ISSN 1342-2812

Research Reports on Mathematical and Computing Sciences

Steganographic Signature

Hirotoshi Takebe and Keisuke Tanaka

December 2006, C–233

Department of
Mathematical and
Computing Sciences
Tokyo Institute of Technology

SERIES C: Computer Science

Steganographic Signature

Hirotoshi Takebe and Keisuke Tanaka

Dept. of Mathematical and Computing Sciences
Tokyo Institute of Technology
W8-55, 2-12-1 Ookayama Meguro-ku, Tokyo 152-8552, Japan
{takebe3, keisuke}@is.titech.ac.jp

December 26, 2006

Abstract

Steganography is the science of sending messages hidden in harmless communications over a public channel so that an adversary eavesdropping on the channel cannot even detect the presence of the hidden messages. In this paper, we formalize and propose a steganographic signature scheme. We define the security condition of steganographic signature, the steganographic security and the unforgeability. We construct a steganographic signature scheme, and we show that our proposed steganographic signature scheme with the extended Schnorr signature scheme is steganographically secure and unforgeable.

Keywords: Digital signature, Steganography

1 Introduction

Steganography is the science of sending messages hidden in harmless communications over a public channel so that an adversary eavesdropping on the channel cannot even detect the presence of the hidden messages. Public-key steganography is the protocol which allows two parties, who have never met or exchanged a secret, to send hidden messages over a public channel so that an adversary cannot even detect that these hidden messages are being sent.

Public-key steganography with a passive adversary was formalized by von Ahn and Hopper [7]. They defined the security notion which was the analogue of a cryptosystem with the security against the chosen-plaintext attack. They constructed the stegosystem which satisfied this notion. Backes and Cachin [1] formalized public-key steganography with an active adversary. They defined the security notion against such an adversary. A stegosystem which satisfies this notion is called *steganographically secure against the adaptive chosen-covertext attack* (SS-CCA). Analogously to the standard cryptographic notion of a chosen-ciphertext attack, this seems to be the most general type of attack possible on a system for steganography. They also defined a relaxed notion of the security, against the *replayable* adaptive chosen-covertext attack (SS-RCCA). They showed that an SS-RCCA stegosystem could be constructed from any RCCA-secure [2] public-key cryptosystem whose ciphertexts were pseudorandom. Hopper [3] constructed an SS-CCA stegosystem, which relied on the existence of public-key encryption schemes which satisfied the indistinguishability from random bits under the chosen-ciphertext attack. They showed the existence of such encryption schemes under the Decisional Diffie-Hellman assumption.

In this paper, we propose a steganographic signature scheme. We consider the following scenario. By signing the message, there is a possibility that only the signature is removed and only the message is used. Furthermore, the third party's signature might be applied. We can prevent such situations if the signature seems a message and be mingled with other messages, and only the signer knows where to be hidden it. By making the signed message be kept by the court, we can show that it is a work of the signer. It can be used for the copyright protection.

We propose the definition of steganographic signature. We also define the security of steganographic signature, the steganographic security and the unforgeability. Generally, digital signatures should be unforgeable. In addition to the unforgeability, steganographic signatures should be indistinguishable from messages so that an eavesdropper cannot detect the presence of the hidden signature.

In this paper, we also propose a steganographic signature scheme by modifying public-key steganography schemes. In order to construct it satisfying the steganographic security, we define the security notion of digital signature. It implies the following property: for a value, it is indistinguishable a random value from the signature for a message which consists of the concatenation the value and randomly chosen message. We show that the extended Schnorr signature scheme [9] satisfies this notion, and our proposed steganographic signature scheme with the extended Schnorr signature scheme is steganographically secure and unforgeable.

We give preliminaries in section 2. We propose definitions and the security properties for steganographic signature in section 3. We construct a steganographic signature scheme in section 4. We show that our proposed steganographic signature scheme with the extend Schnorr signature scheme is steganographically secure and unforgeable in section 5. We give the conclusion in section 6.

2 Preliminaries

A function $\mu : \mathbb{N} \to [0,1]$ is said to be *negligible* if for every $c > 0$, for all sufficiently large n, $\mu(n) < \frac{1}{n^c}$. We denote the length (in bits) of a string or an integer s by $|s|$. The concatenation of a string s_1 and a string s_2 is denoted by $s_1||s_2$. The assignment $a||_l b = c$ means that a is the first l bits of c and b is the remaining $|c| - l$ bits of c. We assume the existence of efficient and unambiguous *pairing* and *un-pairing* operations, so (s_1, s_2) is not the same as $s_1||s_2$.

We denote the uniform distribution on k bit strings by U_k. We denote the complement of an event V in some probability spaces by $\overline{\mathsf{V}}$. We denote the *minimum entropy* of a probability distribution $\mathcal{D}$ with finite support X by $H_\infty(\mathcal{D}) = \min_{x \in X} \left\{ \log_2 \frac{1}{\Pr_{\mathcal{D}}[x]} \right\}$. For a probability distribution $\mathcal{D}$, we denote by $x \leftarrow \mathcal{D}$ the action of drawing a sample x according to $\mathcal{D}$. We denote the statistical difference between distributions $\mathcal{D}$ and $\mathcal{E}$, with finite the support X, by $\|\mathcal{D} - \mathcal{E}\| = \frac{1}{2} \sum_{x \in X} |\Pr_{\mathcal{D}}[x] - \Pr_{\mathcal{E}}[x]|$.

A family F of functions $X \to Y$ is called *strongly universal* [8] if for all distinct x_1, $x_2 \in X$ and all y_1, $y_2 \in Y$ which are not necessarily distinct, exactly $|F|/|Y|^2$ functions in F take x_1 to y_1 and x_2 to y_2.

2.1 Digital Signature

Definition 1 (digital signature)**.** *A digital signature scheme $\mathcal{SD}$ is a triple of probabilistic algorithms denoted by $(\mathcal{G}, \mathcal{S}, \mathcal{V})$.*

- $\mathcal{G}$*: The key generation algorithm $\mathcal{G}$ is a randomized algorithm. On input a security parameter 1^k, $\mathcal{G}$ returns a pair of (pk, sk). pk and sk are public and secret keys, respectively.*
- $\mathcal{S}$*: The signing algorithm $\mathcal{S}$ is a (possibly randomized) algorithm. On input 1^k, a message m, and the secret key sk, $\mathcal{S}$ returns a signature σ for m.*
- $\mathcal{V}$*: The verification algorithm $\mathcal{V}$ is a deterministic algorithm. On input 1^k, a message m, the public key pk, and a candidate signature σ for m, $\mathcal{V}$ returns 1 if σ is the valid signature for m. Otherwise, $\mathcal{V}$ returns 0.*

(*Correctness.*) We require that $\mathcal{V}(1^k, m, pk, \mathcal{S}(1^k, m, sk)) = 1$ for any $(pk, sk) \leftarrow \mathcal{G}(1^k)$ and m in the message space (in this paper, we denote the message space by $\mathcal{M}$).

