Using the Flawed Codes In Niederreiter Crypto-Code Structure

Oleksii Tsyhanenko
dept. of cybersecurity and information technology
Simon Kuznets Kharkiv National University of Economics
Kharkiv, Ukraine
oleksii.tsyhanenko@hneu.net

Serhii Yevseiev
dept. of cybersecurity and information technology
Simon Kuznets Kharkiv National University of Economics
Kharkiv, Ukraine
serhii.yevseiev@hneu.net

Stanislav Milevskyi
dept. of cybersecurity and information technology
Simon Kuznets Kharkiv National University of Economics
Kharkiv, Ukraine
stanislav.milevskiy@hneu.net

Abstract—the paper highlights basis of methods for constructing flawed codes and approaches for using the Niederreiter hybrid crypto-code structure on modified elliptic codes. Practical algorithms are proposed for using the MV2 damage mechanism in the Niederreiter crypto-code structure on modified elliptic codes, which makes it possible to implement a hybrid crypto-code structure.

Keywords—modified crypto-code system Niederreiter, crypto-code construction, confidentiality, integrity.

I. INTRODUCTION

Today, cybersecurity can be fully considered an important aspect of any society. With the rapid development of the Internet information environment, the complexity of information protection against unauthorized access, the growing vulnerabilities of critical systems to hybrid cyberattacks is a significant problem for various users.

In addition, despite the fact that most organizations are improving information security systems, cybercriminals continue to find ways to circumvent them by carrying out destructive measures. Information security involves achieving and maintaining security features in user resources aimed at preventing relevant cyber threats. As a result, the development of quality software products and national production will increase the level of cybersecurity of the state.

According to experts, NIST USA one of the promising areas is the use of crypto-code schemes McEliece and Niederreiter. Their classic variations should not be used in Internet technologies due to their vulnerabilities and high energy consumption in practice. Therefore, it is advisable to develop a crypto-code structure (CCS) of Niederreiter using flawed codes, which will reduce the field strength to GF (2^4), with a guaranteed level of stability and form a hybrid crypto-code structure (HCCS) of Niederreiter.

In [1] the approach of unprofitable codes use in crypto-code systems is proposed. This approach allows to build complex cryptosystems based on the synthesis of CCC (model of evidence-based stability) and cryptosystems on flawed codes (multichannel cryptography). This approach allows to reduce energy costs in the practical implementation of CCS Niederreiter on modified (MCCC) (shortened / extended) elliptical codes (MEC) while maintaining the cryptographic resistance of the entire system.

In [2] methods of flawed codes construction and approaches to use of a hybrid crypto-code construction of Niederreiter on the modified elliptical codes are considered. Practical algorithms for the use of the MV2 damage mechanism in the Niederreiter crypto-code structure on modified elliptical codes are proposed, which allows to implement a hybrid crypto-code structure. The results of comparative assessment of energy consumption for the formation of an information package with different methods of damage, which determined the choice of method of damage in practical algorithms. The conducted research confirms the competitiveness of the proposed cryptosystem in Internet technologies and mobile networks, providing practical implementation on modern platforms and the necessary cryptographic power under post-quantum cryptography.

II. THE PRINCIPLE OF BUILDING HCCS NIEDERREITER ON FLAWED CODES

The main advantage of HCCC Niederreiter is the high speed of information conversion (relative coding speed is close to 1). To reduce energy consumption with a guaranteed level of safety in operation, the MCCC Niederreiter for MEC proposed. This approach reduces the field strength and allows to implement the classic version of the Niederreiter scheme with a guaranteed level of stability.

In the classical Niederreiter scheme, in the first stage of cryptogram generation, the plaintext characters are converted into error vector characters based on the equilibrium coding algorithm. The obtained error vector in the second stage of cryptogram generation is shortened on the basis of the code reduction algorithm, multiplied by the check matrix of the algebraic (elliptical) code.

After the formation of private key matrices, the authorized user must form elements of a set of fixed plaintext, which are not suitable for further formation of the cryptogram (error vector syndrome).

The theoretical basis for the construction of flawed texts is to eliminate the order of the symbols of the source text and, as a consequence, reduce the redundancy of language symbols in the defective text. At the same time, the amount of information expressing this ordering will be equal to the decrease in the entropy of the text compared to the maximum possible value of entropy, ie equivalent to any letter after any previous letter. To obtain imperfect text (FTC) and damage (DCH), the method of "perfect" compression is used after performing m cycles of the damage mechanism C_m. The use of the damage procedure in the CCC is possible in the following ways:

- Method 1: damage to plaintext with subsequent encryption of the losing text and/or its loss;
- Method 2: damaging the ciphertext;

Method 3: damage to plaintext with subsequent encryption of unprofitable text and damage to flawed ciphertext (Fig. 1).

Using the plaintext damage approach (third) from the MCCC Niederreiter for MEC increases the bandwidth starting from the GF field (2^9). This method is the best approach for building a hybrid MCCC Niederreiter for MEC.

The synthesis of Niederreiter's crypto-code structure with a cryptosystem with flawed codes allows to build complex (hybrid) crypto-code schemes, the stability of which is determined by the strength of two cryptosystems to ensure the implementation of fast cryptotransformations by reducing field strength.

