Journal of WoCrypt
www.uow.edu.au/~fuchun/jow
Volume: 2023 (54)

Practice Makes Perfect: Attack Encryption Schemes *

Fuchun Guo, Willy Susilo, and Yumei Li

University of Wollongong, Australia
{*fuchun,wsusilo,yl182*}@*uow.edu.au*
Fuchun: See you at ChinaCrypt 2023 in GuangZhou.

Abstract

Practice makes perfect if and only if you practice and find the answers by yourself.

1 Introduction

The tricks for attacking encryption schemes are somehow different from that for attacking signature schemes. We classify 5 types but cannot say much here; Otherwise, Section 2 will be split into two pages and it looks ugly.

2 Summary Attacks

The practice can be classified into the following 5 types.

- **Type 1:** Given a challenge ciphertext in PKE, the adversary can break the IND (indistinguishability) with pk only.
- **Type 2:** Given a challenge ciphertext in PKE, the adversary can break the IND with the help of decryption queries. The adversary can make very special queries to break IND.
- **Type 3:** Given a challenge ciphertext in ABE or further, the adversary can break the IND with mpk only. There is no need to know any private key.
- **Type 4:** Given a challenge ciphertext in ABE or FE, the adversary can break the IND with mpk and some private keys. If the adversary needs many private keys, it means that these private keys can be combined together to break the IND.
- **Type 5:** Given a challenge ciphertext in ABE or further, the adversary can break the IND with mpk, some private keys, and decryption queries. (We are not going to introduce this case since the solution for CCA borrows the ideas from tricks for CCA-secure PKE.)

*We decided to collect insecure schemes in 2022 but don't have time to finish this project until recently.

3 Public-Key Encryption

3.1 Scheme (ElGamal)

Let $(\mathbb{G}, g, p)$ be the cyclic group and $H : \{0,1\}^* \rightarrow \{0,1\}^n$ be the cryptographic hash function that will be shared by all users.

KeyGen: The key generation algorithm chooses a random number $\alpha \in \mathbb{Z}_p$, computes $g_1 = g^\alpha$, and returns a public/secret key pair (pk, sk) as follows:

$$pk = g_1, sk = \alpha.$$

Encrypt: The encryption algorithm takes as input a message $m \in \{0,1\}^n$ and the public key pk. It chooses a random number $r \in \mathbb{Z}_p$ and computes the ciphertext as

$$CT = (C_1, C_2) = (g^r, H(g_1^r) \oplus m)$$

Decrypt: The decryption algorithm takes as input CT and the secret key sk. It decrypts the ciphertext by computing

$$M = H(C_1^{sk}) \oplus C_2.$$

Question 1 *Is this scheme secure in the IND-CPA security model?*

Question 2 *Is this scheme secure in the IND-CCA security model?*

3.2 Scheme (ElGamal +)

Let $(\mathbb{G}, g, p)$ be the cyclic group and $H : \{0,1\}^* \rightarrow \{0,1\}^n, H_1 : \{0,1\}^* \rightarrow \mathbb{Z}_p$ be the cryptographic hash functions that will be shared by all users.

KeyGen: The key generation algorithm chooses a random number $\alpha \in \mathbb{Z}_p$, computes $g_1 = g^\alpha$, and returns a public/secret key pair (pk, sk) as follows:

$$pk = g_1, sk = \alpha.$$

Encrypt: The encryption algorithm takes as input a message $m \in \{0,1\}^n$ and the public key pk. It chooses a random number $r \in \mathbb{Z}_p$ and computes the ciphertext as

$$CT = (C_1, C_2, C_3) = (g^r, (g_1 g^T)^r, H(g_1^r) \oplus m), \text{where } T = H_1(C_1, C_3).$$

Decrypt: The decryption algorithm takes as input CT and the secret key sk. It decrypts the ciphertext by computing

$$M = H(C_1^{sk}) \oplus C_3.$$

It checks the validity of the ciphertext by checking whether C_2 is equal to

$$C_1^{\alpha + H_1(C_1, C_3)}.$$

Question 3 *Is this scheme secure in the IND-CPA security model?*

Question 4 *Is this scheme secure in the IND-CCA security model?*

3.3 Scheme (ElGamal ++)

Let $(\mathbb{G}, g, p)$ be the cyclic group and $H : \{0,1\}^* \rightarrow \{0,1\}^n, H_1 : \{0,1\}^* \rightarrow \mathbb{Z}_p$ be the cryptographic hash functions that will be shared by all users.