Unforgeability. Let $\mathcal{SD} = (\mathcal{G}, \mathcal{S}, \mathcal{V})$ be a digital signature scheme. Let A be an adversary. A plays a game as follows:

1. A is given pk.
2. A queries messages to the signing oracle $\mathcal{S}$, and receives the corresponding signatures, adaptively.
3. A finally outputs (m^*, σ^*). If A has not queried m^* and $\mathcal{V}(1^k, m^*, pk, \sigma^*) = 1$, then A wins.

We denote the event that A wins this game by $\mathsf{WIN}(A, k)$, where k is the security parameter. We define A's advantage against $\mathcal{SD}$ by

$$\mathbf{Adv}_{\mathcal{SD}}^{\mathsf{ucma}}(A, k) = \Pr[\mathsf{WIN}(A, k)],$$

where $(pk, sk) \leftarrow \mathcal{G}(1^k)$. We say that $\mathcal{SD}$ is *existentially unforgeable under the chosen message attack* (EUF-CMA) if for every probabilistic polynomial adversary A, $\mathbf{Adv}_{\mathcal{SD}}^{\mathsf{ucma}}(A, k)$ is negligible in k.

2.2 Pseudorandom Generators

Let $G : \{0,1\}^k \to \{0,1\}^{l(k)}$ be a function which is computable in polynomial time and $k < l(k)$. We define a distinguishing game by an adversary A and a challenger. We consider the experiments $\mathbf{Exp}_{\mathbf{PRG}}^i$ for $i \in \{0,1\}$ as follows:

$\mathbf{Exp}_{\mathbf{PRG}}^0$

1. The challenger chooses $x \leftarrow U_k$ and computes $z = G(x)$. Then the challenger passes z to A.
2. A outputs a bit d.
3. Return d.

$\mathbf{Exp}_{\mathbf{PRG}}^1$

1. The challenger chooses $z \leftarrow U_{l(k)}$. Then the challenger passes z to A.
2. A outputs a bit d.
3. Return d.

We define A's advantage against G by

$$\mathbf{Adv}_{G,A}^{\mathsf{prg}}(k) = |\Pr[\mathbf{Exp}_{\mathbf{PRG}}^0(A) = 1] - \Pr[\mathbf{Exp}_{\mathbf{PRG}}^1(A) = 1]|,$$

We also define A's insecurity of G by $\mathbf{InSec}_G^{\mathsf{prg}}(t, k) = \max_{A \in \mathcal{A}(t)}\{\mathbf{Adv}_{G,A}^{\mathsf{prg}}(k)\}$, which $\mathcal{A}(t)$ is a set of adversaries in running time t. We say that G is a *pseudorandom generator* if for every probabilistic polynomial adversary A, $\mathbf{Adv}_{G,A}^{\mathsf{prg}}(k)$ is negligible in k.

2.3 Channels

We follow previous works [4, 5, 7, 1, 3] about steganography in modeling the communication between two parties by a *channel*. We define a channel $\mathcal{C}$ as a family of probability distributions on documents from a set D, indexed by sequences $h \in D^*$ where $D^* = D \times D \times \cdots$. A channel implicitly specifies an indexed distribution on sequences of ℓ documents — given an index h, draw $d_1 \leftarrow \mathcal{C}_h$, $d_2 \leftarrow \mathcal{C}_{(h,d_1)}$, …, $d_\ell \leftarrow \mathcal{C}_{(h,d_1,\ldots,d_{\ell-1})}$. We call the index h the *history* and we label this distribution on sequences by $\mathcal{C}_h^\ell$. A history $h = (d_1, d_2, \ldots, d_\ell)$ is called *legal* if for all i, $\Pr_{\mathcal{C}_{(d_1,\ldots,d_{i-1})}}[d_i] > 0$. A channel is *always informative* if for every legal history h, $H_\infty(\mathcal{C}_h^\ell) = \Omega(\ell)$. A channel is *efficiently sampleable* if there is an efficiently computable algorithm $\mathsf{channel}$ such that $\mathsf{channel}(h, U_k)$ and $\mathcal{C}_h$ are computationally indistinguishable.

3 Steganographic Signature

In this section, we propose the definition and the security properties for steganographic signature.

We first define the steganographic signature scheme.

Definition 2 (steganographic signature)**.** *A steganographic signature scheme is a triple of probabilistic algorithms denoted by $(\mathcal{SG}, \mathcal{SS}, \mathcal{SV})$.*

- *$\mathcal{SG}$: The key generation algorithm $\mathcal{SG}$ is a randomized algorithm. On input a security parameter 1^k, $\mathcal{SG}$ returns a key pair (pk, sk).*
- *$\mathcal{SS}$: The signing algorithm $\mathcal{SS}$ is a (possibly randomized) algorithm. On input 1^k, a message m, a history h, and the secret key sk, $\mathcal{SS}$ returns a signature σ for m.*
- *$\mathcal{SV}$: The verification algorithm $\mathcal{SV}$ is a deterministic algorithm. On input 1^k, a message m, a history h, the public key pk, and a candidate signature σ for m, $\mathcal{SV}$ returns 1 if σ is the valid signature for m. Otherwise, $\mathcal{SV}$ returns 0.*

(*Correctness.*) We require that $\mathcal{SV}(1^k, m, h, pk, \mathcal{SS}(1^k, m, h, sk)) = 1$ for any $(pk, sk) \leftarrow \mathcal{SG}(1^k)$, $m \in \mathcal{M}$, and legal history h.

We next define the security for steganographic signature.

Steganographic security. Let $\mathcal{SSD} = (\mathcal{SG}, \mathcal{SS}, \mathcal{SV})$ be a steganographic signature scheme and ℓ^* the function which implies the length of the signature. We define a distinguishing game under the chosen message-and-history attack against $\mathcal{SSD}$ by an adversary W and a challenger. We consider the experiments $\mathbf{Exp}^i_{\mathbf{CMHA}}$ for $i \in \{0, 1\}$ as follows:

$\mathbf{Exp}^0_{\mathbf{CMHA}}$

1. W is given pk.
2. W produces a history h^* and passes h^* to the challenger. The challenger chooses $m^* \in \mathcal{M}$ randomly and computes $\sigma^* = \mathcal{SS}(m^*, h^*, sk)$. Then the challenger passes σ^* to W.
3. W outputs a bit d.
4. Return d.