III. Cryptography Incryption And Encryption Algorithms In Niederreiter Hccs

The algorithm for generating a cryptogram in a hybrid Niederreiter CCC on MEC using flawed codes can be represented as a sequence of steps:

Step 1. Entering the information to be encoded, the elements of a set of valid plaintext. Entering the public key H_x.

Step 2. The formation of the error vector e, the weight of which does not exceed t, corrects the ability of the elliptical code based on the algorithm of non-binary equilibrium coding.

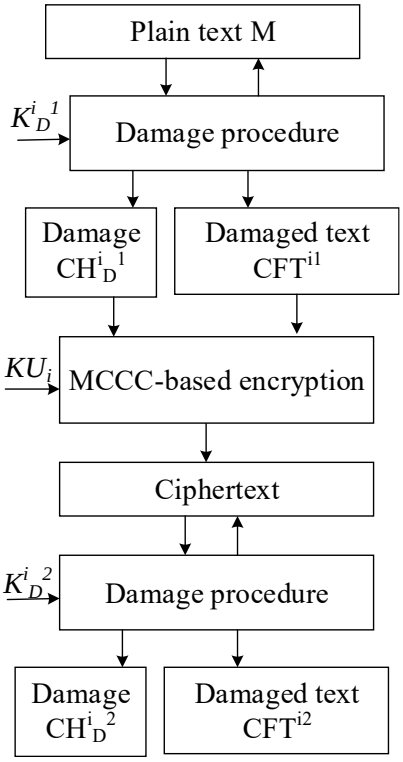

Fig. 1. Block diagram of a hybrid crypto-structure construction based on the ciphertext damage.

Step 3. Formation of the initialization vector IV_1.

Step 4. Formation of the reduction vector (1)

$$e_x = \mathrm{e}(A) - IV_2 \tag{1}$$

Step 5. Formation of the codegram (2)

$$s^*_{r-h_e} = (e_n - h_e) \cdot H_X \tag{2}$$

Step 6. Formation of unprofitable CFT text and CHD loss.

The algorithm for decrypting the cryptogram in the Niederreiter hybrid CCC on MEC using flawed codes can be represented as a sequence of the following steps:

Step 1. Enter the flawed CFT text that is decoded. Enter the private key - matrices X, P, D. Entering loss CHD.

Step 2. Obtaining the length of the errors and splitting the unprofitable text

Step 3. Getting S_{Xi} codogram characters and forming a complete codogram (3)

$$s_x = s_{x_i} \| \ldots \| s_{x_n} \tag{3}$$

Step 4. Search for one of the possible solutions of the equation (4)

$$s^*_{(r-h_e)} = c^* \cdot \left(H_x \right) \quad (4)$$

Step 5. Removal of mixing and multiplicity matrices (5)

$$c^* = c_x \cdot D^{-1} \cdot P^{-1} \quad (5)$$

Step 6. Decoding the vector c*. Getting e_x.

Step 7. Convert vector e_x (6)

$$e_x = c_x \cdot D \cdot P \quad (6)$$

Step 8. Formation of the error vector (7)

$$\mathrm{e} = \mathrm{e}_x + IV_2 \quad (7)$$

Step 9. The transformation of the vector e is based on the use of non-binary equilibrium coding in the information sequence.

The use of a modified crypto-code construction of Niederreiter (MCCC) with additional initialization vectors (with set of invalid position vectors, error vector and multiple error vector reduction positions) requires increasing the rate of cryptographic transformation of the system as a whole. The use of the Niederreiter MCCC on flawed codes can increase the speed of code conversion by reducing the field strength when causing damage to plaintext and reducing the amount of data transmitted by damaging the ciphertext. This approach allows to build hybrid cryptocode structures based on the synthesis of Niederreiter modified crypto-code structures on modified (shortened or extended) codes on elliptic curves with damage procedures. A significant difference from classical hybrid (complex) cryptosystems is the use of asymmetric cryptosystems to ensure data security with fast crypto-transformations (generation and decoding of codograms).

REFERENCES

[1] Evseev, S., "Ispol'zovaniye ushcherbnykh kodov v kripto-kodovykh sistemakh" [Using flawed codes in crypto-code systems] // SOI . – 2017. – № 5(151). P. 109-121. https://doi.org/10.30748/soi.2017.151.15.

[2] Yevseiev, S. Development of Niederreiter hybrid crypto-code structure on flawed codes / Serhii Yevseiev, Oleksii Tsyhanenko, Alla Gavrilova, Viktor Guzhva, Oleksandr Milov, Valentina Moskalenko, Ivan Opirskyy, Oleksandr Roma, Bogdan Tomashevsky, Olexander Shmatko // Eastern-European Journal of Enterprise Technologies. – 2019. – Vol. 1, N 9 (97). - P. 27-38. – Way of Access : DOI : 10.15587/1729-4061.2019.156620.

[3] Mishchenko, V.A. and Vilansky, Yu.V. (2007), “Ushherbnye teksty i mnogokanal'naja kriptografija” [Damage texts and multichannel cryptography], Encyclopedic, Minsk, 292 p.