Public Key Encryption in the Random Oracle Model

Hongrui Cui

Shanghai Jiao Tong University

RickFreeman@sjtu.edu.cn

April 29, 2019

Overview

1. The Random Oracle Model
   - Introduction to Random Oracle
   - Definition of Random Oracle
   - Intuition Behind Random Oracle
2. IND-CPA PKE in ROM
   - Construction
   - Provable Security
3. IND-CCA2 PKE in ROM
   - IND-CCA2 PKE from Mac
   - OAEP^{+}

Content

Random Oracle as a Security Model

The Random Oracle Model is a popular and useful security model.

- Note that a new security model is not the same as a new assumption.
- (In my opinion) A security model defines the adversary's ability.
- An assumption conjectures on what can (or can not) be done under some model.

Illustration of Random Oracle

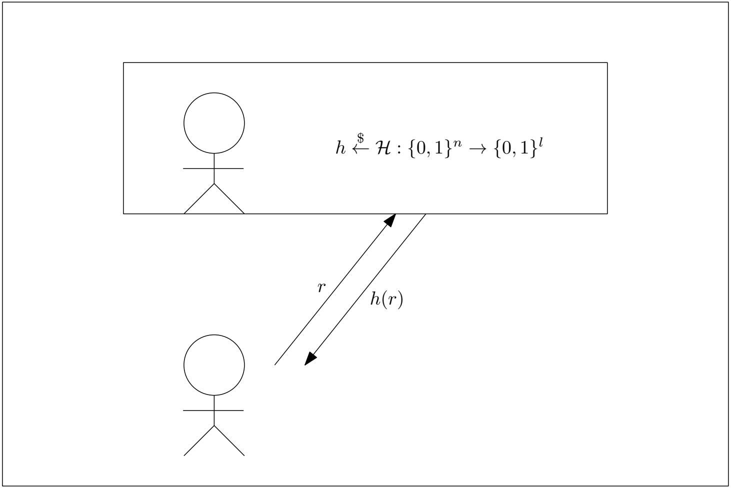

Figure: Illustration of the Random Oracle Model

Illustration of Random Oracle II

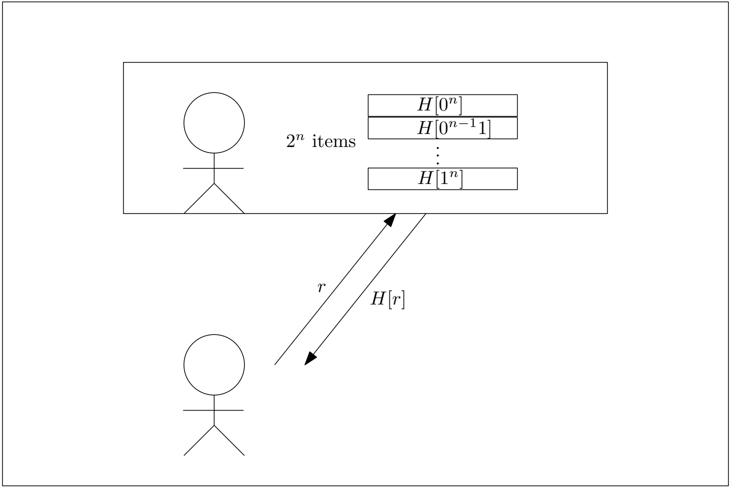

Figure: Illustration of the Random Oracle Model (Dynamically Built)

Informal Definition of Random Oracle

A Random Oracle is an oracle that is

- public, and
- random.

We often use the notation $A^{H(\cdot)}(1^\kappa)$ to denote a machine A that has access to random oracle $H(\cdot)$.

As H implements a random function, there is no way of knowing the result without specific querying (i.e. writing the query to query tape and read from response tape).

