Journal of Information Hiding and Multimedia Signal Processing ©2014 ISSN 2073-4212
Ubiquitous International Volume **5**, Number **2**, April **2014**

A New Framework of Steganography Using the Content of Cover Data

Takashi Mihara

Department of Information Sciences and Arts
Toyo University
2100 Kujirai Kawagoe, Saitama, 350-8585, Japan
mihara@toyo.jp

Received April, 2013; revised September, 2013

Abstract. *In today's information-oriented societies, the information is a weapon. Therefore, the information is encrypted and is transmitted to the legitimate parties. However, messages made by cryptography are unnatural, and eavesdroppers can easily target these encrypted messages. That is why steganography is proposed. Steganography is a technique hiding secret information within innocent-looking information (e.g., text, audio, image, video, and so on). In this paper, we propose a stegosystem that uses not only cover data as media transmitting secret messages but also cover data as information recovering secret messages. Secret messages are recovered under cooperating with cover messages. Our systems use also the contents of cover messages themselves. Furthermore, encoded cover messages can have the same forms in before and after embedding secret messages because secret messages are embedded as random values used as one element of the encoded process when cover messages are encoded.*
Key words: Information hiding, Steganography, Cryptography, Entangled state.

1. **Introduction.** Nowadays, the information is very important to information-oriented societies. Therefore, some messages must be sent secretly and must be protected against eavesdroppers. Cryptography is one of the methods to solve this problem. Cryptography is a technique making secret messages unreadable and is a technique hiding the contents of the messages against eavesdroppers. However, these encrypted messages are obviously unnatural, and eavesdroppers can easily notice that these messages may be important.

Another method to solve the problem mentioned above is to use steganography. Steganography is a technique hiding secret messages within innocent-looking information called cover data (e.g., text, audio, image, video, and so on), i.e., steganography is a technique hiding the existence of secret messages against eavesdroppers. Messages made by steganography (i.e,. messages used as cover data) are natural and secret messages are hidden in these messages. Therefore, eavesdroppers may pass them with high probability.

In the similar way as cryptography, there might be this way of thinking from old days. Simmons introduced the *Prisoners' Problem* as a typical problem of steganography [1].

> Two prisoners, Alice and Bob want to hatch an escape plan. However, the prisoner warden monitors any communication between them. Since messages made by cryptography are detected by the warden, they cannot attain their purpose. Therefore, Alice and Bob must design a method to keep their communications as natural as possible against the warden.

In order to solve the Prisoners' Problem, many methods have been proposed. Namely, both many media and many methods embedding secret messages have been proposed. For more details on concrete methods, see, e.g., [2] and references therein. However, many of them are heuristic approaches such as using video systems and digital images made modifications to be hard to notice human beings (also see [3, 4, 5] and references therein).

Moreover, in the Prisoners' Problem, Alice and Bob must share keys against the warden in order to be recovered the embedded messages by Bob. This situation is the same as cryptography up to the early 1970s, i.e., there existed the key exchange problem. In cryptography, this problem was solved by the public-key cryptography. Also in steganography, stegosystems using public-key cryptosystems, public-key steganography, are proposed [2, 6, 7].

Major characteristics of our proposed steganography are as follows. First, secret messages are recovered under cooperating with cover messages. In ordinary steganography, the structures of cover messages are used when secret messages are embedded. On the other hand, our proposed steganography uses also the contents of cover messages themselves. Second, encoded cover messages can have the same forms in before and after embedding secret messages unlike ordinary stegosystems. Encoded cover messages of ordinary stegosystems are modified by embedding secret messages in general. However, secret messages in our cryptosystem are randomized and are embedded as random values used when cover messages are encoded. Therefore, the form of encoded cover messages is same in before and after embedding secret messages. In addition, overall communication protocols using random values can also use our system.

The remainder of this paper has the following organization. In Section 2, we define our proposed stegosystems and show some characteristics. In Section 3, we give examples of our proposed stegosystems. One is cryptographic steganography, i.e., we show a method embedding secret messages to ciphertexts. Another is quantum steganography, i.e., we show a method using cover messages as secret keys in addition to hiding secret messages. Finally, in Section 4, we describe some concluding remarks.

2. **Proposed Steganography.**

2.1. **Basic Form.**

In this subsection, we show a basic form of our steganography. Our proposed stegosystem uses not only cover data as media transmitting secret messages but also cover data as information recovering secret messages. First, we show our stegosystem in the following way.

