

Public-Key Encryption Theory

Yu Zhang

HIT/CST/NIS

Cryptography, Autumn, 2014

- 1** Definitions and Securities of Public-Key Encryption
- 2** Trapdoor Permutations
- 3** Security Against Chosen-Ciphertext Attacks
- 4** Public-Key Encryption from TDP in ROM

1 Definitions and Securities of Public-Key Encryption

2 Trapdoor Permutations

3 Security Against Chosen-Ciphertext Attacks

4 Public-Key Encryption from TDP in ROM

Limitations of Private-Key Cryptography

- The key-distribution need physically meeting.
- The number of keys for U users is $\Theta(U^2)$.
- Secure communication in open system:

Solutions that are based on private-key cryptography are not sufficient to deal with the problem of secure communication in open systems where parties cannot physically meet, or where parties have transient interactions.

Merkle Puzzles (Key Exchange W/O TTP)

Alice prepares 2^{32} puzzles Puzzle_i , and sends to Bob.

$$\text{Puzzle}_i \leftarrow \text{Enc}_{(0^{96} \| p_i)}(\text{"Puzzle \#"} \| x_i \| k_i),$$

where Enc is 128-bit, $p_i \leftarrow \{0, 1\}^{32}$ and $x_i, k_i \leftarrow \{0, 1\}^{128}$.

Bob chooses Puzzle_j randomly, guesses p_j in 2^{32} time, obtains x_j, k_j and sends x_j to Alice.

Alice lookups puzzle with x_j , and uses k_j as secret key.

■ **Adversary** needs 2^{32+32} time.

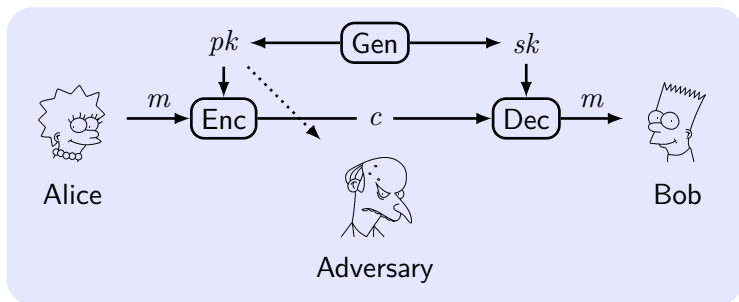
Better Gap?

Quadratic gap is best possible if we treat cipher as a black box oracle.

Public-Key Revolution

- In 1976, Whitfield Diffie and Martin Hellman published “*New Directions in Cryptography*”.
- **Asymmetric** or **public-key** encryption schemes:
 - **Public key** as the encryption key.
 - **Private key** as the decryption key.
- **Public-key primitives:**
 - Public-key encryption.
 - Digital signatures. (non-repudiation)
 - Interactive key exchange.
- **Strength:**
 - Key distribution over public channels.
 - Reduce the need to store many keys.
 - Enable security in open system.
- **Weakness:** slow, active attack on public key distribution.

Definitions



- **Key-generation** algorithm: $(pk, sk) \leftarrow \text{Gen}$, key length $\geq n$.
- **Plaintext space** \mathcal{M} is associated with pk .
- **Encryption** algorithm: $c \leftarrow \text{Enc}_{pk}(m)$.
- **Decryption** algorithm: $m := \text{Dec}_{sk}(c)$, or outputs \perp .
- **Requirement**: $\Pr[\text{Dec}_{sk}(\text{Enc}_{pk}(m)) = m] \geq 1 - \text{negl}(n)$.

Security against Eavesdroppers = CPA

The eavesdropping indistinguishability experiment $\text{PubK}_{\mathcal{A}, \Pi}^{\text{eav}}(n)$:

- 1 $(pk, sk) \leftarrow \text{Gen}(1^n)$.
- 2 \mathcal{A} is given input pk and so oracle access to $\text{Enc}_{pk}(\cdot)$, outputs m_0, m_1 of the same length.
- 3 $b \leftarrow \{0, 1\}$. $c \leftarrow \text{Enc}_{pk}(m_b)$ (challenge) is given to \mathcal{A} .
- 4 \mathcal{A} continues to have access to $\text{Enc}_{pk}(\cdot)$ and outputs b' .
- 5 If $b' = b$, \mathcal{A} succeeded $\text{PrivK}_{\mathcal{A}, \Pi}^{\text{eav}} = 1$, otherwise 0.

