Security Codes Based on Optimum Error Detection Codes for Unconditional Secure Communications

Fei Pan[1, 2], Guangnan Zou[1], Yun Shi[1], Jianlang Wu[2], Yifan Wu[2], Hong Wen[2], Qiang Liu[2]

[1]Space Star Technology Co. Ltd., Beijing, 100086
[2] University of Electronic Science & Technology of China, Chengdu, 611731, China
panfeivivi@hotmail.com, sunlike@uestc.edu.cn.

Abstract. Unlike traditional security communication systems, unconditional security communication system takes the advantage of the channel noisy to keep the transmitted signals secret to Eve while the legitimate partners can receive the signals perfectly without distribution and management of the secret keys. Security coding is important to an unconditional security communication system. The basic principle of the security codes is introduced and the analysis of security properties is given. Finally, extensive simulations are conducted by using the security code constructed from the optimal error-checking binary primitive BCH code and the non-optimal error-checking binary primitive BCH code as security codes**.**

Keywords: Unconditional security communication, security codes, wire-tap channel

1. Introductions

In application layer, traditional security communication systems encrypt data by encrypting secret message by a pre-shared secret key between two partners. However, this solution is called computing limited security communication which can be broken if the computing time and source is unlimited. With the development of computing abilities, the existing traditional secure system can be broken easily in the near future. In addition, this kind of data encryption generally requires a strictly secure channel between legitimate partners to distribute, manage and destroy the secret keys. Once the secure channel is intercepted, the security communication system will be destroyed.

Different from classical security communication systems, information security of physical layer makes full use of the properties of the channel itself, such as noisy, coding, modulation etc. to hide information. As a result, the legitimate partners are able to get correct messages while Eve can never distinguish useful information from noise. It has been proved that if the error probability of the eavesdropper's channel is higher than the main channel's, it will be possible to build unconditional secure communications without pre-shared secret keys [1, 2]. The study in [3] presents that there are two steps to achieve unconditional secure communications. Firstly, we have to establish superiorities of legitimate channel and then to extend superiorities by using security coded. It is proved [3, 4] that the dual code of optimum error detection code [6,

7] is one of the best security codes among error correction codes. In this paper, we studied the security codes constructed from the dual codes of the BCH codes [5] on the basis of the model of the wire-tap channel. Our research shows that when the input information exceeds the error threshold, the optimum error detection code is able to extend errors. In the end, we performed a simulation by taking the dual code of the optimum error detection code as security code and the result proved the system has the ability to achieve unconditional secure communications.

2. The Model of Unconditional Secure Communication System

In figure 1, we present an unconditional security communication system model which is based on the wiretap channel I. Under the initial conditions, $\sum$ and ^{TM} are the error probabilities of the main channel and the eavesdropper's channel, respectively. Under the initial conditions, the quality of the main channel is worse than the quality of the wiretap channel which means $\sum \varepsilon^{TM}$.

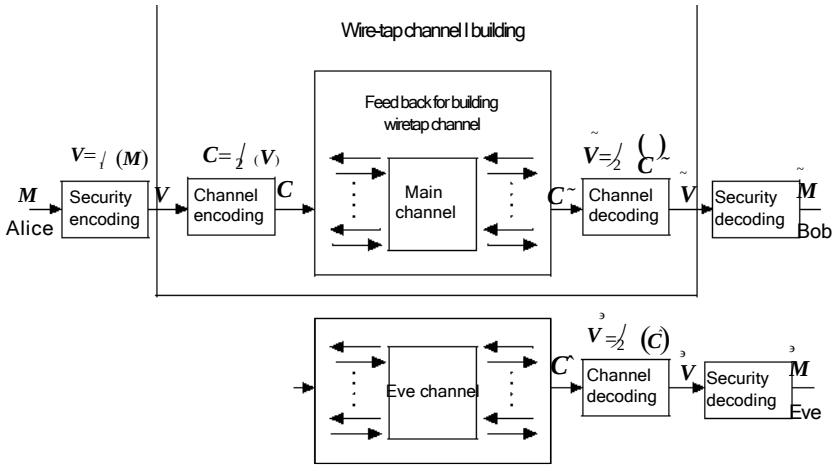

Fig. 1. The model of unconditional security communication system

Alice wants to transmit a *k*-bit message $\boldsymbol{M}$ to Bob and she selects a $(n_1,n_1 - k)$ linear binary code $\boldsymbol{V}$ such that

