SCIENCE CHINA
Information Sciences

• RESEARCH PAPER •

July 2012 Vol. 55 No. 7: 1639–1649
doi: 10.1007/s11432-012-4598-3

Efficient construction of provably secure steganography under ordinary covert channels

ZHU Yan[1,2]*, YU MengYang[3], HU HongXin[4], AHN Gail-Joon[4] & ZHAO HongJia[1,2]

[1]*Beijing Key Laboratory of Internet Security Technology, Peking University, Beijing* 100871*, China;*
[2]*Institute of Computer Science and Technology, Peking University, Beijing* 100871*, China;*
[3]*School of Mathematical Sciences, Peking University, Beijing* 100871*, China;*
[4]*School of Computing, Informatics, and Decision Systems Engineering, Arizona State University, Tempe, AZ* 85287*, USA*

Received January 6, 2011; accepted October 15, 2011; published online May 10, 2012

Abstract Steganography is the science of hiding information within seemingly harmless messages or innocent media. This paper addresses the problems of efficient construction of secure steganography in ordinary covert channels. Without relying on any sampling assumption, we provide a general construction of secure steganography under computational indistinguishability. Our results show that unpredictability of mapping function in covertext sampler is indispensable for secure stegosystem on indistinguishability against adaptive chosen hiddentext attacks. We completely prove that computationally secure steganography can be constructed on pseudorandom function and unbiased sampling function under ordinary covert channels, that is, its security is inversely proportional to the sum of errors of these two functions, as well as the legth of hiddentexts. More importantly, our research is not dependent upon pseudorandom ciphertext assumption of cryptosystem or perfect sampling assumption. Hence, our results are practically useful for construction and analysis of secure stegosystems.

Keywords steganography, cryptography, indistinguishability, sampler, unpredictability, adversary models

Citation Zhu Y, Yu M Y, Hu H X, et al. Efficient construction of provably secure steganography under ordinary covert channels. Sci China Inf Sci, 2012, 55: 1639–1649, doi: 10.1007/s11432-012-4598-3

1 Introduction

Steganography is the science of hiding information within seemingly harmless messages or innocent media to supply various applications, such as anonymous communications [1], anonymous online transactions, covert channels in computer systems [2], covert or subliminal communications, invisible watermarking and fingerprinting [3] for protection of intellectual property rights, etc. It is quite obvious that hiding-information messages (stegotext) must be indistinguishable from harmless messages (covertext) if we expect that communication is unconscious for human beings or undetectable for computers. Thereby, the starting point of this paper is also indistinguishability.

The security, as robustness and imperceptiveness, is a vital aspect of the research of steganography. Cachin [4] firstly formalized an information-theoretic model for steganography in 1998. They introduced

*Corresponding author (email: yan.zhu@pku.edu.cn)

a relative entropy function as a basic measure of information contained in an observation to define unconditionally secure stegosystem. Up to 2002, Hopper et al. [5,6] firstly attempted to formalize steganography from a complexity-theoretic point of view. However, the security proofs only hold under perfect sampling oracle assumption, which requires the samplers are independent each other. However, it is not practical in most circumstances. Moreover, this paper obtains the precondition for the existence of secure steganography on a strong assumption that IND-CPA security cryptosystems have pseduorandom ciphertext, as well as the perfect sampling without bias. Unfortunately, this assumption does not hold in some existing cryptosystems (see [7]).

Following these works, many scholars began to research various technologies of semantic security for steganography. For instance, Dedic et al. [8] further lowered the requirement for hiding-channel and provided 'black-box steganography'. This paper provided two improved algorithms based on rejection-sample encoder of [5]. Ahn et al. [9] created a public-key steganography and chosen-stegotext attacks (SS-CSA). Backes et al. [10], as well as Hopper [11], considered adaptive chosen-covertext attacks. Lysyanskaya et al. [12] discussed the problem of imperfect sample by weakening assumption, in which the covertext distribution is modeled as a stateful Markov process. But further discussions of the underlying questions and unconditional imperfect sample are still needed in order to construct more practical stegosystems.

As is known to all, indistinguishability is a significant factor in cryptographic security analysis. We also believe that it is the foundation of security analysis in steganography. Although this point has already been discussed in prior papers [5,8,11,12], there is still a lack of thoughtful attention to show how to construct secure stegosystems without sampling assumption. The real-world stegosystems are most often broken because they make invalid assumptions about the adversary's abilities. Typically, this is an assumption about an adversary's lack of knowledge about covertext distribution. There are many ways to characterize this sort of abilities: perfect sampling for independent distribution [5], semi-adaptive sampling for α-memoryless distribution from some Markov process of order α [12], etc. These assumptions are still too strong for real-world applications. Hence, it is essential to examine whether it is possible to weaken or eliminate these assumptions. Fortunately, pseudorandomness and unpredictability methods on complexity-theory, as well as randomized unbiased sampling functions will help settle this issue in ordinary covert channels.

In this paper, we focus on the construction of secure steganography under ordinary covert channels without sampling assumption. By constructing a more general model of stegosystem, we prove that unpredictability of mapping function in covertext sampler is indispensable for secure stegosystem on indistinguishability against adaptive chosen hiddentext attack (IND-CHA). Furthermore, computationally secure steganography is feasible if there exist ϵ_1-pseudorandom function and ϵ_2-unbiased sampling function, where ϵ_1 and ϵ_2 are two negligible errors. Although some previous studies have induced similar conclusions, our results provide more complete line of investigations and a more general conclusion. Especially, our research was not based upon the strong IND-CPA assumption and perfect sampling assumption, in which the ciphertext of cryptosystem used to build stegosystem must be pseudorandom. Hence, our construction reveals important insights into more general constructibility of secure steganography, and these results are also practically useful for construction and analysis of stegosystems.

The rest of the paper is organized as follows. In Section 2, we describe some basic notions and general definition of stegosystem. In Section 3, we define a formal model of IND-CHA security based on left-right oracle. In Section 4, a practical construction of stegosystem is proposed for IND-CHA security, and a security analysis of this construction is described as well. Finally, we conclude this paper in Section 5.

2 Preliminary and definition

2.1 Notions and preliminaries

The security in this paper is stated as a game in which an adversary has the ability to select two messages. One of the messages is randomly selected and hidden. The stegosystem is then called secure if no adversary can do better than a random guess in finding out which message was hidden. Before we formalize the game, we recall the concept of negligible function:

Definition 1 (Negligible). A function $f : \mathbb{N} \to [0, 1]$ is called negligible if for every polynomial $p(\cdot)$ there exists an N such that $|f(n)| < 1/p(n)$ for all $n > N$.

That is, f is asymptotically smaller than any inverse polynomial. This paper will focus on languages in BPP (bounded-error probabilistic polynomial time), which can be recognized by probabilistic polynomial-time machines with a negligible error probability.