Why RO Enables More Efficient Schemes

- Recall that random oracle implements a random function, whose value is only available through querying the external oracle.
- This means that given any OTM A in ROM, we can simulate its evaluation by reading its query and placing arbitrary results.
- This also implies without querying the oracle on r, $H(r)$ is uniform and independent of any other randomness.

Content

IND-CPA Secure PKE in ROM

Assuming TDP is a family of trapdoor permutations, we can construct the following public key encryption scheme that encrypts l-bit messages.

- $\mathsf{Gen}(1^\kappa)$:
  - $(f, f^{-1}) \leftarrow \mathsf{TDP.Gen}(1^\kappa)$;
  - output $\langle pk, sk\rangle = \langle f, f^{-1}\rangle$.
- $\mathsf{Enc}(pk, m)$:
  - $r \leftarrow U_\kappa$;
  - output $c = \langle f(r), H(r) \oplus m\rangle$.
- $\mathsf{Dec}(sk, \langle y, C\rangle)$:
  - $r' = f^{-1}(y)$;
  - output $m' = H(r) \oplus C$.

IND-CPA Security I

Formally we have the following theorem.

Theorem (IND-CPA Security)

The scheme above is IND-CPA secure in the random oracle model if f is chosen from an trapdoor permutation family.

IND-CPA Security II

Proof.

Let query denote the event that at some point the adversary queried r, and let succ denote the event $b = b'$. We have that

$$
\begin{aligned}
Adv_A^{cpa}(\kappa) &= |\Pr[\text{succ}] - 1/2| \\
&= |\Pr[\text{succ}|\text{query}] \cdot \Pr[\text{query}] + \Pr[\text{succ}|\overline{\text{query}}] \cdot \Pr[\overline{\text{query}}] - 1/2| \\
&= |\Pr[\text{succ}|\text{query}] \cdot \Pr[\text{query}] + 1/2 \cdot (1 - \Pr[\overline{\text{query}}])| \\
&= |\Pr[\text{succ}|\text{query}] - 1/2| \cdot \Pr[\text{query}] \\
&\leq 1/2 \cdot \Pr[\text{query}]
\end{aligned}
$$

□

IND-CCA1 Security

The above scheme actually achieves indistinguishability under non-adaptive chosen ciphertext attack.
We will use a (trivial) hybrid argument to prove that.

