An Essay on Unconditionally or Information-Theoretically Secure Cryptographic Protocols*

A Tutorial Organized by IEICE Technical Committee on Information Security
Tokyo, 18 May 2006

Tsutomu Matsumoto
Graduate School of Environment and Information Sciences
Yokohama National University

* This presentation is based on discussions with Junji Shikata and other members of cryptography research group in my research lab. at Yokohama National University.
Agenda

• What is Unconditional Security?
• Authenticated Encryption (TI model)
• Stegosystems (TI model)
• Unconditionally Secure Blind Signature Scheme (TI model)
• Summary
Introduction
How can we guarantee security theoretically?

• Underlying theories to guarantee security are:
  – Complexity Theory
  – Information Theory
  – Others
Security

• **Computational Security**
  – Underlying theory is *complexity theory*
  – Security is proved based on *computational assumption* such as hardness of solving the integer factoring and the discrete logarithm.
  – The computational power of an adversary is assumed to be *limited* (adversary’s computational power is of polynomial order).

• **Unconditional Security (Information-theoretic Security)**
  – Underlying theory is *information theory*
  – Security is proved based on some assumption, but *no computational assumption* is required.
  – The computational power of an adversary is assumed to be *unlimited* (i.e. infinite computational power).
Computational security

v.s.

Unconditional security

In general, ....

- Computationally secure schemes
  - Small memory size
  - Dependent on computational assumptions

- Unconditionally secure schemes
  - Larger memory size
  - Independent of computational assumptions (but often require some other assumptions)
Models for Unconditional Security Setting (1)

- **Trusted Initializer (TI) model**
  - In the initial step, an off-line trusted initializer distributes users’ secrets in a secure manner.

- **Shared Key model**
  - In the initial step, two or more users share a common key in a secure manner.

- **Private Channel model**
  - For any pair of users, a private channel is established in advance.

- **Broadcast Channel model**
  - There exists a broadcast channel for all users.
Models for Unconditional Security Setting (2)

- **Quantum Channel Model (Quantum Cryptography)**
  - For a pair of users, there exists a quantum channel.

- **Bounded Storage Model**
  - The size of an adversary’s storage is limited.

- **Noisy Channel Model**
  - For a pair of users, there exists a noisy channel.

These three models are based on physical assumptions, which in turn provide more efficient schemes.
**Trusted Initializer (TI) Model**

- A trusted initializer (TI) distributes users’ secrets only in the initial step.
  - TI deletes his memory after distributing the keys.
- Simple model for unconditional setting
Authenticated Encryption

This Terminology is used when the target encryption scheme is expected to have integrity capability.
Authenticated Encryption
(TI model, two party ← for simplicity)

• Entities: S (sender), R (receiver),
  TA (trusted authority)

• Spaces:
  – M: space of plaintexts
  – C: space of ciphertexts
  – E: space of encryption keys
  – D: space of decryption keys
Authenticated Encryption
(TI model, two party)

- GEN: key generation algorithm
- ENC: encryption algorithm
- DEC: decryption algorithm

\[ c = \text{ENC}(e, m) \]
\[ \text{DEC}(d, c) = m \text{ (or } \bot \text{)} \]

\[ (e, d) = \text{GEN}(k) \]

Symmetric case: \( e = d \)
Asymmetric case: \( e \neq d \)

Secure channel
Public channel
A Map of Theoretical Studies on Authenticated Encryption

<table>
<thead>
<tr>
<th>Active Attacks</th>
<th>Unconditional Security</th>
<th>Computational Security</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>[McAven, Safavi-Naini, Yung: 04]</td>
<td></td>
</tr>
<tr>
<td>Classical Attacks</td>
<td>[Simmons: 84]</td>
<td></td>
</tr>
<tr>
<td></td>
<td>[Stinson:88] etc.</td>
<td></td>
</tr>
</tbody>
</table>
Security Notions of AE
(Confidentiality)

• Goals

1. Perfect Secrecy (PS) [Shannon49]:
   - It is difficult for the adversary to derive any partial information on the plaintext from a target ciphertext.

2. Almost Perfect Secrecy (APS):
   - The partial information on the plaintext from a target ciphertext which the adversary can derive might exist, but it is very small.

