2004

Information Hiding

Tri Van Le

FLORIDA STATE UNIVERSITY

COLLEGE OF ARTS AND SCIENCES

INFORMATION HIDING

By

TRI VAN LE

A Dissertation submitted to the
Department of Computer Science
in partial fulfillment of the
requirements for the degree of
Doctor of Philosophy

Degree Awarded:
Spring Semester, 2004.

The members of the Committee approve the dissertation of Tri Van Le defended on April 5, 2004.

Yvo Desmedt
Professor Directing Dissertation

Joe Mott
Outside Committee Member

Mike Burmester
Committee Member

Kyle Gallivan
Committee Member

Michael Mascagni
Committee Member

The Office of Graduate Studies has verified and approved the above named committee members.

ACKNOWLEDGMENTS

I wish to thank my family for their encouragement, wonderful and loving support, especially my wife, Hoang Viet Ha, my daughter, Le Hoang Dieu Minh, and my parent Le Van Thanh and Le Thi Chuyen. I am thankful that I have a chance to work with outstanding researchers of the field during my PhD program, including (but not limited to) Professors Mike Burmester, Yvo Desmedt, Kaoru Kurosawa and Alex Yasinsac as well as many other faculties in the beautiful landscape of Florida State University. I appreciate the time and support my PhD Program Committee and many other staffs at the University have reserved for me. Last but not least, this dissertation would have been impossible without financial support of National Science Foundation via NSF grant CCR-9903216.

TABLES OF CONTENTS

LIST OF FIGURES

LIST OF ALGORITHMS

ABSTRACT

The Prisoners' Problem can be stated as follows: Two prisoners, Alice and Bob, want to communicate a secret escape plan under the surveillance of a warden, Wendy. To be indiscernible, the communication must appear to Wendy to be "innocent". If a traditional cryptographic mechanism (such as encryption) is used to protect their secret plan, Alice and Bob will be caught by Wendy because of the visible randomness of the ciphertexts. Therefore a new approach must be used in which information is hidden, not just encrypted. Information hiding, and more specifically steganography deals with such problems.

This dissertation investigates the Prisoners' Problem in a game theoretic setting in which Alice plays against Wendy. The objective of Alice is to encode her secret messages so that they are indistinguishable from innocent messages. The goal of Wendy is to distinguish Alice's messages with concealed information from innocent messages.

We study this game theoretic problem in three security models: perfect, statistical and computational security. These models correspond to three adversarial models of Wendy, namely: unbounded; polynomial number of queries; polynomial time. We show that under very general conditions, efficient and secure steganography can be achieved. In each of the three models, we give necessary and sufficient conditions for the existence of secure steganography. Our proofs yield efficient and proven secure steganographic systems. In almost all of the cases, these constructions are also optimal. We then extend these models to introduce the novel concepts of invisible steganography and steganographic secret sharing.

CHAPTER 1

INTRODUCTION

Overview

History of Modern Steganography

According to the Greek historian Herodotus [24, 28], who lived around 474 B.C., Histiaeus of Miletus shaved the head of a slave and tattooed a secret message on his scalp. When the slave's hair grew back, Histiaeus dispatched him to the Greeks, who shaved the slave's head and read the message. During WWII, invisible inks and micro dots were used to embed hidden messages in newspapers, books, etc. [28]. In these examples, using cryptographic operations, such as encryptions or digital signatures, would lead to immediate failure because of their *visible* randomness or information.

The Prisoners' Problem

The *Prisoner's Problem*, introduced first in the context of subliminal channels (G.J. Simmons [45]), is often used to illustrates steganography (Anderson [4]). It can be stated as follows: Two prisoners, Alice and Bob, want to communicate to each other their secret escape plan under the surveillance of a warden, Wendy. In order to be undetected by Wendy, Alice and Bob must keep their communications as "*innocent*"

Figure 1.1: Non-steganographic communications between Alice and Bob.

as possible. In practice, such model is applicable when Alice and Bob wish to communicate privately via a public channel. Another example is when Alice want to hide her digital watermarks or fingerprints from a traitor (Wendy) but not say from a judge (Bob).

The Steganographic Game

We consider steganography as a game theory problem where Alice and Bob play against Wendy. The objective of Alice is to encode her messages to Bob so that they appear *innocent* to Wendy, while the task of Wendy is to detect whether the communication channel between Alice and Bob has been modified to transmit hidden information. If we call $\mathcal{C}$ the original communication channel between Alice and Bob, and $\mathcal{C}'$ the modified communication channel between Alice and Bob, then Alice and Bob's goal is to make $\mathcal{C}'$ look identical to $\mathcal{C}$ whereas Wendy's goal is to distinguish $\mathcal{C}'$ from $\mathcal{C}$. This is called the *steganographic game*.

Figure 1.1 illustrates a non-steganographic communication between Alice and Bob. There is no hidden information in the messages. When the communication channel is used to *cover* (hide) steganographic communication, we have a steganographic channel.

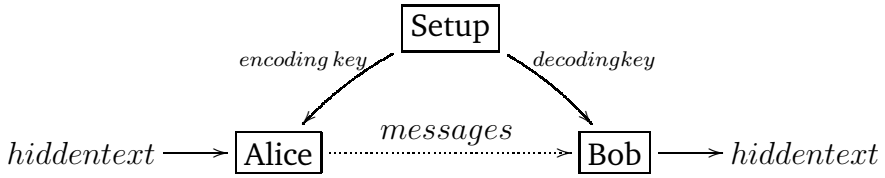

Figure 1.2: Steganographic communication between Alice and Bob.

Figure 1.2 illustrates a steganographic communication between Alice and Bob. Alice hides her secret messages, called *hiddentexts*, inside other "innocent" looking

messages, called *stegotexts*. Bob obtains Alice's message by extracting it from the stegotext. To ensure their privacy, Alice and Bob share a pair of secret keys, called the *encoding* and *decoding* key, shared in the setup stage. Messages that appear in normal non steganographic communications are also called *covertexts*.

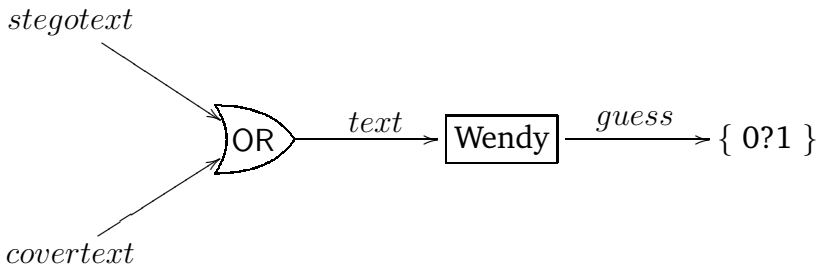

Figure 1.3: Detection of steganographic communications by Wendy.

Figure 1.3 illustrates the detection procedure. Wendy detects steganographic communications by deciding whether a given text belongs to a steganographic or non-steganographic channel. Wendy wins if she can tell with a probability better than guessing which case it is, and she loses otherwise. We may allow Wendy to look at more than one texts, in order to improve her chance of success. However, such an extension will not make any difference in the security model if Wendy is limited to taking a polynomial number of samples [20].

Two Approaches to Formal Security

Depending on the computing power of Wendy, there are two security approaches: an *information theoretic* approach and a *computational complexity* approach. In the information theoretic security approach, Wendy has *unbounded* resources. She can calculate every functions at her desire. This is the strongest *unconditional security* model.

In contrast, in the *computational complexity* approach, Wendy is usually restricted to probabilistic polynomial time. Security in this approach is based on the assumed intractability of certain hard computational problems, such as the RSA problem [42] or the Decision Diffie-Hellman (DDH) problem [6]. However these

problems are tractable by quantum computing, if such a technology can be developed in the future [44]. In that case, the information theoretic approach is the only one that is provably secure. Nevertheless until then, the computational approach is preferred in practice because the secret keys are *reusable*.

Steganographic Attacks. In the unconditional security setting, there is only one type of attack, namely the *chosen hiddentext attack*. In this attack, Wendy is allowed to force Alice to send hiddentexts of Wendy's choice to Bob. For example, if Wendy is a Prime Minister, who suspects that some of her cabinet members are traitors, and may leak secret documents to news agencies, but isn't sure exactly who the traitors are [4], she may choose secret messages to inform her cabinet and trace the traitors. A traitor Alice who wants to send a secret message to her accomplice Bob will have to use these secret messages chosen by Wendy.

In practice, the conditional security setting is much more convenient because the secret keys are *reusable*. However, reusable keys also open the door for a much more powerful type of attack, namely an *(adaptive) chosen stegotext* attack.

In a *non-adaptive* chosen stegotext attack, Wendy is allowed to run an additional setup stage, prior to her real attack. In this stage, Wendy can extract hiddentexts from arbitrary stegotexts, but she does not have direct access to the secret key. Wendy can use information obtained in this stage (regarding the secret key) for later detection of steganographic communication (that use the same key).

In an *adaptive* chosen stegotext attack, Wendy can extract hiddentexts from arbitrary stegotexts in both the setup and the attack stages. This means that Wendy can decrypt stegotexts that are related to the text she suspects, except that she cannot decrypt the exact suspected text in question. In practice, Alice will face these two attack modes when Wendy has access to the extraction hardware or capability, but Wendy does not know who uses it. It should be noted that these two types of active attack originate from the strongest chosen ciphertext [37, 39] and adaptive chosen ciphertext attacks [16] in cryptography.

Literature

Fingerprinting and Traitor-Tracing. Steganography is related to traitor-tracing and digital fingerprinting. Traitor-tracing attempts to embed unique identification information into copies of an object in order to trace traitors who release illegal copies. However, most of the work in fingerprinting currently deals with cryptographic data only. Watermarking on the other hand, embeds the same copyright information into all objects so that they can be identified later [2, 5, 38].

Covert Channels. *Covert channels* have been studied since 1973 in computer security [32], where one secretly abuses certain parts of a computer system so as to create an anonymous and secret communication channel. In the area of cryptography, covert channels embedded in cryptographic protocols are called *subliminal channels* [45], named by Gus Simmons who first studied them in authentication protocols. He introduced the *prisoners' problem*. One real life example of such a scenario involves the SALT 2 accord between the US and the Soviet Union [46].

Desmedt generalized the concept of subliminal channels to the more general case of cryptographic protocols [13]. These channels allow an insider to send secret *side* information through cryptographic protocol messages. It is important to prevent such abuses since they allow insider leakage and electronic espionage through cryptographic communication systems [13].

Kleptography. Young and Yung further applied this concept to cryptographic hardware and software products [48, 49]. They demonstrated that viruses or *malwares* with cryptographic capabilities can use subliminal channels in a very damaging and undetectable ways to leak information and to destroy data integrity. This suggests that secure cryptosystems should not be built from externally built black-boxes with computer processing capabilities.

Even though subliminal channels and kleptography are special cases of information hiding, their objectives are different. With subliminal channels one hides

information into cryptographic protocols, which often contain strings that are uniformly random, whereas uniform random messages are generally considered suspicious and unsuitable for use in modern information hiding. Nowadays secret information is hidden in more natural data such as audio, pictures, or video. This difference leads to entirely different methods used for information hiding.

Anonymous Communications. In [9], Chaum introduced the concept of *unconditional anonymity*, and illustrated this with the *dining cryptographers' problem*. Unconditional anonymity has many applications in electronic voting and payment systems. In its basic form it involves an end-to-end communication network where no one *knows* who are the real senders and receivers of each message. Other variants of this concept are *MIX networks* [8, 1], where several layers of servers are used to hide the origin of each messages . *Onion routing* [40] is a special implementation of MIX networks.

Steganography. The Prisoner's Problem was considered in the unconditional security setting by various people, including Cachin [7], Mittelholzer [35], Moulin [36], Zollner et.al. [50] and Ettinger [17]. The computational approach is also considered by [30, 26, 41, 12, 4, 27]. Katzenbeisser and Petitcolas [30], Hopper, Langford and von Ahn [26], Reyzin and Russell [41] formulated the problem using symmetric keys; while Craver [12], Anderson[4], Katzenbeisser and Petitcolas [30] and Hopper and von Ahn [27] applied asymmetric keys.

Current results in the literature have several drawbacks:

- *Unsolved Problem*: [50, 17, 30] formalized the Prisoner's problem using various models, but gave no solutions to this problem.

- *Unproven security*: [4, 12] give heuristic solutions but offer no formal proof of security. Similarly, there are many other heuristic schemes proposed but these were broken shortly after their birth, see e.g. [2, 5, 38].

- *Low information rate*: [7] has a rate of only one bit per cover, while [26, 27, 41] have even a lower rate of a fraction of bit per cover, regardless of how much entropy the underlying covertext channel carries.

- *Inflexible*: [35, 36] consider the hiding problem with numerical data tables, however, with independent data items only.

Background

In this section, we review basic concepts and results from probability, computational complexity and coding theory that will be applied later in the dissertation. Readers familiar with these notions should skip this section.

Probability Theory

Probability Distribution. Let $\mathcal{S}$ be a set. Denote the power set of $\mathcal{S}$ by $2^{\mathcal{S}}$. A family of subsets $\mathcal{A} \subset 2^{\mathcal{S}}$ is called a σ-field if: (i) if $A \in \mathcal{A}$ then $A^{\complement} = \mathcal{S} - A \in \mathcal{A}$; (ii) if $A_1, A_2, \ldots,$ are pairwise disjoint sets in $\mathcal{A}$, that is, $A_i \cap A_j = \emptyset$ for $i \neq j$, then $\cup_{i=1}^{\infty} A_i \in \mathcal{A}$; (iii) $\emptyset \in \mathcal{A}$. For example, $2^{\mathcal{S}}$ is itself a σ-field. Each subset $A \in \mathcal{A}$ is called an *event* and $\{a\} \in \mathcal{A}$ is called an elementary event.

A *probability space* is a tuple $(\mathcal{S}, \mathcal{A}, P)$ where $\mathcal{S}$ is a set, called *sample space*, $\mathcal{A}$ is a σ-field, called the set of *permissible events*, and $P : \mathcal{A} \to \mathbb{R}$ is a real function defined on $\mathcal{A}$ such that: (i) $0 \leq P(A) \leq 1$ for all $A \in \mathcal{A}$, called the *probability* of event A; (ii) if $A_1, A_2, \ldots$ are pairwise disjoint subsets in $\mathcal{A}$, then $P(\bigcup_{i=1}^{\infty} A_i) = \sum_{i=1}^{\infty} P(A_i)$; (iii) $P(S) = 1$. P is called a *probability distribution*.

Two events $A, B \in \mathcal{A}$ are called *independent* if $P(A \cap B) = P(A)P(B)$. The *conditional probability* of A given B is defined by $P(A|B) = P(A \cap B)/P(B)$ for $P(B) \neq 0$. When there is no ambiguity, we identify the event $a \in \mathcal{S}$ with $\{a\} \subset \mathcal{S}$.

A *discrete* probability space is one for which $\mathcal{S}$ is *countable* and the corresponding σ-field is the power set of S.

The *Borel* field on $\mathbb{R}$, denoted by $\mathcal{B}$, is the smallest σ-field on $\mathbb{R}$ that contains all open intervals $(a, b) = \{x : a < x < b\}$. See [31, 34, 22].

Random Variable A *random variable* X is a function $X : \mathcal{S} \to \mathbb{R}$ for which the *preimage* $X^{-1}(B) \in \mathcal{A}$ for all $B \in \mathcal{B}$, where $X^{-1}(B) = \{a \in \mathcal{S} \mid X(a) \in B\}$. The probability $P(X^{-1}(B))$ is called the probability of event $X \in B$ and is denoted by $\Pr[X \in B]$. The function $P_X : \mathcal{B} \to \mathbb{R}$ defined by $P_X(B) = \Pr[X \in B]$ is called the *probability distribution* of X. The function $F_X : \mathbb{R} \to \mathbb{R}$ defined by $F_X(a) = \Pr[X \leq a]$ is called the *cumulative distribution function* of random variable X. Let X, Y be two random variables. The *multivariate* random variable (X, Y) is defined by parallel application of the two functions X, Y.

The expected value of a random variable X is defined by $E[X] = \sum_x \Pr[X = x]x$. The conditional expected value of random variable X given $Y = y$ is defined by $E[X|Y = y] = \sum_x \Pr[X = x|Y = y]x$. The conditional expectation of X given Y is a function $E[X|Y]$ on variable Y such that: when $Y = y$, $E[X|Y] = E[X|Y = y]$. We have double expectation rule $E[E[X|Y]] = E[X]$. A *Bernoulli* random variable is a random variable which takes value 1 with probability p, and value 0 with probability $q = 1 - p$. Let P_S be a probability distribution over sample space $\mathcal{S}$. We write $X \leftarrow P_S$ when X is a random variable over sample space $\mathcal{S}$, whose value is chosen from $\mathcal{S}$ accordingly to P_S. Denote the uniform probability distribution over $\mathcal{S}$ by $\mathcal{U}_\mathcal{S}$. See [31, 34, 22] for more details.

Random Process. A *random process* [19] is a family of random variables $X = \{X_t\}_{t=1}^{\infty}$. The distribution of random variable X_t may depend on the values of random variables X_i for $i < t$. Time series, random walks, Markov processes and other random fields are examples of random processes. If the underlying sample space is discrete then the process is called discrete.

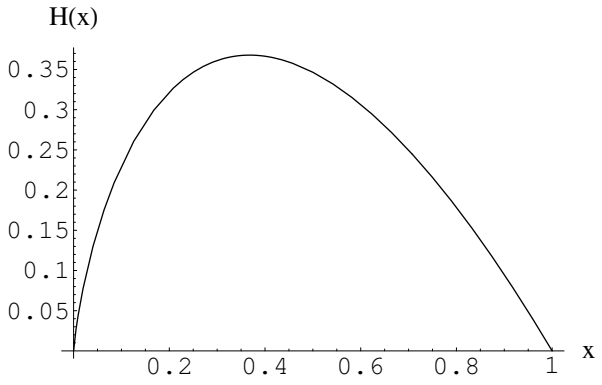

Figure 1.4: Entropy function $H(x)$.

Let X be a random process over sample space $\mathcal{S}$. The *marginal* probability distribution of X is defined by the function $P_X : \mathcal{S}^* \to \mathbb{R}^{\geq 0}$ such that,

$$\forall s \in \mathcal{S}^n : \; P_X(s) = \Pr\left[(X_1, \ldots, X_{|s|}) = s\right].$$

Entropy. For $0 \leq x \leq 1$, define the entropy function $H(x) = -x \log(x)$, where the base of the logarithm is 2 and the unit of entropy is a *bit*. $H(x)$ is a nonnegative concave function which maximizes at $x = \frac{1}{e}$. Figure 1.4 is the graph of $H(x)$.

The *entropy* of an event A is defined by $H(A) = -\log P(A)$. The entropy of a discrete probability distribution P is defined by $H(P) = \sum_{a \in \mathcal{S}} P(a) H(a)$. The *min entropy* of P is defined by $H_{\min}(P) = \min_{a \in \mathcal{S}}(-\log P(a))$. Clearly,

$$H_{\min}(P) \leq H(P).$$

Let X, Y, Z be discrete random variables. The entropy of X is defined by

$$H(X) = \sum_x H(P_X(x)) = H(P_X).$$

The *joint entropy* of X, Y is defined by

$$H(X,Y) = \sum_{x,y} H(P_{X,Y}(x,y)).$$

The *conditional entropy* of X given Y is defined by

$$H(X|Y) = \sum_{x,y} \Pr[Y=y] H(\Pr[X=x|Y=y]) = H(X,Y) - H(Y).$$

The *entropy function* of a discrete random process X is defined by:

$$H_t(X) = H(X_1, \ldots, X_t),$$

where $(X_1, \ldots, X_t)$ is a multivariate random variable. See [11].

Type. Let $\Sigma = \{c_1, \ldots, c_{|\Sigma|}\}$ be a finite set, and let $x = (x_1, \ldots, x_n) \in \Sigma^n$ be a sample. Define n_k to be the number of occurrences of c_k in x. Then $n_1 + \cdots + n_{|\Sigma|} = n$. The type of x is $type(x) = (\frac{n_1}{n}, \ldots, \frac{n_{|\Sigma|}}{n})$. Let $f(c,x)$ be the frequency of occurrences of c in x. See [11].

Define the *sample entropy* of x by:

$$H_{\text{smp}}(x) = -\sum_{k:n_k>0} \frac{n_k}{n} \log \frac{n_k}{n}.$$

The n^{th} sample entropy of a probability distribution P is

$$H^n_{\text{smp}}(P) = \sum_x \prod_{i=1}^{n} P(x_i) H_{\text{smp}}(x).$$

By entropy law for large numbers (Theorem 3, page 12) we have $H^n_{\text{smp}}(P) \to H(P)$ in probability.

