Multi-Recipient Public-Key Encryption with Shortened Ciphertext

Kaoru KUROSAWA

Department of Computer and Information Sciences,
Ibaraki University,
4-12-1 Nakanarusawa, Hitachi, Ibaraki, 316-8511, Japan
Tel/Fax. +81-294-38-5135
E-mail. kurosawa@cis.ibaraki.ac.jp

Abstract. In the trivial n-recipient public-key encryption scheme, a ciphertext is a concatenation of independently encrypted messages for n recipients. In this paper, we say that an n-recipient scheme has a "*shortened ciphertext*" property if the length of the ciphertext is almost a half (or less) of the trivial scheme and the security is still almost the same as the underlying single-recipient scheme. We first present (multi-plaintext, multi-recipient) schemes with the "*shortened ciphertext*" property for ElGamal scheme and Cramer-Shoup scheme. We next show (single-plaintext, multi-recipient) hybrid encryption schemes with the "*shortened ciphertext*" property.

Keywords: public-key encryption, multi-recipient setting, ElGamal, Cramer-Shoup, hybrid encryption, concrete security.

1 Introduction

1.1 Background

Suppose that there are n recipients. Let pk_i be the public key of recipient i for $1 \leq i \leq n$. The security of a public-key encryption scheme in the multi-recipient setting is different from the single-recipient setting. For example, if e is the common public exponent in RSA, then e encryptions of the same plaintext M under different moduli lead to an easy recovery of M. Further results by Hastad [11] and Coppersmith [7, 8] proved that even the time-stamp variants can be successfully attacked with e ciphertexts.

In the trivial n-recipient public-key encryption scheme, a ciphertext is just a concatenation of independently encrypted messages for n recipients using a single-recipient public-key encryption algorithm $\mathcal{E}$. That is, $\mathcal{E}_{pk_1}(M_1)||\cdots||\mathcal{E}_{pk_n}(M_n)$, where $||$ denotes concatenation. In general, this trivial scheme is not secure in the sense of invertibility even if $\mathcal{E}$ is secure in the same sense, as shown in the above RSA example.

Recently, Bellare et al. [2] and Baudron et al. [1] independently proved that the trivial n-recipient scheme is secure in the sense of indistinguishability [10] if $\mathcal{E}$ is secure in the same sense, where indistinguishability is a stronger security notion than invertibility.

However, their nice results [2, 1] still do not capture the essence of the multi-recipient setting:
(1) The length of the ciphertext of the trivial n-recipient scheme is n times larger than that of the underlying single-recipient scheme.
(2) Consider a single-recipient hybrid encryption scheme which encrypts a long message M using a pseudorandom generator G and sends the seed r of G using a public-encryption scheme. That is,

$$C = M \oplus G(r)||\mathcal{E}_{pk}(r), \tag{1}$$

where $||$ denotes concatenation. A natural extension of the hybrid scheme to an n-recipient scheme will be that

$$M \oplus G(r)||\mathcal{E}_{pk_1}(r)||\cdots||\mathcal{E}_{pk_n}(r). \tag{2}$$

Their results [2, 1] only imply that the latter part $\mathcal{E}_{pk_1}(r)||\cdots||\mathcal{E}_{pk_n}(r)$ is secure in the sense of indistinguishability if the single-recipient part $\mathcal{E}_{pk}(r)$ is secure in the same sense.

1.2 Our Contribution

In this paper, we consider n-recipient public-key encryption schemes such that the length of the ciphertext is almost a half (or less) of the trivial n-recipient scheme and the security is still almost the same as the underlying single-recipient scheme. We say that such a scheme has a "*shortened ciphertext*" property.

1. We first give the definitions of our model and the security.

2. We next present (*multi*-plaintext, multi-recipient) schemes with the "*shortened ciphertext*" property for ElGamal scheme and Cramer-Shoup scheme and prove their security.

3. We also prove that the above mentioned (*single*-plaintext, multi-recipient) scheme of eq.(2) is secure in the sense of indistinguishability against chosen plaintext attack if the underlying single-recipient public-key scheme is secure in the same sense.

4. We finally present how to construct a (single-plaintext, multi-recipient) scheme secure against chosen *ciphertext* attack with the "shortened ciphertext" property. The underlying single-recipient public-key scheme needs to be secure in the sense of indistinguishability against chosen ciphertext attack. (For example, we can use Rabin-SAEP or RSA-SAEP$^+$ [4] as the underlying single-recipient scheme.)

Cramer-Shoup scheme is a practical public-key encryption scheme which is secure in the sense of indistinguishability against chosen-ciphertext attack under the decision Diffie-Hellman (DDH) assumption in the standard model [9]. The basic Cramer-Shoup scheme uses universal one-way hash functions (UOH) [9, Sec.3]. Bellare et al. derived the concrete security of the basic Cramer-Shoup scheme by assuming the concrete security of UOH [2]. On the other hand, Cramer and Shoup also presented a hash-free variant which does not use UOH [9, Sec.5.3].

We derive the concrete security of the hash-free variant of Cramer-Shoup scheme. It is of independent interest because it truly depends only on the DDH assumption, but not UOH. We then present a (multi-plaintext, multi-recipient) hash-free Cramer-Shoup scheme that has the "*shortened ciphertext*" property.

One further advantage of our multi-recipient schemes (in the discrete log setting) is that the encryption operation can be significantly faster than if the encryption operations were performed separately for each recipient.

Finally, in all of our multi-recipient schemes, the decryption algorithm is the same as the single-recipient one. Therefore, no extra cost is required for each recipient.

1.3 Related Works

The "broadcast" problem has been addressed by other authors in the context of traitor-tracing [6, 12, 5, 13]. The traitor-tracing schemes such that [12, 5, 13] can have even shorter ciphertexts than our schemes, but with the tradeoff that a small coalition of recipients can break the traitor-tracing aspect of the scheme, i.e., construct a new private key that does not identify anyone in the coalition. In our schemes, no coalition can do this since each private key uniquely identifies the recipient.

Bellare and Rogaway [3] proved that the single recipient hybrid encryption scheme shown in eq.(1) is secure in the sense of indistinguishability against chosen plaintext attack under the random oracle moel if $\mathcal{E}_{pk}$ is a trapdoor oneway permutation. They also proved that the following scheme secure in the sense of indistinguishability against chosen ciphertext attack under the random oracle moel.

$$C = \mathcal{E}_{pk}(r)||M \oplus G(r)||H(M||r),$$

where H is a hash function. Before that, Zheng and Seberry [16] proposed a scheme such that

$$C = \mathcal{E}_{pk}(r)||(G(r) \oplus (M||H(M)).$$

2 Single-Recipient Encryption Scheme

A single-recipient public-key encryption scheme $\mathcal{PE} = (\mathcal{K}, \mathcal{E}, \mathcal{D})$ consists of three algorithms. The key generation algorithm $\mathcal{K}$ outputs (pk, sk) on input some global information I, where pk is a public key and sk is the secret key; we write $(pk, sk) \stackrel{R}{\leftarrow} \mathcal{K}(I)$. The encryption algorithm $\mathcal{E}$ outputs a ciphertext C on input the public key pk and a plaintext M; we write $C \stackrel{R}{\leftarrow} \mathcal{E}_{pk}(M)$. The decryption algorithm $\mathcal{D}$ outputs M or *reject* on input the secret key sk and a ciphertext C; we write $x \leftarrow \mathcal{D}_{sk}(C)$, where $x = M$ or *reject*. We require that $\mathcal{D}_{sk}(\mathcal{E}_{pk}(M)) = M$ for each plaintext M.

An adversary B runs in two stages. In "find" stage, it takes a public key pk and outputs two equal length messages M_0 and M_1 together with some state information $state$. In "guess" stage, it gets a challenge ciphertext $C_b \stackrel{R}{\leftarrow} \mathcal{E}_{pk}(M_b)$ from the encryption oracle $\mathcal{E}_{pk}$, where b is a randomly chosen bit. B finally outputs a bit $\tilde{b}$. The advantage of B is measured by the probability $\Pr(\tilde{b} = b)$.

Formally, the security of $\mathcal{PE}$ in the sense of indistinguishability against chosen-plaintext attack is defined as follows.

Definition 2.1 *For $b = 0$ and 1, define the experiment as follows.*

$$(pk_1, sk_1) \stackrel{R}{\leftarrow} K(I), (M_0, M_1, state) \stackrel{R}{\leftarrow} B(find, pk), C_b \stackrel{R}{\leftarrow} \mathcal{E}_{pk}(M_b), \tilde{b} \stackrel{R}{\leftarrow} B(guess, C_b, state).$$

Let

$$\begin{aligned} \mathtt{Adv}^{\text{s-cpa}}_{\mathcal{PE},I}(B) &\stackrel{\text{def}}{=} \Pr(\tilde{b} = 0 \mid b = 0) - \Pr(\tilde{b} = 0 \mid b = 1) \\ \mathtt{Adv}^{\text{s-cpa}}_{\mathcal{PE},I}(t) &\stackrel{\text{def}}{=} \max_B \mathtt{Adv}^{\text{s-cpa}}_{\mathcal{PE},I}(B), \end{aligned}$$

where the maximum is over all B with time-complexity t.

