International Journal of Information, Control and Computer Sciences
ISSN: 2517-9942
Vol:2, No:12, 2008

Random Oracle Model of Information Hiding System

Nan Jiang, and Jian Wang

***Abstract*—**Random Oracle Model (ROM) is an effective method for measuring the practical security of cryptograph. In this paper, we try to use it into information hiding system (IHS). Because IHS has its own properties, the ROM must be modified if it is used into IHS. Firstly, we fully discuss why and how to modify each part of ROM respectively. The main changes include: 1) Divide the attacks that IHS may be suffered into two phases and divide the attacks of each phase into several kinds. 2) Distinguish Oracles and Black-boxes clearly. 3) Define Oracle and four Black-boxes that IHS used. 4) Propose the formalized adversary model. And 5) Give the definition of judge. Secondly, based on ROM of IHS, the security against known original cover attack (KOCA-KOCA-security) is defined. Then, we give an actual information hiding scheme and prove that it is KOCA-KOCA-secure. Finally, we conclude the paper and propose the open problems of further research.

***Keywords*—**Attack, Information Hiding, Provable Security, Random Oracle Model.

I. Introduction

THE theoretical issues related to Information Hiding System (IHS) are gained more and more attention. Security is one of these theoretical issues as well as modeling, capacity and *etc*.

At present, most of the research works about security use the methods of information theory [1]-[3]. Cachin [2] uses the relative entropy between original cover c and stego-cover s. If $D(c||s)\leq\varepsilon$, then the system is defined as ε-secure. Zöllner [3] points out that a system is secure if the mutual information $I(m;s\wedge c)=0$, where m is the message. Although there have some differences between the definitions of security, they all consider that the adversary has infinitely strong calculating ability.

Whereas Stefan [4] and Jiang [5] take the practical attacking ability of the adversary into account and define the provable security of IHS using Random Oracle Model (ROM). ROM roots in the provable security theory of cryptanalysis. It provides a new method for researching the security of IHS.

Stefan and *et al* [4] analyses the main drawbacks of information-theoretical method in detail: 1) it might not be easy to construct unconditionally secure steganographic systems; 2) the probability distribution of a cover is not known in practice; 3) the approximated distribution is useless in the decision process; and 4) an eavesdropper has only limited computing power. He uses the term "Oracle" in IHS firstly and gives a secure embedding scheme based on RSA. However Stefan does not analyze the attacks. He only uses ROM formally and does not prove the scheme's security strictly.

Jiang and *et al* [5] analyses the attacks that IHS may be suffered. Based on ROM, they define and prove Chosen-Message-and-Original-Cover-Security. Whereas the ROM they used is the ROM that cryptograph used. They do not modify ROM according to the properties of IHS.

In this paper, we try to use ROM into IHS to define its provable security. Section II introduces ROM simply. However IHS has its own properties, section III modifies ROM to fit IHS. The main changes include: 1) Divide the attacks that IHS may be suffered into two phases and divide the attacks of each phase into several kinds. 2) Distinguish Oracles and Black-boxes clearly. 3) Define Oracle and four Black-boxes that IHS used. 4) Propose the formalized adversary model. And 5) Give the definition of judge. Section IV uses the modified ROM to define Known-Original-Cover-Security. Section IV also gives an information hiding scheme and prove that it is secure against Known-Original-Cover-Attack. Section V describes the concluding remarks and some problems for further research.

For the sake of simplicity, we call the ROM of IHS (i.e., the modified ROM) as "IHS ROM" and call the ROM of cryptography as "cipher ROM" in the following.

II. Cipher ROM

In 1993, Bellare and Rogaway [6] advanced the famous ROM methodology. It is derived from Fiat and Shamir's early work [7]. Before the appearance of ROM, provable security was regarded as pure theoretical issue. But now ROM is used more and more widely and a lot of practical secure schemes based on it are proposed. ROM is the most successful practical application of provable security theory [8].

ROM has two basic members: Oracle and Black-box.