Computational indistinguishability, introduced by Goldwasser and Bellare [13] and defined in full generality by Yao [14], is defined as follows:

Definition 2 (Computational indistinguishability). Two probability ensembles, $X = \{X_n\}_{n\in\mathbb{N}}$ and $Y = \{Y_n\}_{n\in\mathbb{N}}$, are computationally indistinguishable, if for every probabilistic polynomial-time (PPT) distinguisher D, every positive polynomial $p(\cdot)$, and all sufficiently large n's,

$$|\Pr[D(1^n, X_n) = 1] - \Pr[D(1^n, Y_n) = 1]| < \frac{1}{p(n)}. \quad (1)$$

Note that, $|X_n| = \Omega(n)$ denotes the length of samples in X_n. Clearly, if two ensembles are statistically close then they are also computationally indistinguishable. The converse, however, is not true. Let U_n denote uniform distribution on n-bit strings. The ensemble $\{U_n\}_{n\in\mathbb{N}}$ is called standard uniform ensemble. Given the above definition, it is easy to define pseudorandomness:

Definition 3 (Pseudorandom ensembles). An ensemble $X = \{X_n\}_{n\in\mathbb{N}}$ is called pseudorandom if there exists a uniform ensemble $U = \{U_n\}_{n\in\mathbb{N}}$ such that X and U are indistinguishable in polynomial time.

Furthermore, let $f : \{0, 1\}^s \times \{0, 1\}^L \to \{0, 1\}^l$ denote a family of functions. We call the function f is a pseudorandom function if f is a deterministic polynomial-time algorithm and the ensemble $\{f_k(U_n)\}_{n\in\mathbb{N}}$ is also pseudorandom[1)].

Other important notions involve sampling and unbiased function. The simplest method for sampling from a complex combinatorial structure is Monte Carlo method, often known as rejection sampling. Without lost of generality, we will also use the method in this paper and write $\text{Sample}_f^{\mathcal{C}}(k, b)$ to denote a rejection-sampling algorithm, which samples from a covertext distribution $\mathcal{C}$ according to oracle $\mathcal{O}^{\mathcal{C}}$ such that multi-bit symbol b can be embedded in it, for a function $f_k(\cdot)$ with a certain key k. However, this algorithm differs greatly from general Monte Carlo method due to Oracle.

To evaluate the statistical property of mapping function in sampling space, we define the unbiased function as follows:

Definition 4 (Unbiased function). A function $f : \mathcal{K} \times \mathcal{C} \to \mathcal{R}$ is a (t_b, ϵ)-unbiased function on the distribution $\mathcal{K}, \mathcal{C}, \mathcal{R}$, if for all $r \in \mathcal{R}$, $|\Pr_{x\leftarrow\mathcal{C}}[f_k(x) = r] - 1/|\mathcal{R}|| \leqslant \epsilon$, where $|\mathcal{R}|$ is the number of elements in $\mathcal{R}$ and t_b denotes the time-complexity in f.

We say that a function f is unbiased if $\epsilon = 0$, that is, $\Pr_{x\leftarrow\mathcal{C}}[f_k(x) = r] = 1/|\mathcal{R}|$. An ϵ-biased function is called an unbiased function if ϵ is a negligible function.

2.2 Definition of stegosystem

We assume that there is a public channel in which a sender can communicate with a receiver and to which an adversary can have perfect read-only access. In addition, there is a covertext source by which any covertext is generated to hide message. The model of stegosystems [5,6] can be formally defined as follows:

• $\mathcal{C}$ is a covertext space with probability distribution $\Pr_{\mathcal{C}}$. We assume that $\mathcal{C}$ can be denoted by all finite sequences $\{(c_1, \ldots, c_l)|l \in \mathbb{N}, c_i \in \Sigma, 1 \leqslant i \leqslant l\}$ after sampling, where Σ is a finite source alphabet[2)].

1) The extensive property of pseudorandom function in cryptography may be unnecessary for steganography, thus a universal hash function is often used in practice.

2) Without loss of generality, we can also map a symbol r_i in a finite alphabet Σ into an element c_i in a finite field $\mathbb{F}_q$. For example, the image watermarking is regarded as the modular operation in $GF(2^8)$ finite field.

• $\mathcal{P}$ is a hiddentext space with probability distribution $\Pr_{\mathcal{P}}$, which is statistically independent of $\Pr_{\mathcal{C}}$.

• $\mathcal{S}$ is a stegotext space with probability distribution $\Pr_{\mathcal{S}}$. We assume that $\mathcal{S}$ is equal to $\mathcal{C}$ as sets ($\mathcal{S}=\mathcal{C}$) according to the requirement of imperceptibility, but $\Pr_{\mathcal{S}}$ might be different from $\Pr_{\mathcal{C}}$, sometimes.

We assume that any sequence of covertexts over the public channel consists of independent repetitions of covertexts. Similar to cryptography, let $\mathcal{K}=\{0,1\}^*$ denote a key space. Then, a stegosystem Φ can be defined in terms of the above $(\mathcal{C},\mathcal{P},\mathcal{S},\mathcal{K})$, as follows:

Definition 5 (Stegosystem [11,12])**.** An efficient stegosystem is a triple, $\mathcal{SS}=(\mathcal{G},\mathcal{E},\mathcal{D})$, of probabilistic polynomial-time algorithms satisfying the following conditions:

• On input 1^n, algorithm $\mathcal{G}$ (called key-generator) outputs a bit strings k as the private-key, where n is a security parameter.

• For a private-key $k\in\mathcal{K}$ in the range of $\mathcal{G}(1^n)$, a covertext distribution $\mathcal{C}$, and every hiddentext $m\in\mathcal{P}$, the encoding algorithm $\mathcal{E}$ outputs a stegotext $s\in\mathcal{S}$, i.e., $s\leftarrow\mathcal{E}^{\mathcal{C}}(1^n,k,m)$.

• For a private-key $k\in\mathcal{K}$ in the range of $\mathcal{G}(1^n)$, a covertext distribution $\mathcal{C}$, and every stegotext $s\in\mathcal{S}$, the decoding algorithm $\mathcal{D}$ outputs a message $m\in\mathcal{P}$ or an invalid symbol $\perp$, i.e., $\{m,\perp\}\leftarrow\mathcal{D}^{\mathcal{C}}(1^n,k,s)$, and the probability that

$$\Pr\left[\mathcal{D}^{\mathcal{C}}\left(1^n,k,\mathcal{E}^{\mathcal{C}}(1^n,k,m)\right)\neq m\right]$$

is negligible in n, where the probability is taken over the internal coin tosses of algorithms $\mathcal{E}$ and $\mathcal{D}$, as well as the covertext distribution $\mathcal{C}$.

The algorithm $\mathcal{D}$ returns either a symbol $\perp$ indicating failure (an empty message), or a hiddentext $m\in\mathcal{P}$. Especially, we require that $\Pr[\mathcal{D}^{\mathcal{C}}(1^n,k,\mathcal{E}^{\mathcal{C}}(1^n,k,\perp))=\perp]=1$ holds. We sometimes rewrite the encoding and decoding algorithms as $\mathcal{E}_k^{\mathcal{C}}(m)$ and $\mathcal{D}_k^{\mathcal{C}}(s)$ for short. In this paper, we focus on an efficient algorithm to detect whether a hiddentext is presented instead of decrypting the stegotext. In this case, the decoding algorithm $\mathcal{D}$ is also called a deterministic algorithm if it outputs a bit $b\in\{0,1\}$, where $b=1$ denotes the presence of hiding information, otherwise $b=0$. We call this kind of $\mathcal{D}$ a detector.