Statistical Difference. Let P and Q be two discrete probability distributions over $\mathcal{S}$. Define:

$$\textit{diff}(P,Q) = \sum_{a \in \mathcal{S}} |P(a) - Q(a)|,$$

to be the difference metric of probability distributions P, Q.

Statistical Indistinguishability. A function $\varepsilon : \mathbb{N} \to \mathbb{R}^{\geq 0}$ is called *negligible* if for *all* polynomial $p(n)$, $\varepsilon(n) < p(n)^{-1}$ for all large enough n. $\varepsilon(n)$ is also called a sub inverse-polynomial function. For example, $\varepsilon(n) = e^{-n}$ is negligible.

A family of probability distributions $\{P_n\}_{n=1}^{\infty}$ over Σ^* is called *polynomial length* if the length $|x|$ of each element $x \in \text{support}(P_n)$ is at most polynomial in n.

Two polynomial length families of discrete probability distributions $P = \{P_n\}_{n=1}^{\infty}$ and $Q = \{Q_n\}_{n=1}^{\infty}$ are called *statistically indistinguishable* if $\textit{diff}(P_n, Q_n)$ is a negligible function in n [21, 20]. A function $f(n) : \mathbb{Z}^+ \to [0,1]$ is called *overwhelming* if $1 - f(n)$ is negligible.

Two families of discrete random processes $X = \{X_n\}_{n=1}^{\infty}$ and $Y = \{Y_n\}_{n=1}^{\infty}$ are called statistically indistinguishable if for all $t > 0$, the two families of probability distributions $\{P_{(X_{n,1}, X_{n,2}, \ldots, X_{n,t})}\}_{n=1}^{\infty}$ and $\{P_{(Y_{n,1}, Y_{n,2}, \ldots, Y_{n,t})}\}_{n=1}^{\infty}$ are statistically indistinguishable.

Theorem 1 (Fano's Inequality). *Let X, Y be two random variables over domain D and let $P_e = \Pr[X \neq Y]$. Then*

$$H(P_e) + P_e \log(|D| - 1) \geq H(X|Y).$$

Proof. See [11]. □

Theorem 2 (Indistinguishability and Entropy). *If $\{P_n\}$ and $\{Q_n\}$ are statistically indistinguishable then $f(n) = H(P_n) - H(Q_n)$ is a negligible function.*

Proof. Let $P_n = (p_1, \ldots, p_N)$, $Q_n = (q_1, \ldots, q_N)$ and $\epsilon_n = \text{diff}(P_n, Q_n)$. Let D_n be the support of P_n and Q_n. Define two random variables X, Y with the following joint

probability distribution:

$$\Pr[X=i,Y=j]=\begin{cases}\min(p_i,q_i), & \text{if } i=j\\ p_i-\min(p_i,q_i), & \text{if } j=i+1\\ q_i-\min(p_i,q_i), & \text{if } i=j+1\\ 0, & \text{if } (i>j+1) \text{ or } (j>i+1).\end{cases}$$

It is not hard to see that $P_X = P_n$ and $P_Y = Q_n$ and that $\Pr[X \neq Y] = e_n$. Apply Fano's inequality to X, Y we get:

$$H(\epsilon_n) + \epsilon_n \log(|D_n| - 1) \geq H(X|Y) = H(X,Y) - H(Y) \geq H(X) - H(Y).$$

Reverse the roles of X, Y and apply Fano's inequality again to Y, X we get a double inequality:

$$H(\epsilon_n) + \epsilon_n \log(|D_n| - 1) \geq |H(X) - H(Y)| = |H(P_n) - H(Q_n)| \tag{1.1}$$

Since P and Q are polynomial length families, there exist a polynomial $p(n)$ such that $D_n \subset \Sigma^{\leq p(n)}$. This means that $|D_n| < |\Sigma|^{p(n)+1}$. Substituting this into (1.1) to get:

$$|H(P_n) - H(Q_n)| < H(\epsilon_n) + \epsilon_n \log(|\Sigma|^{p(n)+1} - 1) < \epsilon_n q(n) + 1$$

where $q(n) = \log|\Sigma|(p(n)+1)$ is a polynomial in n. Since ϵ_n is negligible, $e_n q(n) + 1$ is also negligible, which proves the theorem. □

The Asymptotic Equipartition Property (AEP) states that the sample entropy of a probability distribution approaches its entropy in probability [11]. We prove a stronger theorem, which says that the rate of convergence is exponential.

Theorem 3 (Entropy Law for Large Numbers). *Let $X_1, \ldots, X_n$ be n independent, identically distributed random variables over finite sample space $\mathcal{S}$ and have probability distribution P. Let H^n_{smp} be the random variable defined by $H^n_{smp} = H_{smp}(X_1, \ldots, X_n)$. Then for all $0 < \delta < 1$, $\Pr\left[H^n_{smp} < \delta H(P)\right]$ is a negligible function in n.*

Proof. Without loss of generality, let us assume that $P(s) > 0$ for all $s \in \mathcal{S}$. Let T_s be the number of occurrences of s in $X_1, \ldots, X_n$. Fix an $s \in \mathcal{S}$ and let $B_1, \ldots, B_n$ be n Bernoulli random variables defined by:

$$B_i = \begin{cases} 1, & \text{if } x_i = s, \\ 0, & \text{if } x_i \neq s. \end{cases}$$

Apply Lemma 2 (page 15) to the n random variables $B_1, \ldots, B_n$, whose expected value is $P(s)$, and let $\epsilon = (1 \pm \alpha)P(s)$, where $\alpha > 0$ to be determined. We get:

$$\Pr\left[\left|\frac{T_s}{n} - P(s)\right| \geq \alpha P(s)\right] \leq e^{-n\lambda_s^+} + e^{-n\lambda_s^-},$$

where $\lambda_s^+ = D((1+\alpha)P(s), P(s))$ and $\lambda_s^- = D((1-\alpha)P(s), P(s))$.

Apply Lemma 1 (page 14) to $u = P(s) \in [\Delta, 1-\Delta]$, $v = \frac{T_s}{n} \in [0,1]$, $\delta \in (0,1)$ and $\Delta = \min_{s \in \mathcal{S},\, P(s)>0} P(s) \in (0,1)$, to get that there exists $\alpha > 0$ such that for all $u \in [\Delta, 1-\Delta]$ and all $v \in [0,1]$: $H(v) < \delta H(u) \Rightarrow |v-u| \geq \delta u$. Thus:

$$\begin{aligned} \Pr\left[H\left(\frac{T_s}{n}\right) < \delta H(P(s))\right] &= \Pr\left[H(v) < \delta H(u)\right] \\ &\leq \Pr\left[|v-u| \geq \alpha u\right] \\ &= \Pr\left[\left|\frac{T_s}{n} - P(s)\right| \geq \alpha P(s)\right] \\ &\leq e^{-n\lambda_s^+} + e^{-n\lambda_s^-}. \end{aligned}$$

This bound is true for all $s \in \mathcal{S}$ so we have:

$$\Pr\left[\sum_{s \in \mathcal{S}} H\left(\frac{T_s}{n}\right) \leq \delta \sum_{s \in \mathcal{S}} H(P(s))\right] \leq |S|(e^{-n\lambda^+} + e^{-n\lambda^-}).$$

where $\lambda^+ = \min_{s \in \mathcal{S}} \lambda_s^+$ and $\lambda^- = \min_{s \in \mathcal{S}} \lambda_s^-$. Lowering $\alpha > 0$ until $(1 \pm \alpha)P(s) \in (0,1)$ for all $s \in \mathcal{S}$ (lowering α does not effect Lemma 1). So we have $\lambda^+ > 0$ and $\lambda^- > 0$. By definition, we have $\sum_{s \in \mathcal{S}} H(P(s)) = H(P)$, $\sum_{s \in \mathcal{S}} H\left(\frac{T_s}{n}\right) = H^n_{\text{smp}}$, and $|S|(e^{-n\lambda^+} + e^{-n\lambda^-})$ is negligible. Therefore we get $\Pr\left[H^n_{\text{smp}} \leq \delta H(P)\right]$ is negligible. □

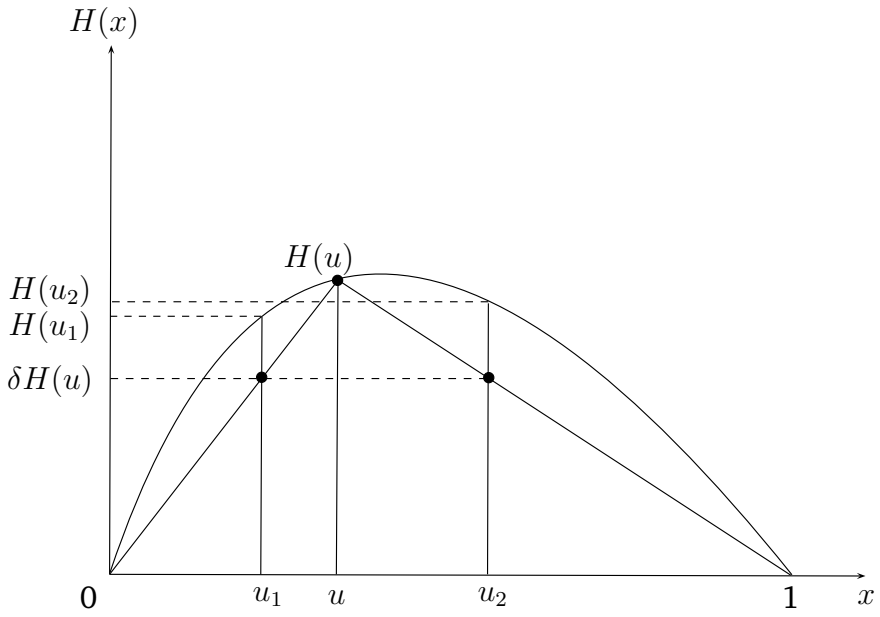

Figure 1.5: Bounds on $H(u)$

Lemma 1. *For all $\delta, \Delta \in (0,1)$, there exists $\alpha > 0$ such that for all $u \in [\Delta, 1-\Delta]$ and all $v \in [0,1]$:*

$$|u - v| \leq \alpha u \Rightarrow H(v) \geq \delta H(u).$$

Proof. Since $H(u)$ is concave in the range $0 \leq u \leq 1$ and $H(0) = H(1) = 0$, we get for all $v \in [u_1, u] \cap [0,1]$, $u_1 = \delta u$:

$$H(v) \geq (1-\delta)H(0) + \delta H(u) = \delta H(u); \tag{1.2}$$

and for all $v \in [u, u_2] \cap [0,1]$, $u_2 = u + \delta(1-u)$:

$$H(v) \geq \delta H(u) + (1-\delta)H(1) = \delta H(u). \tag{1.3}$$

This is illustrated in Figure 1.5. Combining 1.2 and 1.3 we get $H(v) \geq \delta H(u)$ for all $v \in [u_1, u_2]$. Since $|\frac{u_1-u}{u}|$ and $|\frac{u_2-u}{u}|$ are continuous over the compact range $\Delta \leq u \leq 1-\Delta$, we have a minimum $\alpha = \min_{u \in [\Delta, 1-\Delta]} |\frac{u_1-u}{u}|, |\frac{u_2-u}{u}| \geq 0$. Now $\alpha = 0$ if and only if $\delta = 0$, or $\delta = 1$ or $u = 1$, which are all impossible for $u \in [\Delta, 1-\Delta]$.

Therefore we must have $\alpha > 0$. By definition, $|u - v| < \alpha u \Rightarrow v \in [u_1, u_2] \Rightarrow H(v) \geq \delta H(u)$. □

Lemma 2 (Chernoff's bound [10, 25]). *Let $X_1, X_2, \ldots, X_n$ be n independent, identically distributed Bernoulli random variables, with the same expected value p. Then, for any $0 < \epsilon < 1$:*

$$\Pr\left[\frac{1}{n}\sum_{i=1}^{n} X_i \geq \epsilon\right] \leq e^{-nD(\epsilon,p)} \qquad \textit{if } \epsilon \geq p,$$

$$\Pr\left[\frac{1}{n}\sum_{i=1}^{n} X_i \leq \epsilon\right] \leq e^{-nD(\epsilon,p)} \qquad \textit{if } \epsilon \leq p,$$

where $D(x, y) = x\log(\frac{x}{y}) + (1 - x)\log(\frac{1-x}{1-y})$ is a convex nonnegative function over the domain $0 < x, y < 1$. It equals zero only when x equals y.

Complexity Theory

Let Σ by a finite alphabet and let $\{\Sigma^n, \Sigma^{\leq n}, \Sigma^*, \Sigma^\infty, \Sigma^\circledast\}$ be the set of all Σ-sequences whose length is $\{$*exactly* n, *at most* n, *finite*, *infinite*, *arbitrary*$\}$, respectively.

Let $x \in \Sigma^*$. Denote $|x|$ the length of x. For $y \in \Sigma^\circledast$, denote $x\|y$ the concatenation of x and y. We say x is a prefix of y, and write $x \vdash y$, if there exists a $z \in \Sigma^\circledast$ such that $y = x\|z$.

For $i \in \mathbb{Z}^+$, denote $x[i]$ and $y[i]$ the i^{th} element of x and y, respectively. For $a \in \Sigma$ and $x \in \Sigma^\circledast$, denote $y = x \downarrow_i a$ the sequence which is identical to x everywhere except at the i^{th} position, where $y[i] = a$. Let $\sqcup \in \Sigma$ be a special blank symbol. Let *content*$(x) \in \Sigma^*$ be the shortest sequence such that $x =$ *content*$(x)\|\sqcup^\infty$, if there is such a sequence, and *content*$(x) = x$ otherwise.

Probabilistic Turing Machines. A probabilistic Turing machine PTM is a tuple $(Q, \Sigma, \Gamma, \delta, q_{\text{start}}, q_{\text{halt}})$ where: (i) Q is a finite set of states; (ii) Σ and Γ are finite, input and tape, alphabets such that $\Sigma \subset \Gamma$, and $\sqcup \in \Gamma - \Sigma$; (iii) δ :

$Q \times \Gamma \times \{0,1\} \rightarrow Q \times \Gamma \times \{+1,-1\}^2$ is a transition function; (iv) $q_{\text{start}}, q_{\text{halt}}$ are start and halt states. [20, 47]

A *computation* $C(w,r)$ of PTM is a sequence $\{C_i\}_{i=0}^{t}$ such that: (i) $w \in \Sigma^*$ and $r \leftarrow \mathcal{U}_{\{0,1\}^\infty}$, called the *input* and *random tape input* of PTM, respectively; (ii) $C_0 = (w \| \sqcup^\infty, 1, 1, q_{\text{start}})$, called the *initial configuration*; (iii) for all $i \geq 1$: (a) $C_i = (W_i, h_i, h'_i, q_i) \in \Gamma^\infty \times (\mathbb{Z}^+)^2 \times Q$, called the configuration of PTM *at step* i, where W_i is the content of the work tape, h_i is the position of the work tape's read-write head, h'_i is the position of the random tape's read-only head, and q_i is the state of PTM, (b) for $(q_i, w_i, \delta_i, \delta'_i) = \delta(q_{i-1}, W_{i-1}[h_{i-1}], r[h'_{i-1}])$, we have $W_i = W_{i-1} \downarrow_{h_{i-1}} w_i$, $h_i = \max\{1, h_{i-1} + \delta_i\}$ and $h'_i = \max\{1, h'_{i-1} + \delta'_i\}$; (iv) $q_i \neq q_{\text{halt}}$ for all $i < t$; (v) if $t < \infty$ then $q_t = q_{\text{halt}}$.

The *output* of computation $C(w,r)$ is *content*(W_t). The *time complexity* of PTM is the function $\text{time}_{\text{PTM}} : \mathbb{Z}^+ \rightarrow \mathbb{Z}^+$ defined by:

$$\text{time}_{\text{PTM}}(n) = \max\{|C(w,r)| : |w| \leq n, r \leftarrow \mathcal{U}_{\{0,1\}^\infty}\}.$$

PTM is called a *probabilistic polynomial time* Turing machine if for some polynomial $p(n)$, $\text{time}_{\text{PTM}}(n) \leq p(n)$ for all large enough n.

Oracle Turing Machine. let $A : \Sigma^* \rightarrow \Sigma^*$ be any function. An *oracle* Turing machine PTM^A [47, 21, 20] is a probabilistic Turing machine PTM with an additional *oracle work tape* and two additional internal *oracle query* and *oracle complete* states called q_{query} and q_{complete}. The oracle Turing machine PTM^A works as follows. When the PTM is in the q_{query} state, in a *single step*, the PTM is transitioned to the q_{complete} state, and its oracle work tape content x is replaced by $A(x)$.

Computational Indistinguishability. Let $P = \{P_1, P_2, \dots\}$ and $Q = \{Q_1, Q_2, \dots\}$ be two *families* of probability distributions over some finite sample space $\mathcal{S} \subset \Sigma^*$. P and Q are called *computationally indistinguishable* [21, 20] if for all probabilistic polynomial time Turing machine A with input alphabet Σ, the difference function

$d^A_{PQ}(n) = \mathit{diff}(A(P_n), A(Q_n))$ is negligible, where $A(P_n)$ (respectively, $A(Q_n)$) is the probability distribution of the output of A when its input is chosen randomly accordingly to P_n (respectively, Q_n).

Theorem 4. *If P and Q are statistically indistinguishable then they are computationally indistinguishable.*

Proof. Let $P'_n = A(P_n)$ and $Q'_n = A(Q_n)$. We have $P'_n(y) = \sum_{x \in \mathcal{S}} P_n(x) \Pr[A(x) = y]$ and $Q'_n(y) = \sum_{x \in \mathcal{S}} Q_n(x) \Pr[A(x) = y]$, so:

$$\begin{aligned} d^A_{PQ}(P_n, Q_n) &= \sum_{y \in \Sigma^*} \left| \sum_{x \in \mathcal{S}} (P_n(x) - Q_n(x)) \Pr[A(x) = y] \right| \\ &\leq \sum_{y \in \Sigma^*} \sum_{x \in \mathcal{S}} |P_n(x) - Q_n(x)| \Pr[A(x) = y] \\ &= \sum_{x \in \mathcal{S}} |P_n(x) - Q_n(x)| \sum_{y \in \Sigma^*} \Pr[A(x) = y] \\ &= \sum_{x \in \mathcal{S}} |P_n(x) - Q_n(x)|, \end{aligned}$$

which is negligible. Also see [20]. □

Coding Theory

Let Σ be a finite alphabet, and M be a finite set. A coding scheme Γ of M over Σ is a pair of two algorithms $\Gamma_{\text{Encode}} : M \to \Sigma^*$ and $\Gamma_{\text{Decode}} : \Sigma^* \to M$. Scheme Γ is called *uniquely decodable* if for all $m_1 \neq m_2 \in M$, we have $\Gamma_{\text{Encode}}(m_1) \neq \Gamma_{\text{Encode}}(m_2)$. The rate of encoding of Γ is defined as:

$$rate(\Gamma) = \frac{1}{\log |M|} \sum_{m \in M} H(\Gamma_{\text{Encode}}(m)).$$

For more details, see [11].

The Steganographic Game Problem

In this dissertation, we model a communication channel as a random process [19].

Definition 1 (Communication channel). *A communication channel $\mathcal{C}$ is a discrete random process $\{\mathcal{C}_t\}_{t=1}^{\infty}$, where $\mathcal{C}_t$ is a random variable whose value is the message sent in channel at time t.*

The conditional probability distribution of C_{t+1} given $(C_1, \ldots, C_t) = h$ is denoted by P_C, where h is the sequence of past messages. Furthermore, the set of all messages is denoted by C.

Definition 2 (Steganographic System). *A steganographic system is a tuple $(K, M, C, Setup, Embed, Extract)$ consisting of the key space K, the hiddentext space M and the covertext space C, together with three probabilistic Turing machines, $\texttt{Setup} : \{1\}^* \to K$, $\texttt{Embed} : K \times M \to C$ and $\texttt{Extract} : K \times C \to M$, such that: if $k = \texttt{Setup}(1^n)$ then for all $m \in M$ we have $\Pr[\texttt{Extract}(k, \texttt{Embed}(k, m)) = m]$ is overwhelming in n, where the probability is taken over the random tape content of Setup, Embed and Extract. Here n is the security parameter.*

Definition 3 (Chosen Hiddentext Attack). *A* CHA(n)*-attack is a game between two players, Alice and Wendy, who play as follows:*

1. *Alice generates a secret key $k = \texttt{Setup}(1^n)$.*
2. *Wendy chooses a hiddentext $m \in M$.*
3. *Alice chooses a secret bit $b \in_R \{0, 1\}$ and computes $c \in C$ as follows:*
   (a) *If $b = 0$, then c is chosen randomly according to P_C.*
   (b) *If $b = 1$, then $c = \texttt{Embed}(k, m)$.*

   Alice then returns c to Wendy.
4. *Wendy makes her guess b' of b.*

Wendy wins the game if $b' = b$ and loses otherwise.