$\mathbf{Exp}^1_{\mathbf{CMHA}}$

1. W is given pk.

2. W produces a history h^* and passes h^* to the challenger. The challenger samples $\sigma^* \leftarrow \mathcal{C}_{h^*}^{\ell^*}$. Then the challenger passes σ^* to W.
3. W outputs a bit d.
4. Return d.

In the above experiments, W can make access to the signing oracle $\mathcal{SS}$. We define W's advantage against $\mathcal{SSD}$ with respect to $\mathcal{C}$ by

$$\mathbf{Adv}^{\mathsf{scmha}}_{\mathcal{SSD},\mathcal{C},W}(k) = |\Pr[\mathbf{Exp}^0_{\mathbf{CMHA}}(W(pk)) = 1] - \Pr[\mathbf{Exp}^1_{\mathbf{CMHA}}(W(pk)) = 1]| \ ,$$

where $(pk, sk) \leftarrow \mathcal{SG}(1^k)$. We also define the insecurity of $\mathcal{SSD}$ with respect to $\mathcal{C}$ by

$$\mathbf{InSec}^{\mathsf{scmha}}_{\mathcal{SSD},\mathcal{C}}(t, q, \mu, c, l^*, k) = \max_{W \in \mathcal{W}(t,q,\mu,c,l^*)} \left\{ \mathbf{Adv}^{\mathsf{scmha}}_{\mathcal{SSD},\mathcal{C},W}(k) \right\} \ ,$$

where $\mathcal{W}(t, q, \mu, c, l^*)$ is the set of adversaries that make q signing queries of total length μ and c challenge queries in running time t, and $l^* = |m^*|$. We say that $\mathcal{SSD}$ is $(t, q, \mu, c, l^*, k, \epsilon)$-*steganographically secure under the chosen message-and-history attack* if $\mathbf{InSec}^{\mathsf{scmha}}_{\mathcal{SSD},\mathcal{C}}(t, q, \mu, c, l^*, k) \leq \epsilon$. We say that $\mathcal{SSD}$ is *steganographically secure under the chosen message-and-history attack* (SS-CMHA) if for every probabilistic polynomial adversary W, $\mathbf{Adv}^{\mathsf{scmha}}_{\mathcal{SSD},\mathcal{C},W}(k)$ is negligible in k.

Unforgeability. Let $\mathcal{SSD} = (\mathcal{SG}, \mathcal{SS}, \mathcal{SV})$ be a steganographic signature scheme and $\mathcal{C}$ a channel. Let W be an adversary. W plays a game as follows:

1. W is given pk.
2. W queries pairs of the message and the history to the signing oracle $\mathcal{SS}$, and receives the corresponding signatures, adaptively.
3. W finally outputs (m^*, h^*, σ^*). If W has not queried m^* and $\mathcal{SV}(1^k, m^*, h^*, pk, \sigma^*) = 1$, then W wins.

We denote the event that W wins this game by $\mathsf{sWIN}_{\mathcal{C}}(W, k)$, where k is the security parameter. We define W's advantage against $\mathcal{SSD}$ with respect to $\mathcal{C}$ by

$$\mathbf{Adv}^{\mathsf{ucmha}}_{\mathcal{SSD},\mathcal{C}}(W, k) = \Pr[\mathsf{sWIN}_{\mathcal{C}}(W, k)],$$

where $(pk, sk) \leftarrow \mathcal{SG}(1^k)$. We say that $\mathcal{SSD}$ is *existentially unforgeable under the chosen message-and-history attack* (EUF-CMHA) if for every probabilistic polynomial adversary W, $\mathbf{Adv}^{\mathsf{ucmha}}_{\mathcal{SSD},\mathcal{C}}(W, k)$ is negligible in k.

4 The Construction of Steganographically-Secure and Unforgeable Scheme

In this section, we show how to construct the scheme with the steganographic security. We first define the security notion for digital signature called the indistinguishability from random bits under the chosen-message attack(IND\$-CMA). Then, we construct the steganographic signature scheme by using a digital signature scheme. We employ the idea for constructing the public-key steganography by Hopper [3]. We show that our scheme is steganographically secure if the underlying digital signature scheme satisfies IND\$-CMA. We also show that our scheme is unforgeable if the underlying digital signature scheme satisfies EUF-CMA.

4.1 The Indistinguishability from Random Bits

In this section, we define the security notion for digital signature called the indistinguishability from random bits under the chosen-message attack(IND\$-CMA).

Let $\mathcal{SD}$ be a digital signature scheme and k a security parameter. Let ℓ be the function which implies the length of the signature. We define a distinguishing game under the chosen-message attack against $\mathcal{SD}$ by an adversary A and a challenger. We consider the experiments $\mathbf{Exp}^i_{\mathbf{CMA}}$ for $i \in \{0, 1\}$ as follows:

$\mathbf{Exp}^0_{\mathbf{CMA}}$

1. A is given pk.
2. A produces $u^* \in \{0,1\}^k$ and passes u^* to the challenger. The challenger chooses $m^* \in \mathcal{M}$ randomly and computes $\sigma^* = \mathcal{S}(u^*||m^*, sk)$. Then the challenger passes σ^* to A.
3. A outputs a bit d.
4. Return d.

$\mathbf{Exp}^1_{\mathbf{CMA}}$

1. A is given pk.
2. A produces $u^* \in \{0,1\}^k$ and passes u^* to the challenger. The challenger chooses $\sigma^* \leftarrow U_\ell$. Then the challenger passes σ^* to A.
3. A outputs a bit d.
4. Return d.