KeyGen: The key generation algorithm chooses random numbers $\alpha, \beta \in \mathbb{Z}_p$, computes $g_1 = g^\alpha, g_2 = g^\beta$, and returns a public/secret key pair (pk, sk) as follows:

$$pk = (g_1, g_2), sk = (\alpha, \beta).$$

Encrypt: The encryption algorithm takes as input a message $m \in \{0,1\}^n$ and the public key pk. It chooses a random number $r \in \mathbb{Z}_p$ and computes the ciphertext as

$$CT = (C_1, C_2, C_3) = \left(g^r, (g_2 g^T)^r, H(g_1^r) \oplus m\right), \text{where } T = H_1(C_1, C_3).$$

Decrypt: The decryption algorithm takes as input CT and the secret key sk. It decrypts the ciphertext by computing

$$M = H(C_1^{sk}) \oplus C_3.$$

It checks the validity of the ciphertext by checking whether C_2 is equal to

$$C_1^{\beta + H_1(C_1, C_3)}.$$

Question 5 *Is this scheme secure in the IND-CPA security model?*

Question 6 *Is this scheme secure in the IND-CCA security model?*

3.4 Scheme (ElGamal ★)

Let $(\mathbb{G}, g, p)$ be the cyclic group and $H_1 : \{0,1\}^* \rightarrow \{0,1\}^n, H_2 : \{0,1\}^* \rightarrow \{0,1\}^{2n}$ be the cryptographic hash functions that will be shared by all users.

KeyGen: The key generation algorithm chooses a random number $\alpha \in \mathbb{Z}_p$, computes $g_1 = g^\alpha$, and returns a public/secret key pair (pk, sk) as follows:

$$pk = g_1, sk = \alpha.$$

Encrypt: The encryption algorithm takes as input a message $m \in \{0,1\}^n$ and the public key pk. It chooses a random number $r \in \mathbb{Z}_p$ and computes the ciphertext as

$$CT = (C_1, C_2) = (g^r, H_2(g_1^r) \oplus [m||H_1(m)]\ )$$

Decrypt: The decryption algorithm takes as input CT and the secret key sk.

- Compute $m||h = H_2(C_1^{sk}) \oplus C_2$
- Return m if and only if $h = H_1(m)$.

Question 7 *Is this scheme secure in the IND-CPA security model?*

Question 8 *Is this scheme secure in the IND-CCA security model?*

3.5 Scheme (ElGamal ★★)

Let $(\mathbb{G}, g, p)$ be the cyclic group and $H_1 : \{0,1\}^* \rightarrow \{0,1\}^n, H_3 : \{0,1\}^* \rightarrow \{0,1\}^{3n}$ be the cryptographic hash functions that will be shared by all users. Supposing that each group element and each integer inside $\mathbb{Z}_p$ can be also represented with n bits.

KeyGen: The key generation algorithm chooses a random number $\alpha \in \mathbb{Z}_p$, computes $g_1 = g^{\alpha}$, and returns a public/secret key pair (pk, sk) as follows:

$$pk = g_1, sk = \alpha.$$

Encrypt: The encryption algorithm takes as input a message $m \in \mathbb{G}$ and the public key pk. It chooses a random number $r \in \mathbb{Z}_p$ and computes the ciphertext as

$$CT = (C_1, C_2) = (g^r, H_3(g_1^r) \oplus [m||m^r||r]\ )$$

Note: the group elements and integers should be encoded into bit strings before encryption. While decryption should do the encoding in the opposite way.

Decrypt: The decryption algorithm takes as input CT and the secret key sk.

- Compute $m||u||r' = H_3(C_1^{sk}) \oplus C_2$
- Compute $g^{r'}$ and $m^{r'}$.
- Return the message m if $C_1 = g^{r'}$ and $u = m^{r'}$.

Question 9 *Is this scheme secure in the IND-CPA security model?*

Question 10 *Is this scheme secure in the IND-CCA security model?*

3.6 Pairing-Based Public-Key Encryption Scheme

Let $(\mathbb{G}, \mathbb{G}_T, g, e, p)$ be the pairing group and $H : \{0,1\}^* \rightarrow \mathbb{Z}_p$ be the cryptographic hash function that will be shared by all users.