Game 0

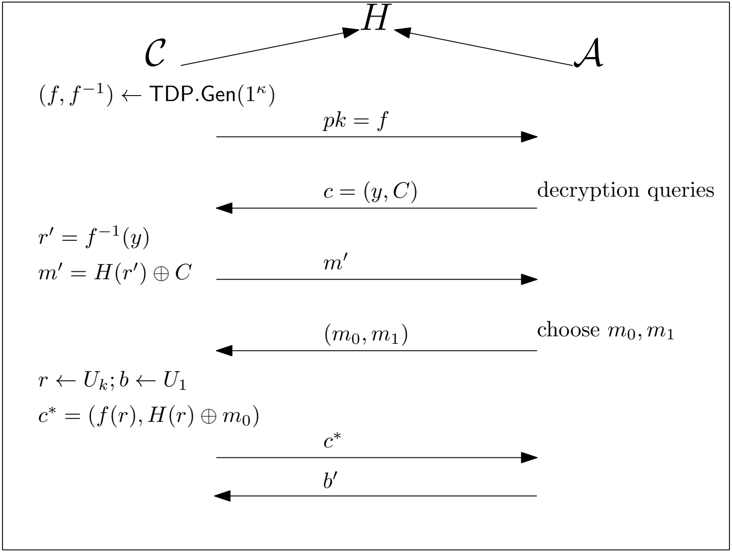

Figure: Game 0

Game 1

$\mathcal{C}$ $\qquad\qquad$ $\mathcal{A}$

$(f, f^{-1}) \leftarrow \mathsf{TDP.Gen}(1^\kappa)$

$\xrightarrow{pk = f}$

$\xleftarrow{c = (y, C)}$ decryption queries

if $y \in \{f(x) : \langle x, f(x), H(x)\rangle \in S\}$

$\quad m' = C \oplus H(f^{-1}(y))$

else

$\quad m' \leftarrow U_l;$

$\quad S = S \cup \{\langle \cdot, y, C \oplus m'\rangle\};$

$\xrightarrow{m'}$

$\xleftarrow{(m_0, m_1)}$ choose m_0, m_1

$r \leftarrow U_k; b \leftarrow U_1$

$c^* = (f(r), H(r) \oplus m_b)$

$\xrightarrow{c^*}$

$\xleftarrow{b'}$

Figure: Game 1

Game 2

$\mathcal{C}$		$\mathcal{A}$
$(f, f^{-1}) \leftarrow \mathsf{TDP.Gen}(1^\kappa)$ $r \leftarrow U_k$	$\xrightarrow{\quad pk = f \quad}$	
	$\xleftarrow{\quad c = (y, C) \quad}$	decryption queries
if $y \in \{f(x) : \langle x, f(x), H(x) \rangle \in S\}$ $m' = C \oplus H(f^{-1}(y))$ else $m' \leftarrow U_l$; $S = S \cup \{\langle \cdot, y, C \oplus m' \rangle\}$;	$\xrightarrow{\quad m' \quad}$	
	$\xleftarrow{\quad (m_0, m_1) \quad}$	choose m_0, m_1
$b \leftarrow U_1$ $c^* = (f(r), H(r) \oplus m_b)$	$\xrightarrow{\quad c^* \quad}$	
if $r' \neq r$ $z \leftarrow U_l$	$\xleftarrow{\quad r' \quad}$	
else $z = H(r')$	$\xrightarrow{\quad z \quad}$	
	$\xleftarrow{\quad b' \quad}$	

Figure: Game 2

Content

Simple Message Authentication

Let $\mathbb{F}_q$ be some field of order q. Then for message $m \in \mathbb{F}_q$, and $a, b \xleftarrow{\$} \mathbb{F}_q$,

$$t = a \cdot m + b$$

is a information-theoretic mac for m.

Note that for any $m' \neq m$, for any successful forged tag t', we have

$$\begin{bmatrix} t \\ t' \end{bmatrix} = \begin{bmatrix} m & 1 \\ m' & 1 \end{bmatrix} \cdot \begin{bmatrix} a \\ b \end{bmatrix},$$

and (t, t') is uniform over $\mathbb{F}_q^2$.

Modified PKE in ROM I

We modify the aforementioned PKE scheme by adding a Mac to achieve IND-CCA2 security.

Notations:

- $H : \{0, 1\}^{\kappa} \rightarrow \mathbb{F}_q^3$
- $\mathcal{M} : \mathbb{F}_q$
- $\mathsf{Mac}_{a,b}(m) : a \cdot m + b$

Modified PKE in ROM II

- $\mathsf{Gen}(1^\kappa)$:
  - $(f, f^{-1}) \leftarrow \mathsf{TDP.Gen}(1^\kappa)$;
  - output $\langle pk, sk\rangle = \langle f, f^{-1}\rangle$.
- $\mathsf{Enc}(pk, m)$:
  - $r \leftarrow U_\kappa$;
  - $\langle a, b, c\rangle = H(r)$;
  - output $c = \langle f(r), C = c + m, \mathsf{Mac}_{a,b}(C)\rangle$.
- $\mathsf{Dec}(sk, \langle y, C, t\rangle)$:
  - $r' = f^{-1}(y)$;
  - $\langle a', b', c'\rangle = H(r)$;
  - if $t \neq a' \cdot C + b'$, output $\perp$;
  - else output $m' = C - c$.

Provable Security

Now we argue the IND-CCA2 security of the PKE scheme.

The (somewhat trivial) proof relies on

- One-wayness of TDP,
- Security of Mac.