Definition 2.1. *A stegosystem is a seven-tuple (*$\mathbf{M}$*,* $\mathbf{C}$*,* $\mathbf{D}$*,* $\mathbf{D}'$*,* $\mathbf{S}$*,* **EMB***,* **REC***), where the following conditions are satisfied:*

$\mathbf{M}$ *is a set of secret messages(i.e., embedded messages),*
$\mathbf{C}$ *is a set of cover messages,*
$\mathbf{D}$ *is a set of fragmental messages,*
$\mathbf{D}'$ *is a set of randomized fragmental messages,*
$\mathbf{S}$ *is a set of stego messages,*
EMB *is a set of embedding procedures (*$\mathbf{F}_A$,$\mathbf{G}_A$,**CO***) (i.e.,* $Emb : \mathbf{M} \times \mathbf{C} \to \mathbf{S}$ *for* $Emb \in$ **EMB** *satisfying* $f_A : \mathbf{M} \times \mathbf{C} \to \mathbf{D}$*,* $g_A : \mathbf{D} \to \mathbf{D}'$*, and* $Code : \mathbf{C} \times \mathbf{D}' \to \mathbf{S}$ *for* $f_A \in \mathbf{F}_A$*,* $g_A \in \mathbf{G}_A$*, and* $Code \in$ **CO***), and*
REC *is a set of recovering procedures (*$\mathbf{F}_B$,$\mathbf{G}_B$,**DEC***) (i.e.,* $Rec : \mathbf{S} \to \mathbf{M}$ *for* $Rec \in$ **REC** *satisfying* $f_B : \mathbf{C} \times \mathbf{D} \to \mathbf{M}$*.* $g_B : \mathbf{D}' \to \mathbf{D}$*, and* $Dec : \mathbf{S} \to \mathbf{C} \times \mathbf{D}'$ *for* $f_B \in \mathbf{F}_B$*,* $g_B \in \mathbf{G}_B$*, and* $Dec \in$ **DEC***).*

Next, we show a general processing flow for using our stegosystem. Now, let us consider that Alice wants to send a secret message $m \in \mathbf{M}$ (i.e., an embedded message) to Bob. They regularly exchange messages each other because he is her boss. In this case, however, she hates her colleagues to know about this because the secret message m is her resignation. Therefore, she thinks of hiding the message m to a report $c \in \mathbf{C}$(i.e., a cover message) to him. Here, m and c may be plaintexts or may be ciphertexts used between them.

First, Alice computes $f_A(m, c) = d \in \mathbf{D}$. This is a process obtaining some information including both the secret message m and the cover message c. However, the secret message m may be able to be guessed by using d(and c). Therefore, she further computes $g_A(d) = d' \in \mathbf{D}$ (By this process, the message d is randomized). Finally, she encodes the message d' by $Code(c, d') = s \in \mathbf{S}$, and sends it to Bob. Bob decodes the message s by $Dec(s) = (c, d')$, and computes $g_B(d') = d$. Finally, he recovers the secret message m by computing $f_B(c, d) = m$.

Major characteristics of our proposed steganography are as follows. First, secret messages are recovered under cooperating with cover messages. Secret messages of ordinary stegosystems are independent of cover messages. Cover messages are only media transmitting secret messages, and are not explicitly used as recovering secret messages. The structures of cover messages are used when secret messages are embedded. On the other hand, our proposed stegosystem uses also the contents of cover messages themselves, i.e., first, Bob obtains the cover message c by $Dec(s) = (c, d')$, obtains the fragmental message d (the message made by the secret message m and the cover message c) by $g_B(d') = d$), and can recover m by using the cover message c and the fragmental message d and by computing $f_B(c, d) = m$.

Second, encoded cover messages can have the same forms in before and after embedding secret messages unlike ordinary stegosystems. In our proposed stegosystem, when cover messages are encoded, secret messages are randomized by $g_A(d) = d'$ and are embedded as random values by $Code(c, d') = s$. The random value d' is one element of the encoded process of $Code(c, d')$. Namely, we can also select such an encoded procedure using random values in general. Encoded cover messages of ordinary stegosystems are modified by embedding secret messages in general.

Finally, overall communication protocols using random values can use our system as steganography. Moreover, as cover data, our system can not only use texts but also use image data, sound data, and so on.

2.2. **Modified Form.** In the previous subsection, we showed a stegosystem using cover messages in the recovering process. In some encoded/decoded processes, however, cover messages may not be recovered perfectly because of the encoded structures. Next, we show a stegosystem using two different cover messages.