3. Non-Malleability (NM):
   - From a ciphertext c of a plaintext m, the adversary cannot create a ciphertext c’ of a plaintext m’ which is meaningfully related to m.
Security Notions of AE (Authenticity)

1. Integrity of Ciphertexts (IntC) (cf. [BN00]):
   • It is difficult for the adversary to create a ciphertext \( c \) that has not been previously created by the sender but will be accepted by the receiver.

2. Integrity of Plaintexts (IntP) (cf. [BN00]):
   • It is difficult for the adversary to create a ciphertext \( c \) that will be accepted by the receiver but the underlying plaintext has not been created by the sender.
Security Notions of AE

• Attacking models
  – Chosen Plaintext Attacks and Chosen Ciphertext Attacks (CPA&CCA):
    – Attacks using the information which the adversary obtains by having an access to both the encryption oracle and the decryption oracle.
Conditions

Security is considered under the following conditions.

• t is the number:
  – up to which the sender is allowed to encrypt plaintexts; and
  – up to which the receiver is allowed to decrypt ciphertexts
Relation among Notions of AE


- **Theorem:** \( \text{IntC} \rightarrow \text{IntP} \)

- **Theorem:** \( \text{APS} \land \text{IntC} \iff \text{NM} \land \text{IntC} \)

- **Definition:** An authenticated encryption \( \Pi \) is \((\varepsilon, t)\)-secure against CPA and CCA, if the attacking probability for the following notions is at most \(\varepsilon\):
  1. APS: Almost Perfect Secrecy; and
  2. IntC: Integrity of Ciphertext.
Security Definitions of AE

• **Definition (IntC)**

The following probability is at most \( \varepsilon \):

\[
P_{\text{IntC}} := \max_{(M_S, C_R)} \max_c \Pr \left( \text{R's decryption result of } c \text{ is not } \bot \mid M_S, C_R \right)
\]

- \( M_S \) is taken over \( P(M \times C, t) \)
- \( C_R \) is taken over \( P(C \times (M \cup \{ \bot \}), t-1) \)
- \( c \) is taken over ciphertexts such that \( c \) does not appear in \( M_S \) and \( C_R \)

[Notation]

- \( T \): set, \( n \): non-negative integer,

\[
P(T, n) := \{X \mid X \text{ is a subset of } T \text{ and } |X| \leq n\}
\]
Security Definitions of AE

• **Definition (APS)**
  The following probability is at most $\varepsilon$:
  \[ P^{\text{APS}} := \max_{(M_S, C_R)} \max_c \sum_m | \Pr(m | c, M_S, C_R) - \Pr(m) | \]

  • $M_S$ is taken over $P(M \times C, t-1)$
  • $C_R$ is taken over $P(C \times (M \cup \{ \bot \}), t-1)$
  • $c$ is taken over valid ciphertexts such that $c$ does not appear in $M_S$ and $C_R$
Security Definitions of AE

• **Definition (Ciphertext Randomness)**
  The following probability is at most $\varepsilon$:
  \[
  P^{CR} := \max_{z = (M_S, C_R)} \sum_c \left| \Pr_{C|Z=z} (c) - \Pr_{\text{uniform}} (c) \right|
  \]

• $M_S$ is taken over $P(M \times C, t-1)$
• $C_R$ is taken over $P(C \times (M \cup \{⊥\}), t-1)$
Stegosystems
What is a Stegosystem?

- Prisoner’s Problem
  ([Simmons 83])

Alice → Wendy → Bob

Warden
detect
c (covertext)

Public channel

Prisoner

Prisoner
What is a Stegosystem?

• Stegosystems
  – Systems which hide the *presence* of a message (while encryption schemes hide the *content* of a message).

• The purpose is, *from an information-theoretic viewpoint*,
  – to provide security notions for stegosystems; and
  – to propose a construction method which meets the security definitions.
A Simple Model

Embedding (Encoding)

Stego-key $e$

Cover-data $c$

Embedded (hidden) data $m$

Extracting (Decoding)

Stego-data $s$

Stego-key $e$

Embedded (hidden) data $m$
Attacks (Informal Def.)

• Passive attacks
  – The attacker is only able to analyze the data he could intercept. (valid in read-only public channel)

• Active attacks
  – The attacker is allowed to modify the data.
  – The attacker can obtain some additional information from steganographic algorithms equipped with secret keys.
Security Goals (Informal Def.)

