Symmetric Encryption for Error Correction

Nikolai Moldovyan
St. Petersburg Institute
for Informatics and Automation of
the Russian Academy of Sciences
St. Petersburg
nmold@domain.edu

Alla Levina, Sergey Taranov
ITMO University
Saint Petersburg
$alla\_levina, serg.tvc$@mail.ru

***Abstract*—The article presents applying basis of symmetric encryption (block ciphering) in the area of coding theory, a specially in detecting and correcting errors of various types: bit inversion, insertion and skipping. For the case of bit inversion, it has been formulated the conditions of guaranteed fix for a given number of errors.**

I. Introduction

Symmetric-key algorithms are algorithms for cryptography that use the same cryptographic keys for both encryption of plaintext and decryption of ciphertext. The keys may be identical or there may be a simple transformation to go between the two keys [1]. The keys, in practice, represent a shared secret between two or more parties that can be used to maintain a private information link. This requirement that both parties have access to the secret key is one of the main drawbacks of symmetric key encryption, in comparison to public-key encryption (also known as asymmetric key encryption).

Symmetric ciphers are commonly used to achieve other cryptographic primitives than just encryption.

Encrypting a message does not guarantee that this message is not changed while encrypted. Hence often a message authentication code is added to a ciphertext to ensure that changes to the ciphertext will be noted by the receiver. Message authentication codes can be constructed from symmetric ciphers (e.g. CBC-MAC).

However, symmetric ciphers cannot be used for non-repudiation purposes except by involving additional parties. See the ISO/IEC 13888-2 standard.

Another application is to build hash functions from block ciphers. See one-way compression function for descriptions of several such methods.

In this paper we consider the using of block ciphers for error correction.

In information theory and coding theory with applications in computer science and telecommunication, error detection and correction or error control are techniques that enable reliable delivery of digital data over unreliable communication channels. Many communication channels are subject to channel noise, and thus errors may be introduced during transmission from the source to a receiver. Error detection techniques allow detecting such errors, while error correction enables reconstruction of the original data in many cases.

The general idea for achieving error detection and correction is to add some redundancy (i.e., some extra data) to a message, which receivers can use to check consistency of the delivered message, and to recover data that has been determined to be corrupted. Error-detection and correction schemes can be either systematic or non-systematic: In a systematic scheme, the transmitter sends the original data, and attaches a fixed number of check bits (or parity data), which are derived from the data bits by some deterministic algorithm. If only error detection is required, a receiver can simply apply the same algorithm to the received data bits and compare its output with the received check bits; if the values do not match, an error has occurred at some point during the transmission. In a system that uses a non-systematic code, the original message is transformed into an encoded message that has at least as many bits as the original message.

Good error control performance requires the scheme to be selected based on the characteristics of the communication channel. Common channel models include memory-less models where errors occur randomly and with a certain probability, and dynamic models where errors occur primarily in bursts. Consequently, error-detecting and correcting codes can be generally distinguished between random-error-detecting/correcting and burst-error-detecting/correcting. Some codes can also be suitable for a mixture of random errors and burst errors.

If the channel capacity cannot be determined, or is highly variable, an error-detection scheme may be combined with a system for retransmissions of erroneous data. This is known as automatic repeat request (ARQ), and is most notably used in the Internet. An alternate approach for error control is hybrid automatic repeat request (HARQ), which is a combination of ARQ and error-correction coding. Error correction is the detection of errors and reconstruction of the original, error-free data.

Little-known application fields of block ciphers are protection against side channel attacks (using known key encryption), guaranteed destruction of information on magnetic carriers [2] and construction of random Latin squares of large size [3]. Quite unexpected is that the block ciphers can be used to perform the error-correcting coding. Codes based on block ciphers have several interesting properties for practical application. For example, the combination of encrypting and coding properties as a single transformation is able to correct errors of different natures: the inversion bits, error skipping and inserting bits in the transmitted data block. Also different types of errors presented in the same data block can be corrected.