Oracle can be regarded as a random generator. ROM can ensure the security of a scheme under the premises that random generator (Oracle) has no weaknesses.

Black-box is a public Oracle, i.e., all parties (including the adversary) can use it. It is relevant to the formalized adversary model. According to what kind of Black-boxes and how many Black-boxes the adversary has, he can implement different kind of attack. The definitions of security against different attacks

Manuscript received October 26, 2006.

Nan Jiang is with College of Computer Science, Beijing University of Technology, Beijing 100022, China (phone: +86-10-67396063; e-mail: jiangnan@bjut.edu.cn).

Jian Wang is with Information Security Center, Beijing University of Posts and Telecommunications, Beijing 100876, China (e-mail: wangsap@yeah.net).

are different.

ROM has two basic applications: prove the security of a protocol and construct secure protocols [9]-[12].

When prove a protocol's security, we reduce the protocol's security to an Oracle's security. Theoretically, Oracle is a random generator. But as we all know, there has no genuine random generator in practical protocols. In general, Oracle is a basic cryptographic algorithm or a mathematical difficult problem, i.e. the adversary can not break the Oracle with limited calculating ability at present. Oracle can be considered as the "atomic primitives" of the protocol. Based on the formalized adversary model, we point out that the only method to break the protocol is to break the Oracle. But it is impossible now. So the protocol is secure.

When construct a secure protocol, firstly we should figure the protocol using ROM and prove that the formalized protocol is secure. Then we replace oracle by an "appropriately chosen" function h to change the formalized protocol into a practical one.

Note that function h is relevant to whether the practical protocol can keep the formalized protocol's security. Function h must satisfy the two requirements: 1) Function h is generally considered to be a function that can satisfy the practical security of the protocol although it impossibly is a genuine random function. And 2) Function h is independent of the protocol.

III. IHS ROM

In order to fit the properties of IHS, we modify the cipher ROM. In the following of this section, we describe why and how to modify it part by part.

A. Space

IHS has three entities: covers, messages and keys. Accordingly IHS has three spaces. But these three spaces are not the same as the three spaces of cryptograph (plaintext space, ciphertext space and key space):

- A cover space C which is the set of all possible covers. It includes stego-covers as well as original covers. Stego-covers and original covers come from the same space C. This indicates that IHS must satisfy imperceptibility.
- A message space M which is the set of all possible messages.
- A key space K which is the set of all possible keys.

Without loss of generality, we assume in this paper that all elements of the three spaces are represented as binary strings, i.e., $X \subseteq \{0,1\}^*$, where $X \in \{C,M,K\}$, $\{0,1\}^*$ denotes the space of finite binary strings.

$a\|b$ or just ab denotes the string which is the concatenation of strings a and b, $\|a\|$ denote its length in bit, where $a,b \in X$.

B. Algorithm

As in cryptograph, the algorithms of IHS ROM can be divided into two kinds: one is deterministic algorithms, the other is probabilistic algorithms.

For probabilistic algorithm, we write "PS" for "probability space". If X is a PS, then $x \leftarrow X$ denotes the algorithm which assigns to x an element randomly selected according to X.

If algorithm X receives only one input we write "$X(\cdot)$", if it receives two inputs we write "$X(\cdot,\cdot)$" and so on.

In IHS ROM, Oracle and Black-box are different concepts (We will give their definitions in the following.). In order to clearly distinguish them in form, we prescribe that if X uses an Oracle R, R is written at the top right corner of X: $x \leftarrow X^R$; if X uses a Black-box Q, Q is written at the foot right corner of X: $x \leftarrow X_Q$.