- What is security in steganography?
  - It is difficult for the adversary to detect the presence or absence of embedded data.
  - It is difficult for the adversary to read the embedded data. (security of cryptosystems)
### A Map of Theoretical Studies on Steganography

<table>
<thead>
<tr>
<th>Active attacks</th>
<th>Information-Theoretic Security</th>
<th>Computational Security</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>[Shikata, Matsumoto: SCIS04]</td>
<td>[Hopper, Langford, von Ahn: Crypto02]</td>
</tr>
<tr>
<td></td>
<td>[Shikata, Takanohashi, Matsumoto: SCIS05]</td>
<td>[Dedic, Itkis, Reyzin, Russell: TCC05]</td>
</tr>
<tr>
<td></td>
<td>[Matsumoto, Shikata: ITW05 Japan]</td>
<td>etc.</td>
</tr>
<tr>
<td>Passive attacks</td>
<td>etc.</td>
<td>[Backs, Cachin: TCC05]</td>
</tr>
<tr>
<td></td>
<td>[Cachin: Info. Hiding98]</td>
<td>[van Lee, Kurosawa: 03]</td>
</tr>
<tr>
<td></td>
<td>[Cachin: Info. and Comp. 04]</td>
<td>etc.</td>
</tr>
<tr>
<td></td>
<td>[Zhang, Li: ACNS04] etc.</td>
<td></td>
</tr>
</tbody>
</table>
Related Works

  - Informal discussion about steganography: history, model, security, etc.
  - Formal model and security definitions are not discussed.
Related Works
(Def. of Steganography)

  – Formal security definition (by entropy):
    knowledge of stego-data and cover-data do not decrease the uncertainty about embedded data
    \[ H(M \mid S, C) = H(M) \]
Related Works  
(Def. of Steganography)

- [T. Mittelholzer: 1999]
  - Formal security definition (by distortion):
    perfect secrecy for the embedded message and
    the encoder constraint imposed in terms of a
    distortion measure (e.g. expected mean squared
    error distorsion) between cover-data and stego-
    data

\[
E[d(c, s)] < \delta
\]
\[
c = (c_1, c_2, \ldots, c_n), s = (s_1, s_2, \ldots, s_n),
\]
\[
(e.g. d(c, s) = (1/n) \sum (c_i - s_i)^2)
\]
Related Works
(Def. of Steganography)

• [C. Cachin: 1998]
  – Formal security definition (by divergence, relative entropy):
    it is difficult for the adversary to detect the presence of embedded data, that is, difficult to distinguish stego-data from cover-data.
    \[ D(P_C \parallel P_S) < \varepsilon \]
Related Works
(Def. of Steganography)

• [W. Zhang, S. Li: 2004]
  – Formal security definition (by variational distance):
    it is difficult for the adversary to detect the presence of embedded data, that is, difficult to distinguish stego-data from cover-data.
    \[d(P_C, P_S) < \varepsilon\]
    \[
    (d(P_C, P_S) = \sum |P_C(c) - P_S(c)|)
    \]
Example ([C. Cachin: 98])

- Secure or Insecure?

\[ c = (c_1, c_2, \ldots, c_n): \text{even parity} \]

\[ s_1 = c_1 + k \]

\[ s = (s_1, c_2, \ldots, s_n): \text{odd parity} \]

[J. Zollner et al: 98], [T. Mittelholzer: 99]: Secure

[C. Cachin: 98] [W. Zhang, S. Li: 04]: Insecure
Model (TI model, two party ← for simplicity)

- Public channel: insecure channel where the adversary can read and write a message
- Entities: S (sender), R (receiver), TA (trusted authority)
- Spaces:
  - \( C \): space of covertexts
  - \( \tilde{C} = C^{lc} \): space of sequences of covertexts (with length \( l_c \))
    (Assumption: any sequence of covertexts over the public channel consists of independent repetitions of covertexts)
  - \( M \): space of hiddentexts (or embedded texts)
  - \( S \): space of stegotexts
  - \( E \): space of secret keys for embedding
  - \( D \): space of secret keys for extracting
  - \( Y = S \) or \( \tilde{C} \)
**Model (TI model, two party)**