Block encryption functions have strong scattering properties that define their effectiveness to the error detection. Such using of scattering transformations is mentioned in [4], but in general case, these transformation do not use for error corrections.

Implementation of symmetric block ciphers in coding theory will be presented in this paper.

II. Overview of existing techniques combining encryption and encoding

A. Theory of high diffusion ciphers

Avalanche effect gives ciphers their cryptographic strength, but the same properties makes them sensitive to errors. So, there is problem with using of cryptographically secure ciphers in noisy channel environments. Single bit inversion in block ciphers which operates on a fixed block length of data at a time can cause a complete decryption failure. In result due to this sensitivity cause, it is necessary to retransmit overall block, which in turn leads to additional hardware loads.

For improving the throughput in noisy environments, channel coding can be performed after encryption. Performing both encryption and coding separately can potentially be too computationally intensive for many devices.

Between error correction and cryptography there is many mathematical relationships [5], [6], [7], [8], [9], but there have been only a few attempts to build error-correcting ciphers. Some of the results include the McEliece cipher [10], the Hwang and Rao cipher [11], and the Godoy-Pereira scheme [12]. But there are some of the issues with these ciphers. Firstly, these systems were not designed based on well-known security principles (and hence are vulnerable to various attacks [13]). Secondly, these systems are not as efficient as traditional error-correcting codes in terms of error correction, because they trade error-correction capacity to achieve security. For achieving meaningful error-correction capacity, the parameters of the system have to be very large, leading to higher computational complexity. Also, the difficulty in designing error-correcting ciphers arise from the fact that error correction and encryption work at cross purposes with each other. The avalanche effect, which is desirable for security, causes too much error expansion thereby undermining the goal of an error correcting code.

Currently, theory error-correcting block cipher called the high diffusion (HD) has been developed [17]. HD cipher as standard block ciphers [14] is composed of several iterations of the round function and mixing with the secret key. Round function is composed of a nonlinear substitution layer and a linear diffusion layer.

Definition of HD codes [17] Let us consider an $[n, k, q]$ block code, defined on the Galois field (GF) of order q; where n refers to the number of output symbols and k refers to the number of input symbols. The HD codes are defined as follows. An $[n, k, q, b]$ code C is a high diffusion (HD) code with the encoding operation θ and branch number b if it satisfies the following inequality for all $i, j \in 1, 2, ..., (q^k 1)$ and $i \neq j$:

$$b = B(\theta) = min(H_d(m_i, m_j) + H_d(c_i, c_j)) \geq n + 1,$$

where $c_i = \theta(m_i)$.

So the branch number of θ is lower bounded by $n + 1$ since the maximum output difference corresponding to a single nonzero symbol input difference is n. The upper bound for branch number is $n + 1$. Hence, the branch number of HD codes should be exactly equal to $n + 1$.

Properties of HD codes The HD codes possess the maximum possible diffusion and error correction capacity as desired in the design criteria.

Optimality in diffusion. By definition, HD code has a branch number of $n+1$. For any Boolean transformation with n-tuples as its output the maximum branch number possible is n+1. As the HD coding operation θ is a Boolean transformation from k-tuples to n-tuples with the lower bound on the branch being $n + 1$ they achieve optimal diffusion.

Optimality in error correction. HD codes are maximum distance separable codes (MDS) [17] and hence they are optimal in terms of the minimum distance of the code.

B. Construction of HD codes

The branch number criterion for HD codes consist of pairs of messages and their associated codewords. This makes deriving a closed form expression (or encoding transformation θ) for the construction of the codes tricky. A brute force search produces the complete mapping with the highest expected runtime. Then, the θ has to derived from these mappings. There are some techniques to generate HD codes. A brief outline of these techniques follow:

1) Coset Based Search: Cosets are formed such that the codewords are assigned to the coset leaders only. The codewords for the rest of the coset elements are related to each other, often they are rotations of each other. The coset based search makes use of cosets to reduce the complexity of the code assignment. This searching technique only needs to find codewords for the coset leaders. Then it is used the message to codeword mapping to derive θ.
2) Transformation from Reed Solomon Codes. Known MDS code transform the encoding transformation of this MDS code into an encoding transformation of the HD code. Reed Solomon (RS) code with $[q - 1, k, q]$ can be transform into $[q - 1, k, q]$ HD codes using permutations of the message-codeword assignments that satisfy the branch number criterion. The traditional method [14] to generate an RS code cannot be directly used to generate an HD code, because the HD codes have a second property to be satisfied the branch number criterion.
3) Puncturing Existing Codes.