(In the superscript, *s-* denotes "single recipient".)

Definition 2.2 *We say that $\mathcal{PE}$ is secure against chosen-plaintext attack if $\mathtt{Adv}^{\text{s-cpa}}_{\mathcal{PE},I}(t)$ is negligible for polynomially bounded t, where the complexity is measured as a function of a security parameter.*

It is easy to see that

$$\Pr(\tilde{b} = b) = \frac{1}{2} + \frac{1}{2}\mathtt{Adv}^{\text{s-cpa}}_{\mathcal{PE},I}(B) \tag{3}$$

The security against chosen-ciphertext attack is defined similarly except for that the adversary B gets the decryption oracle $\mathcal{D}_{sk}$ and is allowed to query any ciphertext C at most q_d times, where it must be that $C \neq C_b$ in the guess stage. We denote the advantages by $\mathtt{Adv}^{\text{s-cca}}_{\mathcal{PE},I}(B)$ and $\mathtt{Adv}^{\text{s-cca}}_{\mathcal{PE},I}(t, q_d)$, respectively.

3 Multi-Recipient Encryption Scheme

Suppose that there are n recipients. Let $N \stackrel{\text{def}}{=} \{1, \cdots, n\}$. We define (*single*-plaintext, multi-recipient) public-key encryption schemes and (*multi*-plaintext, multi-recipient) public-key encryption schemes as follows.

- In a (*single*-plaintext, multi-recipient) public-key encryption scheme, a sender sends the same plaintext M secretly to a subset of recipients $S \subseteq N$ by broadcasting a ciphertext C_S.
- In a (*multi*-plaintext, multi-recipient) public-key encryption scheme, a sender sends an independent plaintext M_i secretly to each recipient $i \in S$ by broadcasting a ciphertext C_S.

3.1 "Shortened Ciphertext" Property

A multi-recipient public-key encryption scheme is naturally constructed from a single-recipient public-key encryption scheme $\mathcal{PE} = (\mathcal{K}, \mathcal{E}, \mathcal{D})$ as follows. The key generation algorithm runs $\mathcal{K}(I)$ n times independently. A ciphertext C_N is

$$C_N = \mathcal{E}_{pk_1}(M_1)||\cdots||\mathcal{E}_{pk_n}(M_n),$$

where $||$ denotes concatenation. We call this scheme the *trivial multi-recipient* scheme.

Bellare et al. [2] proved that the trivial multi-recipient scheme is secure in the sense of indistinguishability if $\mathcal{PE}$ is secure in the same sense. Baudron et al. [1] proved the same result independently. However, the length of the ciphertext of the trivial multi-recipient scheme is n times larger than that of the single-recipient scheme.

In this paper, we consider multi-recipient public-key encryption schemes such that (1) the length of the ciphertext is almost a half (or less) of the trivial multi-recipient scheme and (2) the security is still almost the same as the underlying single-recipient scheme. We say that such a scheme has a "*shortened ciphertext*" property.

3.2 Our Model

For a single-recipient public-key encryption scheme $\mathcal{PE} = (\mathcal{K}, \mathcal{E}, \mathcal{D})$, we define a (multi-plaintext, multi-recipient) public-key encryption scheme $\mathcal{PE}^n = (\mathcal{K}^n, \mathcal{E}^n, TAKE)$ as follows.

- The key generation algorithm $\mathcal{K}^n$ outputs $\underline{pk} \stackrel{\text{def}}{=} (pk_1, \cdots, pk_n)$ and $\underline{sk} \stackrel{\text{def}}{=} (sk_1, \cdots, sk_n)$ on input some global information I, where (pk_i, sk_i) is a pair of encryption/decryption keys of recipient i.
- For $S = \{1_1, \cdots i_s\}$, let M_{i_j} be a plaintext for recipient $i_j \in S$. Let $\underline{M}_S \stackrel{\text{def}}{=} (M_{i_1}, \cdots, M_{i_s})$. Then the encryption algorithm $\mathcal{E}^n$ computes a ciphertext C_S for $\underline{M}_S$ on input $\underline{pk}$, S and $\underline{M}_S$; we write $C_S \stackrel{R}{\leftarrow} \mathcal{E}^n_{\underline{pk}}(S, \underline{M}_S)$.
- $TAKE$ is a hash function that takes a part of a ciphertext as follows. For $T \subset S \subseteq N$, it outputs C_T on input T, S and C_S. We write $C_T \leftarrow TAKE_T(C_S)$.

  Especially, for $i \in S$, we write $C_i \leftarrow TAKE_i(C_S)$.

We require that $\mathcal{D}_{sk_i}(TAKE_i(C_S)) = M_i$ for all $i \in S$ and any M_i.

A (single-plaintext, multi-recipient) public-key encryption scheme is defined similarly.

Remark 3.1 *In our multi-recipient schemes, the decryption algorithm is the same as the single-recipient scheme. Therefore, no extra cost is required for each recipient.*

3.3 Security

We generalize the definition of security for the multi-recipient setting given by Bellare et al. [2] to (multi-plaintext,multi-recipient) schemes as follows.

We consider an experiment as follows. At the beginning, a challenge bit b is randomly chosen and fixed. An adversary B is provided with the encryption oracle $\mathcal{E}^n_{\underline{pk}}$ and it is allowed to query $(S, \underline{M}^0_S, \underline{M}^1_S)$ at most q_e times. $\mathcal{E}^n_{\underline{pk}}$ returns a ciphertext $\mathcal{E}^n_{\underline{pk}}(S, \underline{M}^b_S)$. (Since b is fixed at the beginning, the same b is used across all the queries.) B finally outputs a bit $\tilde{b}$. We require that $|M^0_{i_j}| = |M^1_{i_j}|$ for all $i_j \in S$, where $\underline{M}^0_S = (M^0_{i_1}, \cdots, M^0_{i_s})$ and $\underline{M}^1_S = (M^1_{i_1}, \cdots, M^1_{i_s})$.

Each time, B can choose $(S, \underline{M}^0_S, \underline{M}^1_S)$ arbitrarily, where S as well as $(\underline{M}^0_S, \underline{M}^1_S)$ may be related to his other queries to $\mathcal{E}^n_{\underline{pk}}$. Then the security of $\mathcal{PE}^n$ against chosen-plaintext attack is defined as follows.

Definition 3.1 *For $b = 0$ and 1, define the experiment as follows.*

$$(\underline{pk}, \underline{sk}) \stackrel{R}{\leftarrow} K^n(I),\ \tilde{b} \leftarrow B^{\mathcal{E}^n_{\underline{pk}}}(I, \underline{pk}).$$

Let

$$\begin{aligned} \mathtt{Adv}^{n\text{-cpa}}_{\mathcal{PE}^n,I}(B) &\stackrel{\text{def}}{=} \Pr(\tilde{b} = 0 \mid b = 0) - \Pr(\tilde{b} = 0 \mid b = 1) \\ \mathtt{Adv}^{n\text{-cpa}}_{\mathcal{PE}^n,I}(t, q_e) &\stackrel{\text{def}}{=} \max_B \mathtt{Adv}^{n\text{-cpa}}_{\mathcal{PE}^n,I}(B), \end{aligned}$$

where the maximum is over all B with time-complexity t.

In the superscript, n- denotes "n recipients".

Definition 3.2 *We say that $\mathcal{PE}^n$ is secure against chosen-plaintext attack if $\mathtt{Adv}^{n\text{-cpa}}_{\mathcal{PE}^n,I}(t)$ is negligible for polynomially bounded t, where the complexity is measured as a function of a security parameter.*

The security against chosen-ciphertext attack is defined similarly except for that the adversary B gets n decryption oracles $\mathcal{D}_{sk_1}, \cdots, \mathcal{D}_{sk_n}$. It is allowed to query any ciphertext C to any decryption oracle $\mathcal{D}_{sk_i}$ at most q_d times for each i, where it must be that $C \neq TAKE_i(C_S)$ for any output C_S of the encryption oracle $\mathcal{E}_{x\underline{pk}}$. We denote the advantages by $\mathtt{Adv}^{n\text{-cca}}_{\mathcal{PE}^n,I}(B)$ and $\mathtt{Adv}^{n\text{-cca}}_{\mathcal{PE}^n,I}(t, q_e, q_d)$, respectively.