Definition 1

Π is **CPA-secure** if \forall PPT \mathcal{A} , \exists negl such that

$$\Pr \left[\text{PubK}_{\mathcal{A}, \Pi}^{\text{cpa}}(n) = 1 \right] \leq \frac{1}{2} + \text{negl}(n).$$

Security Properties of Public-Key Encryption

Theorem 2

No deterministic public-key encryption scheme is secure in the presence of an eavesdropper.

Proposition 3

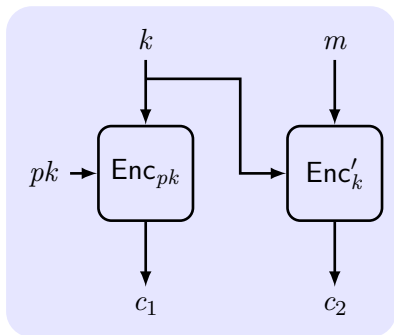
If Π is secure in the presence of an eavesdropper, then Π also is CPA-secure, and secure for multiple encryptions.

Proposition 4

Perfectly-secret public-key encryption is impossible.

Construction of Hybrid Encryption

To speed up the encryption of long message, use private-key encryption Π' in tandem with public-key encryption Π .



Construction 5

$\Pi^{\text{hy}} = (\text{Gen}^{\text{hy}}, \text{Enc}^{\text{hy}}, \text{Dec}^{\text{hy}})$:

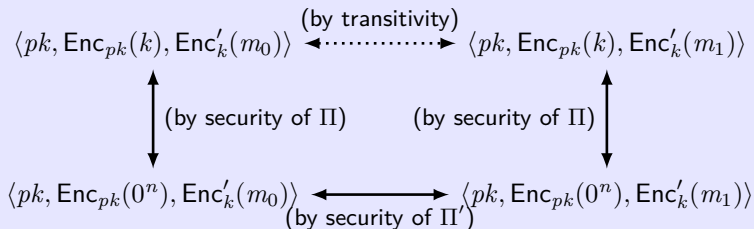
- Gen^{hy} :
 $(pk, sk) \leftarrow \text{Gen}(1^n)$.
- Enc^{hy} : pk and m .
 - 1 $k \leftarrow \{0, 1\}^n$.
 - 2 $c_1 \leftarrow \text{Enc}_{pk}(k)$,
 $c_2 \leftarrow \text{Enc}'_k(m)$.
- Dec^{hy} : sk and $\langle c_1, c_2 \rangle$.
 - 1 $k := \text{Dec}_{sk}(c_1)$.
 - 2 $m := \text{Dec}'_k(c_2)$.

Q: is hybrid encryption a public-key enc. or private-key enc. ?

Security of Hybrid Encryption

Theorem 6

If Π is a CPA-secure public-key encryption scheme and Π' is a private-key encryption scheme that has indistinguishable encryptions in the presence of an eavesdropper, then Π^{hy} is a CPA-secure public-key encryption scheme.

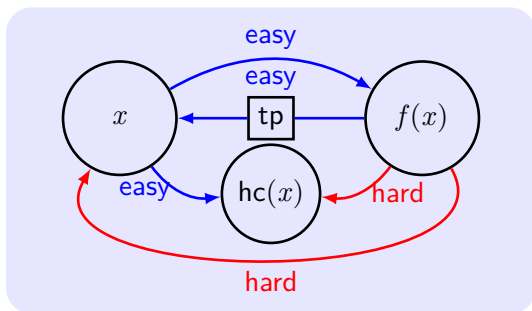


- 1 Definitions and Securities of Public-Key Encryption
- 2 Trapdoor Permutations**
- 3 Security Against Chosen-Ciphertext Attacks
- 4 Public-Key Encryption from TDP in ROM