C. Information Hiding System

An information hiding system (see Fig. 1) has three parts and can be denoted by a triple $<G,E,D>$, where:

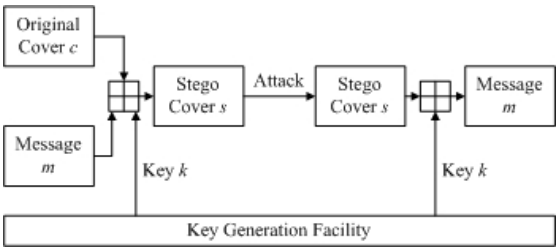

Fig. 1 Steganographic systems

- A key generation algorithm G which generates in polynomial time a random key k on input 1^n (a string consisting of n bits). By following Kerckhoffs' principle, the security of an information hiding system should lie exactly in the keys. Therefore, n will be referred to as "security parameter".
- An embedding algorithm E which produces a stego-cover $s \in C$ on input an original cover $c \in C$, a message $m \in M$ and a key k (in the range of G), i.e. $s=E(c,m,k)$.
- A detecting algorithm D which outputs a message $m' \in M$ on input a stego-cover $s \in C$ and a key k (in the range of G), i.e. $m'=D(s,k)$.

An adversary trying to detect steganographic communication is faced to solve the steganographic decision problem [4]:

Definition 1 (Steganographic Decision Problem). Given $s \in C$, determine if there exists a $k \in \{0,1\}^*$ in the range of G and a message $m \in M$ such that $D(s,k)=m$.

D. Attack / Adversary

We divide the whole attacking process into two phases: reasoning phase and attacking phase. The aim of reasoning phase is to get an approximate IHS according to some information, such as messages, original covers and *etc*. The approximate system can simulate the IHS to embed and/or detect messages. The aim of attacking phase is to analyze an arbitrarily given cover using the approximate system. In attacking phase, an adversary can estimate whether the given cover is a stego-cover or extract the message hidden in the cover.

Accordingly, we give two basic kinds of attacks:

- Reasoning Attacks: the attacks happened in reasoning phase.
- Attacking Attacks: the attacks happened in attacking phase.

Reasoning attacks can be categorized based on what kind of Black-boxes the adversary has. For an arbitrary Black-box, we

don't know its internal structure. On input what it needs, it can output the result. Through observing the input and output of the Black-box, the adversary may speculate some useful information to break the IHS.

According to what kind of Black-boxes the adversary has, we divide an adversary's attacks into five types:

- Known Message Attack (KMA): the adversary has no Black-boxes but knows the messages hiding in the stego-covers.
- Known Original Cover Attack (KOCA): the adversary has no Black-boxes but knows the corresponding original covers.
- Chosen Message Attack (CMA): the adversary has a Black-box which output a stego-cover on input a message and an original cover. So the adversary can choose some special messages, such as 00…00, 11…11, and so on.
- Chosen Original Cover Attack (COCA): the adversary has a Black-box which output a stego-cover on input a message and an original cover. So the adversary can choose some special original covers, such as an image consisting of constant color and *etc* (see Fig. 2).

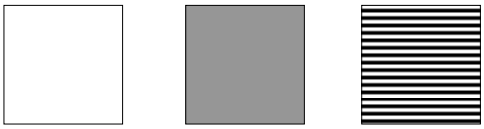

Fig. 2 Special covers

- Chosen Stego-Cover Attack (CSCA): the adversary has a Black-box which output the message on input a stego-cover. So the adversary can choose some special stego-covers.

Note that, in reasoning phase, the stego-covers are always known. Sometimes the adversary can combine some kinds of reasoning attacks. For example, CMA and COCA are always happened at the same time. We call them CMOCA.

In attacking phase, according to the input parameters of the approximate system, we divide an adversary's attack into three types:

- Blind Attack (BA): the approximate system only needs the cover. On input a cover, it answers whether the cover is a stego-cover or extracts the message.
- Known Message Attack (KMA): except for the cover, the approximate system also needs the message. On input a cover and a message, it answers whether the cover hides the message.
- Known Original Cover Attack (KOCA): except for the cover, the approximate system also needs the original cover. On input a cover and an original cover, it answers whether the cover is a stego-cover or extracts the message.

The whole attack can be named as "XXX-YYY", where "XXX" is the abbreviation of reasoning attacks and "YYY" is the abbreviation of attacking attacks.