The security of (single-plaintext, multi-recipient) schemes is defined similarly. For simplicity, the same notation as above will be used.

Remark 3.2 *In the definition of Bellare et al. [2], (i) $|S| = 1$ and there are n encryption oracles $\mathcal{E}_{pk_1}, \cdots, \mathcal{E}_{pk_n}$. (ii) B is allowed to query at most q_e times to each $\mathcal{E}_{pk_i}$. It is easy to see that our definition is more general if we ignore (ii).*

3.4 Sufficient Condition

We say that an adversary is type 0 if $q_e = 1$ and his query to $\mathcal{E}^n_{\underline{pk}}$ is $(N, \underline{M}^0_N, \underline{M}^1_N)$. That is, we consider an adversary which runs in two stages, the find stage and the guess stage, as in the single-recipient case.

Definition 3.3 *Let $\mathtt{AdvTO}^{n\text{-cpa}}_{\mathcal{PE}^n,I}(t)$ be the $\max_B \mathtt{Adv}^{n\text{-cpa}}_{\mathcal{PE}^n,I}(B)$, where the maximum is over all type 0 adversaries B with time-complexity t. Define $\mathtt{AdvTO}^{n\text{-cca}}_{\mathcal{PE}^n,I}(t, q_d)$ similarly.*

The next lemma shows that $\mathcal{PE}^n$ is secure if $\mathtt{AdvTO}^{n\text{-x}}_{\mathcal{PE}^n,I}(t)$ is negligible, where $x = cpa$ or cca. Therefore, we do not have to evaluate $\mathtt{Adv}^{n\text{-x}}_{\mathcal{PE}^n,I}(t, q_e)$ directly.

Let T_n denote the time to compute a ciphertext $C_N = \mathcal{E}^n_{\underline{pk}}(N, \underline{M}_N)$.

Lemma 3.1 *In an n-recipient broadcast/multicast public-key encryption scheme $\mathcal{PE}^n$,*

$$\begin{aligned} \mathtt{Adv}^{n\text{-cpa}}_{\mathcal{PE}^n,I}(t, q_e) &\leq q_e \cdot \mathtt{AdvTO}^{n\text{-cpa}}_{\mathcal{PE}^n,I}(t'), \\ \mathtt{Adv}^{n\text{-cca}}_{\mathcal{PE}^n,I}(t, q_e, q_d) &\leq q_e \cdot \mathtt{AdvTO}^{n\text{-cca}}_{\mathcal{PE}^n,I}(t', q_d), \end{aligned}$$

where $t' = t + O(q_e T_n)$.

A proof is given in Appendix.

4 Multi-Recipient "ElGamal" Encryption Scheme

In this section, we show a (multi-plaintext, multi-recipient) ElGamal scheme which has the "*shortened ciphertext*" property. Let $\mathcal{G}$ be a group with a prime order p and let g be a generator of $\mathcal{G}$. Let $I = (p, g)$ be the global information.

Let $T^{\exp}$ denote the time needed to perform an exponentiation in $\mathcal{G}$.

4.1 ElGamal scheme and DDH problem

Informally, the decision Diffie-Hellman (DDH) problem is stated as follows. Given g^x, g^y, g^z, decide if $z = xy \bmod p$ with nonnegligible probability. Formally, let

$$\begin{aligned} DH &\stackrel{\mathrm{def}}{=} \{(g^x, g^y, g^{xy}) \mid x \in Z_p, y \in Z_p\} \\ RA &\stackrel{\mathrm{def}}{=} \{(g^x, g^y, g^z) \mid x \in Z_p, y \in Z_p, z \in Z_p\}. \end{aligned}$$

Let D be a distinguisher which outputs 0 or 1. Define

$$\begin{aligned} \mathtt{Adv}^{ddh}_{p,g}(D) &\stackrel{\mathrm{def}}{=} \Pr[D(X) = 0 | X \in DH] - \Pr[D(X) = 0 | X \in RA], \\ \mathtt{Adv}^{ddh}_{p,g}(t) &\stackrel{\mathrm{def}}{=} \max_{D} \mathtt{Adv}_{p,g}(D), \end{aligned}$$

where the maximum is over all D with "time-complexity" t. The DDH assumption is that $\mathtt{Adv}^{ddh}_{p,g}(t)$ is negligible.

ElGamal encryption scheme $\mathcal{EG} = (\mathcal{K}, \mathcal{E}, \mathcal{D})$ is as follows.

$$\begin{aligned} \mathcal{K}(I) &: sk = x, pk = X (\leftarrow g^x), \text{ where } x \stackrel{R}{\leftarrow} Z_p. \\ \mathcal{E}_{I,X}(M) &: (Y, W) = (g^r, M \cdot X^r), \text{ where } r \stackrel{R}{\leftarrow} Z_p. \\ \mathcal{D}_{I,x}(Y, W) &: M \leftarrow W \cdot Y^{-x}. \end{aligned}$$

It is well known that ElGamal scheme is secure in the sense of indistinguishability against chosen plaintext attack under the DDH assumption.

4.2 Proposed Scheme

Now we present the proposed (multi-plaintext,multi-recipient) ElGamal scheme $\mathcal{EG}^n = (\mathcal{K}^n, \mathcal{E}^n, TAKE)$. The key generation algorithm $\mathcal{K}^n(I)$ runs $\mathcal{K}(I)$ n times independently. Let x_i be the secret key and $X_i (= g^{x_i})$ be the public-key of recipient i.

For $S = \{1_1, \cdots i_s\}$, let M_{i_j} be a plaintext for recipient $i_j \in S$. Then a ciphertext for S is

$$C_S = (g^r, M_{i_1} X_{i_1}^r, \ldots, M_{i_s} X_{i_s}^r),$$

where $r \stackrel{R}{\leftarrow} Z_p$. $TAKE_i$ is defined as $(g^r, M_i X_i^r) \leftarrow TAKE_i(C_S)$. For $T \subset S \subseteq N$, $C_T \leftarrow TAKE_T(C_S)$ is defined naturally.

We will show that our scheme has the "*shortened ciphertext*" property. First, in the trivial multi-recipient scheme, a ciphertext is

$$C_S^{trivial} = (g^{r_{i_1}}, M_{i_1} X_{i_1}^{r_{i_1}}) || \cdots || (g^{r_{i_s}}, M_{i_s} X_{i_s}^{r_{i_s}}).$$

Therefore, in our scheme, the size of the ciphertext is almost a half of that of the trivial multi-recipient scheme. We next prove that our scheme is still secure. More precisely, we prove that our scheme is secure in the sense of indistinguishability against chosen plaintext attack under the DDH assumption.

Lemma 4.1 *In the proposed (multi-plaintext,multi-recipient) ElGamal encryption scheme,*

$$\mathtt{AdvTO}^{n\text{-cpa}}_{\mathcal{EG}^n(p,g)}(t) \leq 2 \cdot \mathtt{Adv}^{\text{ddh}}_{p,g}(t') + \frac{1}{p}, \tag{4}$$

where $t' = t + O(n \cdot T^{\exp})$.

A proof is given in Appendix. From lemma 4.1 and lemma 3.1, we obtain the following theorem.

Theorem 4.1 *In the proposed (multi-plaintext,multi-recipient) ElGamal encryption scheme,*

$$\mathtt{Adv}^{n\text{-cpa}}_{\mathcal{EG}^n(p,g)}(t, q_e) \leq q_e(2 \cdot \mathtt{Adv}^{\text{ddh}}_{p,g}(t') + \frac{1}{p}), \tag{5}$$

where $t' = t + O(q_e n \cdot T^{\exp})$.

The concrete security of the trivial multi-recipient ElGamal encryption scheme derived by Bellare et al. [2] satisfies the same equation as eq.(4). Hence, the coefficient q_e in eq.(5) can be considered as the cost for the "*shortened ciphertext*" property.

4.3 S/MIME CMS

S/MIME CMS (IETF RFC 2630) is a (single-plainext, multi-recipient) scheme such that

$$C_S = (g^r, Wrap(X_{i_1}^r, K), ..., Wrap(X_{i_s}^r, K)),$$

where K is a content-encryption key to be transported, $Wrap$ is a symmetric key-wrapping operation.

The Wrap operation takes the role of the multiplication in the basic ElGamal scheme. Therefore, Theorem 4.1 shows that this scheme is secure if Wrap is secure enough.

5 Multi-Recipient "Cramer-Shoup" Encryption Scheme

In this section, we first show the concrete security of the hash-free variant of Cramer-Shoup scheme. We next present a (multi-plaintext,multi-recipient) hash-free Cramer-Shoup scheme which has the "*shortened ciphertext*" property.