Overview

Trapdoor function: is easy to compute, yet difficult to find its inverse without special info., the “trapdoor”. (One Way Function with the “trapdoor”)

A public-key encryption scheme can be constructed from any trapdoor permutation. (*“Theory and Applications of Trapdoor Functions”*, [Yao, 1982])



Definition of Families of Trapdoor Permutations

A tuple of polynomial-time algorithms $\Pi = (\text{Gen}, \text{Samp}, f, \text{Inv})$ is a **family of trapdoor permutations (TDP)** if:

- **parameter generation** algorithm Gen , on input 1^n , outputs (I, td) with $|I| \geq n$. (I, td) defines a set $\mathcal{D}_I = \mathcal{D}_{\text{td}}$.
- Gen_I outputs only I . $(\text{Gen}_I, \text{Samp}, f)$ is OWP.
- deterministic **inverting algorithm** Inv . $\forall (I, \text{td})$ and $\forall x \in \mathcal{D}_I$,

$$\text{Inv}_{\text{td}}(f_I(x)) = x.$$

Deterministic polynomial-time algorithm hc is a **hard-core predicate** of Π if \forall PPT \mathcal{A} , $\exists \text{negl}$ such that

$$\Pr[\mathcal{A}(I, f_I(x)) = \text{hc}_I(x)] \leq \frac{1}{2} + \text{negl}(n).$$

Public-key Encryption Schemes from TDPs

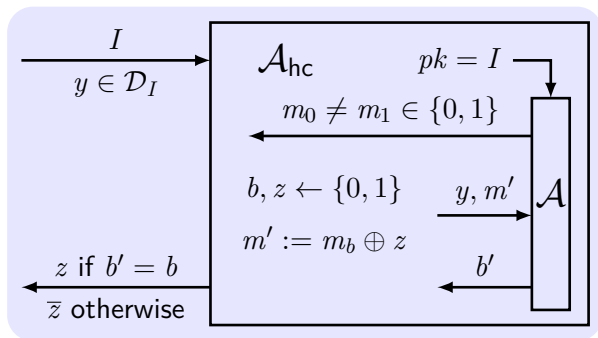
Construction 7

- Gen: $(I, \text{td}) \leftarrow \widehat{\text{Gen}}$ output **public key** I and **private key** td .
- Enc: on input I and $m \in \{0, 1\}$, choose a random $x \leftarrow \mathcal{D}_I$ and output $\langle f_I(x), \text{hc}_I(x) \oplus m \rangle$.
- Dec: on input td and $\langle y, m' \rangle$, compute $x := f_I^{-1}(y)$ and output $\text{hc}_I(x) \oplus m'$.

Theorem 8

If $\widehat{\Pi} = (\widehat{\text{Gen}}, f)$ is TDP, and hc is HCP for $\widehat{\Pi}$, then Construction Π is CPA-secure.

Idea: $\text{hc}_I(x)$ is pseudorandom. Reduce \mathcal{A}_{hc} for hc to \mathcal{A} for Π .



$$\Pr[\mathcal{A}_{\text{hc}}(I, f_I(x)) = \text{hc}_I(x)] =$$

$$\frac{1}{2} \cdot (\Pr[b' = b | z = \text{hc}_I(x)] + \Pr[b' \neq b | z \neq \text{hc}_I(x)]).$$

$$\Pr[b' = b | z = \text{hc}_I(x)] = \Pr[\text{PubK}_{\mathcal{A}, \Pi}^{\text{eav}}(n) = 1] = \varepsilon(n).$$

$$\text{If } z \neq \text{hc}_I(x), m' = m_b \oplus \overline{\text{hc}}_I(x) = m_{\bar{b}} \oplus \text{hc}_I(x),$$

$$\Pr[b' = b | z \neq \text{hc}_I(x)] = \Pr[\text{PubK}_{\mathcal{A}, \Pi}^{\text{eav}}(n) = 0] = 1 - \varepsilon(n).$$

$$\Pr[b' \neq b | z \neq \text{hc}_I(x)] = \varepsilon(n).$$

$$\Pr[\mathcal{A}_{\text{hc}}(I, f_I(x)) = \text{hc}_I(x)] = \frac{1}{2} \cdot (\varepsilon(n) + \varepsilon(n)) = \varepsilon(n).$$

Encrypting Longer Messages

Theorem 9

If \exists TDP Π , then \exists TDP $\hat{\Pi}$ with a HCP hc for $\hat{\Pi}$.