According to the definition in [5,8,11,12], we assume that there exists an encoding algorithm to realize $c_n\leftarrow\mathcal{E}^{\mathcal{C}}_{\mathcal{G}(1^n)}(\perp)$ for an empty message, and then we have the definition of hiding property, as follows:

Definition 6 (Computational hiding property [5,12])**.** A stegosystem $(\mathcal{G},\mathcal{E},\mathcal{D})$ has computational hiding property if the following holds: Given a covertext distribution $\mathcal{C}$, both a covertext $c_n\leftarrow\mathcal{E}^{\mathcal{C}}_{\mathcal{G}(1^n)}(\perp)$ and its any stegotext $s_n\leftarrow\mathcal{E}^{\mathcal{C}}_{\mathcal{G}(1^n)}(m)$ are indistinguishable in polynomial-time if for any probabilistic polynomial-time algorithm D, every hiddentext $m\in\mathcal{P}$, every polynomial $p(\cdot)$, and all sufficiently large n, the following inequation holds,

$$\left|\Pr\left[D^{\mathcal{C}}\left(1^n,\mathcal{E}^{\mathcal{C}}_{\mathcal{G}(1^n)}(m)\right)=1\right]-\Pr\left[D^{\mathcal{C}}\left(1^n,\mathcal{E}^{\mathcal{C}}_{\mathcal{G}(1^n)}(\perp)\right)=1\right]\right|<\frac{1}{p(n)}.$$

The probability is taken over the internal coin tosses of algorithms $\mathcal{G},\mathcal{E}$ and the property of $\mathcal{C}$.

3 Definition of IND-CHA security

The security in this paper is stated as a game in which an adversary has the ability to select two messages. One of the messages is randomly selected and hidden. The stegosystem is then called secure if the adversary cannot do better than a random guess in finding out which message is hidden. Loosely speaking, this game means that it is hard to distinguish between covertext and stegotext.

We will use a formal definition to describe the IND-CHA attack, in which indistinguishability is measured via the "left-or-right" model [13]. Define the left-or-right oracle $\mathcal{E}_k^{\mathcal{C}}(\mathcal{LR}(\cdot,\cdot,b))$, where $b\in\{0,1\}$, to take input (x_0,x_1) and do the following: if $b=0$ it computes $c_0\leftarrow\mathcal{E}_k^{\mathcal{C}}(x_0)$ and returns c_0; else it computes $c_1\leftarrow\mathcal{E}_k^{\mathcal{C}}(x_1)$ and returns c_1. In this case, the goal of such an adversary is to distinguish whether he is seeing the encodings of the hiddentext that he supplied to the encoder, or simply random samples from the channel. This choice is decided by a left-or-right oracle $\mathcal{E}_k^{\mathcal{C}}(\mathcal{LR}(\cdot,\perp,b))$ except that the second variable is replaced by the null strings $\perp$. We fix a specific stegosystem $\mathcal{SS}=(\mathcal{G},\mathcal{E},\mathcal{D})$. Such an experiment consists of four stages as follows:

1. Key generation: A key k is generated by the key generation algorithm $\mathcal{G}$.

2. Training stage: Malice prepares some hiddentext messages and sends to the oracle $\mathcal{O}$, $\mathcal{O}$ encodes them and returns the results to Malice. After repeating many times, Malice halts and chooses a messages $m \in \mathcal{P}$;

3. Challenge stage: Malice sends m to the oracle $\mathcal{O}$. $\mathcal{O}$ tosses a fair coin $b \in_U \{0,1\}$, then provides $c \leftarrow \mathcal{E}_k^C(\mathcal{LR}(m, \perp, b))$ to Malice;

4. Guessing stage: Upon receipt of c, Malice must answer a bit b' as his guess of $\mathcal{O}$'s coin tossing b.

Definition 7 (Hiding attack of stegosystem)**.** Let $\mathcal{SS} = (\mathcal{G}, \mathcal{E}, \mathcal{D})$ be a symmetric stegosystem. Let $b \in \{0,1\}$ and $n \in \mathbb{N}$. Let A_{cha} be an adversary that has access to one oracle. We consider the following experiments:

Algorithm $\text{Exp}^{\text{ind-cha-}b}_{\mathcal{SS},A_{\text{cha}}}(1^n)$.
$k \xleftarrow{R} \mathcal{G}(1^n)$,
$x \leftarrow A_{\text{cha}}^{\mathcal{E}_k^C(\mathcal{LR}(\cdot,\cdot,b))}(1^n)$.
Return x.

Above it is mandated that the two messages queried by $\mathcal{E}_K^{\mathcal{C}}(LR(\cdot,\cdot,b))$ always have equal length, and that $\perp$ denotes a null messages. We define the advantage of the adversaries via

$$\text{Adv}^{\text{ind-cha}}_{\mathcal{SS},A_{\text{cha}}}(1^n) = \left|\Pr\left[\text{Exp}^{\text{ind-cha-1}}_{\mathcal{SS},A_{\text{cha}}}(1^n) = 1\right] - \Pr\left[\text{Exp}^{\text{ind-cha-0}}_{\mathcal{SS},A_{\text{cha}}}(1^n) = 1\right]\right|.$$

We define the advantage functions of the scheme as follows. For any integers t,q_e and u_e, $\text{InSec}^{\text{ind-cha}}_{\mathcal{SS}}(t, q_e, u_e) = \max_{A_{\text{cha}}}\{\text{Adv}^{\text{ind-cha}}_{\mathcal{SS},A_{\text{cha}}}(1^n)\}$ where the maximum is over all A_{cha} with time-complexity t, each making to the $\mathcal{E}_k(LR(\cdot,\cdot,b))$ oracle at most q_e queries the sum of those lengths is at most u_e bits of hiddentext.

So that, we define the secure stegosystem under the hiding attack:

Definition 8 (IND-CHA security)**.** The stegosystem $\mathcal{SS} = (\mathcal{G}, \mathcal{E}, \mathcal{D})$ is called (t, q_e, u_e, ϵ)-indistinguishability against adaptive chosen-hiddentext attack if the function $\epsilon = \text{InSec}^{\text{ind-cha}}_{\mathcal{SS}}(t, q_e, u_e)$ is negligible for any adversary A whose time-complexity is bounded by a polynomial in n.

4 Construction of secure steganography

In this section we address the problems of existence and construction of secure stegosystem on computational complexity. Intuitively, the more unpredictable the appearance of stego-objects is, the more difficult it would be to distinguish from them in covert channels. In support of this idea, we focus on the relationship of unpredictability and hiding property to provide a general construction of secure stegosystem, and then we analyze the security requirements of this construction to explain the preconditions for the existence of IND-CHA stegosystem.

4.1 Construction of IND-CHA stegosystem

In this subsection, we turn attention to the efficient construction of secure steganography with computationally hiding property. Before giving our stegosystem, we present a simple sampling algorithm (sampler), which is a key part in our construction. In this algorithm, we still use the similar construction suggested in [5,6], but just do a little bit of change to satisfy the requirements of an imperfect sampling oracle model. The sampling algorithm can be briefly described as follows:

Algorithm $\text{Sample}^{\mathcal{C}}_f(k, b)$.
Require: a key k, a value $b \in \{0,1\}^e$,
1: **repeat**
2: $s \leftarrow_R \mathcal{O}^{\mathcal{C}}$,
3: **until** $f_k(s) = b$.
4: Return s.