KeyGen: The key generation algorithm chooses a random number $\alpha \in \mathbb{Z}_p$, a random group element g_1, computes $U = e(g,g)^\alpha$, and returns a public/secret key pair (pk, sk) as follows:

$$pk = (g_1, U), sk = \alpha.$$

Encrypt: The encryption algorithm takes as input a message $m \in \mathbb{G}_T$ and the public key pk.

- Choose a random key pair of one-time signature (opk, osk).
- Choose a random $r \in \mathbb{Z}_p$ and compute

$$(C_1, C_2, C_3) = \Big((g_1 g^{H(opk)})^r, g^r, U^r \cdot m \Big)$$

- Use osk to sign (C_1, C_2, C_3) to obtain signature denoted by C_4.
- Set $C_5 = opk$.

The ciphertext is $CT = (C_1, C_2, C_3, C_4, C_5)$.

Decrypt: The decryption algorithm takes as input CT and the secret key sk.

- Verify that C_4 is a valid signature on (C_1, C_2, C_3) with the public key C_5.
- Verify that $e(C_1, g) = e(g_1 g^{H(C_5)}, C_2)$
- Choose a random $s \in \mathbb{Z}_p$ and compute

$$(d_1, d_2) = (g^\alpha (g_1 g^{H(C_5)})^s, g^s)$$

- Return message by computing

$$m = \frac{C_3 \cdot e(d_2, C_1)}{e(d_1, C_2)}$$

Question 11 *Is this scheme secure in the IND-CPA security model?*

Question 12 *Is this scheme secure in the IND-CCA security model?*

3.7 Generic-Construction Scheme

Let CT be a ciphertext generated from an IND-CPA secure encryption scheme. Suppose there is a one-time signature scheme.

- Suppose we have CT computed using pk.
- Run the one-time signature scheme to generate a key pair (opk, osk)
- Use osk to sign (opk, CT) and the signature is σ.
- Set $CT^* \leftarrow (opk, CT, \sigma)$

Question 13 *What is the purpose of computing CT^* instead of CT?*

Question 14 *Is the above solution correct?*

3.8 Scheme (Multi-Message ElGamal)

Let $(\mathbb{G}, g, p)$ be the cyclic group that will be shared by all users.

KeyGen: The key generation algorithm chooses random numbers $\alpha_1, \alpha_2 \in \mathbb{Z}_p$, computes $g_1 = g^{\alpha_1}, g_2 = g^{\alpha_2}$, and returns a public/secret key pair (pk, sk) as follows:

$$pk = (g_1, g_2), sk = (\alpha_1, \alpha_2).$$

Encrypt: The encryption algorithm takes as input a message vector $M = (m_1, m_2, \cdots, m_n) \in \mathbb{G}^n$ and the public key pk. It chooses random numbers $r_1, r_2 \in \mathbb{Z}_p$ and computes the ciphertext as

$$\begin{aligned} CT &= (U_1, U_2, C_1, C_2, \cdots, C_n) \\ &= (g^{r_1}, g^{r_2}, m_1 \cdot g_1^{r_1 2^1} \cdot g_2^{r_2 \cdot 3^1}, m_2 \cdot g_1^{r_1 2^2} \cdot g_2^{r_2 \cdot 3^2}, \cdots, m_n \cdot g_1^{r_1 2^n} \cdot g_2^{r_2 \cdot 3^n}) \end{aligned}$$

Decrypt: The decryption algorithm takes as input CT and the secret key sk.

- Compute $V_0 = U_1^{\alpha_1}, W_0 = U_2^{\alpha_2}$;
- Compute $V_1 = V_0^2, W_1 = W_0^3$ and $m_1 = \frac{C_1}{V_1 \cdot W_1}$
- Compute $V_2 = V_1^2, W_2 = W_1^3$ and $m_2 = \frac{C_2}{V_2 \cdot W_2}$
- $\vdots$
- Compute $V_n = V_{n-1}^2, W_n = W_{n-1}^3$ and $m_n = \frac{C_n}{V_n \cdot W_n}$