Definition 2.2. *A stegosystem is a eight-tuple (*$\mathbf{M}$*,* $\mathbf{C}$*,* $\mathbf{C}'$*,* $\mathbf{D}$*,* $\mathbf{D}'$*,* $\mathbf{S}$*,* **EMB***,* **REC***), where the following conditions are satisfied:*

$\mathbf{M}, \mathbf{C}, \mathbf{D}, \mathbf{D}'$*, and* $\mathbf{S}$ *are the same sets as the sets of Definition 2.1,*
$\mathbf{C}'$ *is a set of second cover messages,*
EMB *is a set of embedding procedures (*$\mathbf{F}_A$,$\mathbf{G}_A$,**CO***) (i.e.,* $Emb : \mathbf{M} \times \mathbf{C} \times \mathbf{C}' \to \mathbf{S}$ *for* $Emb \in$ **EMB** *satisfying* $f_A : \mathbf{M} \times \mathbf{C} \to \mathbf{D}$*,* $g_A : \mathbf{D} \to \mathbf{D}'$*, and* $Code : \mathbf{C}' \times \mathbf{D}' \to \mathbf{S}$ *for* $f_A \in \mathbf{F}_A$*,* $g_A \in \mathbf{G}_A$*, and* $Code \in$ **CO***), and*
REC *is a set of recovering procedures (*$\mathbf{F}_B$,$\mathbf{G}_B$,**DEC***) (i.e.,* $Rec : \mathbf{S} \times \mathbf{C} \to \mathbf{M}$ *for* $Rec \in$ **REC** *satisfying* $f_B : \mathbf{C} \times \mathbf{D} \to \mathbf{M}$*.* $g_B : \mathbf{D}' \to \mathbf{D}$*, and* $Dec : \mathbf{S} \to \mathbf{D}'$ *for* $f_B \in \mathbf{F}_B$*,* $g_B \in \mathbf{G}_B$*, and* $Dec \in$ **DEC***).*

In this stegosystem, even if $d \in \mathbf{D}$(or $d' \in \mathbf{D}'$) is known to the third parties, the secret message $m \in \mathbf{M}$ is safe because $c \in \mathbf{C}$ is independent of $c' \in \mathbf{C}'$ (as far as it is not known that c is the cover message). Moreover, our system can recover the secret message m even if c' cannot be recovered perfectly.

3. Examples.

3.1. **Cryptographic Steganography.** In this subsection, we describe an example of a stegosystem using ciphertexts as cover data. Namely, other secret messages are included in encrypted messages. Although we cannot adapt this method to the Prisoners' Problem [1] because the warden can immediately feel the messages strange, today's information-oriented societies need these encrypted messages on the Internet. One example is as follows:

> Let X and Y be two companies. Alice and Bob are staffs of X company, and Carol is a staff of Y company. Moreover, Alice is on loan to Y company because of a joint research. Messages communicating between the two companies are encrypted naturally because the messages include industrial secrets. In addition, when Alice sends messages to Bob, Carol checks the messages in order not to be leaked another important information of Y company. Alice wants to send Y company's secret information to Bob.

As another situation, it is also considered that Bob wants to send X company's messages to Alice without being known by Carol.

In order to solve this problem, we denote a steganography using ciphertexts as cover messages. Although our steganography uses ciphertexts made by some cryptosystems as cover messages. we cannot use all types of cryptosystems as our steganography. We can only use some restricted cryptosystem as follows:

Definition 3.1. *A cryptosystem is a six-tuple (*$\mathbf{M}_p$, $\mathbf{M}_c$, $\mathbf{K}$, $\mathbf{K}_r$, $\mathbf{F}_e$, $\mathbf{F}_d$*), where the following conditions are satisfied:*

> $\mathbf{M}_p$ *is a finite set of plaintexts,*
> $\mathbf{M}_c$ *is a finite set of ciphertexts,*
> $\mathbf{K}$ *is a finite set of keys,*
> $\mathbf{K}_r$ *is a finite set of random values, and*
> *for* $f_e \in \mathbf{F}_e$ *and* $f_d \in \mathbf{F}_d$, $f_e : \mathbf{M}_p \times \mathbf{K} \times \mathbf{K}_r \to \mathbf{M}_c$ *and* $f_d : \mathbf{M}_c \times \mathbf{K} \to \mathbf{M}_p \times \mathbf{K}_r$.