In the above experiments, A can make access to the signing oracle $\mathcal{S}$. We define A's CMA advantage against $\mathcal{SD}$ by

$$\mathbf{Adv}^{\mathsf{icma}}_{\mathcal{SD},A}(k) = |\Pr[\mathbf{Exp}^0_{\mathbf{CMA}}(A(pk)) = 1] - \Pr[\mathbf{Exp}^1_{\mathbf{CMA}}(A(pk)) = 1]| \ ,$$

where $(pk, sk) \leftarrow \mathcal{G}(1^k)$. We also define the CMA insecurity of $\mathcal{SD}$ by

$$\mathbf{InSec}^{\mathsf{icma}}_{\mathcal{SD}}(t, q, \mu, c, l^*, k) = \max_{A \in \mathcal{A}(t,q,\mu,c,l^*)} \left\{ \mathbf{Adv}^{\mathsf{icma}}_{\mathcal{SD},A}(k) \right\},$$

where $\mathcal{A}(t, q, \mu, c, l^*)$ is the set of adversaries, that make q signing queries of total length μ and c challenge queries in running time t, and $l^* = |m^*|$. We say that $\mathcal{SD}$ is $(t, q, \mu, c, l^*, k, \epsilon)$-*indistinguishable from random bits under the chosen-message attack* if $\mathbf{InSec}^{\mathsf{icma}}_{\mathcal{SD}}(t, q, \mu, c, l^*, k) \leq \epsilon$. We say that $\mathcal{SD}$ is *indistinguishable from random bits under the chosen-message attack* (IND\$-CMA) if for every probabilistic polynomial adversary A, $\mathbf{Adv}^{\mathsf{icma}}_{\mathcal{SD},A}(k)$ is negligible in k.

4.2 The Construction

In this section, we construct the steganographic signature scheme by using a standard digital signature scheme. We employ the idea for constructing the public-key steganography by Hopper [3].

Hopper proposed the deterministic way to hide uniformly chosen bits, which we denote DEncode. Let $\mathcal{F}$ be a strongly universal family of hash functions $D \to \{0, 1\}$ and $f \in \mathcal{F}$. We assume that $\mathcal{C}$ is always informative and efficiently sampleable.

Procedure $\mathsf{DEncode}$:
Input: bits $c_1, \ldots, c_l$, history h, bound k, random values $r_1, \ldots, r_{lk} \in \{0,1\}^k$
Let $\iota = 1$; for $i = 1, \ldots, l$ do
Let $j = 0$;
repeat:
compute $s_i = \mathsf{channel}((h, s_{1\ldots i-1}), r_\iota)$; increment j, ι
until $f(s_i) = c_i$ or $j > k$
Output: $s_1, s_2, \ldots, s_l$

We now propose the steganographic signature scheme by using the standard digital signature scheme.

Definition 3. *Our proposed steganographic signature scheme $\mathcal{SSD} = (\mathcal{SG}, \mathcal{SS}, \mathcal{SV})$ is as follows. Let $\mathcal{SD} = (\mathcal{G}, \mathcal{S}, \mathcal{V})$ be a digital signature scheme. Let $G : \{0,1\}^k \to \{0,1\}^{k \times lk}$ be a hush function. Let $\mathcal{F}$ be a strongly universal family of hash functions $D \to \{0,1\}$ and $f \in \mathcal{F}$. We assume that $\mathcal{C}$ is always informative and efficiently sampleable.*

The key generation algorithm $\mathcal{SG}$ is the same as $\mathcal{G}$. The signing and verification algorithms are as follows:

Algorithm $\mathcal{SS}$*:*
Input: m, h, sk
Choose $u \leftarrow U_k$
Compute $\sigma = \mathcal{S}(u||m, sk)$
Output: $\mathsf{DEncode}(\sigma||u, h, k, G(u))$

Algorithm $\mathcal{SV}$*:*
Input: m, $\sigma_1, \ldots, \sigma_l$, h, pk
Compute $\sigma||_{l-k}u = f(\sigma_1)|| \cdots ||f(\sigma_l)$
If $\sigma_1|| \cdots ||\sigma_l \neq \mathsf{DEncode}(\sigma||u, h, k, G(u))$, $d = \perp$.
Otherwise, $d = \mathcal{V}(u||m, pk, \sigma)$
Output: d

We show that our scheme is steganographically secure if $\mathcal{SD}$ satisfies $\mathsf{IND\$\text{-}CMA}$ and G is a pseudorandom generator.

Theorem 4. *Let f be a function in $\mathcal{F}$ and let $\epsilon = \max_{h \in \mathcal{H}} \left\{ 2^{-H_\infty(\mathcal{C}_h^k)/2} \right\} = 2^{-\Omega(k)}$. Then*

$$\mathbf{InSec}^{\mathsf{cmha}}_{\mathcal{SSD},\mathcal{C}}(t, q, \mu, c, l, k) \leq \mathbf{InSec}^{\mathsf{icma}}_{\mathcal{SD}}(t', q, \mu', c, l, k) + c\mathbf{InSec}^{\mathsf{prg}}_{G}(t', k) + c\{\ell(l+k) + k\}\epsilon,$$

where $t' \leq t + O(lk)$ and $\mu' \leq \mu + qk$.

Proof. Let W be an adversary in $\mathcal{W}(t, q, \mu, c, l)$ who breaks the steganographic security of $\mathcal{SSD}$. We consider the case that $c = 1$. Let (pk, sk) be public and secret keys generated by $\mathcal{SG}(1^k)$. We consider the experiments $\mathbf{Exp}^i$ for $i \in \{1, 2, 3, 4, 5\}$ as follows:

$\mathbf{Exp}^i$

1. W is given pk.
2. W produces h^*. The challenger gives σ_i^* to W.
3. W outputs a bit d.
4. Return d.

In the above experiments, W can make access to the signing oracle $\mathcal{SS}$. We define σ_i for $i \in \{1,2,3,4,5\}$ as follows:

- $\sigma_1^* \leftarrow \mathcal{C}_{h^*}^{\ell(l+k)+k}$
- $\sigma_2^* = \mathsf{DEncode}(\hat{u}, h^*, k, U_{k\times lk})$,
  where $\hat{u} \leftarrow U_{\ell(l+k)+k}$
- $\sigma_3^* = \mathsf{DEncode}(u'||u^*, h^*, k, U_{k\times lk})$,
  where $u' \leftarrow U_{\ell(l+k)}$, $u^* \leftarrow U_k$
- $\sigma_4^* = \mathsf{DEncode}(u'||u^*, h^*, k, G(u^*))$,
  where $u' \leftarrow U_{\ell(l+k)}$, $u^* \leftarrow U_k$
- $\sigma_5^* = \mathsf{DEncode}(\mathcal{SS}(u^*||m)||u^*, h^*, k, G(u^*))$,
  where $u^* \leftarrow U_k$