III. Adding redundancy to the data block and the general cryptocoding properties of block ciphers

For implementing block ciphers in cryptocoding mode (error correction mode), redundancy is entered in transmitted data as a specifiable label. For example, the encrypted block of n bits is defined as concatenation of the data block T of size $n - \mu$ bits and a predetermined label, for example, that is consist of repeating μ zero bits. During transmission of encrypted blocks in noisy channel errors are occurred. If the error number is small, for example $1-3$ errors of a transmitted block, process of recovery performs as processing all possible combinations of inverted (erroneously received) bit. This is easily done by a secret encryption key that is known for the recipient. Multiple decryption of received data block is performed until the decrypted data block containing mark would be obtained in one of variants of the block bits inverting in the received cryptogram.

The exhaustive search method for error correction determines the possibility of corrections both the inversion-type bit errors and errors occurred in the data synchronization transferring (bit skipping and bit inserting). Thus it is possible to fix different types of errors occurring in one data block, so the above method has the versatility for the type of corrected errors. The implementation of such possibility is achieved by specifying the algorithm of exhaustive search for expected errors which is implemented by the decoding procedure. The intruder who does not know the secret key have not the practical ability to read the transmitted message, even if the errors are not occurred in transmission channel. If there are errors, the difficulty of cryptanalysis increases for an attacker. Thus the proposed method of using the block encryption solves the problem of simultaneous message protection from unauthorized access and recovery of errors occurring in messages transmitted via the noisy channels.

In the case of correcting the inversion type of error, there are the following features of the proposed cryptocoding method:

1) The probability of an incorrect data block recovery does not depend on the number of errors, and for multiple (k) errors is approximately equal $2^{-\mu}C_n^k$ (C_n^k is the number of combinations of n from k; μ is a label bit size; n is a bit size of input data block). By the defining of label size we can specify acceptable value of this probability.
2) This is a probabilistic cryptocode. It corrects the k inversion-type errors $(k << n)$ with a probability that is approximately equal to the $1-2^{-\mu}C_n^k$.
   In the general case, an arbitrary number of errors could be corrected, however, for large values of k, the computational complexity of the decoding procedure becomes excessively high, and the probability of erroneous decoding approaches to unity.
3) The average speed of the decoding for error probability at 1% and the 64-bit (128-bit) encryption is approximately 64 times (128 times) lower than the speed of encryption (coding). Speed of cryptogram decoding with k errors is less the encryption speed in C_n^k times. However, due to the rarity of multiple errors, the average encryption rate is approximately n times smaller than the encryption rate.

The codes based on block ciphers have the next advantages:

1) A high speed of encoding and decoding in the case of single and double errors.
2) Relatively inexpensive hardware implementation allows to apply the parallelization in the decoding process.
3) Ability to use a various encryption transformation for building of cryptocoding algorithms.
4) The ability to combine the process of encryption and error-correcting encoding in one transformation procedure.
5) Variability of including cryptocodes with flexible (depending on the secret key) cryptocoding algorithm. Also, it is interesting the using of deniable encryption for redundancy insertion into the transmitted data.
6) Versatility cryptocoding algorithm by types of corrected errors and the number of corrected errors.