In this construction, given a mapping function $f_k(\cdot) : \mathcal{K} \times \mathcal{C} \rightarrow \mathcal{R}$ with the key k and $\mathcal{R} = \{0,1\}^e$, the encoding algorithm in our stegosystem is based on the rejection-sampling algorithm $\text{Sample}_f^{\mathcal{C}}(k, b)$. This algorithm can sample a covertext distribution $\mathcal{C}$ according to oracle $\mathcal{O}^{\mathcal{C}}$, such that an e-bit symbol b would been embedded in it. For the sake of simplification, this algorithm is sometimes abbreviated to $g_k^{\mathcal{C}}(b)$. $S = \{s_1, s_2, \ldots, s_m\}$ is a set of all different candidate samples, which are usually some inconspicuous samples based on models of human (auditory and visual) perception. And then, the algorithm randomly chooses a sample s from them until $f_k(s) = b$, where $\leftarrow_R$ denotes the random choosing of oracle $\mathcal{O}$. Our objective is to analyze the property of mapping function $f_k(\cdot)$ by this simple construction.

The rejection-sampling function has the following characters to induce greater usability and flexibility in ordinary covert channels: we do not assume the existence of a perfect oracle $\mathcal{O}^{\mathcal{C}}$, "one that can perform independent draws, one that can be rewound, etc". This kind of independence assumption is so strong that it is seldom satisfied in real-life applications [3]. Instead, the sampling oracle $\mathcal{O}^{\mathcal{C}}$ can be executed under arbitrary channel in our rejection-sampling algorithm, so that the samples may be related to each other for multi-times samplings. The reason for making this assumption is that the proof of our subsequent theorem also does not rely on the distribution characteristic of samplers but the choice of mapping function $f_k(\cdot)$, when analyzing the indistinguishability between two sample sequences with polynomial-size.

Algorithm $\mathcal{E}_k^{\mathcal{C}}(m)$.	**Algorithm** $\mathcal{D}_k^{\mathcal{C}}(s)$.
$z \leftarrow$ Encoder (m).	Parse s as $\{s_1 \| s_2 \| \cdots \| s_l\}$,
Parse z as $\{z_1 \| z_2 \| \cdots \| z_l\}$,	**for** $i = 1$ To l **do**
for $i = 1$ To l **do**	$z_i \leftarrow f_k(s_i)$,
$s_i \leftarrow g_k^{\mathcal{C}}(z_i)$,	**end for**,
end for.	$m \leftarrow \mathit{Decoder}(z_1 \| z_2 \| \cdots \| z_l)$.
Return $s \leftarrow \{s_1 \| s_2 \| \cdots \| s_l\}$.	Return m.

We now turn to the description of the stegosystem. Algorithm $\mathcal{E}$ first encodes an input message m using the given encoding function Encoder, which outputs z. And then it repeatedly invokes Sample to embed z into a sequence of covertext symbols. Algorithm $\mathcal{D}$ proceeds analogously: the message is extracted from each constant-size symbols in a covertext s by mapping function f, then the concatenation of these messages is decoded by algorithm Decoder, and the resulting value is returned.

4.2 Unpredictability and steganography

Now we devote into an analysis of the above stegosystem. Apparently, these algorithms ($\mathcal{E}$ and $\mathcal{D}$) construct a valid stegosystem. Without loss of generality, we assume that our analysis is based on binary field $\{0,1\}$, namely the output of Encoder is a binary string and the output of $f_k(\cdot)$ is a value in $\{0,1\}$. We first consider the character of the encoder Encoder. We find that the output of Encoder ought to be unpredictable in order to realize the hiding property. This kind of unpredictability is defined by Goldreich [15] as follows:

Definition 9 (Unpredictability [15]). An ensemble $\{X_n\}_{n\in\mathbb{N}}$ is called (t_p, ϵ)-unpredictable in polynomial time if for every probabilistic polynomial-time algorithm A and a negligible ϵ,

$$\Pr[A(1^{|X_n|}, X_n) = \text{Next}_A(X_n)] < \frac{1}{2} + \epsilon,$$

where $\text{Next}_A(x)$ returns the $i+1$ bit of x if on input $(1^{|x|}, x)$ algorithm A reads only $i < |x|$ of the bits of x, and returns a uniformly chosen bit otherwise (i.e., in case A reads the entire string x), t_p denotes time-complexity in A.

3) As [5,6] had said, "Our definitions (this assumption) do not rule out efficient constructions for channels where more is known about the distribution", "In practice, this oracle is also the weakest point of all our constructions", and "A real-world warden would use this to his advantage".

In the above stegosystem, we require that each stegotext block be unpredictable in order to reach indistinguishability between covertext and stegotext. In the same way, we also require the encoding message hidden in each block is unpredictable. Without loss of generality, we will consider the binary hiding, that is, $z_i \in \{0,1\}$ for any $i \in \{1,2,\ldots,l\}$ in z. We have the following theorem.

Theorem 1 (Unpredictability implies security of steganography). If the output of the encoding function Encoder is $(t_p, \frac{1}{p(n)})$-unpredictable (it can pass all next-bit tests) and the mapping function f is $(t_b, \frac{1}{q(n)})$-unbiased distributed, then the construction $(\mathrm{Sample}_f^{\mathcal{C}}, \mathcal{E}_k^{\mathcal{C}}, \mathcal{D}_k^{\mathcal{C}})$ over the covertext distribute $\mathcal{C}$ is a $(t_p - l(n)t_b, l(n), l(n)|\Sigma|, \frac{l(n)}{p(n)} + \frac{5l(n)}{q(n)})$-secure stegosystem against IND-CHA attack for all sufficiently large n, where $l(n)$ is a polynomial in n, and $|\Sigma|$ denotes the length of source alphabet Σ in $\mathcal{C}$.

Proof. Assume that there is a probabilistic polynomial-time algorithm $A^{\mathcal{C}}$ that can distinguish the output of algorithm $\mathcal{E}$ from the covertext c under $\mathcal{C}$ with at least $\frac{1}{p'(n)}$. Then, for an arbitrary hiddentext m, and all sufficiently large n, we may drop the absolute value and assume that

$$\Pr\left[A^{\mathcal{C}}\left(1^n, \mathcal{E}_k^{\mathcal{C}}(m)\right) = 1\right] - \Pr\left[A^{\mathcal{C}}\left(1^n, \mathcal{E}_k^{\mathcal{C}}(\perp)\right) = 1\right] \geqslant \frac{1}{p'(n)}.$$