Let $\mathbf{Adv}_W^i(k) = |\Pr[\mathbf{Exp}^{i+1}(W(pk)) = 1] - \Pr[\mathbf{Exp}^i(W(pk)) = 1]|$. Note that

$$\begin{aligned}\mathbf{Adv}_{\mathcal{SSD},\mathcal{C},W}^{\mathsf{scmha}}(k) &= \Big|\Pr[\mathbf{Exp}^5(W(pk)) = 1] - \Pr[\mathbf{Exp}^1(W(pk)) = 1]\Big| \\ &\le \sum_{i=1}^{4}\Big|\Pr[\mathbf{Exp}^{i+1}(W(pk)) = 1] - \Pr[\mathbf{Exp}^i(W(pk)) = 1]\Big| \\ &= \mathbf{Adv}_W^1(k) + \mathbf{Adv}_W^2(k) + \mathbf{Adv}_W^3(k) + \mathbf{Adv}_W^4(k).\end{aligned}$$

Thus we proceed to bound $\mathbf{Adv}_W^i(k)$ for $i \in \{1,2,3,4\}$. Hopper [3] proved that $\mathbf{Adv}_W^1(k) \le \{\ell(l+k)+k\}\epsilon$ and $\mathbf{Adv}_W^3(k) \le \mathbf{InSec}_G^{\mathsf{prg}}(t', k)$. The distribution of $\hat{u}$ is identical with that of $u'||u^*$. Therefore $\mathbf{Adv}_W^2(k) = 0$.

We prove that $\mathbf{Adv}_W^4(k) \le \mathbf{InSec}_{\mathcal{SD}}^{\mathsf{icma}}(t', q, \mu', 1, l^*, k)$. We construct an adversary A attacking the indistinguishability from random bits of $\mathcal{SD}$ by using W.

A takes a public key pk where $(pk, sk) \leftarrow \mathcal{G}(1^k)$ and passes it to W. If W makes a signing query (m, h), A chooses $u \leftarrow U_k$. A queries $u||m$ to A's signing oracle and receives σ_a which is a signature for $u||m$. A computes $\sigma_b = \mathsf{DEncode}(\sigma_a||u, h, k, G(u))$ and returns σ_b to W. In the challenge phase, W outputs h^* as its challenge. A chooses $u^* \leftarrow U_k$ and outputs u^* as its challenge. Then, A is given the challenge σ_a^* and returns $\sigma_b^* = \mathsf{DEncode}(\sigma_a^*||u^*, h^*, k, G(u^*))$ to W. A continues to respond signing queries of W as before.

Finally, if W outputs a bit d, A outputs the same bit d.

Notice that when A is given a signature of $u^*||m^*$ (m^* is chosen randomly), A perfectly simulates $\mathbf{Exp}^5$ for W. Therefore $\Pr[\mathbf{Exp}_{\mathbf{CMA}}^0(A(pk)) = 1] = \Pr[\mathbf{Exp}^5(W(pk)) = 1]$. On the other hand, when A is given a random string, A perfectly simulates $\mathbf{Exp}^4$ for W. Therefore $\Pr[\mathbf{Exp}_{\mathbf{CMA}}^1(A(pk)) = 1] = \Pr[\mathbf{Exp}^4(W(pk)) = 1]$. Then we have that

$$\begin{aligned}\mathbf{Adv}_W^4(k) &= \big|\Pr[\mathbf{Exp}^5(W(pk)) = 1] - \Pr[\mathbf{Exp}^4(W(pk)) = 1]\big| \\ &= \big|\Pr[\mathbf{Exp}_{\mathbf{CMA}}^0(A(pk)) = 1] - \Pr[\mathbf{Exp}_{\mathbf{CMA}}^1(A(pk)) = 1]\big| \\ &= \mathbf{Adv}_{\mathcal{SD},A}^{\mathsf{icma}}(k).\end{aligned}$$

We can consider the case that $c > 1$ by applying the hybrid arguments to the analysis of $\mathbf{Adv}_W^1(k)$ and $\mathbf{Adv}_W^3(k)$, and get the claimed result. $\square$

We show that our scheme is unforgeable if $\mathcal{SD}$ satisfies EUF-CMA.

Theorem 5. *Let $\mathcal{SD}$ be a digital signature scheme and $\mathcal{SSD}$ our proposed steganographic signature scheme with $\mathcal{SD}$. If $\mathcal{SD}$ satisfies* EUF-CMA*, then $\mathcal{SSD}$ satisfies* EUF-CMHA.

Proof. We assume that $\mathcal{SSD}$ does not satisfy EUF-CMHA. Then, a probabilistic polynomial adversary W that can forge a steganographic signature exists. We construct an adversary A that forges a signature of $\mathcal{SD}$ by using W.

A takes a public key pk where $(pk, sk) \leftarrow \mathcal{G}(1^k)$ and passes it to W. If W makes a signing query (m, h), A chooses $u \leftarrow U_k$. A queries $u||m$ to A's signing oracle and receives σ which is a signature for $u||m$. A computes $\sigma' = \mathsf{DEncode}(\sigma||u, h, k, G(u))$ and returns σ' to W.

W outputs (m^*, h^*, σ^*) where $\sigma^* = \sigma_1^*|| \cdots ||\sigma_z^*$. A computes $\hat{\sigma} = f(\sigma_1^*)|| \cdots ||f(\sigma_z^*)$ and parses $\hat{\sigma} = \tilde{\sigma}||u^*$ where $|u^*| = k$. A outputs $(u^*||m^*, \tilde{\sigma})$. By construction, $\tilde{\sigma}$ is a valid signature for $u^*||m^*$. Therefore, $\mathcal{SD}$ does not satisfy EUF-CMA. $\square$

5 A Concrete Scheme Based on the Extended Schnorr Signature Scheme

In this section, we review the extended Schnorr signature scheme [9]. This is almost the same as the original Schnorr signature scheme [6]. In the extended Schnorr signature scheme, we expand the signature space. The public key contains an additional parameter $b \in \mathbb{N}$ which decides the extended space of signatures.

5.1 The Extended Schnorr Signature Scheme

Let k be a security parameter. The public key pk consists of a set of the group parameters $\mathcal{I} = (p, q, g, G, R)$, an element $y \in G$, and $b \in \mathbb{N}$. The secret key sk is an element $x \in \mathbb{Z}_q$ such that $y = g^x \bmod p$. The values p and q are large primes such that $q|p-1$. G is a subgroup in $\mathbb{Z}_p^*$ of order q and g is a generator of G such that computing discrete logarithms in G is difficult. $R : \{0,1\}^* \rightarrow \{0,1\}^k$ is a hash function where $2^k < q$. The value b is a parameter such that 2^b is $(k+1)$ bits longer than q. Let n be the largest number such that $nq < 2^b$.