- Gen: key generation algorithm
- Emb: embedding algorithm
- Ext: extracting algorithm

\[
\begin{align*}
&\text{Secure channel} \\ &e \quad \text{Secure channel} \\ &\text{Public channel} \\ &\text{Secure channel} \\
&\text{Symmetric case: } e = d \\
&\text{Asymmetric case: } e \neq d
\end{align*}
\]

\[
\begin{align*}
&\text{TA} \\
&(e, d) = \text{Gen}(k) \\
&s = \text{Emb}(e, \tilde{c}, m) \\
&\tilde{c} \text{ or } s \\
&\text{Ext}(d, y) = m \text{ or } \bot \\
&(y = \tilde{c} \text{ or } s)
\end{align*}
\]
Properties: \((\delta_1, \delta_2)\)-stegosystem

1. Reliability [Hopper, Langford, von Ahn 02]
   - If the receiver obtains a valid stegotext, the original hiddentext can be correctly extracted from the stegotext with large probability:

   For any hiddentext \(m\),
   \[
   \delta_1 := \Pr\left(\text{Ext}(d, \text{Emb}(e, \tilde{c}, m)) = m\right)
   \]

   is large, where \((e, d)\) is a possible pair of an embedding key and an extracting key.
Properties: \((\delta_1, \delta_2)-\text{stegosystem}\)

2. *Soundness* [Matsumoto, Shikata 05]
   - Any invalid stegotext (or a covertext) can be detected by the receiver with large probability without having access to an extra mechanism:
   
   \[
   \delta_2 := \min_{d} \min_{\tilde{c}} \left| \Pr_{\tilde{c}} (\tilde{c}) - \Pr_{S|D=d} (\tilde{c}) \right|
   \]

   is large.
Security: Attacking models

- **Chosen Hiddentext Attacks and Chosen Stegotext Attacks (CHA&CSA):**
  - Attacks where the adversary can obtain the stegotext of any hiddentext of his choice and the extracting result of any stegotext (or covertext) of his choice except the target.

[cf.] CPA&CCA in Encryption
Conditions

Security is considered under the following conditions.

• \( t \) is the number:
  – up to which the sender is allowed to embed hiddentexts; and
  – up to which the receiver is allowed to extract hiddentexts

• The adversary can have access to the covertext source; and he can obtain information on covertexts and the probability distribution over \( C \)
**Notations**

- $T$: set, $n$: non-negative integer,
  \[ P(T, n) := \{X \mid X \text{ is a subset of } T \text{ and } |X| \leq n\} \]
- $P(M \times S, t)$ means all possible sets of query/answer pairs for the embedding oracle, that is, all sets of at most $t$ hidddentext/stegotext pairs.
- $P(Y \times (M \cup \{\bot\}), t)$ means all possible sets of query/answer pairs for the extracting oracle, that is, all sets of at most $t$ stegotext (or covertext)/extracting result pairs.
Security: Goals
(Stegosystems)

Steganographic security:
([Cachin98])
- The adversary cannot detect whether the target conceals a hidden text or not.
**Security Definitions**

- **Definition** (SS: Steganographic Security)
  A $(\delta_1, \delta_2)$-stegosystem is $(\varepsilon, t)$-secure if the following probability is at most $\varepsilon$:

\[
P^{\text{SS}} := \max_{z = (M_S, Y_R)} \sum | \Pr_{\tilde{C}}(\tilde{c}) - \Pr_{S|Z=z}(\tilde{c}) |
\]

- $M_S$ is taken over $P(M \times S, t-1)$
  (i.e. $M_S$ is a set of at most $t$ hidentext/stegotext pairs)
- $Y_R$ is taken over $P(Y \times (M \cup \{ \perp \}), t-1)$
Generic Composition Method

Definition:

• \( \Pi = (\text{Gen}_\Pi, \text{ENC}_\Pi, \text{DEC}_\Pi) \): given authenticated encryption,
• \( f: \tilde{C} \rightarrow \overline{C} \), almost unbiased function,
• \( \Pi' = (\text{Gen}_{\Pi'}, \text{Emb}_{\Pi'}, \text{Ext}_{\Pi'}) \): stegosystem,
• \( e \): encryption-key, \( d \): decryption-key, \( m \): hiddentext

