Applied Mathematics & Information Sciences
An International Journal

@ 2012 NSP
Natural Sciences Publishing Cor.

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_0^j, $j = \overline{1,n_2}$ of the order n1 (given (n1, ki, d1i) codes of internal level) and m+1 group ones over , GF(2ai), i=$\overline{1,m+1}$ codes of external level with parameters (n2, bi, d2i).

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 Mi represents information block of the form

Mi = {(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 Ei represents a code word of the form Ei = Ci +ei that is the sum of the code word of generalized cascade code with random error vector ei, besides

Ci = {(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),

…

(C1,1, C1,2, …, C1,am+1), (C2,1, C2,2, …, C2, am+1),…, (Cn2,1, Cn2,2, …, Cn2, am+1), };
or, in above introduced symbols,
Ci = {(γ 1,1, γ 1,2, …, γ 1,n2), (γ 2,1, γ 2,2, …, γ 2,n2),…,
(γ m+1,1, γ m+1,2, …, γ m+1, n2);
γ I,j =(Ci,1, Ci,2, …, Ci,aj).

Thus, the codogram is a vector
Ei = {(γ *1,1, γ *1,2, …, γ *1,n2), (γ *2,1, γ *2,2, …, γ *2,n2),…, (γ *m+1,1, γ *m+1,2, …, γ * m+1, n2),
where, γ*ij = γij + eij – a binary vector of the ai length, $\sum_{i=1}^{m+1} a_i = n_1, e_{ij}$ -elements of random error vector of ai length (session key);
set of direct mappings
$\phi = \{\phi_1, \phi_2, ..., \phi_s\}$

where $\phi_i : M \to E,$ i=1,2,…,s
set of inverse mappings
$\phi^{-1} = \{\phi_1^{-1}, \phi_2^{-1}, ..., \phi_s^{-1}\}$

where $\phi_i^{-1} : M \to E,$ i=1,2,…,s
set of keys, parametrizing direct mappings
K= {K1, K2, …, Ks}, $\phi_i =: M \xrightarrow{K_i} E$
where Ki = {$G_X^1, G_X^2, ..., G_X^{m+1}$} – a set of generating matrices, which give m+1 of dissimulated codes of external level;
set of keys, parametrizing inverse mappings
K*= {K1*, K2*, …, Ks*}, $\phi_i^* =: M \xrightarrow{K^*_i} E$
where K_i^* = {{X1, P1, D1}, {X2, P2, D2}, …, {Xm+1, Pm+1, Dm+1}} – set of matrices, dissimulating m+1 of codes of external level.

3 Attacks, based on nonalgebraic methods of decoding

Decoding of certain linear code (code of general position) is a considerably intricate computational task, the intricacy of its decision rises exponentially. So, for correlation decoding of certain (n, k, d) code over GF(q) it is necessary, in the general case, to compare accepted consequence with all qk code words and choose the nearest one (in Hamming distance). Even for small n, k, d and q task of correlation decoding is considerably cumbersome. This position is the basis for all non-symmetrical code-theoretic schemes. Dissimulating the code with rapid algorithm of decoding (polynomial intricacy) in certain (random) linear code, decoding task for outside observer (possible intruder) can be presented as a computationally intricate task (exponential intricacy). For an authorized user (having a secret key) decoding is a polynomially solvable task.

One of the most efficient methods of decoding of linear code is use of a permutable decoder. The main idea of such decoding consists in the fact that unit of information sets is used to form corresponding choice of candidates in code words. Further, according to algorithm, among these candidates the nearest one is chosen. If whereby there is no error in one of the information components in the accepted consequence, transferred code word will be in the list of candidates. Thus, if factual combination of errors can be corrected by the decoder of maximum likelihood, the code word will have the lowest distance to the accepted consequence and be chosen by permutable decoder. While considering resettable decoding errors combination will be found, if finding such information set, fully containing this combination turns out well. Such set, roofing combination of errors, and unit of control sets, covering all units of errors of the given type, are called overlapping. The task of the decoder is to find a control set, covering unknown combination of errors. Let's consider bounds for quantity of roofing sets. Let's suppose that all combinations out of t or smaller quantity of errors are corrected with the help of the code (n, k, d). Let's consider the combination only out of t-multiple 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]:

$$\delta \geq \frac{C_n^t}{C_{n-k}^t} \quad (1)$$

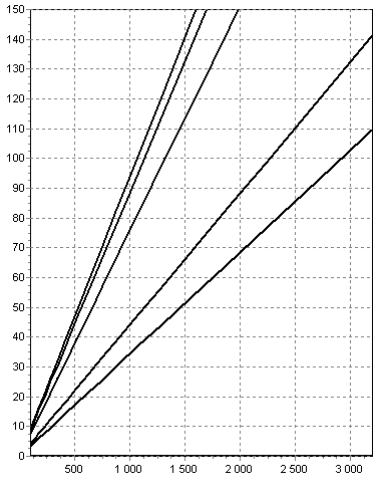


Figure 1: The intricacy of the hacking task of code-theoretic scheme as decoding task decision of a elliptical code by permutable decoder.