The characteristic of this cryptosystem used as steganography is that a sender Alice must generate random values in $\mathbf{K}_r$ and a receiver Bob must be able to obtain them by f_d. Therefore, we specify explicitly $\mathbf{K}_r$ in f_d although it is unnecessary as a cryptosystem.

Here, we modify the system of Definition 3.1 to our proposed steganography in the following way.

Definition 3.2. *A cryptographic steganography based on cryptosystems is a six-tuple (*$\mathbf{M}_p$, $\mathbf{M}_c$, $\mathbf{K}$, $\mathbf{M}_s$, $\mathbf{F}_e$, $\mathbf{F}_d$*), where the following conditions are satisfied (we denote only the difference from Definition 3.1):*

> $\mathbf{M}_s (\subseteq \mathbf{K}_r)$ *is a finite set of embedded messages, and*
> *for* $f_e \in \mathbf{F}_e$ *and* $f_d \in \mathbf{F}_d$, $f_e : \mathbf{M}_p \times \mathbf{K} \times \mathbf{M}_s \to \mathbf{M}_c$ *and* $f_d : \mathbf{M}_c \times \mathbf{K} \to \mathbf{M}_p \times \mathbf{M}_s$.

Since Alice prepares embedded messages and embeds them as elements in $\mathbf{M}_s$, $\mathbf{M}_s \subseteq \mathbf{K}_r$. Namely, embedded messages are created as random values in $\mathbf{M}_s$. Therefore, the correspondence to our stegosystem in the previous section is as follows: $\mathbf{M}_p = \mathbf{C}$, $\mathbf{M}_c = \mathbf{S}$, $\mathbf{M}_s = \mathbf{D}'$, $\mathbf{F}_e = \mathbf{EMB}$, and $\mathbf{F}_d = \mathbf{REC}$.

For example, a stegosystem based on OAEP [8], which is an extension of RSA, is defined as a six-tuple $(\mathbf{M}_p, \mathbf{M}_c, \mathbf{K}, \mathbf{M}_s, \mathbf{F}_e, \mathbf{F}_d) = (\{0,1\}^k, \{0,1\}^{k+k_0+k_1}, \mathbf{K}, \mathbf{M}_s \subseteq \{0,1\}^{k_0}, \mathbf{F}_e, \mathbf{F}_d)$. where the following conditions are satisfied:

> $\mathbf{K}, \mathbf{F}_e$, and $\mathbf{F}_d$ are a set of keys, a set of encryption functions, and a set of decryption functions based on RSA, respectively,
> $G : \{0,1\}^{k_0} \to \{0,1\}^{k+k_1}$ and $H : \{0,1\}^{k+k_1} \to \{0,1\}^{k_0}$ are random functions prepared between Alice and Bob, and
> let $m \in \mathbf{M}_p$, $c \in \mathbf{M}_c$, $m_s \in \mathbf{M}_s$, $f_e \in \mathbf{F}_e$, and $f_d \in \mathbf{F}_d$. Then, encryption rules are $s = (m \| 0^{k_1}) \oplus G(m_s)$ and $c = f_e(s \| m_s \oplus H(s))$, and decryption rules(and extraction rules) are $s = upper_{k+k_1}(f_d(c))$, $m_s = lower_{k_0}(f_d(c)) \oplus H(s)$, and $m = upper_k(s \oplus G(m_s))$, where $x \| y$ is the concatenation of two bit strings x and y, and $upper_a(x \| y) = x$ and $lower_b(x \| y) = y$ for $|x| = a$ and $|y| = b$.

In this stegosystem, the method of extracting the embedded text m_s is obtained as a part of the decryption rules. Moreover, if we make the embedded text m_s by using the Vernam cipher known as an unconditionally secure cryptosystem, we cannot distinguish between m_s and a random value. This means that we cannot distinguish between the cover message and the embedded message.

As another examples, McEliece cryptosystem [9] and Goldwasser-Micali cryptosystem [10], which are probabilistic cryptosystems, are one of candidates of our steganography. Moreover, digital signatures and communication protocols using random values can be also used.

3.2. **Quantum Steganography.** In general stegosystems, stego data are constructed by modifying cover data, i.e., stego data are made by embedding secret messages to cover data. However, our stego data in this subsection are constructed by combining some quantum states with secret messages and classical messages corresponding to cover data.