Game 0

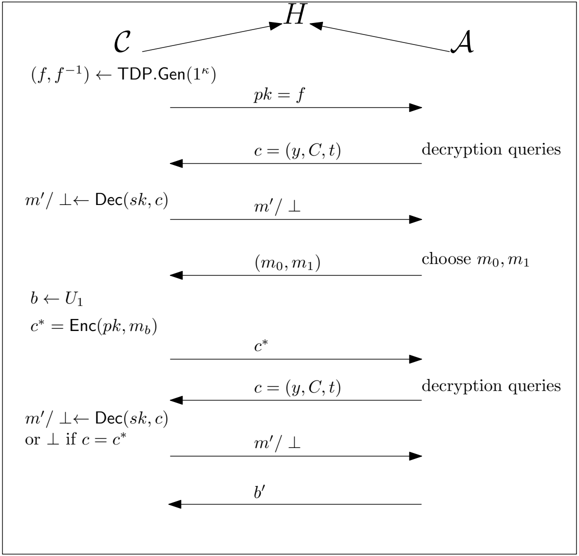

Figure: Game 0

Game 1

$\mathcal{C}$ $\qquad\qquad$ $\mathcal{A}$

$(f, f^{-1}) \leftarrow \mathsf{TDP.Gen}(1^\kappa)$

$\xrightarrow{pk = f}$

$\xleftarrow{c = (y, C, t)}$ decryption queries

if $y \in \{f(x) : \langle x, f(x), H(x)\rangle \in S\}$
$\quad m' = \mathsf{Dec}(sk, c)$
else
$\quad m' = \perp$;

$\xrightarrow{m' / \perp}$

$\xleftarrow{(m_0, m_1)}$ choose m_0, m_1

$b \leftarrow U_1$

$c^* = (f(r), H(r) \oplus m_0)$

$\xrightarrow{c^*}$

$\xleftarrow{c = (y, C, t)}$ decryption queries

if $c = c^*$ or $y \notin \{f(x) : \langle x, f(x), H(x)\rangle \in S\}$
$\quad m' = \perp$;
else
$\quad m' = \mathsf{Dec}(sk, c)$.

$\xrightarrow{m' / \perp}$

$\xleftarrow{b'}$

Figure: Game 1

Game 2

$\mathcal{C}$ $\qquad\qquad\qquad\qquad$ $\mathcal{A}$

$(f, f^{-1}) \leftarrow \mathsf{TDP.Gen}(1^\kappa)$

$\xrightarrow{pk = f}$

$\xleftarrow{c = (y, C, t)}$ decryption queries

if $y \in \{f(x) : \langle x, f(x), H(x) \rangle \in S\}$

$\quad m' = \mathsf{Dec}(sk, c)$

else

$\quad m' = \perp;$ $\qquad \xrightarrow{m' / \perp}$

$\xleftarrow{(m_0, m_1)}$ choose m_0, m_1

$b \leftarrow U_1$

$c^* = (f(r), H(r) \oplus m_0)$

$\xrightarrow{c^* = (y^*, C^*, t^*)}$

$\xleftarrow{c = (y, C, t)}$ decryption queries

if $c = c^*$ or $y \notin \{f(x) : \langle x, f(x), H(x) \rangle \in S\}$ or $y = y^*$