The advantage of Wendy in a *CHA*(n, q)-attack is:

$$adv_{cha}(n, q) = \left| \Pr\left[b' = b\right] - \frac{1}{2} \right|,$$

where the probability is taken over the random tape content of Alice and Wendy.

Definition 4 (Adaptive Chosen Stegotexts Attack). *An* ACS(n, q)*-attack is a game between two players, Alice and Wendy, who play as follows:*

1. *Alice generates a secret key $k = \texttt{Setup}(1^n)$.*
2. *Alice and Wendy repeat the following steps for $i = 1, 2, \ldots, q'$:*
   (a) *Wendy chooses a stegotext $s_i \in C$.*
   (b) *Alice returns $m_i = \texttt{Extract}(k, s_i)$ to Wendy.*
3. *Wendy chooses a hiddentext $m \in M$.*
4. *Alice chooses a secret bit $b \in_R \{0, 1\}$ and computes $c \in C$ as follows:*
   (a) *If $b = 0$, then c is selected randomly according to P_C.*
   (b) *If $b = 1$, then $c = \texttt{Embed}(k, m)$.*

   Alice then returns c to Wendy.
5. *Alice and Wendy repeat the following step for $j = q' + 1, \ldots, q$:*
   (a) *Wendy chooses a stegotext $s_j \in C - \{c\}$.*
   (b) *Alice returns $m_j = \texttt{Extract}(k, s_j)$ to Wendy.*
6. *Wendy makes her guess b' of b.*

   Wendy wins the game if $b' = b$ and loses otherwise.

The advantage of Wendy in an *ACS*(n, q)-attack is:

$$adv_{acs}(n, q) = \left| \Pr\left[b' = b\right] - \frac{1}{2} \right|,$$

where the probability is taken over the random tape content of Alice and Wendy.

Definition 5 (Unconditional Security). *A steganographic system is called statistically secure (against chosen hiddentext attacks) if the advantage* $adv_{cha}(n, q)$ *of Wendy is negligible in* n *for all Wendy and all polynomially bounded* q*.*

Definition 6 (Conditional Security). *A steganographic system is called computationally secure (against adaptive chosen stegotext attacks) if the advantage* $adv_{acs}(n, q)$ *of Wendy is negligible for all polynomially bounded* q *and for every probabilistic polynomial time Turing machine Wendy.*

Dissertation Contribution

We show in this dissertation that secure steganography can be achieved in very general conditions. In particular, the minimal entropy in the perfect security model, and the normal entropy in the statistical security model are the necessary and sufficient condition for information theoretically secure steganography. On the other hand, we show that oneway function is necessary and sufficient for computationally secure steganography, modulo the entropy condition. Our resulting schemes are very efficient and in fact optimal for almost all of the cases.

Along the way, we introduce two new concepts called *invisible steganography* and *steganographic secret sharing*. We provide six solutions to the steganographic game problem, namely: perfect, perfectly invisible, statistical, steganographic secret sharing and computationally secure solutions.

Dissertation Organization

The dissertation is organized as follows. Chapters 2, 3, 4 assume unconditional securities and present information theory based approaches. Chapter 5 assumes conditional security and describes an approach based on computational complexity. Finally, chapter 6 applies the previous chapters' solutions to the case where a probability distribution is not available, and also to the case where successive covertexts are probabilistically dependent. In each chapter, first a formal model of semantic security is given, then a lower bound for schemes achieving that security condition, and finally, constructions of scheme achieving these bounds are presented.

CHAPTER 2

PERFECT STEGANOGRAPHY SOLUTIONS

In this chapter we study *perfect* steganographic schemes in which the stegotext distribution is identical to the covertext distribution and the error decoding probability is zero. We show in this chapter for the first time that one can do covert communication perfectly with unconditional hiding and unconditional secrecy for all allowable general covertext distributions. We will obtain a result similar to Shannon's source coding theorem: the min entropy is the upper bound under which perfect steganography is achievable. We additionally show that perfect hiding implies perfect secrecy. Therefore steganographic schemes can be regarded as special types of general encryption schemes.

An issue overlooked in the current research on steganography is that the secret key is often stored on insecure devices such as computers. So, although steganography may make the computer less suspect to computer viruses and worms that are searching for secret keys, the fact that the key is not steganographic makes it easily available to such computer viruses and worms [3]. We extend the concept of steganography to introduce a new concept called steganographic secret sharing, or invisible steganography, in which both the key and the stegotext are hidden. So a computer could just have a set of family pictures, some corresponding to keys, some to ciphertext. We show that such an extension exists, and then show how to construct such a scheme with a good information rate. We show that obtaining the maximum information rate in this extension is NP hard. Finally we show

that the more general case when the keys correspond to a given key distribution, independently of the covertext distribution, is also NP hard.

Definitions

In this chapter, we denote random variables by letters in bold face (i.e. $\mathbf{k}, \mathbf{m}, \mathbf{c}, \ldots$); their sample spaces by the same letter in caligraphic font (i.e. $\mathcal{K}, \mathcal{M}, \mathcal{C}, \ldots$); and their particular values by the same letter in italic font (i.e. $k, m, c, \ldots$). The letters k, m, c are reserved for the key, message, and ciphertext, respectively. The meaning of other symbols is summarized in the following: $\vec{P}_{\mathbf{x}}$ is the column vector whose entries are the probabilities $P_{\mathbf{x}}(a)$; $\mathcal{A}^T$ is the transpose of matrix $\mathcal{A}$; $\mathcal{A}(i,j)$ is the entry at the i-th row and the j-th column of matrix $\mathcal{A}$; $\mathcal{V}|_k$ is the k-th entry of vector $\mathcal{V}$; $\mathbf{e}_i$ is the i-th standard basis vector ($\mathbf{e}_i|_i = 1$, and $\mathbf{e}_i|_j = 0$ for $j \neq i$); $\mathbf{1}^n$ is the column vector of n ones; n-set is a finite set of n elements.

Note that the terms *stegotext* and *ciphertext* are synonyms. The *minimum entropy* of a distribution is the corresponding entropy of a symbol of the minimum entropy in this distribution. We shall use letter E for the embedding algorithm and letter D for the extraction algorithm.

A perfect information hiding scheme is a steganographic scheme which satisfies the two conditions, called *soundness* and *perfect hiding*, defined below.

Definition 7 (Perfect Steganography). *We say that an information hiding scheme achieves:*

- **Perfect decryptability** *: If for all $k \in \mathcal{K}$ and $m \in \mathcal{M}$: $D(k, E(k,m)) = m$.*
- **Perfect hiding***: If for each message $m \in \mathcal{M}$, $E(k,m)$ distributes exactly like the given distribution $P_{\mathcal{C}}$, where k is taken randomly from $\mathcal{K}$ according to $P_{\mathcal{K}}$. That is, for all $c \in \mathcal{C}$:*

$$\Pr(E(\mathbf{k}, \mathbf{m}) = c) = P_{\mathcal{C}}(c). \tag{2.1}$$

- **Perfect secrecy**: *If m is probabilistically independent of $E(k, m)$. That is:*

$$\Pr(\mathbf{m} \mid E(\mathbf{k}, \mathbf{m})) = \Pr(\mathbf{m}). \tag{2.2}$$

An information hiding scheme achieves *perfect security* if it achieves both *perfect secrecy* and *perfect hiding*.

Secrecy versus Hiding

Let $\mathcal{A}$ be a perfect information hiding scheme. In this section, we will answer the question concerning hiding versus secrecy of $\mathcal{A}$ by studying its characteristic matrices. The characteristic matrices completely determine the properties of $\mathcal{A}$. In later sections, they will also allow us to find the necessary and sufficient condition for the existence of a perfect information hiding scheme. *The characteristic matrices allow us to dramatically simplify our proofs.*

Definition 8 (Characteristic matrices). *We define the set of characteristic matrices $\{A_m\} = \{\mathcal{A}_m \mid m \in \mathcal{M}\}$ as the probability matrices of k and $E(k, m)$ conditional on m:*

$$\mathcal{A}_m = \left[\mathcal{A}_m(k, c) = \Pr(\mathbf{k} = k, E(\mathbf{k}, \mathbf{m}) = c \mid \mathbf{m} = m)\right]_{k \in K, c \in C}. \tag{2.3}$$

We now express the perfect decryptability , perfect secrecy, and perfect hiding properties of $\mathcal{A}$ in terms of the set of characteristic matrices $\{\mathcal{A}_m\}$. We will show in the next two theorems that perfect information hiding schemes are those that satisfy conditions (2.4, 2.5, 2.10) simultaneously.

Theorem 5 (Matrix equivalence for perfect decryptability). *Let $[\mathcal{A}_m] = \{(k, c) \mid \mathcal{A}_m(k, c) \neq 0\}$ be the set of indices of non-zero entries of $\mathcal{A}_m$. We have:*

A. If the tuple $(\mathcal{K}, \mathcal{C}, \mathcal{M}, P_{\mathcal{K}}, P_{\mathcal{C}}, E, D)$, as described in Definition 7, is an informa-

tion hiding scheme then:

$$\forall m_1, m_2 \in \mathcal{M} \quad : \quad m_1 \neq m_2 \Rightarrow [\mathcal{A}_{m_1}] \cap [\mathcal{A}_{m_2}] = \emptyset. \tag{2.4}$$

$$\forall m \in \mathcal{M} \quad : \quad \mathcal{A}_m \times \mathbf{1}^{|\mathcal{C}|} = \vec{P}_{\mathcal{K}}. \tag{2.5}$$

B. If conditions (2.4) and (2.5) are satisfied for a tuple $(\mathcal{K}, \mathcal{C}, \mathcal{M}, P_{\mathcal{K}})$ and an $|\mathcal{M}|$-set of $|\mathcal{K}| \times |\mathcal{C}|$ matrices $\mathcal{A}_m$ over the non-negative reals, then the following scheme is a perfect information hiding scheme:

- *Algorithm* **E:** *input message $m \in \mathcal{M}$ and key $k \in \mathcal{K}$.*
  Randomly output $c \leftarrow P_C$, where $P_C(c) = P_{\mathcal{K}}(k)^{-1}\mathcal{A}_m(k, c)$.
- *Algorithm* **D:** *input ciphertext $c \in \mathcal{C}$ and key $k \in \mathcal{K}$.*
  Output the unique m such that $\mathcal{A}_m(k, c) \neq 0$.

Proof. We prove each part of the theorem separately.

A. Let $\mathcal{A} = (\mathcal{K}, \mathcal{C}, \mathcal{M}, P_{\mathcal{K}}, P_{\mathcal{C}}, E, D)$ be an information hiding scheme. From Definition 7, by perfect decryptability , we have that k and $E(k, m)$ uniquely determine m, hence for all keys k:

$$m_1 \neq m_2 \Rightarrow E(k, m_1) \neq E(k, m_2). \tag{2.6}$$

On the other hand, from the definition of $[\mathcal{A}_m]$ we have:

$$\begin{aligned} [\mathcal{A}_{m_1}] \cap [\mathcal{A}_{m_2}] \neq \emptyset \quad &\Rightarrow \quad \exists\, k, c : \left\{ \begin{array}{l} (\Pr(\mathbf{k} = k, E(\mathbf{k}, \mathbf{m}) = c \mid \mathbf{m} = m_1) \neq 0) \\ (\Pr(\mathbf{k} = k, E(\mathbf{k}, \mathbf{m}) = c \mid \mathbf{m} = m_2) \neq 0) \end{array} \right\} \\ &\Rightarrow \quad \exists\, k, c : c = E(k, m_1) = E(k, m_2) \\ &\Rightarrow \quad \exists\, k : E(k, m_1) = E(k, m_2). \end{aligned} \tag{2.7}$$

Combine (2.6) and (2.7), by the contrapositive rule to get:

$$m_1 \neq m_2 \Rightarrow [\mathcal{A}_{m_1}] \cap [\mathcal{A}_{m_2}] = \emptyset.$$

Hence (2.4) is true. We now show that (2.5) is also true.

From (2.3) and the fact that k and m are independent we have:

$$\begin{aligned}\mathcal{A}_m(k,c) &= \Pr(\mathbf{k}=k, E(\mathbf{k},\mathbf{m})=c \mid \mathbf{m}=m) \\ &= \Pr(E(\mathbf{k},\mathbf{m})=c \mid \mathbf{k}=k, \mathbf{m}=m)\Pr(\mathbf{k}=k \mid \mathbf{m}=m) \\ &= \Pr(E(\mathbf{k},\mathbf{m})=c \mid \mathbf{k}=k, \mathbf{m}=m)\Pr(\mathbf{k}=k). \qquad (2.8)\end{aligned}$$

By substituting (2.8) into the left hand side of (2.5) we have:

$$\begin{aligned}\left(\mathcal{A}_m \times \mathbf{1}^{|\mathcal{C}|}\right)|_k &= \sum_{c\in\mathcal{C}} \mathcal{A}_m(k,c) = \sum_{c\in\mathcal{C}} \Pr(E(\mathbf{k},\mathbf{m})=c \mid \mathbf{k}=k, \mathbf{m}=m)\Pr(\mathbf{k}=k) \\ &= \Pr(\mathbf{k}=k)\sum_{c\in\mathcal{C}} \Pr(E(\mathbf{k},\mathbf{m})=c \mid \mathbf{k}=k, \mathbf{m}=m) = \Pr(\mathbf{k}=k)\times 1 \\ &= P_{\mathcal{K}}(k).\end{aligned}$$

Therefore $\mathcal{A}_m \times \mathbf{1}^{|\mathcal{C}|} = \vec{P}_{\mathcal{K}}$.

B. Assume that (2.4) and (2.5) are true, and that the tuple $(\mathcal{K}, \mathcal{C}, \mathcal{M}, P_{\mathcal{K}}, \{\mathcal{A}_m\})$ satisfies the conditions stated in the second part of the theorem.

First, (2.5) implies that

$$\sum_{\substack{k\in\mathcal{K}\\ c\in\mathcal{C}}} \mathcal{A}_m(k,c) = 1. \qquad (2.9)$$

Let $\mathcal{A}_m(k,c)$ correspond to a probability, i.e. $\mathcal{A}_m(k,c) = \Pr(\mathbf{k}=k, \mathbf{a}=c \mid \mathbf{m}=m)$, where the meaning of $\mathbf{a}$ will be explained later. Due to (2.9), this probability is properly defined.

We now prove that the probability distribution $P_{\mathcal{K}}$ is independent of $P_{\mathcal{M}}$, i.e.,

(2.2) is true. From (2.5) we have:

$$\begin{aligned}\Pr(\mathbf{k}=k \mid \mathbf{m}=m) &= \sum_{c\in\mathcal{C}} \Pr(\mathbf{k}=k, \mathbf{a}=c \mid \mathbf{m}=m) \\ &= \sum_{c\in\mathcal{C}} \mathcal{A}_m(k,c) = \left(\mathcal{A}_m \times \mathbf{1}^{|\mathcal{C}|}\right)|_k = \Pr(\mathbf{k}=k).\end{aligned}$$

Hence $\mathbf{k}$ is independent of $\mathbf{m}$. Therefore (2.2) is true. We finally prove that $(\mathcal{K}, \mathcal{M}, \mathcal{C}, P_{\mathcal{K}}, P_{\mathcal{C}}, E, D)$ is an information hiding scheme.

If $P_{\mathcal{K}}(k) = 0$ then a complete row of $\mathcal{A}_m$ is zero, due to (2.5). We prove that $\mathbf{a}$ corresponds to $E(\mathbf{k}, \mathbf{m})$. Indeed, using elementary probability theory and the fact that $\mathbf{k}$ is independent of $\mathbf{m}$, we have $\Pr(E'(\mathbf{k}, \mathbf{m}) = c_0 \mid \mathbf{k} = k, \mathbf{m} = m) = \Pr(E'(\mathbf{k}, \mathbf{m}) = c_0, \mathbf{k} = k \mid \mathbf{m} = m)/\Pr(\mathbf{k} = k)$. By the definition of $\mathbf{a}$ and E we have that $\mathbf{a}$ corresponds to $E(\mathbf{k}, \mathbf{m})$. We now use this to prove the perfect decryptability property. Denoting "*there exists at most one*" by $\exists_{\leq 1}$, we see that (2.4) implies

$$\begin{aligned}\forall k, \forall c, \exists_{\leq 1}\, m: &\qquad \mathcal{A}_m(k,c) \neq 0 \\ \forall k, \forall c, \exists_{\leq 1}\, m: &\qquad E(k,m) = c.\end{aligned}$$

This says that for any given $k \in \mathcal{K}, c \in \mathcal{C}$, algorithm D can determine at *most one* $m \in \mathcal{M}$ such that $E(k,m) = c$. Moreover, from (2.5) we know that for a given m and a given k with $P_{\mathcal{K}}(k) \neq 0$, there exists at least one c such that $\mathcal{A}_m(k,c) \neq 0$. Combining this with the definition of E we have that if E outputs a c, then $\mathcal{A}_m(k,c) \neq 0$. So for all $k \in \mathcal{K}$ and $m \in \mathcal{M}$: $D(k, E(k,m)) = m$. Therefore the scheme is sound.

Consequently, $\mathcal{A} = (\mathcal{K}, \mathcal{C}, \mathcal{M}, P_{\mathcal{K}}, P_{\mathcal{C}}, E, D)$ is an information hiding scheme.

□

When the conditions of the second part of Theorem 5 are satisfied, we say that the $(\mathcal{K}, \mathcal{C}, \mathcal{M}, P_{\mathcal{K}}, \{\mathcal{A}_m\})$ induces algorithms E and D. From now on, whenever we say we construct a scheme, we actually give the matrices $\{\mathcal{A}_m\}$ in explicit form.

Theorem 6 (Matrix equivalence for perfect security). *A given information hiding scheme $\mathcal{A}$ achieves perfect secrecy and perfect information hiding if and only if for all $m \in \mathcal{M}$:*

$$\mathcal{A}_m^T \times \mathbf{1}^{|\mathcal{K}|} \;=\; \vec{P}_{\mathcal{C}}. \tag{2.10}$$

Proof. We prove each direction in turn.

$\{\Rightarrow\}$ Assume that scheme $\mathcal{A}$ achieves perfect security. From (2.2), (2.1) and the definition of $\mathcal{A}_m$ we have:

$$\begin{aligned}\left(\mathcal{A}_m^T \times \mathbf{1}^{|\mathcal{K}|}\right)|_c &= \sum_{k\in\mathcal{K}} \mathcal{A}_m(k,c) = \sum_{k\in\mathcal{K}} \Pr(\mathbf{k}=k, E(\mathbf{k},\mathbf{m})=c \mid \mathbf{m}=m) \\ &= \Pr(E(\mathbf{k},\mathbf{m})=c \mid \mathbf{m}=m) = \Pr(E(\mathbf{k},\mathbf{m})=c) = P_{\mathcal{C}}(c).\end{aligned}$$

Therefore (2.10) is true.

$\{\Leftarrow\}$ Assume that (2.10) is true. Using the definition of $\mathcal{A}_m$ (see 2.3 and 2.10), we have:

$$\begin{aligned}\Pr(E(\mathbf{k},\mathbf{m})=c \mid \mathbf{m}=m) &= \sum_{k\in\mathcal{K}} \Pr(\mathbf{k}=k, E(\mathbf{k},\mathbf{m})=c \mid \mathbf{m}=m) \\ &= \left(\mathcal{A}_m^T \times \mathbf{1}^{|\mathcal{K}|}\right)|_c = P_{\mathcal{C}}(c). \end{aligned} \tag{2.11}$$

By (2.11) we now have:

$$\begin{aligned}\Pr(E(\mathbf{k},\mathbf{m})=c) &= \sum_m \Pr(E(\mathbf{k},\mathbf{m})=c \mid \mathbf{m}=m)\Pr(\mathbf{m}=m) \\ &= \sum_m P_{\mathcal{C}}(c)\Pr(\mathbf{m}=m) = P_{\mathcal{C}}(c). \end{aligned} \tag{2.12}$$

Combining (2.11) and (2.12) we have that $E(\mathbf{k},\mathbf{m})$ is independent of $\mathbf{m}$, so we have perfect secrecy. Moreover, from (2.12) we see that (2.1) is also true, so we have perfect hiding.

□

We next demonstrate our first application of the characteristic matrices. We show that the hiding property does imply the secrecy.