It returns the decrypted messages $M = (m_1, m_2, \cdots, m_n)$

Question 15 *Is this scheme secure in the OW-CPA security model[1]?*

Question 16 *Is this scheme secure in the IND-CPA security model?*

[1]OW= One Way

4 From IBE to ABE

4.1 Scheme (Identity-Based Encryption)

Setup: The setup algorithm chooses $(\mathbb{G}, \mathbb{G}_T, g, e, p)$ and a cryptographic hash function $H : \{0,1\}^* \rightarrow \mathbb{G}$. Next, it chooses random numbers $\alpha, \beta, \gamma \in \mathbb{Z}_p$ and compute $g_1 = g^\alpha, g_2 = g^\beta, g_3 = g^\gamma$. The master key pair is

$$mpk = (\mathbb{G}, \mathbb{G}_T, g, e, p, H, g_1, g_2, g_3),\ msk = (\alpha, \beta, \gamma).$$

KeyGen: The key generation algorithm takes as input an identity $ID \in \{0,1\}^*$ and returns a private key d_{ID} of ID as follow:

$$d_{ID} = g^{\frac{\gamma}{\alpha + H(ID)\beta}}.$$

Encrypt: The encryption algorithm takes as input a message $m \in \mathbb{G}_T$, identity ID, and the master public key mpk. It chooses a random $r \in \mathbb{Z}_p$ and computes

$$CT = (C_1, C_2, C_3) = \Big((g_1 g_2^{H(ID)})^r,\ \ g^r,\ \ e(g_3, g)^r \cdot m \Big)$$

Decrypt: The decryption algorithm takes as input CT and the private key d_{ID}.

- Verify that CT was created for ID by $e(C_1, g) = e(g_1 g_2^{H(ID)}, C_2)$.
- Decrypt the ciphertext by
$$M = \frac{C_3}{e(C_1, d_{ID})}$$

Question 17 *Is this scheme secure in the IND-ID-CPA security model?*

Question 18 *Is this scheme secure in the IND-ID-CCA security model?*

4.2 Scheme (Identity-Based Encryption)

Setup: The setup algorithm chooses $(\mathbb{G}, \mathbb{G}_T, g, e, p)$ and a cryptographic hash function $H : \{0,1\}^* \rightarrow \mathbb{Z}_p$. Next, it chooses random numbers α, β and computes $g_1 = g^\alpha, g_2 = g^\beta$. Then, it chooses a random group element $h \in \mathbb{G}$. The master key pair is

$$mpk = (\mathbb{G}, \mathbb{G}_T, g, e, p, H, h, g_1, g_2),\ msk = (\alpha, \beta).$$

KeyGen: The key generation algorithm takes as input an identity $ID \in \{0,1\}^*$. It chooses a random number $r \in \mathbb{Z}_p$ and returns a private key d_{ID} of ID as follow:

$$d_{ID} = (g^{\alpha\beta}(h^{H(ID)})^r, g^r).$$

Encrypt: The encryption algorithm takes as input a message $m \in \mathbb{G}_T$, identity ID, and the master public key mpk. It chooses a random $s \in \mathbb{Z}_p$ and computes

$$CT = (C_1, C_2, C_3) = \Big((h^{H(ID)})^s,\ \ g^s,\ \ e(g_1, g_2)^s \cdot m\Big)$$

Decrypt: The decryption algorithm takes as input CT and the private key d_{ID}.

- Decrypt the ciphertext by
$$m = \frac{C_3 \cdot e(C_1, d_{ID}^2)}{e(C_2, d_{ID}^1)}$$

Question 19 *Is this scheme secure in the IND-ID-CPA security model?*

Question 20 *Is this scheme secure in the IND-ID-CCA security model?*

4.3 Scheme (ElGamal Based IBE)

Setup: The setup algorithm chooses $(\mathbb{G}, g, p)$ and a cryptographic hash function $H : \{0,1\}^* \rightarrow \mathbb{Z}_p$. Next, it a chooses random number $\alpha \in \mathbb{Z}_p$ and compute $g_1 = g^\alpha$. The master key pair is

$$mpk = (\mathbb{G}, g, p, H, g_1),\ msk = \alpha.$$

KeyGen: The key generation algorithm takes as input an identity $ID \in \{0,1\}^*$ and returns a private key d_{ID} of ID as follow:

$$d_{ID} = \frac{\alpha}{H(ID)} \mod p.$$

Encrypt: The encryption algorithm takes as input a message $m \in \mathbb{G}$, identity ID, and the master public key mpk. It chooses a random $r \in \mathbb{Z}_p$ and computes

$$CT = (C_1, C_2) = \left(g^{r \cdot H(ID)},\ \ g_1^r \cdot m\right)$$

Decrypt: The decryption algorithm takes as input (ID, CT) and the private key d_{ID}. It decrypts the ciphertext by

$$m = \frac{C_2}{C_1^{d_{ID}}}.$$

Question 21 *Is this scheme secure in the IND-ID-CPA security model without Key Query?*