$$\boldsymbol{V} = \{\quad\}_1 \quad , \quad 0,1^{n}. \qquad \textbf{(1)}$$

The coding rate of the security code is $R_S = k\, n_1$. Alice continues to encode the n_1 -bit sequence V to a n_2 -bit code such that

$$\boldsymbol{C} = \ /_2(\boldsymbol{V}), \boldsymbol{V} \ \{\ \}\ _2$$

$$0,1^{\,n}. \quad \textbf{(2)}$$

Now the coding rate of the error correction code is $R_c = n_1\ n_2$ and the coding rate of the joint code is $R = k\ n_2$. The traffic communication between the main channel and the eavesdropper's channel deteriorates the properties of the eavesdropper's channel. The n_2 -bit sequence $\boldsymbol{C}$ is transmitted in the main channel and the wire-tap channel which are disposed. Bob receives $\boldsymbol{C}^{\sim}$ and Eve receives $\boldsymbol{C}^{\hat{}}$. Both of them decode the sequence in the same way. $\not\prec_1(\square)$ and $\not\prec_2(\square)$ are the invertible functions of the channel encoding function $\not\prec_1(\square)$ and $\not\prec_2(\square)$, respectively.

3. Security Coding Method

As mentioned in this paper, the basic idea of unconditional security communication system is making use of the properties of noise to deteriorate the eavesdropper's channel and then we can achieve the secure communications by using security codes to extend the advantages of the main channel. It is required in the secure communications that the legitimate partners are supposed to realize an almost error-free communication and the error probability of the eavesdropper's channel achieves 0.5. Formally, let

$\boldsymbol{M}=(m_1,m_2,\ldots,m_k)$, $\boldsymbol{M}=(m^{\sim}_1,m^{\sim}_2,\ldots,m^{\sim}_k)$, $\hat{\boldsymbol{M}}=(\hat{m}_1,\hat{m}_2,\ldots,\hat{m}_k)$ denote Alice's message, Bob's decoded message and Eve's decoded message, respectively. Perfect security is said to be achieved if the following relations holds:

$$\Pr(m^{\sim}_i \ \bar{m}_i)= 0, \quad \textbf{(3)}$$

$$\Pr(\hat{m}_i \ \bar{m}_i) = 0.5\ . \quad \textbf{(4)}$$

After the wiretap channel building, the legitimate main channel has almost achieved error-free, although the error probability of the eavesdropper's channel is not 0.5. The security code can extend errors of the eavesdropper's channel and let error probability of the eavesdropper's channel equals to 0.5.

The security codes constructed from the dual codes of the error correction codes is called the coset codes. The encoding process is as the following. If the sender wants to send a *k*-bit message $\boldsymbol{M} = (\ m_0\ ,\ m_1\ ,\ \ldots\ ,\ m_{k\square 1}), 0,1,\ ,2\ 1$, the sender selects a $(n,\ n\ \square\ k)$ code. Let each $\boldsymbol{M}^j$ which is the syndrome of the $(n,\ n\ \square\ k)$ code corresponds to a codeword's head coset $\boldsymbol{W} = (\ w_0\ ,\ w_1\ ,\ \ldots\ ,\ w_{n\square 1})$. Codeword

$\boldsymbol{C}_i = (c^i_1, \square\square, c \quad c^i_{n\square 1} \quad i = 0,1,\ldots,2^{n\square k} 1$ is randomly$\square$ chosen from the $(n, n \square k)$ code. Therefore, we get the sending code $\boldsymbol{V}_i$ by computing $\boldsymbol{V}_i = \boldsymbol{C}\ \boldsymbol{W}+ .$ We can define the *j*th coset set as $_{j\ \ i\ \ j}$