Signing algorithm. On input a message $m \in \mathcal{M}$ and the secret key x, $\mathcal{S}(m, x)$ is computed as follows:

1. Choose $w \in \mathbb{Z}_q$ randomly and compute $t = g^w \bmod p$.
2. Compute $r = R(t, m)$ and $s = w - xr \bmod q$.
3. Choose $\lambda \in \{0, 1, \ldots, n-1\}$ randomly and compute $s' = s + \lambda q$.

The signature for m is $r||s'$.

Verification algorithm. To verify a signature $r||s'$ for message m with the public key $(\mathcal{I}, y, b)$, compute $s = s' \bmod q$ and $t = g^s y^r \bmod p$ and output 1 if $r = R(t, m)$. Otherwise, output 0.

We can easily see that if the original Schnorr signature scheme satisfies EUF-CMA, then the extended Schnorr signature scheme also satisfies EUF-CMA.

5.2 A Steganographic Signature Scheme

We show that the extended Schnorr signature scheme satisfies IND\$-CMA in the random oracle model. We denote what challenge query of the adversary of IND\$-CMA was limited to one time by IND\$-CMA1. We first show that the extended Schnorr signature scheme satisfies IND\$-CMA1 in the random oracle model, and next show that IND\$-CMA1 $\Rightarrow$ IND\$-CMA.

Theorem 6. *Let $\mathcal{SD}$ be the extended Schnorr signature scheme and $(pk, sk) = (((p, q, g, G, R), y, b), x)$. We assume that R is a random oracle. Then, $\mathcal{SD}$ satisfies* IND\$-CMA1.

Proof. Let A be a probabilistic polynomial adversary of $\mathcal{SD}$. We assume that A queries to the signing oracle $\mathcal{S}$ $q_{\mathcal{S}}$ times and to a random oracle R q_R times. We consider the experiments $\mathbf{Exp}^i_{\mathbf{ES}}$ for $i \in \{1, 2, 3, 4, 5, 6\}$ as follows:

$\mathbf{Exp}^i_{\mathbf{ES}}$

1. A is given pk.
2. A produces $u^* \in \{0, 1\}^k$ and passes u^* to the challenger. The challenger gives $r_i||s'_i$ to A.
3. A outputs a bit d.
4. Return d.

We define $r_i||s'_i$ for $i \in \{1, 2, 3, 4, 5, 6\}$ as follows:

- $r_1||s'_1$: The challenger chooses $m \in \mathcal{M}$ randomly, $w \in \mathbb{Z}_q$ randomly, and computes $t = g^w \bmod p$. The challenger computes $r_1 = R(u^*||m, t)$ and $s_1 = w - xr_1 \bmod q$. The challenger chooses $\lambda \in \{0, 1, \ldots, n-1\}$ randomly and computes $s'_1 = s_1 + \lambda q$. Then the challenger makes $r_1||s'_1$.
- $r_2||s'_2$: The challenger chooses $m \in \mathcal{M}$ randomly, $w \in \mathbb{Z}_q$ randomly, and computes $t = g^w \bmod p$. The challenger chooses $r_2 \leftarrow U_k$ and computes $s_2 = w - xr_2 \bmod q$. The challenger chooses $\lambda \in \{0, 1, \ldots, n-1\}$ randomly and computes $s'_2 = s_2 + \lambda q$. Then the challenger makes $r_2||s'_2$.
- $r_3||s'_3$: The challenger chooses $m \in \mathcal{M}$ randomly, $w \in \mathbb{Z}_q$ randomly, and computes $t = g^w \bmod p$. The challenger chooses $r_3 \leftarrow U_k$ and computes $s_3 = w - xr_3 \bmod q$. The challenger chooses $\lambda \in \{0, 1, \ldots, n-1\}$ randomly and computes $s'_3 = s_3 + \lambda q$. Then the challenger makes $r_3||s'_3$.
- $r_4||s'_4$: The challenger chooses $m \in \mathcal{M}$ randomly. The challenger chooses $r_4 \leftarrow U_k$ and $s_4 \in \mathbb{Z}_q$ randomly. The challenger computes $w = s_4 + xr_4 \bmod q$ and $t = g^w \bmod p$. The challenger chooses $\lambda \in \{0, 1, \ldots, n-1\}$ randomly and computes $s'_4 = s_4 + \lambda q$. Then the challenger makes $r_4||s'_4$.
- $r_5||s'_5$: The challenger chooses $m \in \mathcal{M}$ randomly. The challenger chooses $r_5 \leftarrow U_k$, $s'_5 \in \{0, 1, \ldots, nq-1\}$ randomly, and computes $s_5 = s'_5 \bmod q$. The challenger computes $w = s_5 + xr_5 \bmod q$ and $t = g^w \bmod p$. Then the challenger makes $r_5||s'_5$.
- $r_6||s'_6$: The challenger chooses $m \in \mathcal{M}$ randomly. The challenger chooses $r_6 \leftarrow U_k$, $s'_6 \leftarrow U_b$, and computes $s_6 = s'_6 \bmod q$. The challenger computes $w = s_6 + xr_6 \bmod q$ and $t = g^w \bmod p$. Then the challenger makes $r_6||s'_6$.

In the above experiments, A can make access to the signing oracle $\mathcal{S}$ and a random oracle R. However, there is a following restriction in $\mathbf{Exp}^2_{\mathbf{ES}}$: if A queries $(u^*||m, t)$ to R, R returns r_2 rather than $R(u^*||m, t)$.

Let $\mathbf{Adv}^i_A(k) = |\Pr[\mathbf{Exp}^i_{\mathbf{ES}}(A(pk)) = 1] - \Pr[\mathbf{Exp}^{i+1}_{\mathbf{ES}}(A(pk)) = 1]|$. Note that A's advantage is $|\Pr[\mathbf{Exp}^1_{\mathbf{ES}}(A(pk)) = 1] - \Pr[\mathbf{Exp}^6_{\mathbf{ES}}(A(pk)) = 1]|$. Then,

$$\begin{aligned}
\mathbf{Adv}^{\mathsf{icma}}_{\mathcal{SD},A}(k) &= \left|\Pr[\mathbf{Exp}^1_{\mathbf{ES}}(A(pk)) = 1] - \Pr[\mathbf{Exp}^6_{\mathbf{ES}}(A(pk)) = 1]\right| \\
&= \left|\sum_{i=1}^{5}\Big(\Pr[\mathbf{Exp}^i_{\mathbf{ES}}(A(pk)) = 1] - \Pr[\mathbf{Exp}^{i+1}_{\mathbf{ES}}(A(pk)) = 1]\Big)\right| \\
&\leq \sum_{i=1}^{5}\left|\Pr[\mathbf{Exp}^i_{\mathbf{ES}}(A(pk)) = 1] - \Pr[\mathbf{Exp}^{i+1}_{\mathbf{ES}}(A(pk)) = 1]\right| \\
&= \mathbf{Adv}^1_A(k) + \mathbf{Adv}^2_A(k) + \mathbf{Adv}^3_A(k) + \mathbf{Adv}^4_A(k) + \mathbf{Adv}^5_A(k).
\end{aligned}$$