Since the whole attacking process is divided into two phases, the adversary can be denoted by $A=(F,A_1)$, where F denotes the adversary is in reasoning phase and A_1 denotes the adversary is in attacking phase.

Now, researchers have proposed some attacking methods [13]-[17]. We select several of some to analysis as the examples of attacks.

The method Jiang [13] proposed does not contrapose a given embedding algorithm. In reasoning phase, the adversary is given some covers and knows whether they are stego-covers. Then he uses eigenvectors of these covers to train the coefficients of SVM. In attacking phase, the trained SVM is the approximate system. It can analyze whether the given cover is stego-cover without any other information. So this method is KOCA-BA-Attack.

The method Fridrich [14] proposed contraposes LSB embedding algorithm. In reasoning phase, by contrasting the correlation of the bit planes of original covers and stego-covers, Fridrich concludes that LSB destroys the correlation. In attacking phase, the approximate system calculates the correlation of the bit planes and compares it with a given threshold t. If it is smaller than t, then the cover is a stego-cover; otherwise, it is an original cover. So this method is CMOCA-BA-Attack.

The method Lin Guo-Shiang [15] proposed does not contrapose a given embedding algorithm. In reasoning phase, by contrasting the gradient energy of original covers and stego-covers, Lin concludes that the gradient energy of a cover will increase after embedding. In attacking phase, the approximate system compares two covers' gradient energy to decide which one is stego-cover. So this method is KOCA-KOCA-Attack.

E. Oracle

Definition 2 (Oracle) [6]. A Random Oracle R is a map from $\{0,1\}^*$ to $\{0,1\}^\infty$ chosen by selecting each bit of $R(x)$ uniformly and independently, for every $x\in\{0,1\}^*$.

Where $\{0,1\}^\infty$ denotes the space of infinite binary strings. Oracle is a random generator. It maps the seed $x\in\{0,1\}^*$ to infinitely long random sequence. Of course no actual protocol uses an infinitely long output, the use of "∞" is to save us from having to say how long is "sufficiently long". 2^∞ denotes the set of all Random Oracles.

Usually, Oracle is a basic cryptographic algorithm or a mathematical difficult problem. When construct a practical secure protocol, we replace the Oracle by a hash function (or other basic cryptographic algorithms). When prove a protocol's security, we reduce the protocol's security to an Oracle's security.

F. Black-Box

Cipher ROM calls the public Oracle as Black-box. All parties (including the adversary) can use it. In IHS, we assume that all the Oracles are public. So we omit the letter "public" and call it Oracle directly, i.e., the Oracle defined in the above section.

Black-box and Oracle of IHS ROM are two different conceptions. Although all parties (including the adversary) still can use the Black-box, it is not a random generator. We do not know Black-boxes' internal structure. Based on some sealed laws, on input what it needs, it can outputs the result.

IHS ROM has four Black-boxes:

Definition 3 (Information Hiding Black-box). A Information Hiding Black-box U returns a cover $c \in C$.

Definition 4 (Message Generating Black-box). A Message Black-box P returns a message $m \in M$.

Definition 5 (Embedding Black-box). Let $<G,E,D>$ be a stego system and $k \in \{0,1\}^n$ be in the range of $G(1^n)$. An embedding Black-box V_k returns, on input $m \in M$ and $c \in C$, an object $s \in C$ such that $E(c,m,k)=s$ and $D(s,k)=m$.

Definition 6 (Extracting Black-box). Let $<G,E,D>$ be a stego system and $k \in \{0,1\}^n$ be in the range of $G(1^n)$. An extracting Black-box W_k returns, on input $s \in C$, a message $m \in M$ such that $E(c,m,k)=s$ and $D(s,k)=m$, where, $c \in C$ is the original cover of s.

Note that the definition of security is related to Information Hiding Black-box U. Different Black-box U may produce different kind of covers, i.e. different cover space C. For example, U_1 produces nature images and U_2 produces line drawings. Their security is very different.