$_j = \{\boldsymbol{V}_{ij} \quad 2_{n\square k} 1\}$. The legitimate$\square$ partners received almost error free vector $\boldsymbol{V}_i^{j'}$. The decryption process is as the following:

$$\boldsymbol{k}=\boldsymbol{V}_i^{j'}\oplus \boldsymbol{H}^T= (\boldsymbol{0}+ \boldsymbol{W}^j)\ \boldsymbol{H}^T= \boldsymbol{W}* \boldsymbol{H}_T . \quad \textbf{(5)}$$

Owe to the existence of the error vector $\boldsymbol{E} = (e_{j\ 0}, e_{j\ 1}, \ldots, e_{j\ 0})$ in the eavesdropper's channel, the Eve receives $\boldsymbol{V}_i^{j''} = \boldsymbol{V}_{j\ i}\boldsymbol{E}_j+ .$ Both the legitimate users and Eve decode the code by Eq. (5), where the recovering methods are as Eq. (6) and (7).

$$\boldsymbol{M}_j=\boldsymbol{V}^{j'}\oplus \boldsymbol{H}^T= (\boldsymbol{C}^i+ \boldsymbol{W}^j)\ \boldsymbol{H}^T= \boldsymbol{W}\iota \quad \textbf{(6)}$$

$$\boldsymbol{M}_{j''} = \boldsymbol{V}^{j''}\oplus \boldsymbol{H}^T= (\boldsymbol{C}^i+ \boldsymbol{W}^j+ \boldsymbol{E}^j)\ \boldsymbol{H}^T= \boldsymbol{M}^j+ \boldsymbol{E}\lambda\ \boldsymbol{H}^{\mathrm{T}} . \quad \textbf{(7)}$$

where $\boldsymbol{M}_{j'}$ and $\boldsymbol{M}_{j''}$ are the decoded messages of the legitimate and Eve, respectively. $\boldsymbol{H}$ is the parity check matrix of the $(n, n \square k)$ code. The legitimate receiver recovers the message successfully by Eq. (6) while $\boldsymbol{E}^j \oplus \boldsymbol{H}^T$ becomes the extra noise to the decoded message of Eve which has been shown in Eq. (7).

Example 1: Alice sends a 3-bit message $\boldsymbol{M} = (0,\ 1,\ 1)$ to the legitimate partner Bob by choosing a (6, 3) code. Obviously, $\boldsymbol{W} = (0,1,0,0,0,0)$ corresponds to the message. Alice encodes a codeword $\boldsymbol{V} = (0,0,0,0,1,1)$ by randomly choosing $\boldsymbol{C} = (0,1,0,0,1,1)$. $\boldsymbol{V}$ is transmitted in an almost error-free main channel and Bob gets decoded message $\boldsymbol{M}'=(0,1,1)\ \boldsymbol{M}$ by= Eq. (6). An error vector $\boldsymbol{E} =(0,0,0,1,0,0)$ is added to $\boldsymbol{V}$ in the eavesdropper's channel. As a result, Eve gets $\boldsymbol{V}'=(0,0,0,1,1,1)$. By Eq. (7), the Eve recovers a wrong message $\boldsymbol{M}''=(1,1,1)\ \boldsymbol{M}$.

Lemma 1: If the eavesdropper's received vector is $V_i = V_i E + j$ such that $\Pr(V_j \mid V_{j^*}) = 2^{-k}$, which means that the eavesdropper's received vector has the same probability to fall into the jth coset set. We can conclude that the decoding error probability of the eavesdropper is $\Pr(M_j \neq M'_j) = 0.5$

Lemma 1 presents the essential principle that chooses the security code. If we choose the dual code of the optimum error detection code as a security code, Lemma 1 can be realized. Until now, the known optimum error detection codes include Hamming codes, double error-correcting BCH codes, Golay codes and first order RM codes. In this paper, we take the double error-correcting BCH codes as examples.