$\quad m' = \perp;$

else

$\quad m' = \mathsf{Dec}(sk, c).$ $\qquad \xrightarrow{m' / \perp}$

$\xleftarrow{b'}$

Figure: Game 2

Game 3

$\mathcal{C}$		$\mathcal{A}$
$(f, f^{-1}) \leftarrow \mathsf{TDP.Gen}(1^\kappa)$		
	$\xrightarrow{pk = f}$	
	$\xleftarrow{c = (y, C, t)}$	decryption queries
if $y \in \{f(x) : \langle x, f(x), H(x) \rangle \in S\}$ $\quad m' = \mathsf{Dec}(sk, c)$ else $\quad m' = \perp;$	$\xrightarrow{m' / \perp}$	
	$\xleftarrow{(m_0, m_1)}$	choose m_0, m_1
$b \leftarrow U_1$ $c^* = (f(r), H(r) \oplus m_0)$		
	$\xrightarrow{c^* = (y^*, C^*, t^*)}$	
	$\xleftarrow{c = (y, C, t)}$	decryption queries
if $c = c^*$ or $y \notin \{f(x) : \langle x, f(x), H(x) \rangle \in S\}$ or $y = y^*$ $\quad m' = \perp;$ else $\quad m' = \mathsf{Dec}(sk, c).$	$\xrightarrow{m' / \perp}$	
	$\xleftarrow{r'}$	
if $r' \neq r$ $\quad z \leftarrow U_l$ else $\quad z = H(r')$	$\xrightarrow{z}$	
	$\xleftarrow{b'}$	

Figure: Game 3

OAEP

Optimal Asymmetrical Encryption Padding by Shoup (OAEP^+) builds an IND-CCA2 PKE from any TDP family in ROM.

The name **optimal** comes from that the ciphertext length is κ, compared to $\kappa + 2 \cdot |q|$ in the previous scheme.

Notations

Some numbers:

- κ: the input/output length of TDP f
- k_0, k_1: two integers such that $k_0, k_1 < \kappa$, and $1/2^{k_0}, 1/2^{k_1}$ are both negligible (i.e. $k_0, k_1 \in \omega(\log \kappa)$)
- n: $n = \kappa - k_0 - k_1$, the message length

Three random oracles:

- $G : \{0,1\}^{k_0} \to \{0,1\}^n$
- $H' : \{0,1\}^{n+k_0} \to \{0,1\}^{k_1}$
- $G : \{0,1\}^{n+k_1} \to \{0,1\}^{k_0}$

OAEP

- $\mathsf{Gen}(1^\kappa)$:
  - $(f, f^{-1}) \leftarrow \mathsf{TDP.Gen}(1^\kappa)$;
  - output $\langle pk, sk \rangle = \langle f, f^{-1} \rangle$.
- $\mathsf{Enc}(pk, m)$:
  - $r \leftarrow U_{k_0}$;
  - $s = \langle m \oplus G(r), H'(m||r) \rangle$;
  - $t = H(s) \oplus r$;
  - output $c = f(s||t)$.
- $\mathsf{Dec}(sk, y)$:
  - $\langle s', t' \rangle = f^{-1}(y)$;
  - $r' = H(s') \oplus t'$;
  - $s = \langle s'_1, s'_2 \rangle$, $m' = G(r') \oplus s'_1$;
  - if $H'(m'||r') \neq s'_2$, output $\perp$;
  - else output m'.

Actually we only need to show the challenger can simulate the view of the real game without trapdoor f^{-1}.
We only need to show the probability of an unanswerable query is negligible.

Unanswerable Queries I

Lemma

Let c be the decryption query and c^* be the challenge ciphertext. Let (r, s_1, s_2, t) and (r^*, s_1^*, s_2^*, t^*) be the values defined by f from c and c^* respectively, then conditioned on the choice of G, H, H' and the queries of A, the probability of c being valid and $H'(m||r)$ or $H(s)$ having not been queried is negligible.

Unanswerable Queries II

Proof.

Consider the five cases:

- A has not queried $H'(r||m)$ and $r = r^*, m = m^*$,
- A has not queried $H'(r||m)$ and $r \neq r^*$,
- A has not queried $H'(r||m)$ and $m \neq m^*$,
- A has not queried $H(s)$ and $s = s^*$,
- A has not queried $H(s)$ and $s \neq s^*$,

the probability of each case is negligible. □

Reference I

Victor Shoup.
Oaep reconsidered.
In *Annual International Cryptology Conference*, pages 239–259. Springer, 2001.

Jonathan Katz.
Advanced topics in cryptography, 2004.