Let $\mathcal{G}$ be a group with a prime order p and let g_1 be a generator of $\mathcal{G}$. Let $I = (p, g_1)$ be the global information.

5.1 Concrete security of the hash-free Cramer-Shoup Scheme

Bellare et al. derived the concrete security of the basic Cramer-Shoup scheme [9, Sec.3] by assuming the security of universal one-way hash functions (UOH) [2]. In this subsection, we derive the concrete security of the hash-free variant of Cramer-Shoup scheme, which does not need to assume UOH.

The hash-free variant of Cramer-Shoup scheme $\mathcal{CS} = (\mathcal{K}, \mathcal{E}, \mathcal{D})$ is as follows [9, Sec.5.3]. Let F be a polynomial time computable injection from G^3 to $(Z_p^*)^k$ for some k. Let (pk, sk) be

$$\begin{aligned} sk &: z, x_1, x_2, (y_{11}, y_{12}), \cdots, (y_{k1}, y_{k2}), \\ &\quad \text{where each element is randomly taken from } Z_p. \\ pk &: g_2, h(= g_1^z), c(= g_1^{x_1} g_2^{x_2}), d_1(= g_1^{y_{11}} g_2^{y_{12}}), \cdots, d_k(= g_1^{y_{k1}} g_2^{y_{k2}}), \\ &\quad \text{where } g_2 \text{ is randomly chosen from } G. \end{aligned}$$

For a plaintext M, let a ciphertext (u_1, u_2, e, v) be

$$u_1 = g_1^r, u_2 = g_2^r, e = h^r M, v = (c d_1^{\alpha_1} \cdots d_k^{\alpha_k})^r,$$

where $r \stackrel{R}{\leftarrow} Z_p$ and $(\alpha_1, \cdots, \alpha_k) = F(u_1, u_2, e)$.

On input (u_1, u_2, c, v), the decryption algorithm $\mathcal{D}_{sk}$ first computes $F(u_1, u_2, e) = (\alpha_1, \cdots, \alpha_k)$. Next if

$$v = u_1^{x_1+\alpha_1 y_{11}+\cdots+\alpha_k y_{k1}} u_2^{x_2+\alpha_1 y_{12}+\cdots+\alpha_k y_{k2}}, \tag{6}$$

Then $\mathcal{D}_{sk}$ outputs

$$M \leftarrow e/u_1^z. \tag{7}$$

Otherwise, $\mathcal{D}_{sk}$ outputs *reject*. Let

$$\epsilon \stackrel{\text{def}}{=} \left(1 - \frac{1}{p}\right) \frac{q_d}{p} + \frac{1}{p}.$$

Theorem 5.1 *In the hash-free Cramer-Shoup scheme,*

$$\texttt{Adv}^{\text{s-cca}}_{\mathcal{CS},(p,g_1)}(t, q_d) \leq 2 \cdot \texttt{Adv}^{\text{ddh}}_{p,g_1}(t') + 3\epsilon, \tag{8}$$

where $t' = t + O(q_d \cdot T^{\text{exp}})$.

A proof will be given in the final paper.

5.2 Proposed Scheme

Now the proposed (multi-plaintext,multi-recipient) hash-free Cramer-Shoup scheme $\mathcal{CS}^n = (\mathcal{K}^n, \mathcal{E}^n, TAKE)$ is described as follows. The key generation algorithm $\mathcal{K}^n(I)$ runs $\mathcal{K}(I)$ n times independently with a restriction such that g_2 is common for all pk_i, where $pk_i = (g_2, h_i, c_i, d_{1i}, \cdots, d_{ki})$. That is, the encryption keys pk_i are not independent of each other while the secret keys sk_i are independently chosen. This is possible because w is not a part of sk_i, where $g_2 = g_1^w$.

For $S = \{1_1, \cdots i_s\}$, let M_i be a plaintext for recipient $i \in S$. Then a ciphertext for S is

$$C_S = (u_1, u_2, e_{i_1}, v_{i_1}, \cdots, e_{i_n}, v_{i_n})$$

such that $u_1 = g_1^r, u_2 = g_2^r$ and $e_i = h_i^r M_i,\ v_i = (c_i d_{1i}^{\alpha_{1i}} \cdots d_{ki}^{\alpha_{ki}})^r$, where $r \stackrel{R}{\leftarrow} Z_p$ and $(\alpha_{1i}, \cdots, \alpha_{ki}) = F(u_1, u_2, e_i)$. $TAKE_i$ is defined as $(u_1, u_2, e_i, v_i) \leftarrow TAKE_i(C_S)$. $C_S \leftarrow TAKE_S(C_N)$ is defined naturally.

Note that the size of the ciphertext of our scheme is almost a half of the trivial multi-recipient scheme. We next prove that our scheme is still secure. More precisely, we prove that our scheme is secure in the sense of indistinguishability against chosen ciphertext attack under the DDH assumption.

Lemma 5.1 *In the proposed (multi-plaintext,multi-recipient) Cramer-Shoup scheme,*

$$\texttt{AdvTO}^{n\text{-cca}}_{\mathcal{CS}^n,(p,g_1)}(t,q_d) \leq 2\cdot\texttt{Adv}^{\mathrm{ddh}}_{p,g_1}(t') + 3n\epsilon, \tag{9}$$

where $t' = t + O(n\cdot q_d\cdot T^{\exp})$.

The proof is similar to that of Theorem 5.1. From lemma 5.1 and lemma 3.1, we obtain the following theorem.

Theorem 5.2 *In the proposed (multi-plaintext,multi-recipient) Cramer-Shoup scheme,*

$$\texttt{Adv}^{n\text{-cca}}_{\mathcal{CS}^n,(p,g_1)}(t,q_d) \leq q_e(2\cdot\texttt{Adv}^{\mathrm{ddh}}_{p,g_1}(t') + 3n\epsilon), \tag{10}$$

where $t' = t + O(n\cdot q_d\cdot T^{\exp}) + O(q_e n T^{exp})$.

Comparing with the concrte security of the trivial multi-recipient (basic) Cramer-Shoup scheme given by Bellare et al. [2], we can see that our scheme takes no extra cost fot the "*shortened ciphertext*" property except negligible factors.

6 Multi-Recipient Hybrid Encryption Scheme

6.1 Overview

Bellare and Rogaway showed that eq.(1) is secure in the sense of indistinguishability against chosen plaintext attack if $\mathcal{E}_{pk}$ is a trapdoor oneway permutation. However, this does not imply that eq.(2) is secure. Indeed, it is not secure if $\mathcal{E}_{pk}$ is RSA as mentioned in Sec.1.1. On the other hand, the results of [2, 1] imply only that the latter part $\mathcal{E}_{pk_1}(r)||\cdots||\mathcal{E}_{pk_n}(r)$ of eq.(2) is secure in the sense of indistinguishability if $\mathcal{E}_{pk}(r)$ is secure in the same sense.

In this section, we formally prove that eq.(2) is secure in the sense of indistinguishability against chosen plaintext attack if $\mathcal{E}_{pk}$ is secure in the same sense.

More generally, we prove that there exists a (single-plaintext,multi-recipient) *hybrid* encryption scheme $\mathcal{H}^n = (\mathcal{K}^n_H, \mathcal{E}^n_H, TAKEH)$ which is secure in the sense of indistinguishability against chosen plaintext (ciphertext, respectively) attack if there exists a (multi-plaintext,multi-recipient) public-key encryption scheme $\mathcal{PE}^n = (\mathcal{K}^n, \mathcal{E}^n, TAKE)$ which is secure in the same sense against type 0 adversaries.

For example, we can use Rabin-SAEP, RSA-SAEP$^+$ [4] or Cramer-Shoup scheme [9] as the underlying single-recipient scheme secure against chosen *ciphertext* attack.

In what follows, let $\mathcal{PE} = (\mathcal{K}, \mathcal{E}, \mathcal{D})$ be the underlying single recipient public-key scheme. That is,

$$\mathcal{PE} \to \mathcal{PE}^n \to \mathcal{H}^n.$$

Remember that $\mathcal{E}^n_{\underline{pk}}(S, \underline{r})$ denotes a ciphertext of $\underline{r} = (r, \cdots, r)$ for a subset of recipients $S = \{i_1, \cdots i_s\}$ in $\mathcal{PE}^n$.

6.2 IND-CPA Hybrid Scheme

Define a (single-plaintext,multi-recipient) *hybrid* encryption scheme $\mathcal{H}^n = (\mathcal{K}^n_H, \mathcal{E}^n_H, TAKEH)$ from $\mathcal{PE}^n = (\mathcal{K}^n, \mathcal{E}^n, TAKE)$ as follows.