Ways for improving performance of the cryptocoding algorithms based on block ciphers include the following points:

1) Selecting the size of data input block in block cipher and label size.
2) Optimization of the block cipher for hardware implementation [4], [13], [14], [15], [16].
3) Optimization of the block cipher for software implementation.
4) The combination of block and stream encryption.
5) Placing labels in intermediate cryptograms.
6) The using of a label distributed in time.
7) The parallelization of calculations related to the decoding process.

A perspective area of research is the development and justification of labels distributed in time, the development of specific implementations for this method of the performance improving and the assessment of its applicability to the known and new block cipher algorithm.

Helpful for practical application method of the redundancy insertion is joint encryption of information data block and the secondary block in the form of fixed label with using of deniable encryption block algorithms described in [5]. The computational complexity of decoding procedures for such implementation can be significantly reduced due to the fact that iterating of possible errors injected in the data channel, the multiple decryption can be only performed for the secondary data block.

By choosing the secondary block is relatively small, we can achieve significant performance improvements for cryptocoding algorithms based on the procedures of deniable encryption.

IV. Estimation of decoding rate

The average rate of decoding d for the standard method of the redundancy injection (label is embedded in the encrypted original data block) is follows:

$$d = 2V_E\frac{n-\mu}{nC_n^k},$$

where:

n is the input size of the encryption algorithm;

μ is the size of label;

k is the average number of errors in the block;

V_E is the rate of the block encryption.

When label μ is chosen as a redundancy part of the intermediate ciphertext (that is obtained from execution of the incomplete block cipher rounds) and added to the output ciphertext block C, the value can be estimated using the following formula:

$$d = \frac{2V_E R}{(R-i)C_{n+k}^k},$$

where R is the rounds number of the block cipher;

i is the number of rounds, after which the label is selected;

k is the average number of errors in the extended ciphertext block (in the pair (C, μ)).

The extended ciphertext block is transmitted over the communications channel as a single data block.

V. Errors of synchronization violation type

In the development error-correcting codes, it is usually considered the errors of the inversion error bit type. In general, there are errors such as synchronization violation type in process of transmission and reception data, that is the insert-type and skipping-type of error, also there are a composite errors (the presence of inversion errors and synchronization errors in a received data block).

The synchronization violation errors lead to a shift of bit numbers of the received message. One such transmission error lead to the bit inversion from 1 to n bits in the transmitted n-bit block. If there is one insertion error and one the skipping-type error, the size of the received data block is not changed, this does not directly establish the error presence of given type. To correct the errors of a certain type is required an assessment of the error occurrence probability and its account in the algorithm of decoding procedure. Errors are ranked according to the values of their probabilities. The algorithm of sequential search in descending order of the error probability.

The advantage of the exhaustive search of decoding mechanism in the proposed cryptocoding method allows to correct the errors such as inversions and synchronization violation errors. Such possibility is achieved by the fact that error correction is probabilistic (probability of error correction is sufficiently close to 1, but not equal to 1).

A method of error corrections such as bit skipping and bit inserts is the same (namely the exhaustive search) as when the errors of insertion type are corrected. Obviously, the decoding algorithm are fixed only those errors that are described (whose bust is provided in the decoding algorithm). For example, in the case of skipping errors, the unit and zero bits are inserted in different part of received data block in the amount of 1 to k, where k is a predetermined number of expected errors.

Thus it is qualitatively shown the fundamental possibility of reconstructing the type of synchronization violation errors and also the ability to recover the combined errors. Practically acceptable decoding rate is achieved when the total number of different types of errors do not exceed the value $k = 4$, which covers most cases in practice.