4. Simulation Results

Taking double error-correcting binary BCH code as an example where $t = 2$, the minimum code distance is $d = 2t + 1 = 5$. The encryption process is stated as the following:

1) Send a k-bit message $M = (m_0, m_1, \ldots, m_{k-1})$ and choose C from a $(n, n-k, 5)$ BCH code.

2) Find the $W = (w_0, w_1, \ldots, w_{n-1})$ which corresponds to M and satisfies the relationship $M = W H^T$ where H is the check matrix of C.

3) Choose the codeword $C_i = (c_{i0}, c_{i1}, \ldots, c_{i(n-1)})$, $i = 0,1,\ldots 2^{n-k} - 1$ randomly from the $(n, n-k, 5)$ BCH code C.

4) Compute $V_i = W C_i$ to get the sending code V. Encryption completes.

During the simulation, we select a $n = 2^l$ BCH code where l is chosen from 1 to 10. We suppose the eavesdropper's error probability threshold is 0.495 which means that when the error probability of decoded message of the eavesdropper achieves 0.495 the system achieves the security. Table 1 presents the threshold error probabilities when the security codes with different lengths. In this table, R_S denotes the rate of security codes and S is the channel transfer probability of the eavesdropper's channel. By using the security codes constructed from BCH codes, the channel transfer probability S can be extended over 0.495.

Table 1. The error probabilities when BCH codes are used as security codes

BCH codes (t=2)	R_S	δ
(31,21)	0.3226	0.1501
(63,51)	0.1905	0.0761
(127,113)	0.1102	0.0399
(255,239)	0.0627	0.0187

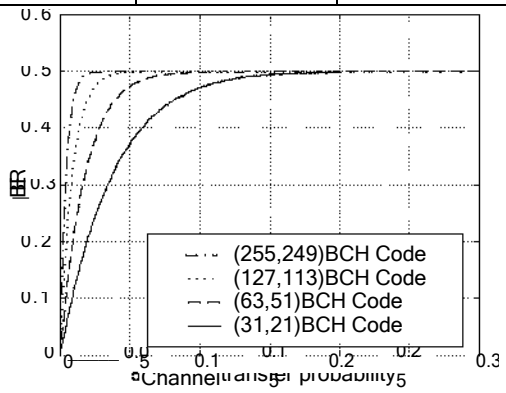

Fig. 2. The performances of the security codes from BCH codes in Table 1

The performances of the security codes from BCH codes in Table 1 are showed in figure 2. In figure 2, if we send a 10-bit message and choose the dual code of a (31, 21) BCH code as the security code, the code rate will be $R_S = 10\ 31\ 0.3226 =$. If the error probability of the eavesdropper's channel is over 0.1501, security codes will be an effective way to extend the eavesdroppers' error probability over0.495. At the meantime, the message is transmitted correctly in the main channel will be almost error-free, and our goal of security has been achieved. To compare with the BCH codes, the performances of the dual codes of the RM codes and the Hamming codes as the secure codes are shown in figure 3 and figure 4, respectively.