Corollary 1 (Hiding Implies Secrecy). *Let $\mathcal{A}$ be an information hiding scheme with perfect hiding, independently of the message distribution. Then $\mathcal{A}$ is an information hiding scheme with perfect secrecy, independently of the message distribution.*

Proof. Assume that scheme $\mathcal{A}$ achieves perfect hiding. From (2.1) we have:

$$\begin{aligned} P_{\mathcal{C}}(c) &= \Pr(E(\mathbf{k},\mathbf{m})=c) = \sum_m \Pr(E(\mathbf{k},\mathbf{m})=c \mid \mathbf{m}=m)\Pr(\mathbf{m}=m) \\ &= \sum_m \sum_k \Pr(\mathbf{k}=k, E(\mathbf{k},\mathbf{m})=c \mid \mathbf{m}=m)\Pr(\mathbf{m}=m) \\ &= \sum_m \sum_k \mathcal{A}_m(k,c)\Pr(\mathbf{m}=m) = \sum_m \Pr(\mathbf{m}=m)\left(\mathcal{A}_m^T \times \mathbf{1}^{|\mathcal{K}|}\right)|_c \,. \end{aligned} \tag{2.13}$$

Using the vector distribution $\vec{P}_{\mathcal{M}} = (P_{\mathcal{M}}(m_1), \ldots, P_{\mathcal{M}}(m_{|\mathcal{M}|}))$ with $P_{\mathcal{M}}(m) = 1$ and $P_{\mathcal{M}}(m') = 0$ for all $m' \neq m$ in (2.13), we get $P_{\mathcal{C}}(c) = \left(\mathcal{A}_m^T \times \mathbf{1}^{|\mathcal{K}|}\right)|_c$. Therefore condition (2.10) is satisfied. By Theorem 6, $\mathcal{A}$ is a perfect information hiding scheme, i.e. $\mathcal{A}$ achieves perfect secrecy. □

This result shows us that a perfect steganographic scheme is indeed a perfect encryption scheme. This proves that the common practice of encrypting data before embedding it using steganography for better security, is unnecessary.

Universal Bounds

In this section, we give some new bounds that are applicable to all perfect information hiding schemes. We find upper bounds that the key and ciphertext distributions impose on each other in a perfect information hiding scheme. We then derive an upper bound on the message space size. This allows us to estimate in advance the information rate, or how much information can be sent in a steganographic scheme. We will show in later sections that the given bound is in fact tight.

Theorem 7 (Necessary conditions). *If $\mathcal{A}$ is a perfect information hiding scheme then:*

A. *There exists a disjoint $\mathcal{M}$-partition $\{\mathcal{C}_1, \mathcal{C}_2, \ldots, \mathcal{C}_{|\mathcal{M}|}\}$ of $\mathcal{C}$ such that:*

$$\min_i \sum_{c \in \mathcal{C}_i} P_{\mathcal{C}}(c) \geq \max_{k \in \mathcal{K}} P_{\mathcal{K}}(k). \tag{2.14}$$

B. *There exists a disjoint $\mathcal{M}$-partition $\{\mathcal{K}_1, \mathcal{K}_2, \ldots, \mathcal{K}_{|\mathcal{M}|}\}$ of $\mathcal{K}$ such that:*

$$\min_i \sum_{k \in \mathcal{K}_i} P_{\mathcal{K}}(k) \geq \max_{c \in \mathcal{C}} P_{\mathcal{C}}(c). \tag{2.15}$$

Proof. A. Let $k^* \in \mathcal{K}$ be such that $P_{\mathcal{K}}(k^*) = \max_{k \in \mathcal{K}} P_{\mathcal{K}}(k)$. Since $\mathcal{A}$ satisfies (2.5), we have for all $m \in \mathcal{M}$:

$$\sum_{c \in \mathcal{C}} \mathcal{A}_m(k^*, c) = P_{\mathcal{K}}(k^*). \tag{2.16}$$

For each $m_i \in \mathcal{M}$, let $C_i = \{c \in \mathcal{C} \mid \mathcal{A}_{m_i}(k^*, c) \neq 0\}$. Since $\mathcal{A}$ also satisfies (2.4), we have for all $m_i, m_j \in \mathcal{M}$:

$$m_i \neq m_j \Rightarrow C_i \cap C_j = \emptyset.$$

We let $\mathcal{C}_i = C_i$, except that we extend some $\mathcal{C}_i$ to include the set $\Delta = \{c \in \mathcal{C} \mid \forall m_i \in \mathcal{M} : \mathcal{A}_{m_i}(k^*, c) = 0\}$ so that $\{\mathcal{C}_1, \mathcal{C}_2, \ldots, \mathcal{C}_{|\mathcal{M}|}\}$ is indeed a partition of $\mathcal{C}$.

Because for each i we have that $\mathcal{A}_{m_i}(k, c) = 0$ when $c \notin \mathcal{C}_i$, we can rewrite

(2.16) as follows:

$$\begin{aligned} P_{\mathcal{K}}(k^*) &= \sum_{c\in\mathcal{C}} \mathcal{A}_{m_i}(k^*, c) = \sum_{c\in\mathcal{C}_i} \mathcal{A}_{m_i}(k^*, c) \\ &\leq \sum_{c\in\mathcal{C}_i}\sum_{k\in\mathcal{K}} \mathcal{A}_{m_i}(k, c) = \sum_{c\in\mathcal{C}_i}\sum_{k\in\mathcal{K}} \Pr(\mathbf{k} = k, E(\mathbf{k}, \mathbf{m}) = c \mid \mathbf{m} = m_i) \\ &= \sum_{c\in\mathcal{C}_i} \Pr(E(\mathbf{k}, \mathbf{m}) = c \mid \mathbf{m} = m_i). \end{aligned} \tag{2.17}$$

Since $\mathcal{A}$ satisfies (2.2), substituting $\Pr(E(\mathbf{k}, \mathbf{m}) = c \mid \mathbf{m} = m_i) = \Pr(E(\mathbf{k}, \mathbf{m}) = c)$ into (2.17) yields: $P_{\mathcal{K}}(k^*) \leq \sum_{c\in\mathcal{C}_i} \Pr(E(\mathbf{k}, \mathbf{m}) = c) = \sum_{c\in\mathcal{C}_i} P_{\mathcal{C}}(c)$, using (2.1). Because the above is true for each i, so is (2.14).

B. Let $c^* \in \mathcal{C}$ such that $P_{\mathcal{C}}(c^*) = \max_{c\in\mathcal{C}} P_{\mathcal{C}}(c)$. Since $\mathcal{A}$ satisfies (2.10), we have for all $m \in \mathcal{M}$:

$$\sum_{k\in\mathcal{K}} \mathcal{A}_m(k, c^*) = P_{\mathcal{C}}(c^*). \tag{2.18}$$

For each $m_i \in \mathcal{M}$, let $K_i = \{k \in \mathcal{K} \mid \mathcal{A}_{m_i}(k, c^*) \neq 0\}$. Since $\mathcal{A}$ also satisfies (2.4), we have for all $m_i, m_j \in \mathcal{M}$:

$$m_i \neq m_j \Rightarrow K_i \cap K_j = \emptyset.$$

We let $\mathcal{K}_i = K_i$, except that we extend some $\mathcal{K}_i$ to include the set $\Delta = \{k \in \mathcal{K} \mid \forall m_i \in \mathcal{M} : \mathcal{A}_{m_i}(k, c^*) = 0\}$ so that $\{\mathcal{K}_1, \mathcal{K}_2, \ldots, \mathcal{K}_{|\mathcal{M}|}\}$ is indeed a partition of $\mathcal{K}$.

Because for each i, $\mathcal{A}_{m_i}(k, c) = 0$ when $k \notin \mathcal{K}_i$, we can rewrite (2.18) as follows:

$$\begin{aligned} P_{\mathcal{C}}(c^*) &= \sum_{k\in\mathcal{K}} \mathcal{A}_{m_i}(k, c^*) = \sum_{k\in\mathcal{K}_i} \mathcal{A}_{m_i}(k, c^*) \\ &\leq \sum_{k\in\mathcal{K}_i}\sum_{c\in\mathcal{C}} \mathcal{A}_{m_i}(k, c) = \sum_{k\in\mathcal{K}_i}\sum_{c\in\mathcal{C}} \Pr(\mathbf{k} = k, E(\mathbf{k}, \mathbf{m}) = c \mid \mathbf{m} = m_i) \\ &= \sum_{k\in\mathcal{K}_i} \Pr(\mathbf{k} = k \mid \mathbf{m} = m_i). \end{aligned} \tag{2.19}$$

Since $\mathcal{A}$ satisfies Definition 7, substituting $\Pr(\mathbf{k} = k \mid \mathbf{m} = m_i) = \Pr(\mathbf{k} = k)$ into (2.19) yields: $P_{\mathcal{C}}(c^*) \leq \sum_{k \in \mathcal{K}_i} \Pr(\mathbf{k} = k) = \sum_{k \in \mathcal{K}_i} P_{\mathcal{K}}(k)$, Because the above is true for each i, so is (2.15). □

Corollary 2. *If $\mathcal{A}$ is a perfect information hiding scheme then:*

$$\log |\mathcal{M}| \leq \min(H_{min}(P_{\mathcal{K}}), H_{min}(P_{\mathcal{C}})). \tag{2.20}$$

Proof. From (2.14) in the above theorem we have: $\sum_{c \in \mathcal{C}_i} P_{\mathcal{C}}(c) \geq P_{\mathcal{K}}(k^*)$. Thus:

$$1 = \sum_{c \in \mathcal{C}} P_{\mathcal{C}}(c) \quad = \quad \sum_{i=1}^{|\mathcal{M}|} \sum_{c \in \mathcal{C}_i} P_{\mathcal{C}}(c) \geq |\mathcal{M}| P_{\mathcal{K}}(k^*).$$

Therefore, $P_{\mathcal{K}}(k^*) \leq 1/|\mathcal{M}|$. Similarly, using (2.15), $|\mathcal{M}| \leq 1/P_{\mathcal{C}}(c^*)$. Hence Corollary 2 is true.

□

Steganographic Schemes

In this section, we construct a covert communication scheme with unconditional hiding and unconditional secrecy [14]. This scheme can be used when one has a secure store for the key, and therefore the restriction on $P_{\mathcal{K}}$ is not needed. This relaxed condition makes the construction of the scheme more efficient. Our scheme have maximum rate, and works with general distributions. The construction of the schemes is given below.

Theorem 8. *Let $c_1, c_2, \ldots, c_n$ be n nonnegative rational numbers, and let m and q be positive integers such that $\forall i \in \{1 \ldots n\} : c_i \leq \frac{1}{m}$, $\sum_{i=1}^{n} c_i = 1$, and qc_i are integers for $i \in \{1, \ldots, n\}$. Then Algorithm 1, on input $(qc_1, qc_2, \ldots, qc_n)$, will produce a perfectly secure information hiding scheme with key space size k, plaintext space size m, and ciphertext distribution $P_{\mathcal{C}} = (c_1, c_2, \ldots, c_n)$.*

ALGORITHM 1 A general steganographic scheme that is perfect

Require: input integers $c'_1, c'_2, \ldots, c'_n$

Ensure: output an integer k and m matrices $\mathcal{A}_1, \ldots, \mathcal{A}_m$ of size $k \times n$

if $\forall i \in \{1, \ldots, n\} : c'_i = 0$ **then**
  $\mathcal{A}_1, \mathcal{A}_2, \ldots, \mathcal{A}_m \Leftarrow$ empty matrices
  $k \Leftarrow 0$
else
  $Q \Leftarrow (c'_1 + c'_2 + \cdots + c'_n)/m$
  $\sigma \Leftarrow$ a permutation of $(1, 2, \ldots, n)$ such that $c'_{\sigma_1} \geq c'_{\sigma_2} \geq \cdots \geq c'_{\sigma_n}$
  $\delta \Leftarrow \min(Q - c'_{\sigma_{m+1}}, c'_{\sigma_m})$
  $c''_{\sigma_i} \Leftarrow c'_{\sigma_i} - \delta$ for $i \in \{1, 2, \ldots, m\}$
  $c''_{\sigma_i} \Leftarrow c'_{\sigma_i}$ for $i \in \{m+1, m+2, \ldots, n\}$
  $\mathcal{A}'_1, \mathcal{A}'_2, \ldots, \mathcal{A}'_m, k' \Leftarrow$ **Algorithm 1**$(c''_1, c''_2, \ldots, c''_n)$
  $Q' \Leftarrow (c''_1 + c''_2 + \cdots + c''_n)/m$
  $k \Leftarrow k' + m$
  for $i = 1$ to m **do**
    for $j = 1$ to m **do**
      $t \Leftarrow ((i + j) \bmod m) + 1$
      Append row $\delta \mathbf{e}_{\sigma_t}$ to $\mathcal{A}'_i$
    end for
    $\mathcal{A}_i \Leftarrow \mathcal{A}'_i$
  end for
end if

To simplify the proof of our theorem, we divide Algorithm 1 in two parts, Reduce and Construct. First we need the following lemma.

Lemma 3 (Rational probabilities). *Let $c_1, c_2, \ldots, c_n$ be n nonnegative rational numbers, and let m be positive integers such that $\forall i \in \{1 \ldots n\} : c_i \leq \frac{1}{m}$, and $\sum_{i=1}^{n} c_i = 1$. Then there exists m matrices $\mathcal{A}_1, \mathcal{A}_2, \ldots, \mathcal{A}_m$ of the same size $k \times n$ with nonnegative entries such that:*

$$\forall i \in \{1 \ldots m\} : (\mathcal{A}_i)^T \times \mathbf{1}^k = c,$$

$$\forall i, j \in \{1 \ldots m\} : \mathcal{A}_i \times \mathbf{1}^n = \mathcal{A}_j \times \mathbf{1}^n,$$

$$\forall i \neq j \in \{1, \ldots, m\} : [\mathcal{A}_i] \cap [\mathcal{A}_j] = \emptyset,$$

where k is a positive integer and $c = (c_1, c_2, \ldots, c_n)$.

Proof. Let Q be the least common multiple of the denominators of $c_1, c_2, \ldots, c_n$. If some $c_i = 0$ then its denominator is 1. For all $1 \leq i \leq n$ let $c'_i = mQc_i$. Then the integers c'_i satisfy $\forall i \in \{1 \ldots n\} : c'_i \leq \frac{1}{m} \sum_{i=1}^{n} c'_i = Q$. By taking some c_i's to be 0, one can always assume that $n > m$. We then consider the following sub-routine (which consists of first 5 steps of the **else** part in Algorithm 1):

Reduce

- **Input**: nonnegative integers $c'_1, c'_2, \ldots, c'_n$ such that:
  - $\forall i \in \{1 \ldots n\} : c'_i \leq \frac{1}{m} \sum_{i=1}^{n} c'_i = Q > 0$,
- **Output**: nonnegative integers $c''_1, c''_2, \ldots, c''_n$ such that:
  - $\forall i \in \{1 \ldots n\} : c''_i \leq \frac{1}{m} \sum_{i=1}^{n} c''_i = Q' < Q$,
  - $\forall i \in \{1 \ldots n\} : (c''_i = c'_i) \vee (c''_i = c'_i + Q' - Q)$.

1) Sort $c'_1, c'_2, \ldots, c'_n$ in descending order to obtain $c'_{\sigma_1} \geq c'_{\sigma_2} \geq \cdots \geq c'_{\sigma_n}$.

2) Compute $\delta = \min(Q - c'_{\sigma_{m+1}}, c'_{\sigma_m})$.

3) Let $c''_{\sigma_i} = c'_{\sigma_i} - \delta$ for $i \leq m$, and let $c''_{\sigma_i} = c'_{\sigma_i}$ for $i > m$.

Subroutine Reduce.

We now show the correctness of this routine. First one can easily verify that the c''_i are nonnegative. We need to show that $\forall i \in \{1 \dots n\} : c''_i \leq \frac{1}{m}\sum_{i=1}^{n} c''_i = Q - \delta < Q$. Because $c'_{\sigma_1}, c'_{\sigma_2}, \dots, c'_{\sigma_n}$ were sorted in descending order, $c''_1, c''_2, \dots, c''_n$ are partially sorted in two descending runs $c''_{\sigma_1} \geq c''_{\sigma_2} \geq \cdots \geq c''_{\sigma_m}$ and $c''_{\sigma_{m+1}} \geq \cdots \geq c''_{\sigma_n}$. Hence we just need to verify that $c''_{\sigma_1}, c''_{\sigma_{m+1}} \leq Q - \delta$, and that $\delta > 0$:

A. $c''_{\sigma_1} \leq Q - \delta$ because $c''_{\sigma_1} = c'_{\sigma_1} - \delta$ and $c'_{\sigma_1} \leq Q$.

B. $c''_{m+1} \leq Q - \delta$ because $c''_{m+1} = (c'_{\sigma_{m+1}} - \delta) + \delta \leq (c'_{\sigma_{m+1}} - \delta) + (Q - c'_{\sigma_{m+1}}) = Q - \delta$.

C. If $c'_{\sigma_m} = 0$ then $c'_{\sigma_{m+1}} = \cdots = c'_{\sigma_n} = 0$, and consequently $\frac{1}{m}\sum_{i=1}^{n} c'_{\sigma_i} = \frac{1}{m}\sum_{i=1}^{m-1} c'_{\sigma_i} \leq \frac{m-1}{m}Q < Q$, contradicting the input assumption. Therefore $c'_{\sigma_m} = 0$ is false, i.e. $c'_{\sigma_m} > 0$. Similarly, if $Q - c'_{\sigma_{m+1}} = 0$ then $\frac{1}{m}\sum_{i=1}^{n} c'_{\sigma_i} \geq \frac{1}{m}\sum_{i=1}^{m+1} c'_{\sigma_i} \geq \frac{m+1}{m}c'_{\sigma_{m+1}} \geq \frac{m+1}{m}Q > Q$, contradicting the input assumption. Hence we must have $Q - c'_{\sigma_{m+1}} \neq 0$, i.e. $Q - c'_{\sigma_{m+1}} > 0$. This shows that $\delta = \min(Q - c'_{\sigma_{m+1}}, c'_{\sigma_m}) > 0$.

D. The condition $(c''_i = c'_i) \vee (c''_i = c'_i + Q' - Q)$ is automatically satisfied since $Q' = Q - \delta$.

We complete the proof of Lemma 3 by describing the subroutine Construct (see page 36) which constructs $\mathcal{A}_1, \mathcal{A}_2, \dots, \mathcal{A}_m$ using our sub-routine Reduce above (see page 35) , and pointing out its correctness.

Soundness For simplicity, let us assume that $(\sigma_1, \dots, \sigma_n)$ is $(1, \dots, n)$, i.e. $\{c'_1, \dots, c'_n\}$ is sorted in descending order. Then,

A. Let $(p'_1, p'_2, \dots, p'_{k'}) = \mathcal{A}'_t \times \mathbf{1}^n$. It is easy to check that

$$\forall i : \mathcal{A}_i \times \mathbf{1}^n = (p'_1, p'_2, \dots, p'_{k'}, \delta, \dots, \delta)^T,$$

where there are m copies of δ. Note that the p'_j's are independent of t.

Construct

- **Input**: nonnegative integers $c'_1, c'_2, \ldots, c'_n$ such that:

$$\forall i \in \{1 \ldots n\} : c'_i \leq \frac{1}{m} \sum_{i=1}^{n} c'_i = Q.$$

- **Output**: m matrices $\mathcal{A}_1, \ldots, \mathcal{A}_m$ and a nonnegative integer k such that:
  - $\forall i, j \in \{1 \ldots m\}$: $\mathcal{A}_i \times \mathbf{1}^n = \mathcal{A}_j \times \mathbf{1}^n$ and $[\mathcal{A}_i] \cap [\mathcal{A}_j] = \emptyset$.
  - $\forall i \in \{1 \ldots m\}$: $(\mathcal{A}_i)^T \times \mathbf{1}^k = (c'_1, c'_2, \ldots, c'_n)^T$.

---

1) If $\forall i : c'_i = 0$ then let $k = 0$, and output m empty matrices $\mathcal{A}_1, \mathcal{A}_2, \ldots, \mathcal{A}_m$, then stop.

2) Otherwise we have $Q = \frac{1}{m} \sum_{i=1}^{n} c'_i > 0$, so compute $(c''_1, c''_2, \ldots, c''_n) = \mathbf{Reduce}(c'_1, c'_2, \ldots, c'_n)$.

3) Let $Q' = \frac{1}{m} \sum_{i=1}^{n} c'_i$ and $\delta = Q - Q'$.

4) Compute $(\mathcal{A}'_1, \mathcal{A}'_2, \ldots, \mathcal{A}'_m, k') = \mathbf{Construct}(c''_1, c''_2, \ldots, c''_n)$.