Let a ciphertext of M for a subset of recipients $S = \{i_1, \cdots i_s\}$ be

$$C_S = \mathcal{E}^n_{\underline{pk}}(S, \underline{r})||M \oplus G(r), \tag{11}$$

where r is a random element and G is a pseudorandom generator. For $T \subset S \subseteq N$, let

$$TAKEH_T(C_S) = TAKE_T(\mathcal{E}^n_{\underline{pk}}(S, \underline{r}))||M \oplus G(r).$$

Now we prove that $\mathcal{H}^n$ is secure in the sense of indistinguishability against chosen plaintex tattack if $\mathcal{PE}^n$ is secure in the same sense only against type 0 adversaries under the random oracle model, where G is modeled as a random oracle.

Suppose that an adversary makes at most q_G queries to the random oracle G. Let r be l-bits long. We first show that $\mathcal{H}^n$ is secure against type 0 adversaries if $\mathcal{PE}^n$ is so.

Lemma 6.1

$$\mathtt{AdvT0}^{n\text{-cpa}}_{\mathcal{H}^n, I}(t') \leq \mathtt{AdvT0}^{n\text{-cpa}}_{\mathcal{PE}^n, I}(t'') + \frac{q_G}{2^{l-3}}, \tag{12}$$

where $t'' = t' + O(q_G) + O(n)$.

A proof is given in Appendix. From lemma 3.1, we have

$$\mathtt{Adv}^{n\text{-cpa}}_{\mathcal{H}^n, I}(t, q_e) \leq q_e \mathtt{AdvT0}^{n\text{-cpa}}_{\mathcal{H}^n, I}(t')$$

where $t' = t + O(q_e T_n)$. Therefore, we obtain the following Theorem.

Theorem 6.1

$$\mathtt{Adv}^{n\text{-cpa}}_{\mathcal{H}^n,I}(t,q_e) \le q_e\left(\mathtt{AdvTO}^{n\text{-cpa}}_{\mathcal{PE}^n,I}(t'') + \frac{q_G}{2^{l-3}}\right),$$

where $t'' = t + O(q_e T_n) + O(q_G) + O(n)$.

(Proof)

$$T'' = t' + O(q_G) + O(n) = t + O(q_e T_n) + O(q_G) + O(n).$$

Q.E.D.

Suppose that $\mathcal{PE}^n$ used in eq.(11) is the trivial multi-recipient scheme. For the trivial scheme, the result of Bellare et al. implies that [2]

$$\mathtt{AdvTO}^{n\text{-cpa}}_{\mathcal{PE}^n,I}(t'') \le n \cdot \mathtt{Adv}^{\text{cpa}}_{\mathcal{PE},I}(t''')$$

where $t''' = t'' + O(nT_s)$ and T_s denotes the time to compte a ciphertext of $\mathcal{PE}$. Since $T_n = nT_s$, we obtain the following corollary.

Corollary 6.1 *In the above (single-plaintext,multi-recipient) scheme* $\mathcal{H}^n$*,*

$$\mathtt{Adv}^{n\text{-cpa}}_{\mathcal{H}^n,I}(t,q_e) \le q_e(n \cdot \mathtt{Adv}^{\text{cpa}}_{\mathcal{PE},I}(t') + \frac{q_G}{2^{l-3}}), \tag{13}$$

where $t' = t + O(q_G) + O(q_e n T_s)$ *and* T_s *denotes the time to compte a ciphertext of* $\mathcal{PE}$*.*

6.3 IND-CCA Hybrid Scheme

First, define a single-recipient hybrid encryption scheme $\mathcal{HY} = (\mathcal{K}_Y, \mathcal{E}_Y, \mathcal{D}_Y)$ from $\mathcal{PE}$ as follows. Let a ciphertext of M be $C = c_1||c_2||c_3$ with

$$c_1 = M \oplus G(r),\ c_2 = H(r||M),\ c_3 = \mathcal{E}_{pk}(r),$$

where r is a random element, H is a hash function and G is a pseudorandom generator. The decryption algorithm $\mathcal{D}_Y$ is defined as

$$\mathcal{D}_{Y\,sk}(c_1||c_2||c_3) = \begin{cases} reject & \text{if } \mathcal{D}_{sk}(c_3) = reject \text{ or } c_2 \ne H(\hat{r}||c_1 \oplus G(\hat{r})) \\ c_1 \oplus G(\hat{r}) & otherwise, \end{cases}$$

where $\hat{r} = \mathcal{D}_{sk}(c_3)$.

Next define a (single-plaintext,multi-recipient) *hybrid* encryption scheme $\mathcal{HY}^n = (\mathcal{K}^n_H, \mathcal{E}^n_H, TAKEH)$ from $\mathcal{PE}^n = (\mathcal{K}^n, \mathcal{E}^n, TAKE)$ as follows. Let a ciphertext of M for a subset of recipients $S = \{i_1, \cdots i_s\}$ be $C_S = c_1||c_2||c_3$, where

$$c_1 = M \oplus G(r),\ c_2 = H(r||M),\ c_3 = \mathcal{E}^n_{\underline{pk}}(S, \underline{r}). \tag{14}$$

For $T \subset S \subseteq N$, let

$$TAKEH_T(C_S) = c_1||c_2||TAKE_T(\mathcal{E}^n_{\underline{pk}}(S, \underline{r})).$$

Now we prove that $\mathcal{HY}^n$ is secure in the sense of indistinguishability against chosen ciphertext attack if $\mathcal{PE}^n$ is secure in the same sense only against type 0 adversaries under the random oracle model, where G and H are modeled as random oracles.

Suppose that an adversary makes at most q_G queries to the G-oracle, at most q_H queries to the H-oracle and at most q_d queries to each decryption oracle $\mathcal{D}_{sk_i}$. Let r be l-bits long, M be k-bits long, $r||M$ be m-bits long and $H(r||M)$ be h bits long. Define

$$\sigma \stackrel{\text{def}}{=} \frac{q_G + q_H}{2^{l-2}} + \frac{nq_d}{2^h}.$$

We first show that $\mathcal{HY}^n$ is secure against type 0 adversaries if $\mathcal{PE}^n$ is so.

Lemma 6.2

$$\mathtt{AdvTO}^{n\text{-cca}}_{\mathcal{HY}^n,I}(t', q_d) \leq \mathtt{AdvTO}^{n\text{-cca}}_{\mathcal{PE}^n,I}(t'', q_d) + \sigma,$$

where $t'' = t' + O(q_G) + O(q_H) + O(q_d) + O(n)$.

A proof is given in Appendix. From lemma 3.1, we have

$$\mathtt{Adv}^{n\text{-cpa}}_{\mathcal{HY}^n,I}(t, q_e, q_d) \leq q_e \mathtt{AdvTO}^{n\text{-cpa}}_{\mathcal{HY}^n,I}(t', q_d)$$

where $t' = t + O(q_e T_n)$. Therefore, we obtain the following Theorem.

Theorem 6.2

$$\mathtt{Adv}^{n\text{-cca}}_{\mathcal{HY}^n,I}(t, q_e, q_d) \leq q_e \left(\mathtt{AdvTO}^{n\text{-cca}}_{\mathcal{PE}^n,I}(t'', q_d) + \sigma \right),$$

where $t'' = t + O(q_e T_n) + O(q_G) + O(q_H) + O(q_d) + O(n)$.

Suppose that $\mathcal{PE}^n$ used in eq.(14) is the trivial multi-recipient scheme. For the trivial scheme, the result of Bellare et al. implies that [2]

$$\mathtt{AdvTO}^{n\text{-cca}}_{\mathcal{PE}^n,I}(t'', q_d) \leq n \cdot \mathtt{Adv}^{\text{cca}}_{\mathcal{PE},I}(t''', q_d),$$

where $t''' = t'' + O(nT_s)$ and T_s denotes the time to compte a ciphertext of $\mathcal{PE}$. Since $T_n = nT_s$, we obtain the following corollary.

Corollary 6.2 *In the above (single-plaintext,multi-recipient) scheme* $\mathcal{HY}^n$*,*

$$\mathtt{Adv}^{n\text{-cca}}_{\mathcal{H}^n,I}(t, q_e, q_d) \le q_e(n \cdot \mathtt{Adv}^{\text{cca}}_{\mathcal{PE},I}(t', q_d) + \sigma), \tag{15}$$

where $t' = t + O(q_e n T_s) + (q_G) + O(q_H) + O(q_d)$ *and* T_s *denotes the time to compte a ciphertext of* $\mathcal{PE}$*.*

6.4 Improvement on Multi-Recipient ElGamal and Cramer-Shoup

In our (multi-plaintext,multi-recipient) ElGamal encryption scheme, suppose that $M = M_{i_1} = \cdots = M_{i_s}$. In this case, let a ciphertext be

$$\bar{C} = (Mg^r, X^r_{i_1}, \cdots, X^r_{i_s}).$$

This scheme is better than our scheme of Sec.4.2 because M is multiplied once. The security is proved similarly. Further, we can consider a hybrid scheme such that

$$\bar{C}' = (Kg^r, X^r_{i_1}, \cdots, X^r_{i_s})||G(K) \oplus M.$$

We can improve our multi-recipient Cramer-Shoup scheme similarly.