For any polynomial $l(\cdot)$, let the encoding result of the hiddentext m be denoted by $z = (z_1, \ldots, z_{n'})$ by Encoder, where each z_i is a bit and the length of z is $n' = l(n)$. We also parse the covertext $c = \mathcal{E}_k^{\mathcal{C}}(\perp)$ as $\{c_1 \| c_2 \| \ldots \| c_{n'}\}$. For all $k \in \mathcal{G}(1^n)$, we consider the following sequence of distributions $\{p_{k,0}, \ldots, p_{k,n'}\}$ on the symbol sets $\Sigma^{n'}$:

$$\begin{cases} p_{k,0} &= \{c_1, c_2, \ldots, c_{n'} : c \leftarrow \mathcal{C}\}, \\ p_{k,1} &= \{g_k^{\mathcal{C}}(z_1), c_2, \ldots, c_{n'} : c \leftarrow \mathcal{C}, z \leftarrow \mathcal{P}\}, \\ & \vdots \\ p_{k,r} &= \{\ g_k^{\mathcal{C}}(z_1), \ldots, g_k^{\mathcal{C}}(z_r), c_{r+1}, \ldots, c_{n'} : c \leftarrow \mathcal{C}, z \leftarrow \mathcal{P}\ \}, \\ p_{k,r+1} &= \{\ g_k^{\mathcal{C}}(z_1), \ldots, g_k^{\mathcal{C}}(z_{r+1}), c_{r+2}, \ldots, c_{n'} : c \leftarrow \mathcal{C}, z \leftarrow \mathcal{P}\ \}, \\ & \vdots \\ p_{k,n'} &= \{g_k^{\mathcal{C}}(z_1), g_k^{\mathcal{C}}(z_2), \ldots, g_k^{\mathcal{C}}(z_{n'}) : z \leftarrow \mathcal{P}\}. \end{cases}$$

We start with the true covertext (see $p_{k,0}$), and in each step we replace one more sample of the covertext from the left by a stegotext block, which is encoded by $g_k^{\mathcal{C}}$. Finally, in $p_{k,n'}$ we have the distribution of the stegotext. So that, we observe that

$$\Pr\left[A^{\mathcal{C}}\left(1^n, \mathcal{E}_k^{\mathcal{C}}(\perp)\right) = 1\right] = \Pr\left[A^{\mathcal{C}}(1^n, y^0) = 1 : y^0 \xleftarrow{p_{k,0}} \Sigma^{n'}\right],$$

$$\Pr\left[A^{\mathcal{C}}\left(1^n, \mathcal{E}_k^{\mathcal{C}}(m)\right) = 1\right] = \Pr\left[A^{\mathcal{C}}(1^n, y^{n'}) = 1 : y^{n'} \xleftarrow{p_{k,n'}} \Sigma^{n'}\right].$$

According to our assumption, algorithm A is able to distinguish between the distribution of stegotext $p_{k,n'}$ and the distribution of covertext $p_{k,0}$. We say that A is able to distinguish between two subsequent distributions $p_{k,r}$ and $p_{k,r+1}$, for some $r \in \mathbb{N}$, as follows:

$$\begin{aligned} \frac{1}{p'(n)} &\leqslant \left(\Pr[A^{\mathcal{C}}(1^n, \mathcal{E}_k^{\mathcal{C}}(m)) = 1] - \Pr[A^{\mathcal{C}}(1^n, \mathcal{E}_k^{\mathcal{C}}(\perp)) = 1]\right) \\ &= \Pr\left[A^{\mathcal{C}}(1^n, y^{n'}) = 1 : y^{n'} \xleftarrow{p_{k,n'}} \Sigma^{n'}\right] - \Pr\left[A^{\mathcal{C}}(1^n, y^0) = 1 : y^0 \xleftarrow{p_{k,0}} \Sigma^{n'}\right] \\ &= \sum_{r=0}^{n'-1} \left(\Pr\left[A^{\mathcal{C}}(1^n, y^{r+1}) = 1 : y^{r+1} \xleftarrow{p_{k,r+1}} \Sigma^{n'}\right] - \Pr\left[A^{\mathcal{C}}(1^n, y^r) = 1 : y^r \xleftarrow{p_{k,r}} \Sigma^{n'}\right]\right). \quad (2) \end{aligned}$$

Since we notice that $p_{k,r}$ differs from $p_{k,r+1}$ only at one position, namely at $r+1$, algorithm A can also be used to successfully predict the next sample $g_k^{\mathcal{C}}(z_{r+1})$ from $\left\{g_k^{\mathcal{C}}(z_1), g_k^{\mathcal{C}}(z_2), \ldots, g_k^{\mathcal{C}}(z_r)\right\}$ for some

r; that is, for randomly chosen r, we expect that the r-th term in the sum is $\geqslant \frac{1}{n'\cdot p'(n)}$[4)].

More precisely, we will derive a probabilistic polynomial-time algorithm D from algorithm A, which can predict the next bit with higher probability from the inputs $z=(z_1,\ldots,z_{n'})\in\{0,1\}^{n'}$ for the infinitely many $k\in\mathcal{G}(1^n)$. We start with a more precise description of algorithm D as follows:

1. Choose r uniformly in $\{0,1,\ldots,n'-1\}$.
2. Choose a covertxt sequence $\{c_{r+1},\ldots,c_{n'}\}$ under distribution $\mathcal{C}$, and sets

$$y^r=\left(g_k^{\mathcal{C}}(z_1),\ldots,g_k^{\mathcal{C}}(z_r),c_{r+1},\ldots,c_{n'}\right).$$

3. If $A^{\mathcal{C}}(i,y^r)=1$, then output $f_k(c_{r+1})$ as a prediction, and otherwise output $1-f_k(c_{r+1})$, namely

$$D^{\mathcal{C}}(r,z)=\begin{cases} f_k(c_{r+1}), & A^{\mathcal{C}}(1^n,y^r)=1,\\ 1-f_k(c_{r+1}), & A^{\mathcal{C}}(1^n,y^r)=0.\end{cases}$$

Without loss of generality, if we can assume that $f_k(\cdot)$ is a $\frac{1}{q(n)}$-unbiased function (the output of function is approximately uniformly distributed with a negligible bias), then we assume $\min(\Pr[f_k(c_{r+1})=z_{r+1}],\Pr[f_k(c_{r+1})=\overline{z}_{r+1}])\geqslant\frac{1}{2}-\frac{1}{q(n)}$ in terms of Lemma 1, where $\overline{z}_{r+1}=1-z_{r+1}$. Moreover, using the definition of A, we get