VI. Guaranteed fix of errors such as bit inversion

The ability of the block cipher to correct errors such as bit inversions associates with the possible difference of output ciphertext blocks. Considering the format of the input block with integrated label, there are 2^τ various input information data blocks which correspond to 2^τ blocks of encrypted data (ciphertext blocks). The values of the ciphertext blocks depends on the selected encryption key. Fixing of the key means the fixing of some 2^τ values of ciphertext blocks, which corresponds to the number of distinct differences that is equal to:

$$N_\oplus \le C_{2^\tau}^2 = \frac{2^\tau(2^\tau - 1)}{2} \approx 2^{2\tau-1}$$

Guarantee correction of k error, it is needed to select the format parameters of the input block that provides the condition that the number of all implemented differences (for the fixed encryption key)

$$N_\oplus \le C_{2^\tau}^2$$

$$N_\oplus \approx \; C_{2^\tau}^2 < 2^{\tau+\mu} - \sum_{i=1}^{k} C_{2^{\tau+\mu}}^i \tag{1}$$

The physical meaning of this condition is to ensure that the number of the different possible $\tau + \mu$ bit differences (obtained in different encryption keys and having a Hamming weight greater than k) exceeds the number of implemented differences for any fixed key. The sum $\sum_{i=1}^{k} C_{2^{\tau+\mu}}^i$ is equal to the all the possible differences of weight no more than k. This condition defines principal possibility of a guaranteed fix for k errors. In practice, this condition must be fulfilled for a particular encryption algorithm and specific encryption key. Therefore, the parameters of the input data block format should be chosen so that with sufficiently high probability for a randomly selected key all realizable output difference will be greater weight than k. Accordingly, the condition (1) should be reinforced and given as:

$$\sum_{i=1}^{k} C_{2^{\tau+\mu}}^i \ll 2^{\tau+\mu} - \sum_{i=1}^{k} C_{2^{\tau+\mu}}^i \tag{2}$$

Or as:

$$2^{\tau+\mu} \gg 2\sum_{i=1}^{k} C_{2^{\tau+\mu}}^i \tag{3}$$

The physical meaning of the formula (2) and (3) consists in the fact that it is required to ensure the condition of smallness proportion for output differences with weight not more than k. If the input block format parameters provide this condition, there is a possibility of practical computing generation of the private key, which provides a guaranteed fix of k errors occurring in the data transmission channel. Guarantee of error correction, the number of which is not more than k, based on the following proposition.

Proposition. If for the selected encryption key, for encryption of 2^τ possible input blocks is implemented only output differences of the weight over k, then in the error correction mode it is guaranteed correction of k errors.

Proof: Let for the selected encryption key, the input block B was transformed into the ciphertext block C and during the transmission was occurred k errors, as a result C' block has been received. Assume that the input value $B' \neq B$ was recovered in the decoding by inverting the various combinations of i bits ($i \leq k$) in the cryptogram and by decryption the corrected ciphertext blocks. But then the input block $B' \neq B$ is encrypted in the ciphertext block C', we have the output difference $C \oplus C'$ and the Hamming weight is not more than k that contradict to the proposition condition. This contradiction proves the formulated proposition.

VII. The computational complexity of key generation providing a guaranteed fix of k errors

When converting the two input blocks by a randomly selected keys we have chance of getting the output difference of weight k or less according to the ratio:

$$p_0 = \frac{\sum_{i=1}^{k} C^i_{2^{\tau+\mu}}}{2^{\tau+\mu}}$$

Accordingly, the probability of obtaining the output difference with weight more than k is equal to:

$$1 - p_0 = 1 - \frac{\sum_{i=1}^{k} C^i_{2^{\tau+\mu}}}{2^{\tau+\mu}}$$

When converting all possible 2^τ input blocks by a randomly selected key, in general case, there are $2^{2\tau-1}$ various output differences and the probability that it all have differences with weight more than k is equal to:

$$Pr(> k) = (1 - p_0)^{2^{2\tau-1}} = (1 - \frac{\sum_{i=1}^{k} C^i_{2^{\tau+\mu}}}{2^{\tau+\mu}})^{2\tau-1} \qquad (4)$$

Under the condition (3) the last relation can be written in the approximate form:

$$Pr(> k) = 1 - 2^{2\tau-1}\frac{\sum_{i=1}^{k} C^i_{2^{\tau+\mu}}}{2^{\tau+\mu}} = 1 - 2^{\tau-\mu-1}\sum_{i=1}^{k} C^i_{2^{\tau+\mu}} \qquad (5)$$