Acknowledgement

The author thanks Dr. Burt Kaliski for providing many comments, who shepherded the rewriting of the paper.

References

[1] O.Baudron, D.Pointcheval and J.Stern: "Extended Notions of Security for Multicast Public Key Cryptosystems", ICALP '2000 (2000)

[2] M.Bellare, A.Boldyreva and S.Micali: "Public-key encryption in a multi-recipient setting: Security proofs and improvements", Advances in Cryptology - Eurocrypt'2000 Proceedings, Lecture Notes in Computer Science Vol.1807, Springer Verlag, pp.259–274 (2000)

[3] M.Bellare and P.Rogaway: "Random oracles are practical: A paradigm for designing efficient protocols", Proc. of the 1st CCS, pp.62–73, ACM Press, New York, 1993.
(http://www-cse.ucsd.edu/users/mihir/crypto2k)

[4] D.Boneh: "Simplified OAEP for the RSA and Rabin Functions", Advances in Cryptology - Crypto'2001 Proceedings, Lecture Notes in Computer Science Vol.2139, Springer Verlag, pp.275–291 (2001)

[5] D. Boneh and M. Franklin: "An efficient public key traitor tracing scheme", Advances in Cryptology - Crypto'99 Proceedings, Lecture Notes in Computer Science Vol.1666, Springer Verlag, pp.338-353 (1999)

[6] B. Chor, A. Fiat, and M. Naor, B. Pinkas: "Tracing traitors", IEEE Trans. on IT, vol.46, no.3, pages 893–910 (2000).

[7] D.Coppersmith: "Finding a small root of a univariate modular equation", Advances in Cryptology - Eurocrypt'96 Proceedings, Lecture Notes in Computer Science Vol.1070, Springer Verlag, pp.155-165 (1996)

[8] D.Coppersmith: "Small solutions to polynomial equations, and low exponent RSA vulnerabilities", Journal of Cryptology, 10, pp.233-260 (1997)

[9] R.Cramer and V.Shoup: "A practical public key cryptosystem provably secure against adaptive chosen ciphertext attack", Advances in Cryptology - Crypto'98 Proceedings, Lecture Notes in Computer Science Vol.1462, Springer Verlag, pp.13–25 (1998)

[10] S.Goldwasser and S.Micali : "Probabilistic encryption", Journal Computer and System Sciences, vol.28, pp.270–299 (1984).

[11] J.Hastad : "Solving simultaneous modular equations of low degree", SIAM Journal of Computing, vol.17, pp.336–341 (1988).

[12] K. Kurosawa and Y. Desmedt: Optimum traitor tracing and asymmetric schemes with arbiter. *Advances in Cryptology – Eurocrypt'98, Lecture Notes in Computer Science #1403, Springer Verlag* (1999) 145–157

[13] K.Kurosawa and T.Yoshida: "Linear code implies public-key traitor tracing", PKC'02 (this proceedings)

[14] M.Naor and O.Reingold : "Number theoretic constructions of efficient pseudo-random functions", FOCS'97, pp.458–467 (1997).

[15] M.Stadler: "Publicly verifiable secret sharing", Advances in Cryptology - Eurocrypt'96 Proceedings, Lecture Notes in Computer Science Vol.1070, Springer Verlag, pp.190–199 (1996)

[16] Y.Zheng amd J.Seberry: "Practical approaches to attaining security against adaptively chosen ciphertext attacks", Advances in Cryptology - Crypto'92 Proceedings, Lecture Notes in Computer Science Vol.740, Springer Verlag, pp.292–304 (1992)

A Proof of Lemma 3.1

We show a proof for (multi-plaintext, multi-recipient) schemes against chosen-plaintext attack. The proofs for the other cases are similar. Let B be an adversary which has time-complexity t and makes at most q_e queries. We will design an type 0 adversary D_B with time-complexity at most t'.

Similar to [2], we consider a hybrid experiment with a parameter l such that $0 \leq l \leq q_e$ as follows.

Experiment-l: Let the i-th query of B be $(S, \underline{M}_S^0, \underline{M}_S^1)$. If $i \leq l$, then $\mathcal{E}_{\underline{pk}}$ returns $\mathcal{E}_{\underline{pk}}(S, \underline{M}_S^1)$. Otherwise, it returns $\mathcal{E}_{\underline{pk}}(S, \underline{M}_S^0)$.

Let

$$p_l \stackrel{\text{def}}{=} \Pr[\tilde{b} = 0 \text{ in Experiment-}l].$$

Then it is easy to see that

$$\mathtt{Adv}^{n\text{-cpa}}_{\mathcal{PE}^n, I}(B) = p_0 - p_{q_e}.$$

Next our D_B works as follows. On input $(I, \underline{pk})$, D_B chooses l randomly such that $1 \leq l \leq q_e$. It runs B by giving $(I, \underline{pk})$ to B. Let the i-th query of B be $(S, \underline{M}_S^0, \underline{M}_S^1)$.

1. If $i < l$, then D_B returns $C_S^1 \stackrel{R}{\leftarrow} \mathcal{E}_{\underline{pk}}(S, \underline{M}_S^1)$.

2. If $i > l$, then D_B returns $C_S^0 \stackrel{R}{\leftarrow} \mathcal{E}_{\underline{pk}}(S, \underline{M}_S^0)$.

3. If $i = l$, then D_B queries $(N, \underline{M}_N^0, \underline{M}_N^1)$ to his encryption oracles, where $\underline{M}_S^0$ and $\underline{M}_S^1$ are naturally embedded in $\underline{M}_N^0$ and $\underline{M}_N^1$, respectively. The oracle returns $C_N^b \stackrel{R}{\leftarrow} \mathcal{E}_{\underline{pk}}(N, \underline{M}_N^b)$ to D_B. D_B finally gives $C_S^b = TAKE_S(C_N^b)$ to B.

Suppose that B outputs $\tilde{b}$ finally. Then D_B outputs $\tilde{b}$.

Now we can see that

$$\begin{aligned}\Pr(\tilde{b}=0 \mid b=0) &= (p_0+\cdots p_{q_e-1})/q_e \\ \Pr(\tilde{b}=0 \mid b=1) &= (p_1+\cdots p_{q_e})/q_e\end{aligned}$$

because l is randomly chosen. Therefore,

$$\mathtt{Adv}^{n\text{-cpa}}_{\mathcal{PE}^n,I}(D_B) = (p_0 - p_{q_e})/q_e = \mathtt{Adv}^{n\text{-cpa}}_{\mathcal{PE}^n,I}(B)/q_e.$$

Hence

$$\mathtt{Adv}^{n\text{-cpa}}_{\mathcal{PE}^n,I}(B) = q_e \cdot \mathtt{Adv}^{n\text{-cpa}}_{\mathcal{PE}^n,I}(D_B).$$

By taking the maximum, we obtain that

$$\mathtt{Adv}^{n\text{-cpa}}_{\mathcal{PE}^n,I}(t,q_e) \le q_e \cdot \mathtt{AdvT0}^{n\text{-cpa}}_{\mathcal{PE}^n,I}(t').$$

Finally, the overhead of D_B is to pick the random number l and execute some conditional statements. It is $O(q_e \cdot T_n)$.

B Proof of Lemma 4.1

By extending the result of Stadler [15, in the proof of Proposition 1] and Naor and Reingold [14, lemma 3.2], Bellare et al. proved the following proposition [2].

Proposition B.1 *[2] There is a probabilistic algorithm R such that on input g^a, g^b, g^c, R outputs $g^{b'}, g^{c'}$, where b' is random and*

$$c' = \begin{cases} ab' \bmod p & \textit{if } c = ab \bmod p \\ \textit{random} & \textit{if } c \ne ab \bmod p \end{cases}$$

R runs in $O(T^{\exp})$ time.

Now we show a proof of lemma 4.1. Let B be a type 0 adversary attacking the proposed scheme with time-complexity at most t. We will design an adversary D_B for the DDH problem, where D_B has time complexity at most t'.