G. Formalized Adversary Model / Negligible Function / Security

The formalized adversary model is the key issue of ROM. Because we have divided the whole attacking process into two phases, the formal adversary model must be modified to fit this change. The form we used is Pr[$s \leftarrow S$, $t \leftarrow T$,…; $x \leftarrow X$, $y \leftarrow Y$,…; $a \leftarrow A$, $b \leftarrow B$,…: $p(l,m,\ldots)$], where "$s \leftarrow S$, $t \leftarrow T$,…" denotes the attacking precondition; "$x \leftarrow X$, $y \leftarrow Y$,…" denotes the reasoning phase; "$a \leftarrow A$, $b \leftarrow B$,…" denotes the attacking phase; "$p(l,m,\ldots)$" is a binary proposition that describes the adversary breaks the system successfully. We divide the content before ":" into three parties. This is the main difference between IHS ROM and cipher ROM. A function $\mu(n)$ is negligible if for every l there exists a n_l such that $\mu(n) \le n^{-l}$ for every $n \ge n_l$.

If we can prove that Pr[$s \leftarrow S$, $t \leftarrow T$,…; $x \leftarrow X$, $y \leftarrow Y$,…; $a \leftarrow A$, $b \leftarrow B$,…: $p(l,m,\ldots)$] $\le 1/2+\mu(n)$, where n is the security parameter and $\mu(n)$ is a negligible function, then the IHS can be called provable secure. "Pr[ ] $\le 1/2+\mu(n)$" means that the adversary's probability of a correct guess is almost the same as 1/2 (the adversary can always make a random decision and succeed with probability 1/2). "Pr[ ]-1/2", i.e. $\mu(n)$, is called the adversary's advantage.

H. Judge

When an adversary attacks an IHS, many information can not be chosen by the adversary himself. For example, in KOCA-attack the adversary can not choose the original covers. What covers he gets is what covers he analyses. Hence, in order to generate the covers that can not be chosen by the adversary himself, we add the definition of Judge in IHS ROM.

Judge J has two functions: 1) If he appears in reasoning phase, he denotes a fair third party. He yields some covers or messages for the adversary. And 2) If he appears in attacking phase, he simulates the normal using process of IHS.

IV. Provable Security using IHS ROM

The provable security of IHS is deeply related to attacks. The definitions of security against different attacks are different. We name every kind of security as "XXX-YYY-security", where "XXX-YYY" is the attack. Jiang and *et al* [5] have defined CMOCA-BA-Security. In this paper, we define and prove KOCA-KOCA-Security using the IHS ROM.

A. Definitions

KOCA-KOCA-attack denotes that in reasoning phase, the adversary has no Black-boxes but he knows the corresponding original covers; in attacking phase, the adversary needs the original cover to estimate whether the cover is stego-cover. Against this kind of attack, the security of information hiding is KOCA-KOCA-security.

Definition 7 (KOCA-KOCA-security). Let $S=<G,E,D>$ is an information hiding system. For every cover $c \in C$, it satisfies $\|c\| \le l$, where l is a given positive integer. U is an Information Hiding Black-box. P is a Message Generating Black-box. $k \in \{0,1\}^n$ is a stego key in the range of $G(1^n)$. $A=(F,A_1)$ is a KOCA-KOCA-adversary. J is a judge. S is KOCA-KOCA-secure if and only if:

$$\Pr[R \leftarrow 2^{\infty}, k \leftarrow G(1^n); s \leftarrow J_{V_k}^R(m,c,k), m \leftarrow F^R(c,s); (m_0,m_1) \leftarrow J_P(\ ), c' \leftarrow J_U(\ ), b \leftarrow \{0,1\}, s' \leftarrow E^R(c',m_b,k): A_1^R(c',s',m_0,m_1)=b] \le \frac{1}{2}+\mu(n) \quad (1)$$

holds, where $\mu(n)$ is a negligible function.

