Research of cryptosystems resistance on cascade codes to nonalgebraic decoding attacks

Zhukabayeva Tamara, Sembiyev Ordabay and Khu Ven–Tsen
South Kazakhstan State University, Tauke khan avenue 5, Shymkent 160012, Kazakhstan

Email: tamara_kokenovna@mail.ru; ordabai@mail.ru; qbcba@bk.ru

Received 20 May 2011; Revised 17 Jan 2012 ; Accepted 20 Jan 2012
Published online: 1 Sep. 2012

Abstract: Cryptosystems of theoretical resistance, construction of which is based on using algebraic block codes (code-theoretic schemes) are considered. Resistance of cascade code-theoretic schemes to hacking by an opponent with the help of the method of permutable decoding is researched.

Keywords: Information security, cryptosystem, cascade codes,

1 Introduction

History is filled with examples of how technology helped usher a new eras of prosperity. Efforts are on streamline technology widening the knowledge canvas. The important indicators of efficiency of the modern system of data transfer are security and fidelity of information, characterizing the ability of the system to resist disclosure of the content of transferred information by an opponent and to provide exact reproduction of transferred messages in receiving points. The aim of the given article is to research cryptosystems resistance on cascade codes to nonalgebraic decoding attacks.

The works [1, 2] show that providing required indicators fidelity and information security is possible on the basis of using code-theoretic schemes – cryptosystems of theoretical resistance, construction of which is based on using algebraic block codes.

In the works [3, 4] code-theoretic schemes, constructed on generalized cascade codes (cascade code-theoretic schemes) are suggested, using of which allows to essentially reduce (for several orders) complexity of practical realization without considerable degradation of code parameters and decreasing energetic gain from coding.

The work [5] shows that cascade coding allows to get the greater effect while using on the external level of algebro-geometric codes.

2 Cascade code-theoretic schemes

Formation of cascade code-theoretic scheme is realized by dissimulation of codes of external levels of generalized cascade code, and codogram formation process corresponds to formation of code word of dissimulated cascade code adding random error vector to it. By definition [6] algebraically given generalized cascade code of the order m is identically determined by n2 square binary matrices $H^j_i, i = \frac{1}{m+1}, n2$ of the order n1 (given (n1, k1, d1) codes of internal level) and m+1 group ones over , GF(2n1), i.e., $\frac{1}{m+1}, n2$ codes of external level with parameters (n2, b1, d2).

Cascade code-theoretic scheme, constructed according to generalized cascade (n, k, d) code of the m order, is given by aggregate of the following sets [7]:

set of clear texts $M = \{M1, M2, ..., Mqk\}$, where each $M_i$ represents information block of the form $M_i = \{(I1,1, I1,2, ..., I1,a1), (I2,1, I2,2, ..., I2,a1),..., (Ib1,1, Ib1,2, ..., Ib1,a1), (I1,1, I1,2, ..., I1,a2), (I2,1, I2,2, ..., I2,a2),..., (Ib2,1, Ib2,2, ..., Ib2,a2),..., (I1,1, I1,2, ..., I1,am+1), (I2,1, I2,2, ..., I2,am+1),..., (Ibm+1,1, Ibm+1,2, ..., Ibm+1,am+1) \}$;

set of cryptograms $E = \{E1, E2, ..., Eqk\}$, where each $E_i$ represents a code word of the form $E_i = C_i + \varepsilon_i$ that is the sum of the code word of generalized cascade code with random error vector $\varepsilon_i$.

(c1,1, c1,2, ..., c1,a1), (c2,1, c2,2, ..., c2,a1),..., (cn2,1, cn2,2, ..., cn2,a1), (c1,1, c1,2, ..., c1,a2), (c2,1, c2,2, ..., c2,a2),..., (cn2,1, cn2,2, ..., cn2,a2),...
The least quantity of sets, which can belong to a set of roofing codes over GF(q), consists in the fact that unit of roofing unit of errors of the given type, are called control sets, covering unknown combination of errors. Let’s consider the combination only out of t errors, as all errors of less multiplicity will be covered. The general quantity of errors in all n positions is equal to C_{n,t}. By virtue of the fact that the volume of roofing set is equal to n-k, maximum quantity of errors combinations, which can be covered by the given set, equals to C_{n-k,t}. The least quantity of sets, which can correct all combinations out of t errors, is restricted to the expression [9]:

\[
\delta \geq \frac{C_{n,t}}{C_{n-k,t}}
\]  

Figure 1: The intricacy of the hacking task of code-theoretic scheme as decoding task decision of a elliptical code by permutable decoder.
In Figure 1 as an example dependences of hacking intricacy of code-theoretic scheme by an opponent, constructed by elliptical code with relative rate of coding \( R \) are given [8].