5) Let $k = k' + m$ and for each $i \in \{1 \ldots m\}$ let $\mathcal{A}_i$ be the result of appending at the bottom to $\mathcal{A}'_i$ m row vectors $\vec{v}_{ij}$ ($1 \leq j \leq m$), where each vector $\vec{v}_{ij}$ is of size $1 \times n$ and is defined by:

$$\vec{v}_{ij} = (0, \ldots, 0, \delta, 0, \ldots, 0),$$

so that δ stands at the $\sigma_{(((i+j) \bmod m)+1)}$ column.

Subroutine Construct.

B. We have $[\mathcal{A}_i] \cap [\mathcal{A}_j] = ([\mathcal{A}'_i] \cap [\mathcal{A}'_j]) \cup (\bigcup_{t=1}^{m} [\vec{v}_{it}] \cap [\vec{v}_{jt}])$. For $i \neq j$ we have $[A_i] \cap [A_j] = \emptyset$ since $[\mathcal{A}'_i] \cap [\mathcal{A}'_j] = \emptyset$ and $[\vec{v}_{it}] \cap [\vec{v}_{jt}] = \emptyset$.

C. We also have: $(\mathcal{A}_i)^T \times \mathbf{1}^k = (\mathcal{A}'_i)^T \times \mathbf{1}^{k'} + \sum_{j=1}^{m} \vec{v}_{ij}^T = (c''_1, c''_2, \ldots, c''_n)^T + (\delta, \delta, \ldots, \delta, 0, 0, \ldots, 0)^T = (c'_1, c'_2, \ldots, c'_n)^T$.

Perfect decryptability follows by Theorem 5.

Perfect Security By Theorem 5, part B, our construction algorithm induces a perfect steganographic scheme with plaintext space size m where $m = \frac{1}{\max(c_i)}$. This plaintext space size is indeed maximum since by Corollary 2, we have $|\mathcal{M}| \leq \frac{1}{\max(c_i)} = m$.

Run time Let l be the maximum bit-length of the numbers c'_i. After each reduction, Q is decreased by $\delta = \min(Q - c'_{\sigma_{m+1}}, c'_{\sigma_m})$. Thus we have two cases:

A. If $Q - c'_{\sigma_{m+1}} \leq c'_{\sigma_m}$, then we have $\delta = Q - c'_{\sigma_{m+1}} \geq Q - \frac{1}{m+1} \sum_{i=1}^{n} c'_i = Q - \frac{mQ}{m+1} = \frac{Q}{m+1}$. Therefore Q' is at most $\frac{m}{m+1}Q$.

B. If $Q - c'_{\sigma_{m+1}} > c'_{\sigma_m}$, then we have $c''_{\sigma_m} = c'_{\sigma_m} - \delta = 0$. Therefore the number of non-zero elements in $(c_1, c_2, \ldots, c_n)$ decreases.

Since there are at most n non-zero elements in $(c_1, c_2, \ldots, c_n)$, after at most $n + t$ steps, we have $Q' \leq \left(\frac{m}{m+1}\right)^t Q$. Besides, for positive integer m we have $\left(1 + \frac{1}{m}\right)^m \geq 2$, therefore after $n + m$ steps, we have $Q' \leq \left(\frac{m}{m+1}\right)^m Q \leq \frac{Q}{2}$. Consequently, after at most $n + mlog(Q)$ steps, we have $0 \leq Q' < 1$, and hence integer Q' as a non-negative integer must be 0. Note that $m \leq n$ and $log(Q) \leq l$, thus the number of reduction steps in the algorithm is at most $O(nl)$. Therefore the running time of the algorithm is at most $O(n^4 l)$.

□

In the next theorem, we also give (polynomial time checkable) necessary and sufficient conditions for the general case of arbitrary m-ary steganographic schemes.

This is important since given a probability distribution of the ciphertexts, we would like to find the maximum possible amount of information that can be sent in a scheme with given ciphertext distribution. When these necessary and sufficient conditions are satisfied, we explicitly construct an optimal scheme. Our construction is also efficient. We first need the following lemma.

Lemma 4 (Real probabilities). *Let m be a positive integer. Let $c = (c_1, c_2, \ldots, c_n)$ where the c_i's are nonnegative real numbers such that:*

$$\sum_{i=1}^{n} c_i = 1 \text{ and } \forall i \in \{1 \ldots n\} : c_i \leq \frac{1}{m}.$$

Then there exists m matrices $\mathcal{A}_1, \mathcal{A}_2, \ldots, \mathcal{A}_m$ of the same size $k \times n$ with nonnegative entries such that:

$$\forall i \in \{1 \ldots m\} : (\mathcal{A}_i)^T \times \mathbf{1}^k = c,$$

$$\forall i, j \in \{1 \ldots m\} : \mathcal{A}_i \times \mathbf{1}^n = \mathcal{A}_j \times \mathbf{1}^n,$$

$$\forall i \neq j \in \{1, \ldots, m\} : [\mathcal{A}_i] \cap [\mathcal{A}_j] = \emptyset.$$

Proof. Let $\mathcal{V}_\mathcal{C}$ be the space of nonnegative vectors $c = (c_1, \ldots, c_n)$ such that there exists m matrices $\mathcal{A}_1, \ldots, \mathcal{A}_m$ satisfying the conclusion of the lemma. We first show that $\mathcal{V}_\mathcal{C}$ is a finite union of n-dimensional polytopes [29].

For each partition I of the set of indices $\{(i, j) \mid 1 \leq i, j \leq m\}$ into m disjoint parts $I_1 = [\mathcal{A}_1], \ldots, I_m = [\mathcal{A}_m]$, the set $\mathcal{V}_\mathcal{C}^\mathcal{I}$ of all nonnegative vectors $c = (c_1, \ldots, c_n)$ such that there exists m matrices $\mathcal{A}_1, \ldots, \mathcal{A}_m$ satisfying the conclusion of the lemma and for which $[\mathcal{A}_i] = I_i$, is a *polyhedron* [29]. In fact, if x_i^{jk} is the (j, k) entry of $\mathcal{A}_i$ then the nonnegative vectors $(c_1, \ldots, c_n, x_1^{11}, \ldots, x_1^{nn}, \ldots, x_m^{11}, \ldots, x_m^{nn})$ have to satisfy the relations $(\mathcal{A}_i)^T \times \mathbf{1}^k = c$ and $\mathcal{A}_i \times \mathbf{1}^n = \mathcal{A}_j \times \mathbf{1}^n$. Each of these relations is a linear relation. Hence the set $\mathcal{V}^I$ of all such nonnegative vectors $(c_1, \ldots, c_n, x_1^{11}, \ldots, x_1^{nn}, \ldots, x_m^{11}, \ldots, x_m^{nn})$ is a polyhedron. Therefore $\mathcal{V}_\mathcal{C}^I$, the projection of polyhedron $\mathcal{V}^I$ onto first n-coordinates, is also a polyhedron. Since each $c_i \in [0, 1]$, $\mathcal{V}_\mathcal{C}^I$ is bounded, hence is a polytope.

Therefore $\mathcal{V}_{\mathcal{C}} = \bigcup_I \mathcal{V}_{\mathcal{C}}^I$ is a finite union of polytopes. This shows that $\mathcal{V}_{\mathcal{C}}$ is compact. Let $\mathcal{V}_{\mathcal{C}}^* = \{(c_1, \ldots, c_n) \in R^n \mid \sum_{i=1}^n c_i = 1 \text{ and } c_i \leq \frac{1}{m}\}$. By Lemma 3 and Corollary 2, we have $\mathcal{V}_{\mathcal{C}} \cap Q^n = \mathcal{V}_{\mathcal{C}}^* \cap Q^n$, where Q^n is the set of all n-tuples $(x_1, \ldots, x_n)$ of rational entries. Since $\mathcal{V}_{\mathcal{C}}$ and $\mathcal{V}_{\mathcal{C}}^*$ are both compact, taking the compactification of both sides of this equality, we get $\mathcal{V}_{\mathcal{C}} = \mathcal{V}_{\mathcal{C}}^*$, which completes our proof. □

We now state and prove our Theorem for the real probability case.

Theorem 9 (Perfect steganographic scheme). *Let m be a positive integer and let P_C be a probability distribution. The necessary and sufficient condition for the existence of a perfect steganographic scheme, whose ciphertext distribution is $P_{\mathcal{C}}$, and whose message space size is m, is that:*

$$H_{min}(P_{\mathcal{C}}) \geq \log m.$$

Proof. $\{\Rightarrow\}$ This is the consequence of Corollary 2.

$\{\Leftarrow\}$ This is the conclusion of Lemma 3 and Lemma 4.

□

Combining Corollary 2 and Theorem 9, we immediately have the following:

Corollary 3. *The maximum achievable information rate of a perfect steganographic scheme with covertext distribution $P_{\mathcal{C}}$ is $H_{min}(P_{\mathcal{C}})$.*

CHAPTER 3

INVISIBLE STEGANOGRAPHIC SOLUTIONS

In this chapter we study invisible steganographic schemes, which are extensions of steganographic schemes where the keys are also hidden. These schemes are used when the key and the ciphertext are stored on the same type of media, e.g. a floppy or hard disk [3]. Hence both the key and the ciphertext distributions are the same, i.e. $P_{\mathcal{K}} = P_{\mathcal{C}}$. We give necessary and sufficient conditions for perfect secrecy and perfect hiding. We also give an efficient construction of a perfect invisible steganographic scheme for a general distribution when the conditions are satisfied.

Definition 9 (Steganographic scheme). *An invisible steganographic scheme is an information hiding scheme* $\mathcal{A} = (\mathcal{K}, \mathcal{C}, \mathcal{M}, P_{\mathcal{K}}, P_{\mathcal{C}}, E, D)$ *with* $\mathcal{K} \equiv \mathcal{C}$ *and* $P_{\mathcal{K}} \equiv P_{\mathcal{C}}$.

Binary Invisible Steganographic Schemes

A *perfect invisible steganographic scheme* is a scheme that achieves both perfect hiding and perfect secrecy. Now we state and prove our main result of this section. The result also yields an efficient construction of a perfect information hiding scheme with binary plaintexts.

Theorem 10. *Algorithm 2 described below will produce a perfect invisible steganographic scheme on input of* n *non-negative rational numbers* $(c_1, c_2, \ldots, c_n)$ *such that* $c_i \leq \frac{1}{2}$ *for* $i \in \{1, \ldots, n\}$*,*

ALGORITHM 2 A general invisible steganographic scheme that is perfect

Require: input n rational numbers $c_1, c_2, \ldots, c_n$

Ensure: output two matrices $\mathcal{A}_1, \mathcal{A}_2$ of size $n \times n$

$h \Leftarrow \min\{i \mid c_1 + c_2 + \cdots + c_i \geq \frac{1}{2}\}$

$s_1 \Leftarrow c_1 + c_2 + \cdots + c_{h-1}$

$s_2 \Leftarrow c_h$

$s_3 \Leftarrow c_{h+1} + c_{h+2} + \cdots + c_n$

$u_i \Leftarrow 1$ for $i \in \{1, 2, \ldots, h-1\}$

$u_i \Leftarrow 2$ for $i \in \{h\}$

$u_i \Leftarrow 3$ for $i \in \{h+1, h+2, \ldots, n\}$

$a \Leftarrow \min(s_1, s_2, s_1 + s_2 - s_3)$

$$\mathcal{B}_0 \Leftarrow \begin{pmatrix} s_1 & 0 & 0 \\ 0 & s_2 & 0 \\ 0 & 0 & s_3 \end{pmatrix},\ \mathcal{B}_1 \Leftarrow \begin{pmatrix} 0 & a & s_1 - a \\ s_1 + s_2 - s_3 - a & 0 & s_3 - s_1 + a \\ s_3 - s_2 + a & s_2 - a & 0 \end{pmatrix}$$

for all $1 \leq i, j \leq n$ **do**

$\mathcal{A}_0(i,j) \Leftarrow c_i c_j \mathcal{B}_0(u_i, u_j) s_{u_i}^{-1} s_{u_j}^{-1}$

$\mathcal{A}_1(i,j) \Leftarrow c_i c_j \mathcal{B}_1(u_i, u_j) s_{u_i}^{-1} s_{u_j}^{-1}$

end for

Proof. Let $P_{\mathcal{K}} = (p_1, p_2, \ldots, p_n)$ satisfy the condition of the theorem. If $n = 3$ then by Lemma 6 there is nothing to show. So let us assume that $n > 3$. By Lemma 5, there is a disjoint 3-partition of $\{1, 2, \ldots, n\} = \{S_1, S_2, S_3\}$ such that $s_t = \sum_{i \in S_t} p_i \leq 1/2$ for $t = 1, 2, 3$. Since $s = (s_1, s_2, s_3)$ is also a probability distribution satisfying the condition of Lemma 6, we can construct two matrices $\mathcal{B}_0, \mathcal{B}_1$ such that the conditions (2.4,2.5,2.10) are satisfied on the probability distribution s, as explained in the proof of Lemma 6. We now consider two matrices $\{\mathcal{A}_0, \mathcal{A}_1\}$, as constructed in Algorithm 2:

$$\mathcal{A}_m(i,j) = p_i p_j \mathcal{B}_m(u_i, u_j) (\sum_{v \in S_{u_i}} p_v)^{-1} (\sum_{v \in S_{u_j}} p_v)^{-1},$$

where $m \in \{0, 1\}$, and $(u_i, u_j) \in \{1, 2, 3\} \times \{1, 2, 3\}$ is the unique pair such that $(i, j) \in S_{u_i} \times S_{u_j}$. We shall show that $\{\mathcal{A}_0, \mathcal{A}_1\}$ satisfies the conditions (2.4), (2.5), (2.10). Indeed:

A. If $\mathcal{A}_m(i,j) \neq 0$ then $\mathcal{B}_m(u_i, u_j) \neq 0$, and since the matrices $\{\mathcal{B}_0, \mathcal{B}_1\}$ satisfy condition (2.4) (i.e. $[\mathcal{B}_0] \cap [\mathcal{B}_1] = \emptyset$) so does $\{\mathcal{A}_0, \mathcal{A}_1\}$, i.e. $[\mathcal{A}_0] \cap [\mathcal{A}_1] = \emptyset$.

B. We now verify condition (2.5):

$$\begin{aligned}
\left(\mathcal{A}_m \times \mathbf{1}^{|\mathcal{C}|}\right)|_i &= \sum_{j=1}^{n} \mathcal{A}_m(i,j) = \sum_{j=1}^{n} p_i p_j \mathcal{B}_m(u_i,u_j)(\sum_{v\in S_{u_i}} p_v)^{-1}(\sum_{v\in S_{u_j}} p_v)^{-1} \\
&= \sum_{u=1}^{3}\sum_{j\in S_u} p_i p_j \mathcal{B}_m(u_i,u)(\sum_{v\in S_{u_i}} p_v)^{-1}(\sum_{v\in S_u} p_v)^{-1} \\
&= \sum_{u=1}^{3} p_i \mathcal{B}_m(u_i,u)(\sum_{v\in S_{u_i}} p_v)^{-1}(\sum_{j\in S_u} p_j)(\sum_{v\in S_u} p_v)^{-1} \\
&= p_i(\sum_{v\in S_{u_i}} p_v)^{-1}\sum_{u=1}^{3}\mathcal{B}_m(u_i,u). \qquad (3.1)
\end{aligned}$$

Since $\mathcal{B}_m$ satisfies (2.5), this means that $\mathcal{B}_m \times \mathbf{1}^3 = (s_1,s_2,s_3)^T$. So we obtain: $\sum_{u=1}^{3}\mathcal{B}_m(u_i,u) = s_{u_i}$. By substituting this into the right hand side of equation (3.1) and using the definition of s_{u_i} we have:

$$\left(\mathcal{A}_m \times \mathbf{1}^{|\mathcal{C}|}\right)|_i = p_i(\sum_{v\in S_{u_i}} p_v)^{-1}s_{u_i} = p_i(\sum_{v\in S_{u_i}} p_v)^{-1}(\sum_{v\in S_{u_i}} p_v) = p_i = P_{\mathcal{K}}(i).$$

Therefore (2.5) is true.

C. We verify condition (2.10):

$$\begin{aligned}
\left(\mathcal{A}_m^T \times \mathbf{1}^{|\mathcal{K}|}\right)|_j &= \sum_{i=1}^{n} \mathcal{A}_m(i,j) = \sum_{i=1}^{n} p_i p_j \mathcal{B}_m(u_i,u_j)(\sum_{v\in S_{u_i}} p_v)^{-1}(\sum_{v\in S_{u_j}} p_v)^{-1} \\
&= \sum_{u=1}^{3}\sum_{i\in S_u} p_i p_j \mathcal{B}_m(u,u_j)(\sum_{v\in S_u} p_v)^{-1}(\sum_{v\in S_{u_j}} p_v)^{-1} \\
&= \sum_{u=1}^{3} p_j \mathcal{B}_m(u,u_j)(\sum_{v\in S_{u_j}} p_v)^{-1}(\sum_{i\in S_u} p_i)(\sum_{v\in S_u} p_v)^{-1} \\
&= p_j(\sum_{v\in S_{u_j}} p_v)^{-1}\sum_{u=1}^{3}\mathcal{B}_m(u,u_j). \qquad (3.2)
\end{aligned}$$

Since $\mathcal{B}_m$ satisfies (2.10), this means that $(\mathcal{B}_m)^T \times \mathbf{1}^3 = (s_1,s_2,s_3)^T$. So we obtain: $\sum_{u=1}^{3}\mathcal{B}_m(u,u_j) = s_{u_j}$. By substituting this into the right hand side of

equation (3.2) and using the definition of s_{u_j} we have:

$$\left(\mathcal{A}_m^T \times \mathbf{1}^{|\mathcal{K}|}\right)|_j = p_j\left(\sum_{v \in S_{u_j}} p_v\right)^{-1} s_{u_j} = p_j\left(\sum_{v \in S_{u_j}} p_v\right)^{-1}\left(\sum_{v \in S_{u_j}} p_v\right) = p_j = P_{\mathcal{K}}(j).$$

Therefore (2.10) is true.

□

We state and prove the following two lemmas.

Lemma 5 (Reduction). *If $S = \{s_1, s_2, \ldots, s_n\}$, $n \geq 3$, is a set of positive real numbers such that $\max_i(s_i) \leq \frac{1}{2}$ and $\sum_{i=1}^n s_i = 1$, then there exists a disjoint partition S_1, S_2, S_3 of $\{1, 2, \ldots, n\}$ such that $\sum_{i \in S_t} s_i \leq \frac{1}{2}$ for $t = 1, 2, 3$.*

Proof. Consider the set $\{t \mid \sum_{i=1}^t s_i \geq 1/2\}$, and let

$$h = \min\{t \mid \sum_{i=1}^{t} s_i \geq 1/2\}. \tag{3.3}$$

Since all $s_i \leq 1/2$, we have $1 < h < n$. Define $S_1 = \{1, \ldots, h-1\}$, $S_2 = \{h\}$, and $S_3 = \{h+1, \ldots, n\}$. We verify that $\sum_{i \in S_t} s_i \leq 1/2$ for $t = 1, 2, 3$ as follows:

A. $\sum_{i \in S_1} s_i \leq 1/2$, otherwise h would not be the minimum t in Equation 3.3.

B. $\sum_{i \in S_2} s_i \leq 1/2$, because from our assumption that $s_h \leq 1/2$.

C. $\sum_{i \in S_3} s_i \leq 1/2$, because $\sum_{i \in S_3} s_i = 1 - \sum_1^h s_i \leq 1 - 1/2 = 1/2$.

This proves our lemma. □

Lemma 6 (Base). *If $|\mathcal{K}| = |\mathcal{C}| = 3$ then the necessary and sufficient condition for the existence of a perfect steganographic scheme is that:*

$$\max_{\substack{k \in \mathcal{K} \\ c \in \mathcal{C}}}(P_{\mathcal{K}}(k), P_{\mathcal{C}}(c)) \leq \frac{1}{2}.$$

Proof.

$\{\Rightarrow\}$ This is the consequence of Corollary 2 for the case $|\mathcal{M}| = 2$.