Let $\mathbf{M}=\mathbf{C}=\mathbf{D}(=\mathbf{D}') = \{0, 1, 2, \ldots, N-1\}$ for a positive integer N. Moreover, let $\mathbf{S}=\{\frac{1}{N}\sum_{x=0}^{N-1}\sum_{y=0}^{N-1} e^{-\imath 2\pi dx/N}|x+y\rangle|y\rangle|x\rangle|y\rangle | x, y \in \{0,1,2,\ldots,N-1\}, d \in \mathbf{D}\}$, where $\imath^2 = -1$. Now, let a secret message $m \in \mathbf{M}$ and a cover message $c \in \mathbf{C}$. Then, we construct a protocol(**EMB** and **REC**) in the following way. For more details on quantum information theory, see, e.g., [11] and references therein.

Our Proposed Protocol.

S_1: Alice and Bob share an entangled state

$$\frac{1}{\sqrt{N}}\sum_{x=0}^{N-1}|x\rangle|x\rangle \text{ and } \frac{1}{\sqrt{N}}\sum_{y=0}^{N-1}|y\rangle|y\rangle$$

in advance, where Alice has each first register, and Bob has each second one. The states must be shared securely between the parties. Note that this step can be executed between them with being independent of both a secret message m and a cover message c, i.e., they do not need to decide the messages in this step.

S_2: After deciding a secret message m sending to Bob and a cover message c(Bob also knows the message c), Alice computes $m + c \equiv d \pmod N \in \mathbf{D}(= \mathbf{D}')$ and makes a state

$$\frac{1}{\sqrt{N}}\sum_{x=0}^{N-1} e^{-\imath 2\pi dx/N}|x\rangle|x\rangle$$

corresponding to the secret message m and the cover message c.

S_3: Alice combines the two entangled states as follows:

$$(\frac{1}{\sqrt{N}}\sum_{x=0}^{N-1} e^{-\imath 2\pi dx/N}|x\rangle|x\rangle)(\frac{1}{\sqrt{N}}\sum_{y=0}^{N-1}|y\rangle|y\rangle)$$
$$\rightarrow \quad \frac{1}{N}\sum_{x=0}^{N-1}\sum_{y=0}^{N-1} e^{-\imath 2\pi dx/N}|x+y\rangle|y\rangle|x\rangle|y\rangle,$$

where Alice has the first two registers and Bob has the remaining two registers.

This state is the stego data corresponding to the message m embedded to the message c. Note that the message m is independent of the message c. Therefore, Alice can use any natural plaintexts as the classical messages constructing cover data, and do not need to modify the messages in constructing the corresponding stego data.

S_4: Alice sends the second register($|y\rangle$) to Bob. This procedure is regarded as same as Step S_1 shared entangled states.

S_5: Bob can recover the message d by applying the quantum Fourier transform to all the registers, i.e.,

$$\frac{1}{N}\sum_{x=0}^{N-1}\sum_{y=0}^{N-1} e^{-\imath 2\pi dx/N}|x+y\rangle|y\rangle|x\rangle|y\rangle$$
$$\rightarrow \quad \frac{1}{N^3}\sum_{x=0}^{N-1}\sum_{y=0}^{N-1}\sum_{x_1=0}^{N-1}\sum_{y_1=0}^{N-1}\sum_{x_2=0}^{N-1}\sum_{y_2=0}^{N-1} e^{-\imath 2\pi dx/N}$$
$$\times e^{\imath 2\pi(x+y)x_1/N} e^{\imath 2\pi y y_1/N} e^{\imath 2\pi x x_2/N} e^{\imath 2\pi y y_2/N}|x_1\rangle|y_1\rangle|x_2\rangle|y_2\rangle$$
$$= \frac{1}{N^3}\sum_{x_1=0}^{N-1}\sum_{y_1=0}^{N-1}\sum_{x_2=0}^{N-1}\sum_{y_2=0}^{N-1}(\sum_{x=0}^{N-1} e^{\imath 2\pi(x_1+x_2-d)x/N})$$
$$\times(\sum_{y=0}^{N-1} e^{\imath 2\pi(x_1+y_1+y_2)x/N})|x_1\rangle|y_1\rangle|x_2\rangle|y_2\rangle$$
$$= \frac{1}{N}\sum_{x_1+x_2\equiv d \pmod N}\ \sum_{x_1+y_1+y_2\equiv 0 \pmod N} |x_1\rangle|y_1\rangle|x_2\rangle|y_2\rangle$$

Then, Bob can recover the message m because he can first obtain x_2, y_1 and y_2, and then he can obtain x_1 satisfying $x_1+y_1+y_2 \equiv 0 \pmod N$. Therefore, he can recover d by $x_1 + x_2 \equiv d \pmod N$ and compute $d - c \equiv m \pmod N$.