As it is seen from the presented dependences, permutable decoder becomes inefficient even at values \( n>500 \). Consequently, hacking of code-theoretic schemes at corresponding choice of parameters of random code is computationally unavailable.

Thus, carried out researches have shown that code-theoretic schemes allow to provide required resistance to cryptanalytic attacks of an opponent at appropriate choosing parameters of dissimulated code. Correlation (1) determines an analytical dependence between parameters of code-theoretic scheme and its stability to corresponding attacks.

4 Research of resistance of cascade code-theoretic schemes to attacks, based on nonalgebraic methods of decoding

Expression (1) while using generalized cascade codes is transformed as:

\[
\delta \geq v \cdot \sum_{i=0}^{m+1} \frac{\binom{n}{n_{2-b_i}}}{\binom{n}{n_{2-b_i}}} (2) \]

where \( t_i \) – correcting ability of \( i \) code of external level, \( d_{2i}=2t_{i+1} \); \( v \) – number of construction variants of generalized cascade code, at unknown order of generalized cascade code – \( v=2n_1-1 \), at known order – \( v= \binom{m+1}{n_1-1} \).

It should be noted that construction of code-theoretic schemes is based on dissimulating error-control (\( n, k, d \)) block code with rapid algorithm of decoding in random code. At this random vector of errors \( e \), weight of which is less or equal to correcting ability of the code \( w(e) \), where \( t=e-d/2 \) is introduced into code word (\( n, k, d \)) of block code. Let’s denote the weight deal of errors vector of vector \( e \), arriving for artificial entry of code-theoretic scheme, with the symbol \( \rho \): \( \rho=w(e)/t \). Then potential resistance of code-theoretic scheme will be defined by magnitude \( \rho \cdot t \), and error-control of transferred codograms is defined by magnitude \( (1-\rho) \cdot t \). At this expression (2) will be rewritten as:

\[
\delta \geq v \cdot \sum_{i=0}^{m+1} \frac{\binom{n}{n_{2-b_i}}}{\binom{n}{n_{2-b_i}}} (3) \]

where \( \rho_1 \) – deal of correcting ability of \( i \) code of external level, arriving for artificial entry of errors.

In Figure 2 dependences of hacking intricacy of cascade code-theoretic scheme by the opponent, constructed by generalized cascade code with relative rate of coding \( R \) are given.

The analysis of dependences shows that the number of searches, necessary for opponent to decode a code word, considerably rises with increasing \( m \) group ones over \( \text{GF}(2^{ai}) \), \( i=1, m+1 \), codes of external levels of generalized cascade code, deal of correcting ability of the code of external level, arriving for artificial entry of errors – \( \rho \), and also with increasing of the number of \( n_1 \) number decomposing variants, extending finite Galois field \( \text{GF}(2^{ai}) \), over which corresponding codes of external level are constructed.

Hence, attack realization intricacy by permutable decoder rises according to exponential dependence and at values:
\[
\rho >0.5-0.7; \quad m=10-20; \quad n>2000
\]
high resistance of suggested constructions to hacking by an opponent with the help of the method of permutable decoding (from 1025 and more group operations) is achieved.

5 Conclusion

Carried out researches of resistance of developed cascade code-theoretic schemes to hacking by an opponent with the help of the method of permutable decoder have shown that using cascade code-theoretic schemes allows to provide information security of data transfer in automatized systems of control.
Hacking intricacy by an opponent with the help of the method of permutable decoding increases exponentially, and at appropriate choice of parameters (n, k, d), ρ and m of dissimulated code this attack is computationally not realized. Rapid growth of permutable decoding intricacy is connected with increasing of the decomposition number of the order of formed field, assigned number of possible variants of generalized cascade codes construction.

References