For randomly selected key of output difference with weight k or less, the probability of obtaining is equal:

$$Pr(< k) = 1 - Pr(> k) = 2^{\tau-\mu-1}\sum_{i=1}^{k} C^i_{2^{\tau+\mu}} \qquad (6)$$

This is the probability of unsuccessful choice of the key as the key corresponds to the selection which does not ensure a guaranteed fix of k errors. For the case of $k << n$, the next approximate formula can be used:

$$Pr(< k) = 2^{\tau-\mu-1}\sum_{i=1}^{k} C^i_{2^{\tau\mu}} = 2^{\tau-\mu-1}\frac{n^k}{k!} \qquad (7)$$

Table I shows the probability estimation of unsuccessful selection key parameters for different sets of input block format. The results obtained using formula (7).

TABLE I. The example of parameter choice for input data block

$\mu+\tau$	τ	μ	K	$Pr(< k)$
32	8	24	2	2^{-8}
32	4	28	2	2^{-15}
32	4	28	1	2^{-19}
64	8	56	1	2^{-43}
64	8	56	2	2^{-38}
64	8	56	3	2^{-33}
64	8	56	4	2^{-29}
96	8	88	2	2^{-68}
96	8	80	3	2^{-58}
128	16	112	2	2^{-84}
126	16	112	4	2^{-73}

The calculated data in Table I shows that the selected relation of the field information data and label sizes can be changed in the direction of increasing the size of the field information data, as a probability $Pr(< k)$ closing to 2^{-1} is quite acceptable. Actually, it is possible to test some trial random values of encryption key during its generation, until the key for which all the output difference have a weight k is found. Table II illustrates the last case.

TABLE II. Applied parameters of input data block format

$\mu+\tau$	τ	μ	K	$Pr(< k)$
32	8	24	3	2^{-4}
32	8	24	4	2^{-1}
64	16	48	1	2^{-27}
64	16	48	2	2^{-22}
64	16	48	3	2^{-17}
64	16	48	4	2^{-13}
64	24	40	2	2^{-6}
64	24	40	3	2^{-1}
128	24	104	3	2^{-58}
128	32	96	3	2^{-46}
128	48	80	4	2^{-9}

For the probability $Pr(< k) \leq 2^{-40}$, the practically any chosen encryption key will ensure the condition of the assurance correction of k errors. This is the case of the lowest complexity of the encryption key generation procedures which is ensure warranty correction for given number of errors.

Complexity of key generation procedure is not critical. The complexity of the decoding procedure and rate of information transmission have more critical importance. The latter depends on the ratio of μ and τ. This value may be significantly altered for the benefit of increasing τ which leads to increasing in data rate. However, this possibility is related to the calculation of the probability of key generation, which provides the conditions of assurance correction for given number of errors. It should also be provided evaluation of block encryption procedures that is required to find all the output differences and checks the weight difference. The number of executed block encryption procedures, which necessary for the compute all the differences, is equal to 2^τ. For small values of the successful key generation probability, the average complexity of successful key generating is equal to $\frac{2^{\tau}}{Pr(>k)}$.

VIII. Conclusion

In this paper was proposed the method for constructing the cryptocoding algorithms based on block encryption functions, its implemented the protection of the transmitted data against unauthorized access and the ability of error correction in noise channel in a single transformation process. In fact, the method of using of block ciphers in error correction mode, implementation of which is ensured by the reversibility of encrypting transformation. An important advantage of the method is its versatility, which consists in the correction possibility of different error types (bit inversion, insertion and skipping) and its combinations. In the case of inversion type errors, it has been formulated conditions that ensure a guaranteed fix of predetermined number of errors.

References

[1] N. P. Smart, “Cryptography”, *Springer International Publishing*, 2009, p. 481

[2] A. U. Mirin, “The method and algorithm of guaranteed destruction of data stored on magnetic disks”, *Phd thesis St. Petersburg*, 2005.