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:

$$\delta \geq \nu \cdot \sum_{i=0}^{m+1} \frac{C_{n2}^{ti}}{C_{n2-bi}^{ti}} \quad (2)$$

where ti – correcting ability of i code of external level, d2i=2ti+1; v – number of construction variants of generalized cascade code, at unknown order of generalized cascade code – v=2n1-1, at known order – v= C_{n1-1}^{m+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)≤t,

where t= d-1/2_ 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 ρ: ρ=w(e)/t. Then potential resistance of code-theoretic scheme will be defined by magnitude ρ·t, and error-control of transferred codograms is defined by magnitude (1-ρ)·t. At this expression (2) will be rewritten as:

$$\delta \geq \nu \cdot \sum_{i=0}^{m+1} \frac{C_{n2}^{\rho iti}}{C_{n2-bi}^{\rho iti}} \quad (3)$$

where ρ1 – 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.

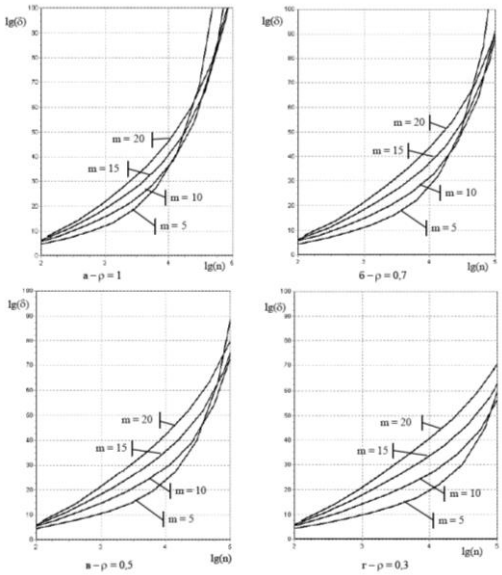


Figure 2: Intricacy of hacking task of cascade code scheme as a decoding task decision of generalized cascade code by permutable decoder, R=1/2.

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 GF(2ai), i= $\overline{1, m+1}$, codes of external levels of generalized cascade code, deal of correcting ability of the code of external level, arriving for artificial entry of errors – ρ, and also with increasing of the number of n1 number decomposing variants, extending finite Galois field GF(2ai), over which corresponding codes of external level are constructed.

Hence, attack realization intricacy by permutable decoder rises according to exponential dependence and at values:

ρ >0.5-0.7;
m=10-20;
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

[1] Sidelnikov V.M. Cryptography and coding theory: Proceedings of the conference "Moscow universities and the development of cryptography in Russia." - Moscow: MGU, 2002.

[2] Stasov Y.V., Kuznetsov A.A. Unbalanced code-theoretic scheme using algebraic-geometric codes, "Cybernetics and systems analysis has: International scientific-theoretical journal. - 2005.

[3] Stasov Y.V, Kuznetsov A.A, Grabchak V.I, Development of code-theoretic schemes for generalized concatenated codes / Hu PS, 2006

[4] Kuznetsov A.A, Grabchak V.I ,Evseev S.P. Cascade code protection scheme information / / H.: Hu PS, 2005. - 9 .

[5] Forney D. Concatenated codes: trans. from English, D. Forney. - Moscow: Mir, 1970. - 207.

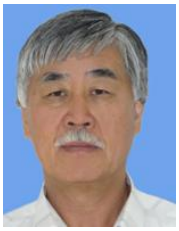
[6] Bloch E.L, V.V. Zyablov, Generalized concatenated codes. - Moscow: Svyaz, 1976. - 240.

[7] Clark Dzh.-ml., Kane J. Encoding linier corrected errors in digital communications: Trans. from English. Ed. B.S Tsybakova. - M.: Radio and Communications, 1987.

[8] Kuznetsov A.A, Lysenko V.N, Evseev S.P. The study of the properties of asymmetric code-theoretic schemes with elliptic codes. / / System information. - H.: HVU, 2004. - . 9 (37).

Ph. D. student, Faculty of Information technology, telecommunications and the automated systems, M. Auezov South Kazakhstan State University (2009-2012). Specialty "System analysis, management and treatment Information.

Prof. Dr Sembiyev Ordabay Zaitayevich, born in 1958, is a Doctor of Engineering, a professor of South Kazakhstan State University, a chief of the chair of "Computer engineering and software programming". O.Z.Sembiyev is the best teacher of Higher Educational Institution in 2008.



Prof. Dr Khu Ven -Tsen, is a Doctor of Technical Sciences on speciality 05.13.06 - Automation and control of technological processes and manufactures.