Question 22 *Is this scheme secure in the IND-ID-CPA security model with Key Query?*

4.4 Scheme (Identity-Based Broadcast Encryption)

Setup: The setup algorithm chooses $(\mathbb{G}, \mathbb{G}_T, g, e, p)$ and a cryptographic hash function $H : \{0,1\}^* \to \mathbb{Z}_p$. Next, it chooses a random number $\alpha \in \mathbb{Z}_p$ and compute $g_1 = g^\alpha$. The master key pair is

$$mpk = (\mathbb{G}, \mathbb{G}_T, g, e, p, H, g_1), msk = \alpha.$$

KeyGen: The key generation algorithm takes as input an identity $ID \in \{0,1\}^*$ and returns a private key d_{ID} of ID as follow:

$$d_{ID} = g^{\frac{1}{\alpha + H(ID)}}.$$

Encrypt: The encryption algorithm takes as input a message $m \in \mathbb{G}_T$, two identities ID_1, ID_2, and the master public key mpk. It chooses a random $r \in \mathbb{Z}_p$ and computes

$$CT = (C_1, C_2, C_3) = \Big((g_1 g^{H(ID_1)})^r, \;\; (g_1 g^{H(ID_2)})^r, \;\; e(g,g)^r \cdot m \Big)$$

Note: This is an encryption for two identities only.

Decrypt: The decryption algorithm takes as input (ID_1, ID_2, CT) and the private key d_{ID_i}. It decrypts the ciphertext by computing

$$m = \frac{C_3}{e(C_i, d_{ID_i})}.$$

Question 23 *Is this scheme secure in the IND-ID-CPA security model?*

Question 24 *Is this scheme secure in the IND-ID-CCA security model?*

4.5 Scheme (Attribute-Based Encryption)

Suppose that a private key is created for an attribute set denoted by T. An application scenario requires that when a message is encrypted with an attribute set E, the private key of T can decrypt this ciphertext if and only if E is a subset of T.

Setup: The setup algorithm chooses $(\mathbb{G}, \mathbb{G}_T, g, e, p)$ and a cryptographic hash function $H : \{0,1\}^* \rightarrow \mathbb{Z}_p$. Next, it chooses a random number $\alpha \in \mathbb{Z}_p$, a random group element h, and compute $g_1 = g^\alpha, U = e(h,h)^\alpha$. The master key pair is

$$mpk = (\mathbb{G}, \mathbb{G}_T, g, e, p, H, g_1, h, U), msk = \alpha.$$

KeyGen: The key generation algorithm takes as input an attribute set $\{A : A \in T\}$. It chooses a random number $s \in \mathbb{Z}_p$ and returns a private key d_T of T as follow:

$$d_T = \{h^\alpha g^s, h^{\frac{-s}{\alpha + H(A)}} : A \in T\}.$$

Encrypt: The encryption algorithm takes as input a message $m \in \mathbb{G}_T$, the attribute set $E = \{A_1, A_2\}$, and the master public key mpk. It chooses a random $r_1, r_2 \in \mathbb{Z}_p$ and computes

$$CT = (C_1, C_1', C_2, C_2', C_3) = \Big(h^{r_1}, (g_1 g^{H(A_1)})^{r_1},\ \ h^{r_2}, (g_1 g^{H(A_2)})^{r_2},\ \ U^{(r_1+r_2)} \cdot m\Big)$$

Decrypt: The decryption algorithm takes as input (A_1, A_2, CT) and the private key d_T of $T = \{A_1, A_2, A_3\}$. It decrypts the ciphertext by computing

$$m = \frac{C_3}{e(h^\alpha g^s, C_1) \cdot e(h^{\frac{-s}{\alpha + H(A_1)}}, C_1') \cdot e(h^\alpha g^s, C_2) \cdot e(h^{\frac{-s}{\alpha + H(A_2)}}, C_2')}.$$

Question 25 *Is this scheme secure in the IND-ID-CPA security model?*

Question 26 *Is this scheme secure in the IND-ID-CCA security model?*

===========We didn't provide answers because this job has no pay :(===========