$\{\Leftarrow\}$ Let $\vec{P}_{\mathcal{K}} = \vec{P}_{\mathcal{C}} = (s_1, s_2, s_3)^T$ satisfy the condition $0 < s_1, s_2, s_3 \leq 1/2$. After considering all possible 2-partitions of 9 index-pairs from the set $\{1, 2, 3\}$ and solving the corresponding linear inequalities, we obtained the following two characteristic matrices $\mathcal{A}_0(k, c)$ and $\mathcal{A}_1(k, c)$:

$$\mathcal{A}_0 = \begin{pmatrix} s_1 & 0 & 0 \\ 0 & s_2 & 0 \\ 0 & 0 & s_3 \end{pmatrix}, \ \mathcal{A}_1 = \begin{pmatrix} 0 & a & s_1 - a \\ s_1 + s_2 - s_3 - a & 0 & s_3 - s_1 + a \\ s_3 - s_2 + a & s_2 - a & 0 \end{pmatrix} \quad (3.4)$$

where $a = \min(s_1, s_2, s_1 + s_2 - s_3)$. Note that $0 < s_1, s_2, s_3 \leq 1/2$, and $s_1 + s_2 + s_3 = 1$ so it is easy to verify that $a \geq \max(0, s_1 - s_3, s_2 - s_3)$. Then it is straightforward to verify that $\{\mathcal{A}_0, \mathcal{A}_1\}$ satisfies conditions (2.4,2.5,2.10) and that the entries are greater than or equal to zero. Hence by Theorem 5, $\{\mathcal{A}_0, \mathcal{A}_1\}$ with $(\mathcal{K}, \mathcal{C}, \mathcal{M}, P_{\mathcal{K}})$ induces a perfect steganographic scheme. The construction of this scheme based on its characteristic matrices was given in page 24.

□

Theorem 11 (Necessary and sufficient conditions). *The necessary and sufficient condition for the existence of a perfect steganographic scheme is:*

$$H_{min}(P_{\mathcal{C}}) \geq 1. \quad (3.5)$$

Proof. $\{\Rightarrow\}$ is from Corollary 2. $\{\Leftarrow\}$ is implied by Theorem 10. □

Obtaining Maximum Bit Rate For a given distribution $P_{\mathcal{C}}$, we are now interested in sending information at the maximum bit rate rather than the sub-optimal one. Unfortunately this problem seems to be hard, as we now explain.

Theorem 12 (Maximum Bit Rate). *Let $P_{\mathcal{K}} = P_{\mathcal{C}}$ be a given probability distribution whose probabilities are rational numbers. Let $n \geq 3$ be a fixed integer. Deciding if there exist a perfect information hiding scheme $\mathcal{A}$ with key distribution $P_{\mathcal{K}}$, ciphertext distribution $P_{\mathcal{C}}$, and whose message space $\mathcal{M}$ contains at least n different messages is an NP-complete problem.*

Proof. We reduce the Integer Partitioning problem [18] to this problem. Note that the symbol n in this proof has been redefined (it has *different meaning* elsewhere). We first recall the Integer Partitioning problem:

- **Instance:** a set of positive integer numbers $\{x_1, \ldots, x_l\}$.
- **Question:** Is there a partition of $\{1, \ldots, l\}$ into disjoint S_0, S_1 such that: $\sum_{i \in S_0} x_i = \sum_{j \in S_1} x_j$.

Given an instance $\{x_1, \ldots, x_l\}$ of the partition problem, we consider the following distributions:

$$P_{\mathcal{K}} = P_{\mathcal{C}} = (2x_1/nS, 2x_2/nS, \ldots, 2x_l/nS, 1/n, 1/n, \ldots, 1/n), \tag{3.6}$$

where $S = \sum_{i=1}^{l} x_i$, there are $n-2$ fractions $1/n$ at the end, and the key and the ciphertext space is $\{1, 2, \ldots, l+n-2\}$. We next show that $\{x_1, x_2, \ldots, x_l\}$ is a **yes** instance of the Integer Partitioning problem if and only if there exists a perfect information hiding scheme with $|\mathcal{M}| = n$, whose key and ciphertext distribution is $P_{\mathcal{K}}$.

$\{\Rightarrow\}$ Assume that $\{x_1, x_2, \ldots, x_l\}$ is a **yes** instance of the Integer Partitioning problem. Then by definition, there exists two disjoint subsets S_0, S_1 of $\{x_1, x_2, \ldots, x_l\}$ such that $\sum_{x_i \in S_0} x_i = \sum_{x_i \in S_1} x_i = S/2$. We define n matrices $\{\mathcal{A}_t\}$, each of

size $(l+n-2)\times(l+n-2)$, for $t=1,2,\ldots,n$ as follows.

$\mathcal{A}_t(i,j)$	$j\in S_0$	$j\in S_1$	$j>l$
$i\in S_0$	$\frac{4x_ix_j\delta^t_{11}}{nS^2}$	$\frac{4x_ix_j\delta^t_{12}}{nS^2}$	$\frac{2x_i\delta^t_{1(j-l+2)}}{nS}$
$i\in S_1$	$\frac{4x_ix_j\delta^t_{21}}{nS^2}$	$\frac{4x_ix_j\delta^t_{22}}{nS^2}$	$\frac{2x_i\delta^t_{2(j-l+2)}}{nS}$
$i>l$	$\frac{2x_j\delta^t_{(i-l+2)1}}{nS}$	$\frac{2x_j\delta^t_{(i-l+2)2}}{nS}$	$\frac{\delta^t_{(i-l+2)(j-l+2)}}{n}$

where $\delta^t_{uv}=1$ if $u\equiv v+t \pmod n$, and $\delta^t_{uv}=0$ otherwise. It is not difficult to verify that the matrices $\mathcal{A}_t$ defined above satisfy conditions (2.4), (2.5), (2.10) of Theorem 5. Hence $\{\mathcal{A}_t\}_{t=1}^n$ together with $(\mathcal{K},\mathcal{C},\mathcal{M},P_{\mathcal{K}})$ induce a perfect information hiding scheme.

$\{\Leftarrow\}$ Assume that there exists a perfect n-ary information hiding scheme $\mathcal{A}$ whose key distribution and ciphertext distribution is $P_{\mathcal{K}}$ as defined in (3.6). Let $\{\mathcal{A}_t \mid t=1,2,\ldots,n\}$ be the set of n characteristic matrices of $\mathcal{A}$. For $t=1,2,\ldots,n$, let $V_t=\{c \mid \mathcal{A}_t(l+n-2,c)\neq 0\}$. Since the matrices $\mathcal{A}_t$ satisfy condition (2.4) of Theorem 5 we conclude that the sets V_t $(t=1,2,\ldots,n)$ are mutually disjoint. We extend some V_t to include the set $\{c \mid \forall t:\mathcal{A}_t(l+n-2,c)=0\}$ so that $\{V_1,V_2,\ldots,V_n\}$ is indeed a disjoint partition of $\{1,2,\ldots,l+n-2\}$. Let $s_t=\sum_{c\in V_t}\mathcal{A}_t(l+n-2,c)$. We have:

$$\begin{aligned}\sum_{t=1}^{n} s_t &= \sum_{t=1}^{n}\sum_{c\in V_t}\mathcal{A}_t(l+n-2,c)=\sum_{t=1}^{n}\sum_{c=1}^{l+n-2}\mathcal{A}_t(l+n-2,c)\\ &= \sum_{t=1}^{n} P_{\mathcal{K}}(l+n-2)=\sum_{t=1}^{n}1/n=1. \qquad (3.7)\end{aligned}$$

On the other hand:

$$\begin{aligned}\sum_{t=1}^{n} s_t &= \sum_{t=1}^{n}\sum_{c\in V_t}\mathcal{A}_t(l+n-2,c) = \sum_{t=1}^{n}\sum_{c\in V_t}\left(\sum_{k=1}^{l+n-2}\mathcal{A}_t(k,c) - \sum_{k=1}^{l+n-3}\mathcal{A}_t(k,c)\right)\\ &= \sum_{t=1}^{n}\sum_{c\in V_t}P_{\mathcal{K}}(c) - \sum_{t=1}^{n}\sum_{c\in V_t}\sum_{k=1}^{l+n-3}\mathcal{A}_t(k,c)\\ &= 1 - \sum_{t=1}^{n}\sum_{c\in V_t}\sum_{k=1}^{l+n-3}\mathcal{A}_t(k,c). \qquad (3.8)\end{aligned}$$

Combine (3.7) and (3.8) to get: $\sum_{t=1}^{n}\sum_{c\in V_t}\sum_{k=1}^{l+n-3}\mathcal{A}_t(k,c) = 0$. In other words, $\forall k \le l+n-3$, $\forall c \in V_t$: $\mathcal{A}_t(k,c) = 0$. This implies that $\forall c \in V_t$:

$$A_t(n+l-2,c) = \sum_{k=1}^{l+n-2}\mathcal{A}_t(k,c) - \sum_{k=1}^{l+n-3}\mathcal{A}_t(k,c) = P_{\mathcal{K}}(c) - \sum_{k=1}^{l+n-3}\mathcal{A}_t(k,c) = P_{\mathcal{K}}(c).$$

Therefore we have $s_t = \sum_{c\in V_t}\mathcal{A}_t(l+n-2,c) = \sum_{c\in V_t}P_{\mathcal{K}}(c)$. This means that $\{s_1, s_2, \ldots, s_n\}$ is an n-partition of $\{P_{\mathcal{K}}(1), P_{\mathcal{K}}(2), \ldots, P_{\mathcal{K}}(l+n-2)\}$ into n disjoint subsets. Furthermore we have for each t: $s_t = \sum_{c\in V_t}A(l+n-2,c) = \sum_{c=1}^{l+n-2}A(l+n-2,c) = P_{\mathcal{K}}(l+n-2) = 1/n$. Since the last $n-2$ values in (3.6) of $P_{\mathcal{K}}$ are $1/n$, we have a partition of $\{2x_1/nS, \ldots, 2x_l/nS\}$ into two disjoint subsets such that the sum of elements in each subset is $1/n$. Equivalently, $\{x_1, \ldots, x_l\}$ can be divided into two disjoint subsets such that the sum of elements in each subset is $S/2$, i.e. $\{x_1, \ldots, x_l\}$ is a **yes** instance of the Integer Partitioning problem.

□

Efficient Invisible Steganographic Scheme

While one can always divide a long message into bits and send each bit separately without affecting its perfect security, however such approach has low information rate. In this section, we present a perfect invisible steganographic scheme with

multi-bit plaintexts. Our construction is recursive. In simulations, the information bit rate is at least 75% of the upper bound implied by Corollary 2. Thus the upper bound and the constructed scheme are very tight.

- **Setup** Let $P_{\mathcal{K}} = P_{\mathcal{C}} = (p_1, p_2, \ldots, p_n)$ be the probability distribution of cover-texts. Since $P_{\mathcal{K}}$ and $P_{\mathcal{C}}$ satisfy $p_i \leq \frac{1}{2}$ for all i, by Lemma 5 we have a disjoint partition S_1, S_2, S_3 of $\{1, 2, \ldots, n\}$ such that $s_t = (\sum_{i \in S_t} p_i) \leq \frac{1}{2}$ for $1 \leq t \leq 3$. By Theorem 11, let $\mathcal{A}^{[0]}$ be the binary invisible steganographic scheme with the ciphertext and key distributions be (s_1, s_2, s_3), and the ciphertext space be $\{c'_1, c'_2, c'_3\}$.

Case A. Suppose that the induced probability distribution $P^t_{\mathcal{K}} = (p_{1t}, \ldots, p_{nt})$, where $p_{it} = p_i s_t^{-1}$ for $i \in S_t$ and $p_{it} = 0$ for all $t \in \{1, 2, 3\}, i \notin S_t$, satisfies the conditions of Theorem 11, and that $\mathcal{A}^{[t]}$ is the perfect steganographic scheme produced by Theorem 11 with ciphertext space $\mathcal{C}$ and probability distribution $P^t_{\mathcal{K}}$. The secret key of our scheme is (k_0, k_1, k_2, k_3), where k_0 is the secret key of $\mathcal{A}^{[0]}$, and k_t is the secret key of $\mathcal{A}^{[t]}$.

Case B. Otherwise, the secret key of our scheme is the same as that of $\mathcal{A}^{[0]}$.

- **Encryption**

Case A. The secret key is (k_0, k_1, k_2, k_3). Let the plaintext $m = (m_1, m_2, \ldots, m_l)$ be a string of bits. Let c'_t $(1 \leq t \leq 3)$ be the encryption of plaintext m_1 with secret key k_0 using $\mathcal{A}^{[0]}$, and c_i be the encryption of plaintext $m' = (m_2, \ldots, m_l)$ with secret key k_t using $\mathcal{A}^{[t]}$. The final ciphertext is $c = c_i$.

Case B. The secret key is k_0. Then the message is m_1. The ciphertext is the encryption of m_1 with secret key k_0 using $\mathcal{A}^{[0]}$.

- **Decryption**

Case A. The secret key is (k_0, k_1, k_2, k_3). Let $1 \leq t \leq 3$ be the unique index such that ciphertext $c \in S_t$. Let m_1 be the decryption of ciphertext c'_t

with secret key k_0 using $\mathcal{A}^{[0]}$, and let $m' = (m_2, m_3, \ldots, m_l)$ be the decryption of ciphertext c with secret key k_t using $\mathcal{A}^{[t]}$. The plaintext is $m = (m_1, m_2, \ldots, m_l)$.

Case B. The secret key is k_0. The plaintext is the decryption of c with secret key k_0 using $\mathcal{A}^{[0]}$.

Since $\mathcal{A}^{[0]}$ and $\mathcal{A}^{[t]}$ $(1 \leq t \leq 3)$ are perfect invisible steganographic schemes, it is straightforward to see that our scheme is a perfect invisible steganographic scheme.

We have simulated our scheme for $100 \leq n \leq 1000$ with distribution $P_{\mathcal{K}}$ chosen at random. On average, the obtained bandwidth is very high, often in the range of $80\% - 90\%$ of the upper bound imposed by Corollary 2. This shows that our scheme is quite efficient.

Generalized Invisible Steganographic Schemes

In this section, we extend the invisible steganographic scheme defined in the previous section to include those cases when the key and the ciphertexts are stored in, or sent through different media types, that are insecure. In such cases, both the ciphertexts and the keys need to be protected, and have different distributions. However, as we will now show, this problem is indeed very hard and it is open to further research.

Theorem 13 (General Invisible Steganographic Scheme). *Suppose that the probability distributions $P_{\mathcal{K}}$ and $P_{\mathcal{C}}$ are given by vectors of rational numbers. Deciding if there exists a perfect binary information hiding scheme whose key distribution is $P_{\mathcal{K}}$ and whose ciphertext distribution is $P_{\mathcal{C}}$ is an NP-complete problem.*

Proof. We prove this theorem by reducing the NP-complete Integer Partitioning problem [18] to the problem of deciding whether a generalized perfect invisible

steganographic scheme exists (see the proof of Theorem 12 for a discussion of the Integer Partitioning problem). Given an instance of the Integer Partitioning problem, we consider the following probability distributions:

$$\begin{aligned} P_{\mathcal{K}} &= (1/2, 1/2) \\ P_{\mathcal{C}} &= (x_1 S^{-1}, x_2 S^{-1}, \ldots, x_n S^{-1}), \end{aligned} \tag{3.9}$$

where $S = \sum_{i=1}^{n} x_i$. We show that $\{x_1, x_2, \ldots, x_n\}$ is a **yes** instance of the Integer Partitioning problem if and only if there exist a perfect binary information hiding scheme whose key distribution is $P_{\mathcal{K}}$ and whose ciphertext distribution is $P_{\mathcal{C}}$. Note that if a perfect information hiding scheme exists, then a perfect binary information scheme exists.

$\{\Rightarrow\}$ Assume that $\{x_1, x_2, \ldots, x_n\}$ is a **yes** instance of Integer Partitioning problem. Let S_0, S_1 be the corresponding partition of $(1, 2, \ldots, n)$. We define the following two matrices:

$$\mathcal{A}_m(k, c) = x_c * (k \oplus S_m(c)) * S^{-1}, \qquad m = 0, 1 \tag{3.10}$$

where $k \in \{0, 1\}$, $c \in \{1, 2, \ldots, n\}$, $S_t(c) = 1$ if $c \in S_t$ and $S_t(c) = 0$ if $c \notin S_t$, and $\oplus$ is the addition mod 2. It is easy to verify that $[\mathcal{A}_0] \cap [\mathcal{A}_1] = \emptyset$, $\mathcal{A}_t \times \mathbf{1}^n = (1/2, 1/2)^T$, and that $\mathcal{A}_t^T \times \mathbf{1}^2 = (x_1 S^{-1}, x_2 S^{-1}, \ldots, x_n S^{-1})^T$. Hence $\{\mathcal{A}_0, \mathcal{A}_1\}$ forms a perfect binary information hiding scheme with key distribution $P_{\mathcal{K}}$ and ciphertext distribution $P_{\mathcal{C}}$.

$\{\Leftarrow\}$ Let $\mathcal{A}$ be a perfect binary information hiding scheme, with key distribution is $P_{\mathcal{K}}$, and ciphertext distribution $P_{\mathcal{C}}$. Let $\{\mathcal{A}_0, \mathcal{A}_1\}$ be the set of characteristic matrices of $\mathcal{A}$. We will show that the Integer Partitioning problem instance $\{x_1, \ldots, x_n\}$ is a **yes** instance. Indeed, let $P_0 = \{i \mid \mathcal{A}_0(0, i) \neq 0\}$, and $P_1 = \{1, 2, \ldots, n\} - P_0$. Note that for each $i \in P_0$, $\mathcal{A}_0(1, i) = 0$, because if there is some $i \in P_0$ such that $\mathcal{A}_0(1, i) \neq 0$, then from (2.4) we have $\mathcal{A}_1(0, i) =$

$\mathcal{A}_1(1,i) = 0$. Consequently, $\mathcal{A}_1^T \times \mathbf{1}^2$ is a column vector whose $i-th$ coordinate is 0, i.e. $\mathcal{A}_1^T \times \mathbf{1}^2 \neq P_{\mathcal{C}}$. This contradicts (2.10). So we have $\mathcal{A}_0(1,i) = 0$ for $i \in P_0$. Similarly we have $\mathcal{A}_1(0,i) = 0$ for $i \notin P_1$. Combine these with (2.10), (2.5) to get $\mathcal{A}_0(0,i) = x_i S^{-1}$ for $i \in P_0$, and

$$\begin{aligned}\sum_{i\in P_0} x_i S^{-1} &= \sum_{i\in P_0}(\mathcal{A}_0(0,i) + \mathcal{A}_0(1,i)) = \sum_{i\in P_0}\mathcal{A}_0(0,i) \\ &= \sum_{i\in P_0}\mathcal{A}_0(0,i) + \sum_{i\notin P_0}\mathcal{A}_0(0,i) = \sum_{i=1}^{n}\mathcal{A}_0(0,i) = 1/2.\end{aligned}$$

Therefore $\sum_{i\in P_0} x_i = \sum_{i\notin P_0} x_i = S/2$, i.e. $\{x_1, \ldots, x_n\}$ is a **yes** instance.

□

CHAPTER 4

STEGANOGRAPHIC CODING SOLUTIONS

In the previous chapter we have considered perfect solutions to the steganographic problem. In this chapter, we consider non-perfect solutions, where the security is statistical or computational and the number of stegotexts required to encode a hiddentext is variable.

Steganographic Codes

A steganographic code is an encoding scheme that encodes uniform probability distribution into a given marginal probability distribution P.

Definition 10 (Steganographic Code). *A steganographic code is an encoding scheme Γ, whose source alphabet is M and destination alphabet is C, together with a marginal probability distribution P over C^* such that the probability distribution of $\Gamma_{Encode}(m)$ is statistically close to P when m is taken uniformly at random from M^*. This means:*

$$\epsilon_\Gamma(n) = \sum_{s \in \Gamma_{Encode}(M^n)} \left| \Pr\left[\Gamma_{Encode}(m) = s \mid m \leftarrow \mathcal{U}_{M^n}\right] - P(s) \right|$$

is a negligible function in n.

It is obvious that the maximum rate for any such steganographic code is $H(P)$. In the following, we construct steganographic codes that approach this limit.

Optimal Steganographic Codes

We present a construction that applies to covertext sequences that may be dependent on each other, while the compression scheme described in [7] must assume that the covertext are independent of each other.

Let $C = \{v_1, v_2, \dots\}$ be finite alphabets and let P be a marginal probability distribution of random process $X = \{X_1, X_2, \dots\}$. In this section, we will construct optimal steganographic codes over any finite source alphabet $M = \{m_1, m_2, \dots\}$.

For each $x = m_{i_1} m_{i_2} \dots m_{i_n} \in M^*$, let $\overline{x} = \sum_{j=1}^{n} (i_j - 1)|M|^{j-1}$ be the integer whose M-ary representation is x. For $P(h) \neq 0$ and $1 \leq t \leq |C|$, define:

$$F_h(v_t) = P(h)^{-1} \sum_{i=1}^{t-1} P(h\|v_i).$$

We formally set $F_h(v_{(|C|+1)}) = 1$. Clearly F_h is the cumulative probability distribution function of the marginal probability distribution P_h defined by:

$$P_h(v) = P(h\|v)P(h)^{-1}.$$

ALGORITHM 3 A steganographic encoding algorithm

Input: $x = (x_1, \dots, x_n) \in M^n$.
Output: $c = (c_1, \dots, c_l) \in C^*$.