In (1), "$s \leftarrow J_{V_k}^R(m,c,k), m \leftarrow F^R(c,s);$" denotes that a judge produces some original-cover-and-stego-cover pairs (c,s) and gives them to the adversary. The adversary uses these pairs to do Known-Original-Cover-Attack. This belongs to reasoning phase. "$(m_0,m_1) \leftarrow J_P(\ )$, $c' \leftarrow J_U(\ )$, $b \leftarrow \{0,1\}$, $s' \leftarrow E^R(c',m_b,k)$;" indicates that the judge selects two messages $m_0,m_1 \in M$ by querying the Black-box P twice and one cover $c' \in C$ by querying the Black-box U once. Then he selects randomly m_0 or m_1 to embed it into c' to get s'. Where, the judge simulates the normal using process of information hiding system. "$A_1^R(c',s',m_0,m_1)=b$" indicates that with the help of original cover c', the adversary correctly estimates which message is embedded into the cover s. If $A_1^R(c',s',m_0,m_1)=0$, the embedded message is m_0; otherwise, the embedded message is m_1.

"Pr[ ] $\le 1/2+\mu(n)$" means that the adversary's probability of a correct guess is almost the same as 1/2 (the adversary can always make a random decision and succeed with probability 1/2), i.e. the adversary randomly guesses the results. He does not break the system.

B. Prove

If we prove that the difficulty of analyzing an information hiding system is equal to that of solving a basal cryptographic algorithm or a mathematics difficult problem, the information hiding system can be defined as provable secure.

We use the information hiding system T based on AES proposed by [5] (see Fig. 3): Before embed a message into a cover, the message should be preprocessed. Concatenate the message with l bits of "0". Then encrypt $m\|00\ldots0$ using AES.

The key k of AES is the key of the whole embedding algorithm. After preprocessing, the message can be embedded into the cover using LSB. The detection process decrypts a potential stego-cover's LSB and checks whether the last l bits of the plaintext equal zero. If this is the case, the other bits correspond to the secret message, whereas the message is meaningless. T can be denoted as: $AES(m\|00\ldots0)\oplus c$, where "$\oplus$" denotes LSB.

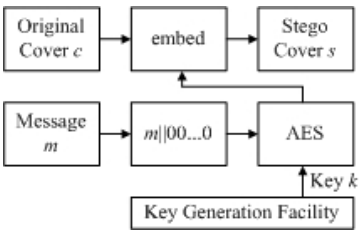

Fig. 2 Embedding algorithm

Theorem 1. T is KOCA-KOCA-secure.

Proof:

In order to prove that T is KOCA-KOCA-secure, we should prove (1) is correct. Firstly we need to find out the Oracle of T. AES is a basal cryptographic algorithm. It is homologous to the Oracle R of S. In the following, we reduce the security of T to the security of Oracle AES.

Based on the above analysis and the description of T, we have

$$\begin{aligned}&\Pr[R\leftarrow 2^{\infty},k\leftarrow G(1^n);s\leftarrow J_{V_k}^{R}(m,c,k),m\leftarrow F^{R}(c,s);(m_0,m_1)\leftarrow J_P(\ ),\\&c'\leftarrow J_U(\ ),b\leftarrow\{0,1\},s'\leftarrow E^{R}(c',m_b,k):A_1^{R}(c',s',m_0,m_1)=b]\\=&\Pr[k\leftarrow G(1^n);s\leftarrow J_{V_k}^{AES}(m,c,k),m\leftarrow F^{AES}(c,s);(m_0,m_1)\leftarrow J_P(\ ),\\&c'\leftarrow J_U(\ ),b\leftarrow\{0,1\},s'\leftarrow E^{AES}(c',m_b,k):A_1^{AES}(c',s',m_0,m_1)=b]\end{aligned}\quad(2)$$

Because the Oracle of T is fixed (AES), "$R\leftarrow 2^{\infty}$" can be omitted and all the R can be replaced with AES. If we can prove that the probability of (2) is less than or equal to $1/2+\mu(n)$ ($\mu(n)$ is a negligible function), T is KOCA-KOCA-secure.

The proof is by contradiction. Let $A=(F,A_1)$ be an adversary that defeats the scheme. The advantage of A is $\lambda(n)$, where $\lambda(n)$ is not negligible. We construct an algorithm $Z(m_{ex})$ to simulate $AES^{-1}(m_{ex})$.