We bound $\mathbf{Adv}^i_A(k)$ for $i \in \{1,2,3,4,5\}$. A's condition given in $\mathbf{Exp}^2_{\mathbf{ES}}$ is identical with that in $\mathbf{Exp}^1_{\mathbf{ES}}$. Therefore $\mathbf{Adv}^1_A(k) = 0$. $\mathbf{Exp}^3_{\mathbf{ES}}$ is identical with $\mathbf{Exp}^2_{\mathbf{ES}}$ if A does not query $(u^*||m, t)$ to R. We denote the event that A queries $(u^*||m, t)$ to R by E. Then

$$\begin{aligned}
\mathbf{Adv}^2_A(k) &= \Big| \Pr[\mathbf{Exp}^2_{\mathbf{ES}}(A(pk)) = 1] - \Pr[\mathbf{Exp}^3_{\mathbf{ES}}(A(pk)) = 1] \Big| \\
&= \Big| \Big(\Pr[\mathsf{E}] \Pr[\mathbf{Exp}^2_{\mathbf{ES}}(A(pk)) = 1 \mid \mathsf{E}] \Pr[\overline{\mathsf{E}}] \Pr[\mathbf{Exp}^2_{\mathbf{ES}}(A(pk)) = 1 \mid \overline{\mathsf{E}}] \Big) \\
&\quad - \Big(\Pr[\mathsf{E}] \Pr[\mathbf{Exp}^3_{\mathbf{ES}}(A(pk)) = 1 \mid \mathsf{E}] + \Pr[\overline{\mathsf{E}}] \Pr[\mathbf{Exp}^3_{\mathbf{ES}}(A(pk)) = 1 \mid \overline{\mathsf{E}}] \Big) \Big| \\
&\leq \Pr[\mathsf{E}] \Big| \Pr[\mathbf{Exp}^2_{\mathbf{ES}}(A(pk)) = 1 \mid \mathsf{E}] - \Pr[\mathbf{Exp}^3_{\mathbf{ES}}(A(pk)) = 1 \mid \mathsf{E}] \Big| \\
&\leq \Pr[\mathsf{E}].
\end{aligned}$$

t is used to compute s_2 and s_3, therefore A may get the value t somehow. However, m is chosen randomly from $\mathcal{M}$. Then,

$$\begin{aligned}
\Pr[\mathsf{E}] &\leq 1 - \frac{|\mathcal{M}| - 1}{|\mathcal{M}|} \cdot \frac{|\mathcal{M}| - 2}{|\mathcal{M}| - 1} \cdot \cdots \cdot \frac{|\mathcal{M}| - q_R}{|\mathcal{M}| - (q_R - 1)} \\
&= \frac{q_R}{|\mathcal{M}|}.
\end{aligned}$$

When we compare $\mathbf{Exp}^4_{\mathbf{ES}}$ with $\mathbf{Exp}^3_{\mathbf{ES}}$, the order to choose random values is changed. However, the distribution of s_4 is identical with that of s_3. Therefore $\mathbf{Adv}^3_A(k) = 0$. The same, $\mathbf{Adv}^4_A(k) = 0$. The difference between $\mathbf{Exp}^6_{\mathbf{ES}}$ and $\mathbf{Exp}^5_{\mathbf{ES}}$ is a distribution of s'. We denote an uniform distribution on $\{0, 1, \ldots, nq-1\}$ by $\mathcal{D}$. Since 2^b is $(k+1)$ bits longer than q and $nq < 2^b \leq (n+1)q$, we have $2^{k+1} + 1 < n$. Then,

$$\begin{aligned}
\|\mathcal{D} - U_b\| &= \frac{1}{2} \left\{ nq \left(\frac{1}{nq} - \frac{1}{2^b} \right) + (2^b - nq) \frac{1}{2^b} \right\} \\
&= 1 - \frac{nq}{2^b} \\
&\leq 1 - \frac{nq}{(n+1)q} = \frac{1}{n+1} < \frac{1}{2^{k+1} + 2}.
\end{aligned}$$

Therefore $\mathbf{Adv}^5_A(k) \leq 1/(2^{k+1} + 2)$. Combining these, $\mathbf{Adv}^{\mathsf{icma}}_{\mathcal{SD},A}(k)$ is negligible. □

We show that IND\$-CMA1 $\Rightarrow$ IND\$-CMA.

Theorem 7. *Let $\mathcal{SD}$ be a digital signature scheme. If $\mathcal{SD}$ satisfies* IND\$-CMA1*, then $\mathcal{SD}$ satisfies* IND\$-CMA.

Proof. Let A_c be an adversary attacking IND\$-CMA of $\mathcal{SD}$ and A_1 an adversary attacking IND\$-CMA1 of $\mathcal{SD}$. We consider the experiments $\mathbf{Exp}^i_{\mathbf{CC}}$ for $i \in \{1, \ldots, c\}$ as follows:

$\mathbf{Exp}^i_{\mathbf{CC}}$

1. A_c is given pk.
2. On j-th challenge query, A_c produces $u^*_j \in \{0,1\}^k$ and passes u^*_j to the challenger. If $i \geq j$, the challenger chooses $m \in \mathcal{M}$ randomly and computes $\sigma_j = \mathcal{S}(u^*_j||m, sk)$. Otherwise, the challenger chooses $\sigma_j \leftarrow U_\ell$. Then the challenger passes σ_j to A_c.
3. A_c outputs a bit d.
4. Return d.