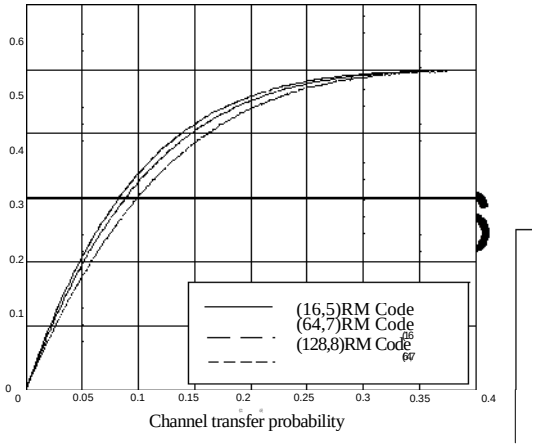

Fig. 3. The performances of the security codes derived from RM codes

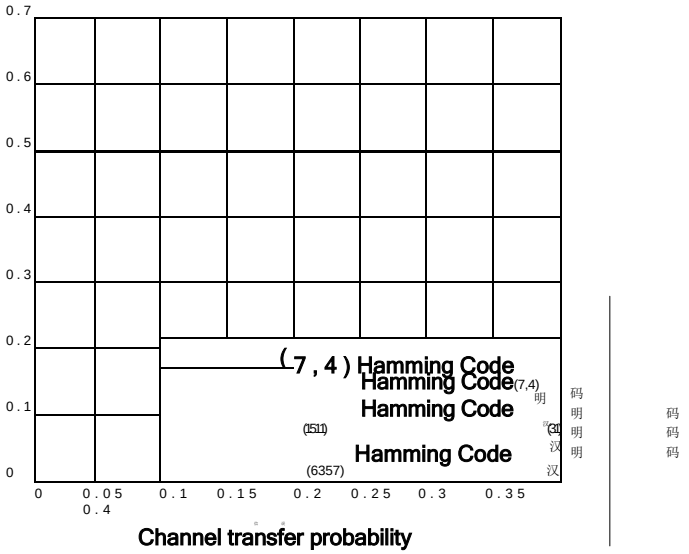

Fig. 4. The performances of the security codes derived from Hamming codes

5. Conclusions

This paper investigated the security codes derived from several kinds of error correction codes over an unconditional secure communication system. By analyzing the security condition of the security codes, we state that if the dual codes of the

optimum error detection codes are taken as security codes the security condition can be realized. By simulation, the performances of security codes derived from the double error correcting BCH codes, RM codes and Hamming codes indicate that the main channel is almost error-free while the error probability of the eavesdropper approaches to 0.5. Thus the desired secure communication is realized.

Acknowledgment

This paper is supported by the Open Research Funds of the Academy of Satellite Application of China Aerospace Science and Technology Corporation under grant NO. SSTC-TX-01-03

References

1. A. D. Wyner: The Wire-tap Channel. Bell Syst. Tech. [J], 1975, 54(2): 1355-1387.
2. U. Maurer: Secret Key Agreement by Public Discussion from Common Information. IEEE Trans. Inform. Theory, 1993, 39(4): 733-742.
3. Hong Wen, P. Ho and X. Jiang: On Achieving Unconditional Secure Communications over Binary Symmetric Channels (BSC). IEEE Wireless Communications Letters, 2012, 1(2): 49-52.
4. A. Thangaraj, S. Dihidar, A. R. Calderbank, S. W. McLaughlin, and J.-M. Merolla: Applications of LDPC Codes to The Wiretap Channels. IEEE Trans. Inf. Theory, 2007, 53(8): 2933-2945.
5. F. J. Mac Williams and N. J. A. Sloane: The Theory of Error Correcting Codes. Amsterdam: North-Holland, 1977.
6. Leung C., Barnes, B. R. Friedman: On Some Properties of The Undetected Error Probability of Linear Codes. IEEE Trans. Inform. Theory, 1979, 37(3): 110-112.
7. Xinmei Wang, Guozhen Xiao: Error Correcting Codes-Principle and Method (in Chinese). Xi'an: Xidian University Press, 2001: 52-161.
8. Ong. C. T and Leung C.: On The Undetected Error Probability of Triple-error-correcting BCH Codes. IEEE Trans. Inform. Theory, 37(3) 1991: 673-678.
9. Shichao Lv, Hong Wen, Qiwei Han: The Security Analysis of Multi-antenna Broadcast Channel Model Based on Block Diagnolization Precoding (in Chinese). Information Security and Communication Secrecy, 2011(8): 50-53.
10. Jianqiang Li, Shichao Lv, Mengying Ren, Jie. Fan, Hong Wen: Research and Design of Instant Message Monitor System (in Chinese). Information Security and Communication Secrecy, 2012(8): 116-118.