[3] N. A. Moldovyan, N. L. Min, H. N. Zoy, “Synthesis of stream ciphers based on block transformations: Latin squares method”, *Questions of information security*, vol. 1, 2008, pp. 27-34.

[4] T. Klove, V. Korzhik, “Error detecting Codes”, *Kluwer Academic Publishers*, 1995.

[5] H. C. A. van Tilborg, Coding theory at work in cryptology and vice versa, in Handbook of Coding Theory, V. S. Pless and W. C. Huffman, Eds., pp. 11951227, North-Holland, Amsterdam, The Netherlands, 1998.

[6] E. R. Berlekamp, R. J. McEliece, and H. C. A. van Tilborg, On the inherent intractability of certain coding problems, IEEE Transactions on Information Theory, vol. 24, no. 3, pp. 384386, 1978.

[7] A. J. Menezes, P. C. van Oorschot, and S. A. Vanstone, Handbook of Applied Cryptography, CRC Press, Boca Raton, Fla, USA, 1996.

[8] C. N. Mathur, K. Narayan, and K. P. Subbalakshmi, On the Design of Error Correcting Ciphers, EURASIP Journal onWireless Communications and Networking, Vol. 2006, pp. 112, 2005

[9] Levina A.B., Borisenko P.S., Implementation of side-channel leakage detection technique based on normalized inter-class variance method. Scientific and Technical Journal of Information Technologies, Mechanics and Optics, Saint-Petersburg, Vol. 16, No. 4(104), pp. 697702, 2016

[10] R. J. McEliece, A public-key cryptosystem based on algebraic coding theory, DNS Progress Reports 42-44, NASA Jet Propulsion Laboratory, Pasadena, Calif, USA, 1978.

[11] T. Hwang and T. R. N. Rao, Secret error-correcting codes (SECC), in Proceedings of the 8th Annual International Cryptology Conference on Advances in Cryptology (CRYPTO 88), pp. 540563, Santa Barbara, Calif, USA, August 1988.

[12] W. Godoy Jr. and D. Pereira Jr., A proposal of a cryptography algorithm with techniques of error correction, Computer Communications, vol. 20, no. 15, pp. 13741380, 1997.

[13] H. N. Zoy, N. A. Moldovyan, “Managed elements $F_{2/4}$ as a primitive of block ciphers”, *Questions of information security*, vol. 1, 2011, pp. 2-10.

[14] N. A. Moldovyan, A. A. Moldovyan, “Data-driven block ciphers for fast telecommunication systems”, *Auerbach Publications. Talor and Francis Group New York, London*, 2008, p. 185

[15] E. V. Morozova, J. A. Mondikova, N. A. Moldovyan, “Methods of deniable encryption with shared key”, *Information and Control Systems*, vol. 6, 2013, pp. 73-78.

[16] Mathur, C. N., K. Narayan, and K. Subbalakshmi: 2005, High Diffusion Codes: A Class of Maximum Distance Separable Codes for Error Resilient Block Ciphers. 2nd IEEE International Workshop on Adaptive Wireless Networks (AWiN), Globecom.

[17] F. J. MacWilliams and N. J. A. Sloane, The Theory of Error Correcting Codes. I and II, vol. 16 of North-Holland Mathematical Library, North-Holland, Amsterdam, The Netherlands, 1977.

[18] T. A. Berson, Failure of the McEliece public-key cryptosystem under message-resend and related-message attack, in Proceedings of the 17th Annual International Cryptology Conference on Advances in Cryptology (CRYPTO 97), Lecture Notes in Computer Science, pp. 213220, Santa Barbara, Calif, USA, August 1997.

[19] D. Stinson, Cryptography: Theory and Practice, CRC/CH, London, UK, 2nd edition, 2002.

[20] Levina A.B., Taranov S.V., Investigation of influence of encoding function complexity on distribution of error masking probability, Scientific and Technical Journal of Information Technologies, Mechanics and Optics, Saint-Petersburg, Vol. 16. No. 2(102), pp. 331-337, 2016