---

1. **let** $z \leftarrow \mathcal{U}_{M^n}$, $r = \overline{x\|z}$.
2. **let** $a = 0, b = |M|^{2n}, h = \epsilon$.
3. **while** $\lceil a/|M|^n \rceil < \lfloor b/|M|^n \rfloor$ **do**
   (a) **let** $1 \leq j \leq |C|$ be the unique integer such that:
   $$F_h(v_j) \leq (r - a)/(b - a) < F_h(v_{j+1}).$$
   (b) **let** $(a, b) = (a, a) + (b - a)(F_h(v_j), F_h(v_{j+1}))$.
   (c) **let** $h = h|v_j$.
4. Output $c = h$.

We denote by $\Gamma_{\text{Encode}}(x)$, $x \in M^*$, the output of the encode Algorithm 3. Let $\underline{x} \in M^*$ be the M-ary representation of $x \in \mathbb{Z}^{\geq 0}$. We denote by $\Gamma_{\text{Decode}}(c)$, $c \in C^*$, the

ALGORITHM 4 A steganographic decoding algorithm

Input: $c = (v_{j_1}, \ldots, c_{j_l}) \in C^*$.
Output: $x = (x_1, \ldots, x_n) \in M^n$.

1. **let** $a = 0, b = |M|^{2n}, h = \epsilon$.
2. **for** i **from** 1 **to** l **do**
   (a) **let** $(a, b) = (a, a) + (b - a)(F_h(v_{j_i}), F_h(v_{(j_i+1)}))$.
   (b) **let** $h = h|v_{j_i}$.
3. Let $r = \lceil a|M|^{-n} \rceil$.
4. Output $x = \underline{r}$.

output of the decode Algorithm 4. Observe that the encoding rule above resembles to the arithmetic decoding [11] of number $\overline{x}/|M|^n$ in the following sense: each time the encoder outputs a covertext v_j, v_j contains some information about r. Therefore the range $[a, b]$ which contains r is scaled by a factor of $F_h(v_j)$. The encoder stops when the decoder can completely determine the value x from r, i.e. when the range $[a, b]$ is less than $|M|^n$.

Theorem 14. *The code Γ presented above is a steganographic code.*

Proof. Observe that, by induction, the values of a, b, h, j, a', b' in the encoding are the same as in the decoding. Due to our choice of j, we have $r \in [a, b)$ both before and after each iteration. Therefore at the end of the encoding, we obtain $\lceil a|M|^{-n} \rceil = \lfloor b|M|^{-n} \rfloor = \overline{x}$. Because the values of a, b in encoding are the same as in the decoding, Γ is uniquely decodable. Next, we will prove that Γ is also steganographic code.

For the sake of argument, let us assume that a, b, r are real numbers. By simple induction we can see that after each iteration $1 \leq i \leq l$, the conditional probability

distribution of $\overline{x}$ given the history $h = c_1 \| \dots \| c_i$, is uniform random over integers in the range $[a|M|^{-n}, b|M|^{-n})$.

Consequently, at the beginning of each iteration i, conditioned on the previous history $h = c_0 \| \dots \| c_{i-1}$, $u = \lfloor (r-a)/(b-a) \rfloor$ is a uniform random variable with range $[0, 1]$. Thus v_j chosen by the encoder, such that $F_h(v_j) \leq u < F_h(v_{j+1})$, is indeed distributed accordingly to probability distribution $F_h(v)$.

However a, b, r are not real numbers, but rather approximations by fractions with denominator $|M|^n$, i.e. with negligible error of at most $O(|M|^{-n})$. We conclude that $\overline{x}$ distribute statistically close to uniform on range $[a|M|^{-n}, b|M|^{-n})$. Therefore, v_j distributes statistically close to $F_h(v)$. This means Γ is a steganographic code. □

Theorem 15. *The code Γ described above is asymptotically optimal.*

Proof. Observe that each iteration in the encoding, the range $[a, b]$ containing r is scaled by a factor of $F_h(v_j)$. Therefore we have for all $t \geq 1$:

$$(b_t - a_t)|M|^{-2n} = \prod_{i=1}^{t} F_{v_{j_1} \dots v_{j_{i-1}}}(v_{j_i}) = P(v_{j_1} \dots v_{j_t}),$$

where (a_t, b_t) is the value of a, b after iteration t. However, the encoder only stops when $b - a < |M|^n$, so we have $b_{l-1} - a_{l-1} \geq |M|^n$. Therefore:

$$P(v_{j_1} \dots v_{j_{l-1}}) = (b_{l-1} - a_{l-1})|M|^{-2n} \geq |M|^{-n}.$$

This implies that $H(v_{j_1} \dots v_{j_{l-1}}) \leq |M|^{-n} n$. Therefore:

$$H(\Gamma_{\text{Encode}}(x)) = H(v_{j_1} \dots v_{j_l}) \leq |M|^{-n}(n + \log |C|).$$

Summing over all $|M|^n$ possible values of $x \in M = \{0,1\}^n$, we have:

$$rate(\Gamma) = \frac{1}{n} \sum_{x \in \{0,1\}^n} H(\Gamma_{\text{Encode}}(x)) \leq \frac{n + \log |C|}{n} = 1 + \frac{1}{n} \log |C|.$$

Since $1 + \frac{1}{n} \log |C| \to 1$, we get Γ is asymptotically optimal. □

It is clear that the encoding and decoding algorithms terminate in polynomial time if and only if the probability distribution P_C have nonnegligible entropy.

Steganographic Schemes

In this section, we consider an application of steganographic coding to construct unconditionally secure steganographic scheme. Our construction is optimal.

Let Γ be a steganographic code whose distribution of code words is statistically close to the marginal probability distribution P (as constructed in Section 4). We view P as the probability distribution of output of some random process X. Our steganographic scheme S_Γ is follows.

Setup (1^n). Generate secret key $k \leftarrow \mathcal{U}_{M^n}$.

Embed (k, x). Output $c = \Gamma_{\text{Encode}}(x \oplus k)$.

Extract (k, c). Output $x = \Gamma_{\text{Decode}}(c) \oplus k$.

Theorem 16. *The steganographic scheme S_Γ is statistically secure.*

Proof. Since $k \leftarrow \mathcal{U}_{M^n}$, we have $x \oplus k \leftarrow \mathcal{U}_{M^n}$. Therefore by the definition of Γ: for all $x \in M$, c distributes statistically close to P.

Now consider a $CHA(n)$-game between Alice, who uses the above steganographic scheme, and Wendy, who tries to detect Alice. Let m be the hiddentext chosen by Wendy. We have shown that regardless of m, $Embed(k, m)$ always distributes statistically close to P. Therefore Wendy cannot distinguish between the two cases: when Alice returns $c = Embed(k, m)$ and when Alice returns $c \leftarrow P$, with more than negligible advantage. This means that our scheme is statistically secure. □

Theorem 17. *The steganographic scheme S_Γ is asymptotically optimal.*

Proof. This follows immediately from the fact that our scheme does not have additional overhead (over Γ), and the fact that Γ is already asymptotically optimal. Our

scheme runs in polynomial time if the entropy of P is nonnegligible, which is the necessary and sufficient condition for statistically secure steganography. □

Steganographic Secret Sharing

In this section, we show how to construct steganographic secret sharing. A (t, n)-*secret sharing scheme* is a scheme to *split* into n shares in such a way that any t shares can be used to reconstruct the secret, but any $t-1$ shares contain no information on the secret.

A *steganographic secret sharing scheme* is a secret sharing scheme in which shares distributes statistically close to a given probability distribution, even when up to $t-1$ shares are known. A *generalized steganographic secret sharing scheme* is a secret sharing scheme in which each (unexposed) share-i distributes statistically close to à priory given probability distributions $P_S^{(i)}$, even when up to $t-1$ other shares are known by the adversary.

Construction. Let $S(t, n)$ be Shamir's (t, n) threshold scheme [43] defined over finite field F_q, where $q = 2^m$ for some integer m such that $n \leq 2^m$. The share of each user i ($1 \leq i \leq n$) in $S(t, n)$ is $s_i = f_t(i)$, where $f_t(x) = \sum_{i=0}^{t-1} a_i x^i$ is a random secret polynomial of degree $t-1$ in $F_q[x]$, and the shared secret is $f_t(0) = a_0$. Let the steganographic share of each user be $S_i = \Gamma_{\text{Encode}}(s_i)$. Then the shared secret a_0 can be reconstructed from $s_i = \Gamma_{\text{Decode}}(S_i)$ by using Lagrange's interpolation [43].

Proof. Observe that even when $t-1$ users collude, the length $t-1$ vector, which consists of their $t-1$ shares s_i, is a random vector in F_q^{t-1}. The reason for this is that if $i_1, \ldots, i_{t-1}$ were the colluders then the corresponding shares are $(s_{i_1}, \ldots, s_{i_{t-1}}) = (a_0, \ldots, a_0) + V(i_1, \ldots, i_{t-1})(a_1, \ldots, a_{t-1})^T$ where $V(i_1, \ldots, i_{t-1})$ is equivalent to a Vandermonde matrix of size $t-1$. Since $V(i_1, \ldots, i_{t-1})$ is invertible and $(a_1, \ldots, a_{t-1})$ is uniformly random, $(s_{i_1}, \ldots, s_{i_{t-1}})$ is also a random vector (uniform distributions

are preserved by non-degenerate affine transformations). Therefore, the steganographic shares of this scheme are hidden even when $t-1$ users are corrupted.

This generalized steganographic threshold scheme can be used to hide secret keys or data securely in multiple distributed storages. Since the underlying secret sharing scheme and the steganographic code are both optimal, our scheme is also asymptotically optimal.

CHAPTER 5

COMPUTATIONAL COMPLEXITY SOLUTIONS

In this chapter, we extends our perfect and statistically secure schemes constructed earlier to obtain computationally secure schemes. The main advantage of these schemes is that a single key can be used for multiple message transmissions.

From Unconditional to Conditional Security

In this section, we construct a computationally secure steganographic system using the perfect invisible steganographic scheme and a uniform pseudorandom generator [14]. Our scheme is computationally secure, i.e. as secure as the pseudo-random generator, and also efficient since Alice and Bob can reuse the key. As a consequence, our scheme implies that pseudo-random generators are sufficient for secure steganography. We also prove later that one-way functions are necessary to secure steganography.

Private Key Steganographic System

Let G be a secure pseudo-random generator. G takes a seed s as input and outputs pseudo-random bit sequence $G[s]$. Denote $State[G \leftarrow s]$ the current state of G when its input seed was s. This state determines the pseudo-random sequence $G[s]$ completely. Let $\mathcal{A}$=($\mathcal{K}$, $\mathcal{C}$, $\mathcal{M}$, $P_{\mathcal{K}}$, $P_{\mathcal{C}}$, E, D) be a perfect steganographic scheme.

Our computationally secure steganographic scheme $A[G]$ involves the following.

- **Setup** Randomly select a seed s from seed space of G, and feed s to G. The shared secret key between Alice and Bob is $State[G \leftarrow s]$.
- **Encrypt** Using $G[s]$ as the random tape, Alice randomly generates a secret subkey $k \in \mathcal{K}$ accordingly to probability distribution $P_{\mathcal{K}}$. Alice sends ciphertext $c = E(k, m)$ to Bob.
- **Decrypt** Using $G[s]$ as the random tape, Bob randomly generates a secret subkey $k \in \mathcal{K}$ accordingly to probability distribution $P_{\mathcal{K}}$. Bob decrypts ciphertext c to obtain plaintext $m = D(k, c)$.

Note that $State[G \leftarrow s]$ is updated accordingly each time $G[s]$ is being used. It is easy to see that the above scheme is sound, i.e. Bob receives the correct plaintext from Alice. We claim the following.

Theorem 18. *In the above steganographic scheme, the ciphertext distribution $P_{E(\mathbf{k},\mathbf{m})}$ is computationally indistinguishable from $P_{\mathcal{C}}$.*

Proof. Assume by contradiction that $P_{E(k,m)}$ is computationally *distinguishable* from $P_{\mathcal{C}}$. Let T be a Turing machine that distinguishes $P_{E(k,m)}$ from $P_{\mathcal{C}}$. By definition we have $\delta = \mid \Pr(T(E(\mathbf{k}, \mathbf{m}) = 1)) - \Pr(T(\mathbf{x}) = 1 \mid \mathbf{x} \leftarrow P_{\mathcal{C}}) \mid$ is non-negligible. We show that using T as a subroutine, we can construct a Turing machine T_G that can efficiently distinguish the output $G[s]$ of G from truly uniform random bit sequences. The machine T_G works as follows. T_G takes a random string r as input and uses r as the random tape to generate a subkey k_r accordingly to distribution $P_{\mathcal{K}}$. Finally, T_G outputs $T(E(k_r, m))$ where m is any fixed plaintext. Note that T_G is polynomial time since T and E are polynomial time.

We next show that T_G distinguishes $G[s]$ from truly random sequences. Indeed, when the input of T_G is taken from $G[s]$, its output is nothing else but $T(E(\mathbf{k}, \mathbf{m}))$. On the other hand, when the input of T_G is taken from a truly random sequence, the output of T_G is $T(E(\mathbf{k}_U, \mathbf{m}))$, where $\mathbf{k}_U$ distributes exactly according to $P_{\mathcal{K}}$ because $\mathbf{k}_U$ was generated using truly random sequence. Since $\mathcal{A}$

is a perfect invisible steganographic scheme, we have $E(\mathbf{k}_U, \mathbf{m})$ distributes accordingly to $P_{\mathcal{C}}$. Therefore the difference between the output of T_G when its input is taken from $G[s]$ and the output of T_G when its input is taken from truly random is $\mid \Pr(T(E(\mathbf{k}, \mathbf{m})) = 1) - \Pr(T(E(\mathbf{k}_U, \mathbf{m})) = 1) \mid = \mid \Pr(T(E(\mathbf{k}, \mathbf{m})) = 1) - \Pr(T(\mathbf{x}) = 1 \mid \mathbf{x} \leftarrow P_{\mathcal{C}}) \mid = \delta$, which is non-negligible. Thus T_G distinguishes $G[s]$ from a truly random sequence. This contradicts our assumption that G is a secure pseudorandom generator. Therefore our assumption that $P_{E(k,m)}$ is distinguishable from $P_{\mathcal{C}}$ is wrong, i.e. our theorem is proven. □

A very useful property of our scheme is that we can always use a small plaintext and ciphertext space and still achieve *maximum* information rate, and yet the parameter size does not effect the security level in perfect schemes.

From Statistical to Computational Security

Our purpose in this section is to construct steganographic systems based on the steganographic coding scheme Γ.

Private Key Steganographic Systems

Let G be a cryptographically secure pseudorandom generator, and k be a shared secret key. In the setup step, k is given as seed to G.

S_1-`Embed`. **Input**: $m \in \Sigma^n$.
Output: $c \in C^*$.

1. **let** $r \in_R \Sigma^n$ be the next n random bits generated by G.
2. Output $c = \Gamma_e(r \oplus m)$.

S_1-`Extract`. **Input**: $c \in C^*$.
Output: $m \in \Sigma^n$.

1. **let** $r \in_R \Sigma^n$ be the next n random bits generated by G.

2. Output $m = \Gamma_d(c) \oplus r$.

Theorem 19. *The steganographic scheme S_1 is CHA-secure.*

Proof. The proof is straightforward: $r \oplus m$ is computationally indistinguishable from uniformly random, so by the property of Γ_e, the output covertext sequence $c = \Gamma_e(r \oplus m)$ is computationally indistinguishable from $\mathcal{P}$. Further, each time the embedding operation is performed, the pseudorandom generator G changes its internal state, so its output r are independent of each others in the attacker's view. Consequently, the values of $r \oplus m$, and so do the values of $c = \Gamma_e(r \oplus m)$, are probabilistically independent of each others to the attacker. This means that the ciphertexts obtained by the attacker in the setup step do not help him in the guessing step in anyway. Therefore our scheme is secure against chosen hiddentexts attack. □

Expansion Rate. It is clear that the expansion rate of this scheme is the same as the expansion rate of the steganographic code. Additionally, both sides must maintain the status of the generator G. However, this status is very small, similar to a synchronized counter used in [26].

Public Key Steganographic Systems

In this section, we use the Diffie-Hellman key exchange primitive [15] to obtain an efficient public key steganographic scheme [33]. Denote $H_{\mathcal{P}}(c) = -\log_2(\mathcal{P}(c))$ the entropy of $c \in C^*$ according to the covertext distribution $\mathcal{P}$. We assume that there exists a constant $0 < \rho < 1$ such that:

$$\forall h \in C^*, \forall c \in C : \mathcal{P}_h(c) < \rho.$$

In other words, $\mathcal{P}_h$ has its minimum entropy bounded from below by a positive constant ($-\log_2(\rho)$).

S_2-Setup. The system parameter is a generator g of a prime order cyclic group $<g>$, whose decisional Diffie-Hellman problem is hard. Let (g, g^a) be the public key of sender Alice, and (g, g^b) be the public key of receiver Bob. Let $F(X, Y)$ be a public cryptographically secure family of pseudorandom functions, indexed by variable $X \in <g>$. Let k be the security parameter and $n = O(poly(k))$. The embedding and extracting operations are as follows.

S_2-Embed. **Input**: $m \in \{0,1\}^n$.

Output: $c \in C^*$.

1. Let $l = \lceil \frac{k}{\log_2 \frac{1}{\rho}} \rceil$, $h_0 = \epsilon$.
2. **for** i **from** 1 **to** l **do** $c_i \leftarrow P_C$; $h_0 = h_0 \| c_i$.
3. Let $r = F((g^b)^a, h_0)$.
4. Output $c = h_0 \| \Gamma_e(r \oplus m)$.

Note that in the call to $\Gamma_e(r \oplus m)$, we initialize h with h_0, instead of ϵ.

S_2-Extract. **Input**: $c \in C^*$.

Output: $m \in \{0,1\}^n$.

1. Let $l = \lceil \frac{k}{\log_2 \frac{1}{\rho}} \rceil$, $c = (h_0, c')$ where $|h_0| = l$.
2. Let $r = F((g^a)^b, h_0)$.
3. Output $m = \Gamma_d(c') \oplus r$.

Theorem 20. *The steganographic scheme S_2 is CHA-secure.*

Proof. By definition of the family F and the hardness of the Diffie-Hellman problem over $<g>$, we obtain that g^{ab}, and therefore r, is computationally indistinguishable from uniformly random. Thus, by definition of our steganographic code, c is computationally indistinguishable from $\mathcal{P}$.

Further, since $H_{\mathcal{P}}(h_0) \geq k$, with overwhelming probability h_0 is different each time we embed. Therefore even when the embedding oracle is queried repeatedly, r still appears to the attacker as independently and uniformly random. Therefore in the attacker's view the ciphertexts obtained by him in the setup step are independent of of the challenged ciphertext, i.e. they are useless for the attack. That means our scheme is CHA-secure. □

Expansion Rate. The expansion rate of this scheme equals to the rate of the underlying steganographic code plus the overhead in sending h_0. Nevertheless, the overhead of h_0, which is $O(\lceil \frac{k}{\log_2(\frac{1}{\rho})} \rceil)$, only depends on the security parameter k. Thus it diminishes when we choose n large enough so that $k = o(n)$, say $n = k\log(k)$. Therefore the expansion rate of our steganographic system is essentially that of the steganographic code.

Necessary and Sufficient Condition

In the following, assume that the covertext probability distribution has nonnegligible entropy.

Theorem 21. *The necessary and sufficient condition for computationally secure steganography is the existence of one-way functions.*

Proof. Theorem 19 shows us that pseudorandom generators are sufficient for computationally secure steganography. Since oneway functions implies pseudorandom generator [23], this shows that the existence oneway functions is sufficient for computationally secure steganography [14]. We now show the reverse.

Let S be any computationally secure steganographic scheme. We construct a oneway function f as follows. Let $l \geq 2|k|$ where $k \in \{0,1\}^*$. For each $v \in \{0,1\}^l$, let $x_v = (Embed(k, v_1), \ldots, Embed(k, v_l))$. Since S is secure, probability distribution of x_v is indistinguishable from P_C^l, where the randomness of x is taken over the random choices of k and the random coins of $Embed$. Let S_v be the set of all possible values of x_v. For each fixed k and $v \neq v'$, we have $x_v \neq x_{v'}$ and $S_v \cap S_{v'} = \emptyset$.