Let the input to D_B be g^r, g^x, g^z. D_B runs R of Proposition B.1 n times independently on input (g^r, g^x, g^z). Then R outputs $X_1 = g^{x_1}, \cdots, X_n = g^{x_n}$ and $Z_1 = g^{z_1}, \cdots, Z_n = g^{z_n}$, where $x_1, \cdots, x_n$ are random and

$$z_i = \begin{cases} rx_i \bmod p & \text{if } z = rx \bmod p \\ \text{random} & \text{if } z \ne rx \bmod p \end{cases}$$

D_B gives $X_1, \cdots, X_n$ to B as n public keys and runs B. Suppose that B queries $(M_{0,1}, \ldots, M_{0,n})$ and $(M_{1,1}, \ldots, M_{1,n})$ in the find stage. Then D_B chooses a random bit b and gives $\tilde{C} = (g^r, M_{b,1} \cdot Z_1, \cdots, M_{b,n} \cdot Z_n)$ to B as a challenge ciphertext. Suppose that B outputs $\tilde{b}$ in the guess stage. Finally, D_B outputs $b \oplus \tilde{b}$.

First suppose that $(g^r, g^x, g^z) \in DH$. Then $\tilde{C}$ is a legal ciphertext. Therefore, as shown in eq.(3), we have

$$\Pr(D_B \text{ outputs } 0) = \Pr(\tilde{b} = b) = \frac{1}{2} + \frac{1}{2}\mathtt{Adv}^{n\text{-cpa}}_{\mathcal{EG}^n,(p,g)}(B). \tag{16}$$

Next suppose that $(g^r, g^x, g^z) \in RA$. If $z \neq rx$, then $Z_1, \cdots, Z_n$ are random and $\Pr(\tilde{b} = b) = 1/2$. Hence, we have

$$\begin{aligned} \Pr(D_B \text{ outputs } 0) &= \Pr(\tilde{b} = b) \\ &\leq \frac{1}{2}(1 - \frac{1}{p}) + \frac{1}{p} = \frac{1}{2} + \frac{1}{2p} \end{aligned} \tag{17}$$

From eq.(16) and eq.(17), we have

$$\begin{aligned} \mathtt{Adv}^{\mathrm{ddh}}_{p,g}(D_B) &\geq \frac{1}{2}\mathtt{Adv}^{n\text{-cpa}}_{\mathcal{EG}^n,(p,g)}(B) - \frac{1}{2p} \\ \mathtt{Adv}^{n\text{-cpa}}_{\mathcal{EG}^n,(p,g)}(B) &\leq 2\mathtt{Adv}^{\mathrm{ddh}}_{p,g}(D_B) + \frac{1}{p} \end{aligned}$$

By taking the maximum, we have

$$\mathtt{AdvTO}^{n\text{-cpa}}_{\mathcal{EG}^n,(p,g)}(t) \leq 2 \cdot \mathtt{Adv}^{\mathrm{ddh}}_{p,g}(t') + \frac{1}{p}.$$

It is easy to see that $t' = t + O(n \cdot T^{\exp})$.

C Proof of Theorem 5.1

(u_1', u_2', e', v') is called valid if $u_1' = g_1^{r'}$ and $u_2' = g_2^{r'}$ for some r'. Otherwise, it is called invalid.

We first consider a slightly modified version of $\mathcal{CS}$ such that $h = g_1^{z_1} g_2^{z_2}$, where $z_1 \stackrel{R}{\leftarrow} Z_p$ and $z_2 \stackrel{R}{\leftarrow} Z_p$, and eq.(7) is replaced by

$$M \leftarrow e/u_1^{z_1} u_2^{z_2}. \tag{18}$$

We denote this modified version by $m\mathcal{CS}$.

Lemma C.1 *In the modified version,*

$$\mathtt{Adv}^{\text{s-cca}}_{m\mathcal{CS},(p,g_1)}(t,q_d) \leq 2\cdot \mathtt{Adv}^{\text{ddh}}_{p,g_1}(t') + \epsilon,$$

where $t' = t + O(q_d \cdot T^{\text{exp}})$.

Proof. Let B be an adversary attacking the modified scheme with time-complexity at most t. We will design an adversary D_B for the DDH problem, where D_B has time complexity at most t'.

Let the input to D_B be $g_2, g_1^{r_1}, g_2^{r_2}$. D_B runs $\mathcal{K}(I)$ and obtains (pk, sk). D_B gives pk to B and runs B. D_B can simulate the decryption oracle $\mathcal{D}_{sk}$ because he knows sk.

Suppose that B queries M_0 and M_1 in the find stage. Then D_B chooses a random bit b and computes a challenge ciphertext $C = (u_1, u_2, e, v)$ such that $u_1 = g_1^{r_1}, u_2 = g_2^{r_2}$ and

$$\begin{aligned} e &= u_1^{z_1}u_2^{z_2}M_b \\ v &= u_1^{x_1+\alpha_1 y_{11}+\cdots+\alpha_k y_{k1}}u_2^{x_2+\alpha_1 y_{12}+\cdots+\alpha_k y_{k2}} \end{aligned} \tag{19}$$

where $(\alpha_1, \cdots, \alpha_k) = F(u_1, u_2, e)$. D_B then gives C to B. Suppose that B outputs $\tilde{b}$ in the guess stage. Finally, D_B outputs $b \oplus \tilde{b}$.

First suppose that $(g_2, g_1^{r_1}, g_2^{r_2}) \in DH$, which means that $r_1 = r_2$. In this case, it is easy to see that C is a legal ciphertext. Therefore, from eq.(3), we have

$$\Pr(D_B \text{ outputs } 0) = \Pr(\tilde{b} = b) = \frac{1}{2} + \frac{1}{2}\mathtt{Adv}^{\text{s-cca}}_{m\mathcal{CS},(p,g_1)}(B) \tag{20}$$

Next suppose that $(g_2, g_1^{r_1}, g_2^{r_2}) \in RA$. As shown in [9], it holds that

$$\Pr(\tilde{b} = b \mid \text{the decryption oracle rejects all invalid ciphertexts}) = 1/2 \tag{21}$$

Let

$$p_0 \stackrel{\text{def}}{=} \Pr(\text{at least one invalid ciphertext is accepted}).$$

Claim C.1 $p_0 \leq \epsilon$.

Proof. Suppose that B queries an invalid ciphertext $C' = (u_1', u_2', e', v')$ to the decryption oracle, where

$$u_1' = g_1^{r_1'},\ u_1' = g_2^{r_2'}$$

with $r'_1 \neq r'_2$. Let $F(u'_1, u'_2, e') = (\alpha'_1, \cdots, \alpha'_k)$. Let $g_2 = g_1^w$. First assume that $w \neq 0$.

(Find stage) For fixed $c, d_1, \cdots, d_k$, let A_1 be the set of $X = (x_1, y_{11}, \cdots, y_{k1}, x_2, y_{12}, \cdots, y_{k2})$ which can form $c, d_1, \cdots, d_k$. For a fixed v', let A_2 be the set of secret keys which can form v'. Each X of $A_1 \cap A_2$ must satisfy the set of linear equations whose coefficients matrix is

$$\begin{pmatrix} 1 & & & & w & & & \\ & 1 & & & & w & & \\ & & \ddots & & & & \ddots & \\ & & & 1 & & & & w \\ r'_1 & r'_1\alpha'_1 & \cdots & r'_1\alpha'_k & r'_2 w & r'_2\alpha'_1 w & \cdots & r'_2\alpha'_k w \end{pmatrix}.$$

where the last row corresponds to the equation about v'. By the Gauss elimination, we have

$$\begin{pmatrix} 1 & & & & w & & & \\ & 1 & & & & w & & \\ & & \ddots & & & & \ddots & \\ & & & 1 & & & & w \\ 0 & 0 & \cdots & 0 & (r'_2 - r'_1)w & (r'_2 - r'_1)\alpha'_1 w & \cdots & (r'_2 - r'_1)\alpha'_k w \end{pmatrix}.$$

The last row is linearly independent of the previous rows because $(r'_2 - r'_1)w \neq 0$ from our assumption. Hence,

$$\Pr(C' \text{ is accepted} \mid w \neq 0) \leq |A_1 \cap A_2| / |A_1| = 1/p.$$

(Guess stage) First suppose that $(u'_1, u'_2, e') = (u_1, u_2, e)$. In this case, $v' \neq v$ because $(u'_1, u'_2, e', v') \neq (u_1, u_2, e, v)$. On the other hand, v satisfies eq.(6) because it is computed by eq.(19). Therefore, v' does not satisfy eq.(6). Hence, (u'_1, u'_2, e', v') is rejected.