In the above experiments, A_c can make access to signing oracle $\mathcal{S}$. Note that A_c's advantage is $|\Pr[\mathbf{Exp}^c_{\mathbf{CC}}(A_c(pk)) = 1] - \Pr[\mathbf{Exp}^0_{\mathbf{CC}}(A_c(pk)) = 1]|$. Then,

$$
\begin{aligned}
\mathbf{Adv}^{\mathsf{icma}}_{\mathcal{SD},A_c}(k) &= \Big|\Pr[\mathbf{Exp}^c_{\mathbf{CC}}(A_c(pk)) = 1] - \Pr[\mathbf{Exp}^0_{\mathbf{CC}}(A_c(pk)) = 1]\Big| \\
&= \Big|\sum_{j=1}^{c}\Big(\Pr[\mathbf{Exp}^j_{\mathbf{CC}}(A_c(pk)) = 1] - \Pr[\mathbf{Exp}^{j-1}_{\mathbf{CC}}(A_c(pk)) = 1]\Big)\Big| \\
&\leq \sum_{j=1}^{c}\Big|\Pr[\mathbf{Exp}^j_{\mathbf{CC}}(A_c(pk)) = 1] - \Pr[\mathbf{Exp}^{j-1}_{\mathbf{CC}}(A_c(pk)) = 1]\Big|.
\end{aligned}
$$

We show that $|\Pr[\mathbf{Exp}^j_{\mathbf{CC}}(A_c(pk)) = 1] - \Pr[\mathbf{Exp}^{j-1}_{\mathbf{CC}}(A_c(pk)) = 1]| \leq \mathbf{Adv}^{\mathsf{icma}}_{\mathcal{SD},A_1}(k)$ for $j \in \{1, \ldots, c\}$. We construct A_1 attacking IND\$-CMA1 by using A_c.

A_1 takes a public key pk where $(pk, sk) \leftarrow \mathcal{G}(1^k)$ and passes it to A_c. If A_c makes a signing query m, A_1 queries m to A_1's signing oracle and receives σ which is a signature for m. A_1 returns σ to A_c. In the challenge phase, A_1 responds to A_c's e-th challenge query u^*_e as follows:

- If $1 \leq e \leq j-1$, A_1 chooses $m \in \mathcal{M}$ randomly and queries $u^*_e||m$ to A_1's signing oracle and receives $\sigma_e = \mathcal{S}(u^*_e||m, sk)$. A_1 passes σ_e to A_c.
- If $e = j$, A_1 queries u^*_e as its challenge query and receives its challenge. A_1 passes it as σ_e to A_c.
- If $e \geq j+1$, A_1 chooses $\sigma_e \leftarrow U_\ell$ and passes σ_e to A_c.

Finally, if A_c outputs a bit d, A_1 outputs the same bit d. Then we have that $|\Pr[\mathbf{Exp}^j_{\mathbf{CC}}(A_c(pk)) = 1] - \Pr[\mathbf{Exp}^{j-1}_{\mathbf{CC}}(A_c(pk)) = 1]| \leq \mathbf{Adv}^{\mathsf{icma}}_{\mathcal{SD},A_1}(k)$ and $\mathbf{Adv}^{\mathsf{icma}}_{\mathcal{SD},A_c}(k) \leq c\mathbf{Adv}^{\mathsf{icma}}_{\mathcal{SD},A_1}(k)$. If $\mathbf{Adv}^{\mathsf{icma}}_{\mathcal{SD},A_c}(k)$ is non-negligible, then $\mathbf{Adv}^{\mathsf{icma}}_{\mathcal{SD},A_1}(k)$ is also non-negligible. □

From Theorem 4, our proposed steganographic signature scheme with the extended Schnorr signature scheme is steganographically secure in the random oracle model.

The extended Schnorr signature scheme satisfies EUF-CMA in the random oracle model. Therefore, from Theorem 5, our proposed steganographic signature scheme with the extended Schnorr signature scheme is unforgeable in the random oracle model.

6 Conclusion

We have formalized and proposed the steganographic signature schemes. We have defined the security notion of steganographic signature, the steganographic security and the unforgeability. In order to construct the steganographic signature scheme satisfying the steganographic security, we have defined the security notion of digital signature, IND\$-CMA. We have shown that the extended Schnorr signature scheme satisfies this notion in the random oracle model. We have also shown that our proposed steganographic signature scheme with the extended Schnorr signature scheme is steganographically secure and unforgeable in the random oracle model.

References

[1] Backes, M., and Cachin, C. Public-key steganography with active attacks. In *TCC* (2005), J. Kilian, Ed., vol. 3378 of *Lecture Notes in Computer Science*, Springer, pp. 210–226.

[2] Canetti, R., Krawczyk, H., and Nielsen, J. B. Relaxing chosen-ciphertext security. In *Advances in Cryptology – CRYPTO 2003* (Santa Barbara, California, USA, August 2003), D. Boneh, Ed., vol. 2729 of *Lecture Notes in Computer Science*, Springer-Verlag, pp. 565–582.

[3] Hopper, N. On steganographic chosen covertext security. In *ICALP* (2005), L. Caires, G. F. Italiano, L. Monteiro, C. Palamidessi, and M. Yung, Eds., vol. 3580 of *Lecture Notes in Computer Science*, Springer, pp. 311–323.

[4] Hopper, N. J., Langford, J., and von Ahn, L. Provably Secure Steganography. In *Advances in Cryptology – CRYPTO 2002* (Santa Barbara, California, USA, August 2002), M. Yung, Ed., vol. 2442 of *Lecture Notes in Computer Science*, Springer-Verlag, pp. 77–92.

[5] Le, T. V., and Kurosawa, K. Efficient public key steganography secure against adaptively chosen stegotext attacks. Cryptology ePrint Archive, Report 2003/244.

[6] Schnorr, C. P. Efficient identification and signatures for smart cards. In *Advances in Cryptology – CRYPTO '89* (Santa Barbara, California, USA, August 1989), G. Brassard, Ed., vol. 435 of *Lecture Notes in Computer Science*, Springer-Verlag, pp. 239–252.

[7] von Ahn, L., and Hopper, N. J. Public-Key Steganography. In *Advances in Cryptology – EUROCRYPT 2004* (Interlaken, Switzerland, May 2004), C. Cachin and J. Camenisch, Eds., vol. 3027 of *Lecture Notes in Computer Science*, Springer-Verlag, pp. 323–341.

[8] Wegman, M. N., and Carter, L. New hash functions and their use in authentication and set equality. *J. Comput. Syst. Sci. 22*, 3 (1981), 265–279.

[9] Yang, G., Wong, D. S., Deng, X., and Wang, H. Anonymous signature schemes. In *Public Key Cryptography* (2006), M. Yung, Y. Dodis, A. Kiayias, and T. Malkin, Eds., vol. 3958 of *Lecture Notes in Computer Science*, Springer, pp. 347–363.