Example: If RSA assumption holds then the least-significant bit is hard-core for the RSA family of TDP.

an ℓ -it message $m = m_1 \cdots m_\ell$, the public key I , the ciphertext is

$$\langle f_I(x_1), \text{hc}_I(x_I) \oplus m_1 \rangle, \dots, \langle f_I(x_\ell), \text{hc}_I(x_\ell) \oplus m_\ell \rangle,$$

with x_1, \dots, x_ℓ chosen independently and *u.r.a* from \mathcal{D}_I .

An alternative way: $x_1 \leftarrow \mathcal{D}_I$ and compute $x_{i+1} := f_I(x_i)$ for $i = 1$ to ℓ . the ciphertext is

$$\langle x_{\ell+1}, \text{hc}_I(x_1) \oplus m_1, \dots, \text{hc}_I(x_\ell) \oplus m_\ell \rangle.$$

- 1 Definitions and Securities of Public-Key Encryption
- 2 Trapdoor Permutations
- 3 Security Against Chosen-Ciphertext Attacks**
- 4 Public-Key Encryption from TDP in ROM

Scenarios of CCA in Public-Key Setting

- 1 An adversary \mathcal{A} observes the ciphertext c sent by \mathcal{S} to \mathcal{R} .
- 2 \mathcal{A} send c' to \mathcal{R} in the name of \mathcal{S} or its own.
- 3 \mathcal{A} infer m from the decryption of c' to m' .

Scenarios

- **login to on-line bank with the password:** trial-and-error, learn info from the feedback of bank.
- **reply an e-mail with the quotation of decrypted text.**
- **malleability of ciphertexts:** e.g. doubling others' bids at an auction.

Definition of Security Against CCA/CCA2

The CCA/CCA2 indistinguishability experiment $\text{PubK}_{\mathcal{A}, \Pi}^{\text{cca}}(n)$:

- 1 $(pk, sk) \leftarrow \text{Gen}(1^n)$.
- 2 \mathcal{A} is given input pk and oracle access to $\text{Dec}_{sk}(\cdot)$, outputs m_0, m_1 of the same length.
- 3 $b \leftarrow \{0, 1\}$. $c \leftarrow \text{Enc}_{pk}(m_b)$ is given to \mathcal{A} .
- 4 \mathcal{A} have access to $\text{Dec}_{sk}(\cdot)$ except for c in **CCA2**¹ and outputs b' .
- 5 If $b' = b$, \mathcal{A} succeeded $\text{PrivK}_{\mathcal{A}, \Pi}^{\text{cca}} = 1$, otherwise 0.

Definition 10

Π has **CCA/CCA2-secure** if \forall PPT \mathcal{A} , \exists negl such that

$$\Pr \left[\text{PubK}_{\mathcal{A}, \Pi}^{\text{cca}}(n) = 1 \right] \leq \frac{1}{2} + \text{negl}(n).$$

¹CCA is also called Lunchtime attacks; CCA2 is also called Adaptive CCA.

State of the Art on CCA2-secure Encryption

- **Zero-Knowledge Proof**: complex, and impractical. (e.g., Dolev-Dwork-Naor)
- **Random Oracle** model: efficient, but not realistic (to consider CRHF as RO). (e.g., RSA-OAEP and Fujisaki-Okamoto)
- **DDH(Decisional Diffie-Hellman assumption) and UOWHF(Universal One-Way Hashs Function)**: $\times 2$ expansion in size, but security proved w/o RO or ZKP (e.g., Cramer-Shoup system).

CCA2-secure implies Plaintext-aware: an adversary cannot produce a valid ciphertext without “knowing” the plaintext.