$$\begin{aligned}
s_D(n')&=\Pr\left[D^{\mathcal{C}}(1^n,z)=\mathrm{Next}_D(z):z\leftarrow\{0,1\}^{n'}\right]\\
&=\frac{1}{n'}\sum_{r=0}^{n'-1}\left\{\begin{array}{l}\Pr\left[A^{\mathcal{C}}\left(1^n,y^r\right)=1,f_k(c_{r+1})=z_{r+1}:y^r\xleftarrow{p_{k,r}}\Sigma^{n'}\right]\\ +\Pr\left[A^{\mathcal{C}}\left(1^n,y^r\right)=0,1-f_k(c_{r+1})=z_{r+1}:y^r\xleftarrow{p_{k,r}}\Sigma^{n'}\right]\end{array}\right\}\\
&=\frac{1}{n'}\sum_{r=0}^{n'-1}\left\{\begin{array}{l}\Pr\left[A^{\mathcal{C}}\left(1^n,y^r\right)=1:f_k(c_{r+1})=z_{r+1},y^r\xleftarrow{p_{k,r}}\Sigma^{n'}\right]\cdot\\ \Pr[f_k(c_{r+1})=z_{r+1}:c_{r+1}\leftarrow\mathcal{O}^{\mathcal{C}}]\\ +\Pr\left[A^{\mathcal{C}}\left(1^n,y^r\right)=0:f_k(c_{r+1})=\overline{z}_{r+1},y^r\xleftarrow{p_{k,r}}\Sigma^{n'}\right]\cdot\\ \Pr[f_k(c_{r+1})=\overline{z}_{r+1}:c_{r+1}\leftarrow\mathcal{O}^{\mathcal{C}}]\end{array}\right\}\\
&=\frac{1}{n'}\cdot\sum_{r=0}^{n'-1}\left\{\begin{array}{l}\Pr\left[A^{\mathcal{C}}\left(1^n,y^{r+1}\right)=1:y^{r+1}\xleftarrow{p_{k,r+1}}\Sigma^{n'}\right]\cdot\\ \Pr[f_k(c_{r+1})=z_{r+1}:c_{r+1}\leftarrow\mathcal{O}^{\mathcal{C}}]+\\ \left(1-\Pr\left[A^{\mathcal{C}}\left(1^n,\overline{y^{r+1}}\right)=1:\overline{y^{r+1}}\xleftarrow{p_{k,r+1}}\Sigma^{n'}\right]\right)\cdot\\ \Pr[f_k(c_{r+1})=\overline{z}_{r+1}:c_{r+1}\leftarrow\mathcal{O}^{\mathcal{C}}]\end{array}\right\}\\
&\geqslant\frac{1}{2}-\frac{1}{q(n)}+\left(\frac{1}{2}-\frac{1}{q(n)}\right)\cdot\frac{1}{n'}\cdot\sum_{r=0}^{n'-1}\left\{\begin{array}{l}\Pr\left[A^{\mathcal{C}}\left(1^n,y^{r+1}\right)=1:y^{r+1}\xleftarrow{p_{k,r+1}}\Sigma^{n'}\right]\\ -\Pr\left[A^{\mathcal{C}}\left(1^n,\overline{y^{r+1}}\right)=1:\overline{y^{r+1}}\xleftarrow{p_{k,r+1}}\Sigma^{n'}\right]\end{array}\right\}\\
&\geqslant\frac{1}{2}-\frac{2}{q(n)}+\frac{1}{2n'}\cdot\sum_{r=0}^{n'-1}\left\{\begin{array}{l}\Pr\left[A^{\mathcal{C}}\left(1^n,y^{r+1}\right)=1:y^{r+1}\xleftarrow{p_{k,r+1}}\Sigma^{n'}\right]\\ -\Pr\left[A^{\mathcal{C}}\left(1^n,\overline{y^{r+1}}\right)=1:\overline{y^{r+1}}\xleftarrow{p_{k,r+1}}\Sigma^{n'}\right]\end{array}\right\},
\end{aligned}\tag{3}$$

where $\overline{y^{r+1}}=(g_k^{\mathcal{C}}(z_1),\ldots,g_k^{\mathcal{C}}(z_r),g_k^{\mathcal{C}}(\overline{z}_{r+1}),c_{r+2},\ldots,c_{n'})$. Note that, $y^r\xleftarrow{p_{k,r}}\Sigma^{n'}$ includes $c_{r+1}\leftarrow\mathcal{O}^{\mathcal{C}}$. On the assumption that $f_k(\cdot)$ is an ϵ-unbiased function, we know that y^r is distributed identically to the distribution obtained by taking y^{r+1} and $\overline{y^{r+1}}$ with probability $\frac{1}{2}+\frac{1}{q(n)}$ and $\frac{1}{2}-\frac{1}{q(n)}$, respectively. Thus, we obtain

$$\Pr\left[A^{\mathcal{C}}(1^n,y^r)=1:y^r\xleftarrow{p_{k,r}}\Sigma^{n'}\right]$$

4) Note that, we cannot have $\Pr\left[A^{\mathcal{C}}(1^n,y^{r+1})=1:y^{r+1}\xleftarrow{p_{k,r+1}}\Sigma^{n'}\right]-\Pr\left[A^{\mathcal{C}}(1^n,y^r)=1:y^r\xleftarrow{p_{k,r}}\Sigma^{n'}\right]\geqslant\frac{1}{n'\cdot p'(n)}$, considering that some elements may be $\geqslant\frac{1}{n'\cdot p'(n)}$ but it is not necessary for others.

$$= \Pr\left[A^{\mathcal{C}}(1^n, y^r) = 1 : f_k(c_{r+1}) = z_{r+1}, y^r \xleftarrow{p_{k,r}} \Sigma^{n'}\right] \Pr[f_k(c_{r+1}) = z_{r+1} : c_{r+1} \leftarrow \mathcal{O}^{\mathcal{C}}]$$

$$+ \Pr\left[A^{\mathcal{C}}(1^n, \overline{y^r}) = 1 : f_k(c_{r+1}) = \overline{z}_{r+1}, \overline{y^r} \xleftarrow{p_{k,r}} \Sigma^{n'}\right] \Pr[f_k(c_{r+1}) = \overline{z}_{r+1} : c_{r+1} \leftarrow \mathcal{O}^{\mathcal{C}}]$$

$$\geqslant \left(\frac{1}{2} - \frac{1}{q(n)}\right)\Big(\Pr\left[A^{\mathcal{C}}(1^n, y^{r+1}) = 1 : y^{r+1} \xleftarrow{p_{k,r+1}} \Sigma^{n'}\right]$$

$$+ \Pr\left[A^{\mathcal{C}}(1^n, \overline{y^{r+1}}) = 1 : \overline{y^{r+1}} \xleftarrow{p_{k,r+1}} \Sigma^{n'}\right]\Big). \quad (4)$$

This equation implies

$$\Pr\left[A^{\mathcal{C}}(1^n, \overline{y^{r+1}}) = 1 : y^{r+1} \xleftarrow{p_{k,r+1}} \Sigma^{n'}\right]$$

$$\leqslant \left(\frac{1}{\left(\frac{1}{2} - \frac{1}{q(n)}\right)} \cdot \Pr\left[A^{\mathcal{C}}(1^n, y^r) = 1 : y^r \xleftarrow{p_{k,r}} \Sigma^{n'}\right] - \Pr\left[A^{\mathcal{C}}(1^n, y^{r+1}) = 1 : y^{r+1} \xleftarrow{p_{k,r+1}} \Sigma^{n'}\right] \right).$$