Let $\mathbf{A}_n$ be the event that adversary A_1 gets $m=Z(s'\text{-}c')$ using Z, where $m=AES^{-1}(s'\text{-}c')$, so

$1/2+\lambda(n)=\Pr[A \text{ succeeds}|\mathbf{A}_n]\Pr[\mathbf{A}_n]+\Pr[A \text{ succeeds}|\bar{\mathbf{A}}_n]\Pr[\bar{\mathbf{A}}_n]$.

Because

$$\Pr[A \text{ succeeds} \mid \mathbf{A}_n]\Pr[\mathbf{A}_n]+\Pr[A \text{ succeeds} \mid \bar{\mathbf{A}}_n]\Pr[\bar{\mathbf{A}}_n]\le \Pr[\mathbf{A}_n]+1/2,$$

So $\Pr[\mathbf{A}_n]\ge\lambda(n)$ is not negligible. This indicates that A_1 breaks AES with not negligible probability. This is contrary to the fact that AES can not be broken now. So $\lambda(n)$ is negligible, therefore

$$\Pr[k\leftarrow G(1^n);s\leftarrow J_{V_k}^{AES}(m,c,k),m\leftarrow F^{AES}(c,s);(m_0,m_1)\leftarrow J_P(\ ),\ c'\leftarrow J_U(\ ),b\leftarrow\{0,1\},s'\leftarrow E^{AES}(c',m_b,k):A_1^{AES}(c',s',m_0,m_1)=b]\le\frac{1}{2}+\lambda(n)$$

Then (1) is correct. That is to say, the scheme T is KOCA-KOCA-Secure. ▌

In the proving process of theorem 1, we construct a reduction from the security of T to the security of a computational difficult problem AES. As long as we believe AES is secure, the information hiding scheme T is secure.

V. Conclusion

Random Oracle Model is an effective method for measuring the practical security of cryptograph. We try to use it into information hiding systems.

ROM method is different from the information theoretical method. It considers the adversary's practical calculating ability and reduces the security of IHS to the difficulty of a basic cryptographic algorithm or a mathematical difficult problem.

In this paper, we discuss why and how to modify ROM based on the properties of IHS. Afterwards using IHS ROM, the KOCA-KOCA-security is defined. At last we give an actual information hiding system and prove that it is KOCA-KOCA-secure.

Provable security theory is a new research direction. We use it into IHS. This work just begins. At present, the issues that worth further research include:

(1) When we construct secure protocols, we replace Oracle by an "appropriately chosen" function h. However, in IHS ROM, must function h also be a random function? If it is, this indicates that we reduce the security of IHS into the security of cryptography and does not incarnate the properties of IHS. Can we find out other kind of functions to replace Oracles? Maybe this kind of functions is not secure form the cryptography perspective, but it is fit for IHS.

(2) This paper and [4]-[5] research the provable security of symmetric IHS. The security of dissymmetrical IHS has not been researched yet.

(3) In IHS ROM, we only consider the security and do not combine it with imperceptibility, robustness, capacity and so on. Although IH scheme T has been proved to be secure, it is a theoretic system and is not useful. How to combine ROM with other theories or other properties of IHS and design secure and useful protocol is worth further research.

References

[1] Francois Cayre, Caroline Fontaine, and Teddy Furon, "Watermarking security: theory and practice," *IEEE Transactions on Signal Processing*, vol. 53, pp. 3976-3987, Oct. 2005.

[2] C. Cachin, "An information-theoretic model for steganography," in *Information Hiding: Second International Workshop*, vol. 1525 of LNCS: Springer, 1998, pp. 306-318.

[3] J. Zöllner, "Modeling the security of steganogrpahic systems," in *Information Hiding: Second International Workshop*, vol. 1525 of LNCS: Springer, 1998, pp. 344-354.