Open problem

Constructing a CCA2-secure scheme based on RSA problem as efficient as “Textbook RSA”.

- 1 Definitions and Securities of Public-Key Encryption
- 2 Trapdoor Permutations
- 3 Security Against Chosen-Ciphertext Attacks
- 4 Public-Key Encryption from TDP in ROM**

Random Oracle Model (ROM) – Overview

- **Random oracle (RO):** a truly random function H answers every possible query with a random response.
 - **Consistent:** If H ever outputs y for an input x “on-the-fly”, then it always outputs the same answer given the same input.
 - No one “knows” the entire function H .
- **Random oracle model (ROM):** the existence of a public RO.
- **Methodology:** for constructing proven security in ROM.
 - 1 a scheme is designed and proven secure in ROM.
 - 2 Instantiate H with a hash function \hat{H} , such as SHA-1.
- No one seriously claims that a random oracle exists.²

With ROM, it is easy to achieve proven security, while keeping the efficiency by appropriate instantiation.

²There exists schemes that are proven secure in ROM but are insecure no matter how the random oracle is instantiated.

Simple Illustrations of ROM

A RO maps n_1 -bit inputs to n_2 -bit outputs.

■ A RO as a OWF, experiment:

- 1 A random function H is chosen.
- 2 A random $x \in \{0, 1\}^{n_1}$ is chosen, and $y := H(x)$ is evaluated.
- 3 \mathcal{A} is given y , and succeeds if it outputs x' : $H(x') = y$.

■ A RO as a CRHF, experiment:

- 1 A random function H is chosen.
- 2 \mathcal{A} succeeds if it outputs x, x' with $H(x) = H(x')$ but $x \neq x'$.

■ Constructing a PRF from a RO: $n_1 = 2n$, $n_2 = n$.

$$F_k(x) \stackrel{\text{def}}{=} H(k \| x), \quad |k| = |x| = n.$$

Construction 11

- Gen: $pk = I, sk = \text{td}$.
- Enc: $r \leftarrow \{0, 1\}^*, \text{ output } \langle f_I(r), H(r) \oplus m \rangle$.
- Dec: *input* (c_1, c_2) ; *compute* $r := f_{\text{td}}^{-1}(c_1)$, *output* $H(r) \oplus c_2$.

Theorem 12

If f is TPD and H is RO, Construction is CPA-secure.

H can not be replaced by PRG, since the partial info on r may be leaked by c_1 .

CCA-secure based on Private Key Encryption

Idea: PubK CCA = PrivK CCA + (Secret Key = TPD + RO).

Construction 13

$\Pi' = (\text{Gen}', \text{Enc}', \text{Dec}')$ is a private-key encryption scheme.

- Gen: $pk = I, sk = \text{td}$.
- Enc: $r \leftarrow D_I$ and compute $k := H(r)$, output $\langle f_I(r), \text{Enc}'_k(m) \rangle$.
- Dec: input $\langle c_1, c_2 \rangle$, compute $r := f_{\text{td}}^{-1}(c_1)$, $k := H(r)$, output $\text{Dec}'_k(c_2)$.

Theorem 14

If f is TDP, Π' is CCA-secure, and H is RO, Construction is CCA-secure.

Idea: PubK CCA = TDP + 2 RO (one for enc, one for mac).

Construction 15

- Gen: $pk = I$, $sk = \text{td}$.
- Enc: $r \leftarrow D_I$, output $\langle c_1 = f_I(r), c_2 = H(r) \oplus m, c_3 = G(c_2 \| m) \rangle$.
- Dec: $r := f_{\text{td}}^{-1}(c_1)$, $m := H(r) \oplus c_2$. If $G(c_2 \| m) = c_3$ output m , otherwise \perp .

Theorem 16

If f is TDP, G, H are ROs, Construction is CCA-secure.

Private Key Encryption vs. Public Key Encryption

	Private Key	Public Key
Secret Key	both parties	receiver
Weakest Attack	Eav	CPA
Probabilistic	CPA/CCA	always
Assumption against CPA	OWF	TDP
Assumption against CCA	OWF	TDP+RO
Efficiency	fast	slow