with dimensions of the 4×8×256 (in case of the four 8-bit S-boxes) or 8×4×16 (in case of eight 4-bit S-boxes). A sequence of round keys K1, K2, K3 of 32 × n × 8 bit each is created from initial key K. Every i-th round key Ki (i = 1, 2, 3) is divided into eight round subkeys Ki0, Ki1, …, Ki7 32 × n bit each; wherein

$$K_{ik} = K_{ik0} \,||\, K_{ik1} \,||\, \ldots \,||\, K_{ikn}, \; \left| K_{ikj} \right| = 32.$$

According to the input block M with bit depth equal to 512 bit a data block S of the same bit depth is formed in accordance with the expression S := M, After that three rounds of transformations are conducted along axises x, y, z, as described above.

4 Conclusion

The high degree of parallelism at the level of elementary transformations is characteristic for the proposed algorithm 3D GOST due to the possibility of parallel execution of MixLayer opera-tions. Thus, the use of CUDA technology (Boreskov 2011, CUDA Zone) allows to significantly simplify the process of software development. Increasing the bit depth of the processed data blocks from 64 to 512 bits allows 3D GOST to be used for the synthesis of hash algorithms. Algorithm improvement agenda may be similar to the DOZEN family of algorithms (Ivanov 2014, Ivanov 2016). For example, a hybrid architecture can be implemented. The essence of it is sequential and parallel composition of round transfor-mations MixLayers. Such a design allows to increase resistance of the transformations without decrease in performance during software and hardware implementation.

Testing 3D GOST algorithm by the NIST technique (NIST 2010, Chugunkov, 2013) showed the statistical security of it.

5 Acknowledgement

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.

References

1. Daemen, Joan, Vincent Rijmen. AES Proposal: Rijndael. Dated 07.06.2016 citeseerx.ist.psu.edu/viewdoc/download;jsessionid=53629D362985331263F38DB3A1667573?doi=10.1.1.36.640&rep=rep1&type=pdf
2. GOST R 34.12-2015. Information Technology. Cryptographic Information Defense. Block Ciphers, 2015. Moscow: Standartinform.
3. Guido Bertoni, Joan Daemen, Michael Peeters, Gilles Van Assche.Keccak sponge function family. Main document. Dated 07.06.2016 http://keccak.noekeon.org/Keccak-main-2.1.pdf.
4. GOST R 34.11-2012. Information Technology. Cryptographic Information Defense. Hash function. 2012. Moscow: Standartinform.
5. Vinokurov A. Yu. GOST ne prost …, a ochen' prost! // Monitor, 1995, No 1, p. 60-73
6. Boreskov A.V., Kharlamov A.A. Basics with CUDA technology. Moscow: DMK Press, 2011.
7. CUDA Zone. [Electronic resource]: URL http://developer.nvidia.com/category/zone/cuda-zone
8. Ivanov M.A., Spiridonov A.A., Chugunkov I.V., et. al. Three-Dimensional Data Stochastic Transformation Algorithms for Hybrid Supercomputer Implementation / Proceedings of 17th

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

9. Ivanov M. A., Matveychikov I. V., Skitev A. A., Strelchenko P. A. Three New Methods of Stochastic Data Transformation. Proceedings of The Radio-Electronic Devices and Systems for the Infocommunication Technologies (REDS-2016), Moscow, Russia, May 22-23, 2016, pp.300-302.
10. A statistical test suite for random and pseudorandom number generators for cryptographic applications. NIST Special Publications 800-22. Revision 1.a. April, 2010.
11. Chugunkov I.V., Kutepov S.V., Shustova L.I. et. al. Reducing of Memory Usage in Statistical Research into Pseudorandom Number Generators by Validation Tests. Proceedings of The Radio-Electronic Devices and Systems for the Infocommunication Technologies (REDS-2013), Moscow, Russia, May 22-23, 2013, pp.148-152.