[4] Stefan Katzenbeisser, Fabien A.P. Petitcolas. Defining security in steganographic systems. in *E. Delp, P. Wong. Proceedings of SPIE, Vortrag: Conference Security and Watermarking of Multimedia Contents IV*. San Jose, USA, 2002, pp. 50-56.

[5] Jiang Nan, Wang Jian, Niu Xinxin, and Yang Yixian, "Symmetric steganography secure against chosen message and original cover attacks," in *2006 International Conference on Innovative Computing, Information and Control*, vol. 3, pp. 661-664, Aug. 2006.

[6] Bellare M, and Rogaway P, "Random oracles are practical: a paradigm for designing efficient protocols," in *Proceedings of the 1st ACM Conference*

on Computer and Communications Security, New York: ACM Press, 1993, pp. 62-77.
[7] Fiat A., and Shamir A, "How to prove yourself: practical solutions to identification and signature problems," in *Proc. CRYPTO'86*, vol. 286, Lecture Notes in Computer Science, Springer-Verlag, 1986, pp. 186-194.
[8] Feng Dengguo, "Research on theory and approach of provable security," *Journal of Software*, vol. 16, pp. 1743-1756, Oct. 2005.
[9] Barthe G., Cederquist J., and Tarento S, "A machine-checked formalization of the generic model and the random oracle model," in *Proceedings of IJCAR'04*, vol. 3097, Lecture Notes in Computer Science, 2004, pp. 385-399.
[10] Bellare M., Boldyreva A., and Palacio A, "An uninstantiable random-oracle-model scheme for a hybrid-encryption problem," in *Advances in Cryptology, EUROCRYPT'04*, Lecture Notes in Computer Science, Cachin C. and Camenisch J. ed., Springer-Verlag, 2004.
[11] Canetti R, Goldreich O, and Halevi S, "The random oracle methodology, revisited," *Journal of the ACM*, vol. 51, pp. 557-594, 2004.
[12] Goldwasser S., Micali S., and Rivest R. L., "A digital signature scheme secure against adaptive chosen-message attacks," *SIAM Journal of Computing*, vol. 17, pp. 281-308, 1998.
[13] Jiang Nan, Wang Jian, Yang Yixian, "A new method for blind image steganalysis," *Journal of Beijing University of Posts and Telecommunications*, vol. 29, no. 2, pp. 1-4, 2006.
[14] Fridrich J., Goljan M., Du R., "Detecting LSB steganography in color and gray-scale images," *Magazine of IEEE Multimedia, Special Issue on Security*, October-November issue, pp. 22-28, 2001.
[15] Lin Guo-Shiang, Lie Wen-Nung, "A study on detecting image hiding by feature analysis," in *The 2001 IEEE International Symposium on Circuits and Systems*, vol. 2, pp. 149-152, 2001.
[16] Sorina Dumitrescu, Xiaolin Wu, "Steganalysis of LSB embedding in multimedia signals," in *2002 IEEE International Conference on Multimedia and Expo*, vol. 1, pp. 581-584, 2002.
[17] Ismail Avcibas, Nair Memon, Bulent Sankur, "Steganalysis based on image quality metrics," in *2001 IEEE Fourth Workshop on Multimedia Signal Processing*, pp. 517-522, 2001.

Nan Jiang was born in Shandong province, China, on August 19, 1977. She received BE and ME degrees from the Department of Computer of Shandong Normal University, Jinan, China in 2000 and 2003 respectively, and the Ph.D. degree from Information Security Center of Beijing University of Posts and Telecommunications, Beijing, China in 2006. She is currently an instructor of the College of Computer Science of Beijing University of Technology. Her research interests include information hiding, digital watermarking, neural computation, and information security. She has published 2 books and more than 20 research papers in Journals and Proceedings.

Jian Wang was born in Shandong province, China, on September 5, 1975. He graduated from Shandong University, Jinan, China, in 1998, received ME degrees from Shandong Normal University, Jinan, China, in 2005, presently was a Ph.D student in Information Security Center of Beijing University of Posts and Telecommunications, Beijing, China since 2005. His main interests include information security, and network security.