Thus, in term of Eq. (2), we get

$$s_D(n') = \frac{1}{2} - \frac{2}{q(n)} + \frac{1}{2n'} \sum_{r=0}^{n'-1} \left\{ \begin{array}{l} \Pr\left[A^{\mathcal{C}}\left(1^n, y^{r+1}\right) = 1 : y^{r+1} \xleftarrow{p_{k,r+1}} \Sigma^{n'}\right] \\ - \Pr\left[A^{\mathcal{C}}\left(1^n, \overline{y^{r+1}}\right) = 1 : \overline{y^{r+1}} \xleftarrow{p_{k,r+1}} \Sigma^{n'}\right] \end{array} \right\}$$

$$\geqslant \frac{1}{2} - \frac{2}{q(n)} + \frac{1}{2n'} \sum_{r=0}^{n'-1} \left\{ \begin{array}{c} \Pr\left[A^{\mathcal{C}}(1^n, y^{r+1}) = 1 : y^{r+1} \xleftarrow{p_{k,r+1}} \Sigma^{n'}\right] - \\ \left(\begin{array}{c} \frac{1}{\left(\frac{1}{2} - \frac{1}{q(n)}\right)} \cdot \Pr\left[A^{\mathcal{C}}(1^n, y^r) = 1 : y^r \xleftarrow{p_{k,r}} \Sigma^{n'}\right] - \\ \Pr\left[A^{\mathcal{C}}(1^n, y^{r+1}) = 1 : y^{r+1} \xleftarrow{p_{k,r+1}} \Sigma^{n'}\right] \end{array} \right) \end{array} \right\}$$

$$= \frac{1}{2} - \frac{2}{q(n)} + \frac{1}{2n'} \sum_{r=0}^{n'-1} \left\{ \begin{array}{c} \Big(2\Pr\left[A^{\mathcal{C}}(1^n, y^{r+1}) = 1 : y^{r+1} \xleftarrow{p_{k,r+1}} \Sigma^{n'}\right] - \\ 2\Pr\left[A^{\mathcal{C}}(1^n, y^r) = 1 : y^r \xleftarrow{p_{k,r}} \Sigma^{n'}\right]\Big) - \\ \frac{4}{q(n)-2} \Pr\left[A^{\mathcal{C}}(1^n, y^r) = 1 : y^r \xleftarrow{p_{k,r}} \Sigma^{n'}\right] \end{array} \right\}$$

$$\geqslant \frac{1}{2} - \frac{2}{q(n)} + \frac{1}{n'p'(n)} - \frac{2}{q(n)-2}$$

$$\geqslant \frac{1}{2} - \frac{5}{q(n)} + \frac{1}{n'p'(n)},$$

where $q(n) \geqslant 6$. This means that the advantage of algorithm D is at least $\frac{1}{n'p'(n)} - \frac{5}{q(n)}$ in this experiment for $n' = l(n)$. This is in contradiction to our hypothesis that the embedded sequence z is unpredictable in a polynomial-time. The time-complexity t of our construction is at most $t_p - n't_b$ since $t_p \geqslant t + n't_b$. Moreover, the advantage of adversaries for this construction $\frac{1}{p'(n)}$ is at most $\frac{l(n)}{p(n)} + \frac{5l(n)}{q(n)}$ since $\frac{1}{p(n)} \geqslant \frac{1}{n'p'(n)} - \frac{5}{q(n)}$ for at most $l(n)$ queries and at most $l(n)|\Sigma|$ bits of hiddentext. The theorem follows.

The proof made use of a so-called "hybrid" argument. More importantly, this proof is provided with the predictability in worst case. This means that secure steganography must be unpredictable for all bits of hiddentext. Conversely, a stegosystem should be insecure only if an adversary can guess successfully on some bits. In the practical applications, we are able to use these bits to predict the message of hiddentext or to implement the steganalysis [16].

4.3 Preconditions of secure stegosystems

In order to prove the existence of computational hiding property in ordinary covert channels, we propose a new construction $(\mathrm{Sample}_f^{\mathcal{C}}, \mathcal{E}_k^{\mathcal{C}}, \mathcal{D}_k^{\mathcal{C}})$ with imperfect oracle, in which the samples are not necessarily to be independent of each other. The conclusion of the above theorem is significant to steganography analysis; moreover the process of proof has some interesting meanings for the construction of the computationally secure stegosystems. In the construction we know that there exist two kernel parts: mapping function f and encoding function Encoder. According to the proof process, we have the following preconditions:

Precondition 1. The mapping function $f_k(\cdot)$ is an unbiased function for a key k.

Precondition 2. The encoding function Encoder$(\cdot)$ can generate an unpredictable sequence.

Precondition 1 is derived from the assumption of Eqs. (3) and (4): the function $f_k(\cdot)$ is a $\frac{1}{q(n)}$-unbiased function with a polynomial negligible bias $\frac{1}{q(n)}$. This means that $|\Pr_{c\leftarrow\mathcal{C}}[f_k(c)=b]-\frac{1}{2}|\leqslant\frac{1}{q(n)}$ over distribution $\mathcal{C}$ for any $b\in\{0,1\}$. It is easy to deduce $\frac{1}{2}-\frac{1}{q(n)}\leqslant\min\{\Pr_{c\leftarrow\mathcal{C}}[f_k(c)=b],\Pr_{c\leftarrow\mathcal{C}}[f_k(c)=\overline{b}]\}$ and $\max\{\Pr_{c\leftarrow\mathcal{C}}[f_k(c)=b],\Pr_{c\leftarrow\mathcal{C}}[f_k(c)=\overline{b}]\}\leqslant\frac{1}{2}+\frac{1}{q(n)}$ for arbitrary distribution $\mathcal{C}$ in terms of the following simple lemma:

Lemma 1. Given an ϵ-unbiased function $f:\mathcal{K}\times\mathcal{C}\rightarrow\mathcal{R}$, that is, $|\Pr_{x\leftarrow\mathcal{C}}[f_k(x)=r]-\frac{1}{|\mathcal{R}|}|\leqslant\epsilon$. Let S be an arbitrary distributed random variable with values in $\mathcal{R}$. Assume that S and f are independent. Then $\frac{1}{|\mathcal{R}|}-\epsilon\leqslant\Pr_{x\leftarrow\mathcal{C}}[f_k(x)=S]\leqslant\frac{1}{|\mathcal{R}|}+\epsilon$.

Proof. In terms of the definition of ϵ-unbiased function, we have $\frac{1}{|\mathcal{R}|}-\epsilon\leqslant\Pr_{x\leftarrow\mathcal{C}}[f_k(x)=r]\leqslant\frac{1}{|\mathcal{R}|}+\epsilon$. Since $f_k(x)$ is independent of S, we have

$$\begin{aligned}\Pr_{x\leftarrow\mathcal{C}}[f_k(x)=S]&=\sum_{r\leftarrow\mathcal{R}}\Pr_{x\leftarrow\mathcal{C}}[S=r|f_k(x)=r]\cdot\Pr_{x\leftarrow\mathcal{C}}[f_k(x)=r]\\&\leqslant\left(\frac{1}{|\mathcal{R}|}+\epsilon\right)\sum_{r\leftarrow\mathcal{R}}\Pr[S=r]=\frac{1}{|\mathcal{R}|}+\epsilon.\end{aligned}$$

Thus, we also have $\Pr_{x\leftarrow\mathcal{R}}[f_k(x)=S]\geqslant\frac{1}{|\mathcal{R}|}-\epsilon$, and the lemma follows.

Normally, the above lemma means that the mapping function f is independent of the covertext distribution $\mathcal{C}$.[5)] In Theorem 1, the success probability of prediction of the algorithm D is at least $\frac{1}{2}-\frac{5}{q(n)}+\frac{1}{n'p'(n)}$. It is obvious that the bias of mapping function $\frac{1}{q(n)}$ decreases the success probability of prediction. Moreover, as a special case of this theorem, the success probability of prediction is at least $\frac{1}{2}+\frac{1}{n'p'(n)}$ when the mapping function $f_k(x)$ is an unbiased function. Note that, we emphasize that this function ought to employ a key k to realize the randomness of the sampling process. Obviously, we can use one-way function with a hard-core predicate or balanced boolean function to construct an unbiased function.