1. Embedding: \( \text{Emb}_{\Pi'}(e, \tilde{c}, m) = s \),
   \( \tilde{c} := \text{ENC}_\Pi(e, m) \), Pick up \( s \) from \( f^{-1}(\tilde{c}) \)

2. Extracting: \( \text{Ext}(d, y) = m' \) or \( \bot \),
   \( \tilde{c} := f(y) \), \( \text{DEC}_\Pi(d, \tilde{c}) = m' \) or \( \bot \)
**Generic Composition Method**

- **Definition** (μ-biased function [Hopper et al. 02])
  
  \( \Pr_{\tilde{c}} \): probability distribution over \( \tilde{C} \),
  
  \( f: \tilde{C} \rightarrow \overline{C} \) is \( \mu \)-biased function if
  
  for any \( \tilde{c} \) in \( \tilde{C} \),
  
  \[
  | \sum_{\tilde{c} \in f^{-1}(\tilde{c})} \Pr_{\tilde{c}} (\tilde{c}) \ - \ 1/|\overline{C}| | \leq \mu
  \]
Generic Composition Method

- Definition (Security of authenticated encryption) [Shikata et al. 04]
  An authenticated encryption $\Pi$ is $(\varepsilon, t)$-secure with ciphertext randomness $\overline{\varepsilon}$ against CPA and CCA, if the attacking probability of the following notions (1) and (3) is at most $\varepsilon$ and that of (2) is at most $\overline{\varepsilon}$:
  1. Almost Perfect Secrecy;
  2. Ciphertext randomness; and
  3. Integrity of Ciphertext.
Generic Composition Method

Theorem:

• $\Pi=((\text{GEN}_\Pi, \text{ENC}_\Pi, \text{DEC}_\Pi))$: authenticated encryption which is $(\varepsilon, t)$-secure with ciphertext randomness $\bar{\varepsilon}$,

• $f: \tilde{C} \rightarrow \bar{C}$, $\mu$-biased function

Then, the stegosystem $\Pi'$ formed by the composition method results in a $(1, \delta)$-stegosystem which is $(\varepsilon', t)$-secure, where $\delta > 0$ (depending on $\varepsilon$), and

$$\varepsilon' = \left\{2|\bar{C}|(\bar{\varepsilon} + \mu)(1 - \bar{\varepsilon}|\bar{C}|)^{-1}\right\}^{1/2}$$
Further Results
(Authenticated stegosystems)

- Int C: Integrity of Ciphertext
- Int S: Integrity of Stegotext

\[
\text{Encryption} \xrightarrow{\text{Int C}} \text{Authenticated Encryption} \\
\text{Stegosystem} \xrightarrow{\text{Int S}} \text{Authenticated Stegosystem}
\]
Security: Goals (Stegosystems)

1. Steganographic security ([Cachin98])
   – The adversary cannot detect whether the target conceals a hiddden text.

2. Integrity of Stegotexts ([Shikata, Matsumoto04])
   – The adversary cannot forge a message which will be accepted by the receiver so that it contains some hidden text.
**Security Definitions**

- **Definition** (Integrity of Stegotexts)
  The following probability is at most $\varepsilon$:

  $$P_{\text{IntS}} := \max_{z = (M_S, Y_R)} \max_y \Pr (R's \text{'s extracting result of } y \text{ is not } \bot | M_S, Y_R)$$

  - $M_S$ is taken over $P(M \times S, t)$
  - $Y_R$ is taken over $P(Y \times (M \cup \{ \bot \}), t-1)$
  - $y$ is taken over stegotexts such that $y$ does not appear in $M_S$ and $Y_R$
Security Definitions
(Authenticated Stegosystems)

• **Definition** (Authenticated Stegosystems)
  
  A \((\delta_1, \delta_2)\)-stegosystem is \((\varepsilon, t)\)-authenticated secure if it is \((\varepsilon, t)\)-secure and \(P_{\text{IntS}}\) is at most \(\varepsilon\)
Conclusion

- Unconditionally secure stegosystems
  - Security definitions: SS under active attacks
  - Construction method: generic composition by the use of
    - unconditionally secure authenticated encryption;
    - (almost) unbiased functions