Therefore there exists a $v^0 \in \{0,1\}^l$ such that $|S_{v^0}| < 2^{|k|-l}|C|^l$. Define a function $f(k,r)$ where $r = (r_1, r_2, \ldots, r_l)$ by $f(k,r) = (Embed(k, v_1^0), \ldots, Embed(k, v_l^0))$ where $Embed(k, v_i^0)$ uses random coins r_i. We show that f is an oneway function.

Assume by contradiction that f is not oneway. Let A be any polynomial time algorithm that inverts f. By our assumption, S is computationally secure. Thus the output of f is indistinguishable from an l-tuple $(s_1, \ldots, s_l)$ when (k,r) is uniformly random, where the $s_i \leftarrow P_C$ are independent of each other. Therefore $A(f(k,r)) = A(Embed(k, v_1^0), \ldots, Embed(k, v_l^0))$ is computationally indistinguishable from $A(s_1, \ldots, s_l)$. But $|S_{v^0}| < 2^{|k|-l}|C|^l < 2^{-|k|}|C|^l$, so for an overwhelming fraction of $(s_1, \ldots, s_l) \in C^l$, we have $(s_1, \ldots, s_l) \notin S_{v^0}$. Therefore for an overwhelming fraction of $(s_1, \ldots, s_l) \in C^l$ there does *not* exists (k,r) such that $(s_1, \ldots, s_l) = f(k,r)$. This means that A fails with overwhelming probability on an overwhelming fraction of its input. This proves that f is indeed a oneway function, i.e. computationally secure steganography implies oneway functions. This completes our proof. □

Remark. Because we can choose the hiddentext to have constant entropy, the stegotext distribution must have nonnegligible entropy. In that case, the covertext probability distribution also has nonnegligible entropy, or otherwise the two will be distinguishable simply by comparing their sample entropies for large enough (but only polynomial) number of samples (cf. Theorem 3). Therefore, in general the necessary and sufficient condition for computationally secure steganography is that the covertext probability distribution has nonnegligible entropy, and that oneway functions exist.

CHAPTER 6

COVERTEXT GENERATOR SOLUTIONS

In the previous chapters, we have shown how to communicate steganographically when the cover distribution is known. However, there are situations in which no such information is immediately available and obtaining it is hard. In this chapter, we construct steganographic schemes using only blackbox covertext generators.

Definition

Definition 11 (Marginal Sampler). *Let P be a marginal probability distribution. A* sampler *G for the channel P is a sampling oracle such that on query $h \in C^*$, G randomly outputs a message $c \in C$ according to the marginal probability distribution P_h. That means $G(h) \leftarrow P_h$.*

Definition 12 (Blackbox Steganography). *A blackbox steganographic scheme is a steganographic scheme in which the* `Embed` *algorithm is an oracle Turing machine with access to the sampling oracle G such that for all G, the output distributions of* $\texttt{Embed}^G$ *and of G are statistically close.*

Construction

Theorem 22. *Let $c = (c_1, \ldots, c_q)$ be q independent identically distributed random variables with probability distribution P. Let X be a random variable such that $\Pr[X|c] = type(c)$. Then the probability distribution of X is P.*

Proof. Let $f_c = type(c)$ be the frequency vector of c. We have for all $v \in C$:

$$\Pr[X = v] = \sum_{c_1,\ldots,c_q} \prod_{i=1}^{q} P(c_i) f_c(v).$$

Let x be the random variable denoting the output of the following experiment. Randomly select $i \leftarrow \mathcal{X}_{\{1,\ldots,q\}}$. Then let $x = 1$ if $c_i = v$, and $x = 0$ otherwise. Thus we have $E[x|c] = \frac{1}{q} \sum_{i:c_i=v} 1 = f_c(v)$ and hence:

$$\Pr[X = v] = \sum_{c_1,\ldots,c_q} \prod_{i=1}^{q} P(c_i) E[x|c] = E[E[x|c]] = E[x].$$

Since i was chosen independently of c, we have $\Pr[c_i = v] = \Pr[c_1 = v]$ and therefore $\Pr[X = v] = E[x] = \Pr[x = 1] = \Pr[c_i = v] = \Pr[c_1 = v] = P(v)$. □

In the following, let S be an existing statistically secure steganographic scheme, such as those constructed in Chapters 2, 3, 4. Let the sampler G be a Turing machine so that $G[r, h]$ distributes accordingly to P_h when r is uniformly random. We apply the result of Theorem 22, and use G and S to construct a statistically secure generator based steganographic scheme as follows. Let h be the history of previously exchanged messages.

`Setup`. $k \leftarrow S.\mathtt{Setup}(1^n), r \leftarrow \mathcal{U}_{\{0,1\}^n}$.

`Embed`. **Input**: $m \in M$.

Output: $c \in C$.

1. Uses $G[r, h]$ to generate $c = (c_1, \ldots, c_t)$.

2. Let $P_C = type(c)$.

3. Let $s = S.\texttt{Embed}(P_C, k, m)$.

4. Output s.

`Extract`. **Input**: $s \in C$.

Output: $m \in M$.

1. Uses $G[r, h]$ to generate $c = (c_1, \ldots, c_t)$.

2. Let $P_C = type(c)$.

3. Let $m = S.\texttt{Extract}(P_C, k, s)$.

4. Output m.

Theorem 23. *The steganographic scheme described above is statistically secure.*

Proof. This is a direct consequence of Definition 12 and Theorem 22. □

Optimality

Lemma 7. *Let S be a perfectly secure blackbox steganographic scheme. Let $c = (c_1, \ldots, c_q)$ be the answer of the sampling oracle G to S. Then the conditional probability distribution of $s = Embed(k, m)$ given c is exactly $type(c)$.*

Proof. Without loss of generality, let $C = \{1, \ldots, |C|\}$. Let $P_C \in \mathbb{R}^{|C|}$ be the probability distribution vector of output of G. Let $p_c = \Pr[s = 1 \mid c] \geq 0$. We have:

$$\Pr[s = 1] = \sum_{c \in C^q} \Pr[c] \Pr[s|c] = \sum_{c \in C^q} \prod_{i=1}^{q} P_C(c_i) p_c.$$

Since the scheme is perfectly secure, we have $\Pr[s = 1] = P_C(1)$, that means:

$$\sum_{c \in C^q} \prod_{i=1}^{q} P_C(c_i) p_c = P_C(1).$$

Denote $x_j = P_C(j)$ then the above equation becomes:

$$\sum_{c \in C^q} p_c \prod_{i=1}^{q} x_{c_i} = x_1. \tag{6.1}$$

Note that (6.1) holds for all G, hence it holds for all probability vector x. We show that there exists a unique vector $p = \{p_c \mid c \in C^1\}$ such that (6.1) holds for all probability vector x.

In fact by Theorem 22, $p' = \{p'_c = type(c) \mid c \in C^q\}$ is such a vector. Therefore we just need to prove that $p = p'$. Let $f = p - p' \in C^q$. Since (6.1) holds for both p and p', we get:

$$\sum_{c \in C^q} f_c \prod_{i=1}^{q} x_{c_i} = 0 \tag{6.2}$$

holds for all probability distribution vector $x \in \mathbb{R}^{|C|}$. For all nonnegative-component vector $x \in \mathbb{R}^{|C|}$, not necessarily a probability distribution vector, let $\text{sum}(x) = \sum_{i=1}^{|C|} x_i$, and let $x' = x/\text{sum}(x)$ then x' is a probability vector and

$$\sum_{c \in C^q} f_c \prod_{i=1}^{q} x_{c_i} = \text{sum}(x)^q \sum_{c \in C^q} f_c \prod_{i=1}^{q} x'_{c_i} = \text{sum}(x)^q 0 = 0.$$

Thus (6.2) holds for all nonnegative component vector x. Equate the two sides of the equation with respect to variables $x_1, \ldots, x_{|C|}$, we get $f_c = 0$ for all $c \in C^q$. Hence $p = p'$. That means $\Pr[s \mid c] = type(c)$. □

Theorem 24. *Assume that a statistically secure blackbox steganographic scheme makes q calls to the sampler oracle G. Then the information rate of the scheme is at most $H^q_{smp}(G)$. As a consequence, the information rate is at most* $\log(q)$.

Proof. First, assume that the scheme is perfectly secure. By Lemma 7, $\Pr[s|c] = type(c)$ hence $H(s|c) = H(type(c)) = H_{\text{smp}}(c)$. Furthermore, $H(m) = H(m|c) \leq H(s|c)$ so we obtain $H(m) \leq H_{\text{smp}}(c) = H^q_{\text{smp}}(P_C)$.

Second, assume that the scheme is not perfectly secure but statistically secure. Let P'_C be the probability distribution of $s = Embed(k, m)$. By definition, P_C and

P'_C are statistically close. By our assumption, the scheme is perfectly secure with respect to probability distribution P'_C. Thus we get $H(m) \leq H^q_{\text{smp}}(P'_C)$.

However, by Theorem 2, $H^q_{\text{smp}}(P'_C)$ and $H^q_{\text{smp}}(P_C)$ are identical to each other modulo a negligible difference, which approaches 0 (exponentially fast) when n approaches infinity. Hence we conclude that the maximum information rate is $H^q_{\text{smp}}(P_C) = H^q_{\text{smp}}(G)$. □

It is not hard to see that the $\log(q)$ bound also applies to computationally secure blackbox steganographic schemes. In fact, let G be a digital signature signing algorithm. Then there exists a polynomial time algorithm that distinguishes outputs of G from those strings which are not are output of G. An example of such an algorithm is the signature verification algorithm. Therefore when c is the vector of q oracle answers of G, then we must have $s \in \{c_1, \ldots, c_q\}$, or otherwise it will be distinguishable. This means that $H(s|c) \leq \log(q)$.

Theorem 25. *Our construction of statistically secure blackbox steganographic scheme in the preceding section is optimal.*

Proof. Since the information rate of our scheme is $H_{\text{smp}}(type(c)) = H^q_{\text{smp}}(G) = H^q_{\text{smp}}(P_h)$, where $c = (c_1, \ldots, c_q)$ is the answer of the oracle G, Theorem 24 shows that it is optimal. □

Remark. Let $X = \{X_1, X_2, \ldots\}$ be the random process corresponding to marginal probability distribution P. As a consequence of Theorem 25, the necessary and sufficient condition for statistically secure blackbox steganography is that there exists a polynomial $p(n)$ such that for all large enough n, $H(X_1, \ldots, X_{p(n)}) \geq n$. It is clear that (cf. Theorem 21), the necessary and sufficient condition for computationally secure blackbox steganography [26] is that $H(X_1, \ldots, X_{p(n)}) \geq n$ and that oneway functions exists.

REFERENCES

[1] M. Abe. Universally verifiable Mix-net with verification work independent of the number of Mix-centers. In K. Nyberg, editor, *Advances in Cryptology — Eurocrypt '98, Proceedings (Lecture Notes in Computer Science 1403)*, pages 437–447. Springer-Verlag, 1998. Espoo, Finland, May 31–June 4.

[2] R. Anderson, editor. *Proceedings of First International Workshop on Information Hiding*, volume 1174 of *LNCS*, Cambridge, UK, May/June 1996. Springer-Verlag.

[3] R. J. Anderson, R. M. Needham, and A. Shamir. The steganographic file system. In D. Aucsmith, editor, *Second International Workshop in Information Hiding*, volume 1525 of *LNCS*, pages 73–82, Porland, Oregan, 1998. Springer-Verlag.

[4] R. J. Anderson and F. A.P. Petitcolas. On the limits of steganography. *IEEE Journal of Selected Areas in Communications*, 16(4):474–481, May 1998.

[5] D. Aucsmith, editor. *Proceedings of Second International Workshop on Information Hiding*, volume 1525 of *LNCS*, Porland, Oregan, April 1998. Springer-Verlag.

[6] D. Boneh. The decision Diffie-Hellman problem. *Lecture Notes in Computer Science*, 1423:48–63, 1998.

[7] C. Cachin. An information-theoretic model for steganography. In *Information Hiding, Second International Workshop, Proceedings (Lecture Notes in Computer Science 1525)*, pages 306–318. Springer-Verlag, 1998. Portland, Oregon, April 15–17.

[8] D. Chaum. Untraceable electronic mail, return addresses, and digital pseudonyms. *Commun. ACM*, 24(2):84–88, February 1981.

[9] D. Chaum. The dinning cryptographers problems: Unconditional sender and recipient untraceability. *Journal of Cryptology*, 1(1):65–75, 1988.

[10] H. Chernoff. A measure of asymptotic efficiency for tests of a hypothesis based on the sum of observations. *Annals of Mathematical Statistics*, 23:493–509, 1952.

[11] T. M. Cover and J. A. Thomas. *Elements of Information Theory*. Wiley Series in Telecommunications. John Wiley & Sons, Inc, 2nd edition, 1991.

[12] S. Craver. On public-key steganography in the presence of an active warden. In David Aucsmith, editor, *Information Hiding, Second International Workshop, Portland, Oregon, USA*, volume 1525 of *Lecture Notes in Computer Science*. Springer, April 14-17 1998.

[13] Y. Desmedt. Abuses in cryptography and how to fight them. In S. Goldwasser, editor, *Advances in Cryptology — Crypto '88, Proceedings (Lecture Notes in Computer Science 403)*, pages 375–389. Springer-Verlag, 1990. Santa Barbara, California, U.S.A., August 21–25.

[14] Yvo Desmedt and Tri Van Le. Efficient perfectly and computationally secure steganography. Unpublished, 2002.

[15] W. Diffie and M. Hellman. New directions in cryptography. *IEEE Transactions on Information Theory*, 22(6):644–654, November 1976.

[16] D. Dolev, D. Dwork, and M. Naor. Non-malleable cryptography. *SIAM Journal on Computing*, 30(2):391–437, 2000.

[17] J.M. Ettinger. Steganalysis and game equilibria. In D. Aucsmith, editor, *Proceedings of Second International Workshop on Information Hiding*, volume 1525 of *LNCS*, pages 319–328. Springer, 1998.

[18] M. R. Garey and D. S. Johnson. *Computers and Intractability: A guide to the theory of NP-completeness*. W. H. Freeman and Company, San Francisco, 1979.

[19] I. I. Gikhman and A. V. Skorokhod. *Introduction to the Theory of Random Processes*. Saunders, Philadenphia, 1965.

[20] O. Goldreich. *Foundations of Cryptography*. Cambridge University Press, 2001.

[21] S. Goldwasser and S. Micali. Probabilistic encryption. *Journal of Computer and System Sciences*, 28(2):270–299, April 1984. A preliminary version was presented at STOC'82.

[22] P. R. Halmos. *Measure Theory*. Van Nostrand Reinhold, New York, 1950.

[23] J. Hastad, R. Impagliazzo, L. A. Levin, and M. Luby. A pseudorandom generator from any one-way function. *SIAM Journal on Computing*, 28(4):1364–1369, 1999.

[24] Herodotus and David Grene (translator). *The History: Herodotus*. University of Chicago Press, 1988.

[25] W. Hoeffding. Probability inequalities for some of bounded random variables. *American Statistical Association Journal*, pages 13–30, 1963.

[26] N. Hopper, J. Langford, and L. von Ahn. Provably secure steganography. In Moti Young, editor, *Advances in Cryptoglogy — Crypto 2002, Proceedings*, volume 2442 of *LNCS*. Springer-Verlag, August 2002.

[27] N. Hopper and L. von Ahn. Public key steganography. Eurocrypt 2004.

[28] D. Kahn. *The Code Breakers*. Simon and Schuster Inc., 1996.

[29] G. Kalai and G. M. Ziegler, editors. *Polytopes: combinatorics and computation*. Birkhauser Verlag, Basel, Boston, 2000.

[30] S. Katzenbeisser and F. Petitcolas. On defining security in steganographic systems, 2002.

[31] A. N. Kolmogorov. *Foundations of The Theory of Probability*. Chelsea, New York, 1950.

[32] B. W. Lampson. A note on the confinement problem. *Communication of the ACM*, 16(10):613–615, October 1973.

[33] Tri Van Le and Kaoru Kurosawa. Efficient public key steganography secure against adaptively chosen stegptext attacks. Technical Report 2003/244, International Association of Cryptographic Research, November 2003.

[34] E. Manoukian. *Modern Concepts and Theorems of Mathematical Statistics*. Springer Series in Statistics. Springer-Verlag, 1985.

[35] Mittelholzer. An information-theoretic approach to steganography and watermarking. In A. Pfitzmann, editor, *Proceedings of Third International Workshop on Information Hiding*, volume 1768 of *LNCS*. Springer-Verlag, September 1998.

[36] P. Moulin and J. O'Sullivan. Information-theoretic analysis of information hiding, 1999.

[37] M. Naor and M. Yung. Public-key cryptosystems provably secure against chosen ciphertext attacks. In *Proceedings of the 22nd Annual ACM Symposium on Theory of Computing*, pages 427–437, 1990.

[38] A. Pfitzmann, editor. *Proceedings of Third International Workshop on Information Hiding*, volume 1768 of *LNCS*, Dresden, Germany, September/October 1999. Springer-Verlag.

[39] C. Rackoff and D. Simon. Non-interactive zero-knowledge proof of knowledge and chosen ciphertext attack. In J. Feigenbaum, editor, *Proceedings of Advances in Cryptoglogy – Crypto'91*, volume 576 of *Lecture Notes in Computer Science*, pages 433–444. Springer-Verlag, 1991.

[40] M. G. Reed, P. F. Syverson, and D. M. Goldschlag. Anonymous connections and onion routing. *IEEE Journal on Selected Areas in Communications*, 16(4):482–494, 1998.

[41] L. Reyzin and S. Russell. More efficient provably secure steganography. Technical report, IACR ePrint Archive 2003/093, 2003.

[42] R. L. Rivest, A. Shamir, and L. M. Adelman. A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, 21(2):120–126, 1978.

[43] A. Shamir. How to share a secret. *Communications of the ACM*, 22:612–613, 1979.

[44] P. W. Shor. Algorithms for quantum computation: Discrete logarithms and factoring. In *IEEE Symposium on Foundations of Computer Science*, pages 124–134, 1994.

[45] G. J. Simmons. The prisoner's problem and the subliminal channel. In David Chaum, editor, *Advances in Cryptology: Proceedings of Crypto '83*, pages 51–70, New York, USA, 1984. Plenum Publishing.

[46] G. J. Simmons. The history of subliminal channels. In R. Anderson, editor, *Information Hiding, First International Workshop, Proceedings (Lecture Notes in Computer Science 1174)*, pages 237–256. Springer-Verlag, 1996. Cambridge, U.K., May 30–June 1.

[47] Michael Sipser. *Introduction to the Theory of Computation*. PWS Publishing Company, Boston, MA, 1997.

[48] A. Young and M. Yung. Cryptovirology: Extortion-based security threats and countermeasures. In *Proceedings of the 1996 IEEE Symposium on Security and Privacy*, pages 129–140. IEEE Computer Society Press, May 6-8 1996.

[49] A. Young and M. Yung. Kleptography: Using cryptography against cryptography. In *Advances in Cryptology: Eurocrypt '97*, pages 62–74. Springer-Verlag, 1997.

[50] J. Zollner, H. Federrath, H. Klimant, A. Pfitzmann, R. Piotraschke, A. Westfeld, G. Wicke, and G. Wolf. Modeling the security of steganographic systems. In *Information Hiding*, pages 344–354, 1998.

BIOGRAPHICAL SKETCH

Le Van Tri was born in Ha Noi, Viet Nam on July 1975.

Education. September 1993 to June 1997, Bachelor of Science in Computer Science, Ha Noi University, Viet Nam. Thesis title: "*Monomial Curves*". September 1997 to June 1999, Master of Science in Computer Science, University of Wisconsin, Milwaukee, USA. Thesis title: "*Audio and Visual Cryptography*". January 2000 to April 2004, Doctorate in Computer Science, Florida State University, Tallahassee, USA. Dissertation title: "*Information Hiding*".

Awards. July 1995, Creative Youth Award, The Viet Nam Student Association. July 1996, Gold and Silver Prizes, Inter-University Competitions on Mathematics and Computer Science, Ha Noi, Viet Nam. July 2002, South East regional finalist, Topcoder Programming Challenge, USA.

Publications. Le Van Tri has published twelve papers and articles in international journal and conferences on cryptography, network security, digital watermarking and fingerprinting, artificial intelligence, computational algebra. Le Van Tri is a member of Association of Computing Machinery, International Association for Cryptographic Research. He is a referee for several international journals and conferences.

Professional Positions. System Analyst, Ha Noi, Viet Nam (1993-1995). Telecommunications Engineer, Vancouver, Canada (2000).