Precondition 2 is the direct consequence of cryptographic theory. Yao has indicated that an ensemble is pseudorandom if and only if it is unpredictable in polynomial time as follows:

Theorem 2 (Yao's Theorem [14,15]). Let $I=(I_n)_{n\in\mathbb{N}}$ be a key set with security parameter n, and $G=(G_k:X_k\longrightarrow\{0,1\}^{l(n)})_{k\in I}$ be a pseudorandom bit generator with polynomial stretch function l and key generator K. Then G is computationally perfect if and only if G passes all next-bit tests.

Yao's theorem means that the proposed scheme is able to realize the Precondition 2 of computational hiding stegosystem if there exists a pseudorandom bit generator. Furthermore, according to relationship between one-way function and pseudorandom bit generator, the weaker assumption of the computational hiding stegosystem is that there exists a strong one-way function, which can induce a pseudorandom bit generator [15].

Taking these two preconditions together, we claim that a (block-based) stegosystem with IND-CHA security enjoys the following characteristics:

Corollary 1. There exists a computationally secure stegosystem with IND-CHA security, if the following two conditions are satisfied: 1) there exists a pseudorandom function with a negligible error, which is used to construct the encoder of the hiddentext message; 2) there exists an unbiased function with a negligible bias, which is used to construct the rejection-sampling function.

Note that, the advantage of adversaries in winning IND-CHA game is at most $\frac{l(n)}{p(n)}+\frac{5l(n)}{q(n)}$ in terms of Theorem 1, where the length of hiddentext $l(n)$ must be far less than the polynomial value $p(n)$ and $q(n)$. This means that the adversary's advantage is proportional to the length of hiddentext $l(n)$ and is inversely proportional to the polynomials $p(n)$ or $q(n)$. The less $l(n)$ or the larger $p(n)$ and $q(n)$ there are, the more secure the stegosystem is.

5) The reason is that we have $\Pr[f_k(x)=r]=\sum_{c\in\mathcal{C}}\Pr[f_k(c)=r]\cdot\Pr_{\mathcal{C}}[c]=\frac{1}{|R|}\sum_{c\in\mathcal{C}}\Pr_{\mathcal{C}}[c]=\frac{1}{|R|}$ for the unbiased function $f_k(x)$.

5 Conclusions and further work

In this paper, we provide a more general construction of secure steganography without any special assumptions. We prove that our construction is a computationally secure stegosystem with indistinguishability against adaptive chosen hiddentext attacks. Based on it, the security analysis proves that the computationally secure steganography is feasible if there exist pseudorandom function and unbiased sampling function. Similarly, both trapdoor one-way permutation and unbiased sampler also are the foundation of construction of secure private-key and public-key steganography schemes. These results are practically useful for construction and analysis of stegosystems. As part of future work, we will construct a proof-of-concept implementation of our method with extensive system evaluation.

Acknowledgements

This work of Zhu Yan, Yu Mengyang, and Zhao Hongjia was supported by National Natural Science Foundation of China (Grant Nos. 61170264, 10990011). Ahn Gail-Joon and Hu Hongxin were partially supported by US National Science Foundation (Grant Nos. NSF-IIS-0900970, NSF-CNS-0831360) and Department of Energy (Grant No. DE-SC0004308). Many thanks to our collaborators, Stephen S. Yau, from Arizona State University for very valuable comments and suggestions.

References

1 Feamster N, Balazinska M, Wang W, et al. Thwarting Web censorship with untrusted messenger discovery. In: Dingledine R, ed. Privacy Enhancing Technologies. LNCS 2760. Berlin: Springer, 2003. 125–140

2 Serjantov A, Danezis G. Towards an information theoretic metric for anonymity. In: Dingledine R, Syverson P F, eds. Privacy Enhancing Technologies. LNCS 2482. Berlin: Springer, 2002. 41–53

3 Boneh D, Shaw J. Collusion-secure fingerprinting for digital data. IEEE Trans Inf Theory, 1998, 44: 1897–1905

4 Cachin C. An information-theoretic model for steganography. In: Aucsmith D, ed. Proceedings of the 2nd Workshop on Information Hiding (IH 1998). LNCS 1525. Portland: Springer, 1998. 306–318

5 Hopper N J, Langford J, Ahn L V. Provably secure steganography. In: Yung M, ed. Advances in Cryptology - CRYPTO 2002. LNCS 2442. Santa Barbara: Springer, 2002. 77–92

6 Hopper N J, Ahn L V, Langford J. Provably secure steganography. IEEE Trans Comput, 2009, 58: 662–676

7 Möller B. A public-key encryption scheme with pseudo-random ciphertexts. In: Samarati P, Ryan P Y A, Gollmann D, et al, eds. Proceedings of the 9th European Symposium on Research in Computer Security, ESORICS 2004. LNCS 3193. Sophia Antipolis: Springer, 2004. 335–351

8 Dedic N, Itkis G, Reyzin L, et al. Upper and lower bounds on black-box steganography. In: Backes M, Cachin C, eds. Theory of Cryptography, Second Theory of Cryptography Conference, TCC 2005. LNCS 3378. Cambridge: Springer, 2005. 227–244

9 Ahn L V, Hopper N J. Public-key steganography. In: Cachin C, Camenisch J, eds. Advances in Cryptology - EUROCRYPT 2004. LNCS 3027. Interlaken: Springer, 2004. 323–341

10 Backes M, Cachin C. Public-key steganography with active attacks. In: Kilian J, ed. Theory of Cryptography, Second Theory of Cryptography Conference (TCC 2005). LNCS 3378. Cambridge: Springer, 2005. 210–226

11 Hopper N J. On steganographic chosen covertext security. In: Caires L, Italiano G F, Monteiro L, et al, eds. Proceedings of the 32nd International Colloquium on Automata Languages and Programming (ICALP 2005). LNCS 3580. Lisbon: Springer, 2005. 311–323

12 Lysyanskaya A, Meyerovich M. Provably secure steganography with imperfect sampling. In: Yung M, Dodis Y, Kiayias A, et al, eds. Proceedings of the 9th International Conference on Theory and Practice of Public-Key Cryptography (PKC 2006). LNCS 3958. New York: Springer, 2006. 123–139

13 Goldwasser S, Bellare M. Lecture Notes on Cryptography. 2008. Http://www-cse.ucsd.edu/ mihir/papers/gb.html

14 Yao A C. Theory and application of trapdoor functions. In: Proceedings of the 23rd IEEE Symposium on Foundations of Computer Science (FOCS 1982). Chicago: IEEE Computer Society, 1982. 80–91

15 Goldreich O. Foundations of cryptography volume I, Basic tools. London: Cambridge University Press, 2001

16 Luo X Y, Liu F L, Yang C F, et al. Image universal steganalysis based on best wavelet packet decomposition. Sci China Inf Sci, 2010, 53: 634–647