Main characteristic of this stegosystem takes the same procedure in Step S_1 and in Step S_4 when such an entangled state $\frac{1}{\sqrt{N}}\sum_{x=0}^{N-1}|x\rangle|x\rangle$ is shared between them. That is why the protocol is a stegosystem. Even if the partial state $|y\rangle$ in Step S_4 is stolen, the secret message m can be secret. In addition, this protocol can be regarded as a cryptosystem using the cover message c as the secret key if the message c is not known as the secret key against eavesdroppers.

4. **Conclusions.** In this paper, we proposed a stegosystem that uses not only cover data as media transmitting secret messages but also cover data as information recovering secret messages. In addition, in consideration of the case that cannot recover the cover data perfectly, we also showed a modified form of stegosystem. In our proposed systems, it is thought that both cover messages and secret messages are texts. However, we will be able to also use other media such as image, audio, and so on.

In our proposed steganography, secret messages are recovered under cooperating with cover messages. Our systems use also the contents of cover messages themselves. Furthermore, encoded cover messages can have the same forms in before and after embedding secret messages unlike ordinary stegosystems because secret messages in our stegosystems are randomized and are embedded as random values used as one element of the encoded process when cover messages are encoded.

Moreover, we described two examples, a cryptographic stegosystem and a quantum stegosystem. A cryptographic stegosystem is steganography using ciphertexts as encoded cover messages and embedding secret messages as random values used in the cryptosystem. In this case, we can also use ordinary steganography, e.g., steganography embedding secret messages in error-correcting codes. We use elements in $\mathbf{C}$ as cover messages and use elements in $\mathbf{D}'$ as secret messages.

A quantum stegosystem is steganography using entangled states shared between parties in advance, and the procedure(i.e., the protocol) sharing entangled states itself is hiding the transmission of secret messages. The system is steganography using cover messages as secret keys. Namely, this system can use also as cryptography. In general, cryptosystems in steganography are only used in order not to reveal the contents of the messages when embedded secret messages are found to the third parties. Obviously, steganography has some kind of associations with cryptography. Therefore, it is an interesting open problem to find a unified concept and theory between cryptography and steganography.

REFERENCES

[1] G. J. Simmons, Prisoners' problem and the subliminal channel, Proceedings of Crypt'83, pp. 51–67, 1984.

[2] R. J. Anderson and F. A. P. Petitcolas, On the limits of steganography, IEEE Journal of Selected Areas in Communications, vol. 16, no. 4, pp. 474–481, 1998.

[3] N. F. Johnson and S. C. Katzenbeisser A survey of steganographic techniques, Proceedings of Information Hiding Techniques for Steganography and Digital Watermarking, pp. 43–78, 2000.

[4] A. Westfeld, F5–A steganographic algorithm high capacity despite better steganalysis, Proceedings of the Fourth International Workshop on Information Hiding, LNCS 2137, pp. 289–302, 2001.

[5] B. Li, J. He, J. Huang, and Y. Q. Shi, A survey on Image steganography and steganalysis, Journal of Information Hiding and Multimedia Signal Processing, vol. 2, no. 2, pp. 142–172, 2011.

[6] L. von Ahn and N. J. Hopper, Public-key steganography, Proceedings of Eurocrypt'04, LNCS 3027, pp. 323–341, 2004.

[7] S. Craver, On public-key steganography in the presence of an active warden, Proceedings of the Second International Workshop on Information Hiding, LNCS 1525, pp. 355–368, 1998.

[8] M. Bellare, and P. Rogaway, Optimal asymmetric encryption, Proceedings of Eurocrypt'94, LNCS 950, pp. 92–111, 1994.

[9] R. J. McEliece, A public-key cryptosystem based on algebraic coding theory, DSN Progress Report, no. 42-44, pp. 114–116, 1978.

[10] S. Goldwasser and S. Micali, Probabilistic encryption, Journal of Computer and System Scienecs, vol. 28, no. 2, pp. 270–299, 1984.

[11] M. A. Nielsen and I. L. Chuang, Quantum computation and quantum information, Cambridge University Press, Cambridge, 2000.