[Note] The methodology of construction is not new, but our contribution is the analysis (i.e. security proof) in unconditional setting.
Research Program

“Computational” Based Schemes

“Unconditional” Versions
Unconditionally Secure Blind Signature Schemes
**Blind Signature Schemes**

Blind Signature Schemes [J LO97]

- \( \text{Kg}(1^k) \rightarrow (\text{pk}, \text{sk}) \)

\( (\text{pk},m) \)

- User

\( \sigma \)

- Verify(\( \text{pk},m,\sigma \)) \rightarrow \text{accept/reject}

Security Notions

- **Unforgeability** [PS96]

  User cannot output \( k+1 \) valid message-signature pairs after \( k \) interactions with signer.

- **Blindness** [J LO97]

  Signer cannot tell which of two messages was signed during which session, even after seeing signatures.
Our Study

We study blind signatures in unconditional setting.

- We newly introduced a model of unconditionally secure blind signature schemes (USBS, for short).
- We consider the security notions and construction of USBS in one-time model.

One-time means that the signer is allowed to generate a signature only once.
Notations

Entities
- TA: Trusted Authority
- U: User
- S: Signer
- V₁,...,Vₙ: Verifiers

Algorithms
- Gen: key generation algorithm
- Blind: \textit{blinded-message} generation algorithm
  ※\textit{blinded-message} means a data made by the user not to reveal the message that is being signed.
- Sign: signing algorithm
- Unblind: unblinding algorithm
- Ver: verification algorithm
The Model of USBS

(1) Key Generation and Distribution by TA

TA generates secret information $e_u, e_s, e_{vi} (i=1,...,n)$ for each member. Then, TA transmits $e_u$ to the user $U$, $e_s$ to the signer $S$ and $e_{Vi}$ to the verifier $V_i$ via a secure channel. After distributing these keys, TA deletes the keys from his memory.
**The Model of USBS**

The Model of USBS involves a user (U) and a signer (S) with the following steps:

1. **Blinding**
   
   \[ m^* = \text{Blind}(m, e_u) \]

2. **Unblinding**
   
   \[ \sigma = \text{Unblind}(m^*, \sigma^*, e_u) \]

3. **Signing**
   
   \[ \sigma^* = \text{Sign}(m^*, e_u) \]

4. **Verification**
   
   \[ \text{Ver}(m, \sigma, e_i) \in \{\text{valid, invalid}\} \]

- **m**: message
- **m^***: blinded-message
- **\sigma^***: signature for \( m^* \)
- **\sigma**: signature for \( m \)

Tsutomu Matsumoto, 18 May 2006
In USBS, we assume that there exists at most $w$ malicious colluders among participants, and they try to perform some attacks.

Based on the security notions of blind signatures [PS96][JLO97], we proposed three notions

- unconditional unforgeability
- unconditional blindness
- unconditional undeniability

as the security notions of USBS, and formulated them in unconditional setting.
Security Notions for USBS

Unconditional unforgeability:
It is difficult for malicious colluders to create a fraudulent signature that has not been legally generated by the signer but will be accepted as a valid by a target entity (a user, a signer or a verifier). We define $P_F$ as the success probability of this attack.

Unconditional blindness:
It is difficult for the signer to guess $(m, \sigma)$ from $(m^*, \sigma^*)$. We define $P_B$ as the success probability that the signer can guess $(m, \sigma)$ from $(m^*, \sigma^*)$.

Unconditional undeniability:
It is difficult for malicious colluders including a signer to produce an invalid signature which the target entity (a user or a verifier) will accept as valid. We define $P_U$ as the success probability that the colluders can produce such a fraudulent signature.
Security Notion for USBS

Definition.
USBS Π is called one-time \((ε, w, n)\)-secure USBS if the following condition is satisfied.

\[
\max\{ P_F, P_B, P_D \} \leq ε
\]

A Construction of USBS

We proposed a construction method of USBS by the use of polynomials over finite fields, which is one-time \((1/q, w, n)\)-secure [Hara, Seito, Shikata, Matsumoto: SCIS2006].
Summary

• What is Unconditional Security?
• Authenticated Encryption (TI model)
• Stegosystems (TI model)
• Unconditionally Secure Blind Signature Scheme (TI model)