Next suppose that $(u'_1, u'_2, e') \neq (u_1, u_2, e)$. For fixed $c, d_1, \cdots, d_k$ and v, let A'_1 be the set of $X = (x_1, y_{11}, \cdots, y_{k1}, x_2, y_{12}, \cdots, y_{k2})$ which can form $c, d_1, \cdots, d_k, v$. For a fixed v', let A'_2 be the set of secret keys which can form v'. Each X of $A'_1 \cap A'_2$ must satisfy the set of linear equations whose coefficients matrix is

$$\begin{pmatrix} 1 & & & & w & & & \\ & 1 & & & & w & & \\ & & \ddots & & & & \ddots & \\ & & & 1 & & & & w \\ r_1 & r_1\alpha_1 & \cdots & r_1\alpha_k & r_2 w & r_2\alpha_1 w & \cdots & r_2\alpha_k w \\ r_1' & r_1'\alpha_1' & \cdots & r_1'\alpha_k' & r_2' w & r_2'\alpha_1' w & \cdots & r_2'\alpha_k' w \end{pmatrix}.$$

where the last row corresponds to the equation about v'. By the Gauss elimination, we have

$$\begin{pmatrix} 1 & & & & w & & & \\ & 1 & & & & w & & \\ & & \ddots & & & & \ddots & \\ & & & 1 & & & & w \\ 0 & 0 & \cdots & 0 & (r_2-r_1)w & (r_2-r_1)\alpha_1 w & \cdots & (r_2-r_1)\alpha_k w \\ 0 & 0 & \cdots & 0 & (r_2'-r_1')w & (r_2'-r_1')\alpha_1' w & \cdots & (r_2'-r_1')\alpha_k' w \end{pmatrix}.$$

If $r_2 - r_1 = 0$, then the last row is linearly independent of the previous rows because $(r_2' - r_1')w \neq 0$ from our assumption. Suppose that $r_2 - r_1 \neq 0$. If the last row depends on the previous rows, then we must have

$$1 = \frac{\alpha_1}{\alpha_1'} = \cdots, \frac{\alpha_k}{\alpha_k'}.$$

Hence $(\alpha_1, \cdots, \alpha_k) = (\alpha_1', \cdots, \alpha_k')$. This means that $(u_1, u_2, e) = (u_1', u_2', e')$ because F is an injection. However, this is a contradiction. Therefore, the last row is linearly independent of the previous rows. Hence,

$$\Pr(C' \text{ is accepted} \mid w \neq 0) \leq |A_1' \cap A_2'|/|A_1'| = 1/p.$$

In each stage, we see that

$$\Pr(\text{an invalid } C' \text{ is accepted} \mid w \neq 0) \leq 1/p.$$

Now suppose that B makes at most q_d queries to the decryption oracle. Then it holds that

$$\Pr(\text{at least one invalid ciphertext is accepted} \mid w \neq 0) \leq q_d/p.$$

Therefore,

$$\Pr(\text{at least one invalid ciphertext is accepted}) \leq \left(1 - \frac{1}{p}\right)\frac{q_d}{p} + \frac{1}{p} = \epsilon.$$

$\square$

Now from eq.(21), we have

$$\begin{aligned} \Pr(D_B \text{ outputs } 0) &= \Pr(\tilde{b} = b) \\ &\leq \frac{1}{2}(1 - p_0) + p_0 = \frac{1}{2} + \frac{1}{2}p_0 \end{aligned} \quad (22)$$

From eq.(20) and eq.(22), we obtain that

$$\begin{aligned} \mathtt{Adv}^{\mathrm{ddh}}_{p,g}(D_B) &\geq \frac{1}{2}\mathtt{Adv}^{\text{s-cca}}_{m\mathcal{CS},(p,g)}(B) - \frac{1}{2}p_0 \\ \mathtt{Adv}^{\text{s-cca}}_{m\mathcal{CS},(p,g)}(B) &\leq 2\mathtt{Adv}^{\mathrm{ddh}}_{p,g}(D_B) + p_0 \end{aligned}$$

By taking the maximum, we have

$$\begin{aligned} \mathtt{Adv}^{\text{s-cca}}_{m\mathcal{CS},(p,g_1)}(t, q_d) &\leq 2 \cdot \mathtt{Adv}^{\mathrm{ddh}}_{p,g}(t') + p_0 \\ &\leq 2 \cdot \mathtt{Adv}^{\mathrm{ddh}}_{p,g}(t') + \epsilon. \end{aligned}$$

It is easy to see that $t' = t + O(q_d \cdot T^{\exp})$.

$\square$

Now we show a proof of Theorem 5.1. Let B_1 be an adversary which attacks $\mathcal{CS}$. We will design an adversary B_2 which attacks the modified version $m\mathcal{CS}$ by using B_1 as a subroutine. Let the input to B_2 be (I, pk). Then B_2 gives (I, pk) to B_1 and runs B_1.

Suppose that B_1 outputs $(M_0, M_1, state)$ at the end of the find stage. Then B_2 outputs $(M_0, M_1, state)$ at the end of his find stage. In the guess stage, B_2 gets a challenge ciphertext C_b for M_b, where $b = 0$ or 1. B_2 gives $(C_b, state)$ to the guess stage of B_1. B_1 finally outputs $\tilde{b}$. Then B_2 outputs $\tilde{b}$.

Let D_1 be the decryption oracle for B_1 and D_2 be the decryption oracle for B_2. If B_1 queries a ciphertext C to D_1, then B_2 queries C to D_2. If D_2 returns σ to B_2, then B_2 returns σ to B_1. We show that B_2 simulates D_1 with overwhelming probability.

Now it holds that D_1 rejects C if and only if D_2 rejects C because eq.(6) does not contain z, z_1, z_2. Next suppose that C is accepted by D_1 and D_2. Then there are two cases, C is valid or C is invalid. If C is valid, then D_1 and

D_2 return the same M. This is verified as follows. Let $C = (u'_1, u'_2, e', v')$, where $u'_1 = g_1^{r'}$ and $u'_2 = g_2^{r'}$ for some r'. Then in $\mathcal{CS}$,

$$h^{r'} = (g_1^z)^{r'} = (g_1^{r'})^z = (u'_1)^z.$$

Therefore, D_1 returns $e'/h^{r'}$ from eq.(7). In $m\mathcal{CS}$,

$$h^{r'} = (g_1^{z_1} g_1^{z_2})^{r'} = (g_1^{r'})^{z_1} (g_2^{r'})^{z_2} = (u'_1)^{z_1} (u'_2)^{z_2}.$$

Therefore, D_2 returns $e'/h^{r'}$ from eq.(18).

Now suppose that C is invalid, but it is accepted by D_1 and D_2. If this happens, then B_2 cannot simulate D_1. Let p_{no} denote the probability that this occurs. Then similarly to Claim C.1, it holds that

$$p_{no} \leq \epsilon.$$

Hence,

$$\Pr(\tilde{b} = b \text{ in } B_2) \geq \Pr(\tilde{b} = b \text{ in } B_1) - p_{no}.$$

From eq.(3),

$$\begin{array}{rcl} \mathtt{Adv}^{\text{s-cca}}_{m\mathcal{CS},(p,g_1)}(B_2) & \geq & \mathtt{Adv}^{\text{s-cca}}_{\mathcal{CS},(p,g_1)}(B_1) - 2p_{no} \\ \mathtt{Adv}^{\text{s-cca}}_{\mathcal{CS},(p,g_1)}(B_1) & \leq & \mathtt{Adv}^{\text{s-cca}}_{m\mathcal{CS},(p,g_1)}(B_2) + 2p_{no} \\ & \leq & \mathtt{Adv}^{\text{s-cca}}_{m\mathcal{CS},(p,g_1)}(B_2) + 2\epsilon. \end{array}$$

Finally, from lemma C.1, we have

$$\mathtt{Adv}^{\text{s-cca}}_{\mathcal{CS},(p,g_1)}(t, q_d) \leq 2 \cdot \mathtt{Adv}^{\text{ddh}}_{p,g_1}(t') + 3\epsilon,$$

where $t' = t + O(q_d \cdot T^{\exp})$ because the time-complexity of B_1 is the same as that of B_2.

D Proof of Lemma 6.1

Lemma D.1 *Let E and Y be two events. If*

$$\Pr(E \mid \neg Y) = 1/2,$$

then

$$\Pr(Y) \geq 2\Pr(E) - 1.$$

(Proof)

$$\begin{aligned}\Pr(E) &= \Pr(E \mid Y)\Pr(Y) + \Pr(E \mid \neg Y)\Pr(\neg Y) \\ &\le \Pr(Y) + \frac{1}{2}(1 - \Pr(Y)) \\ &= \frac{1}{2}\Pr(Y) + \frac{1}{2}\end{aligned}$$

Q.E.D.

Lemma D.2 *Let E_1 and E_2 be two events. Then*

$$\Pr(E_1 \wedge \neg E_2) + \frac{1}{2}\Pr(\neg E_1 \wedge \neg E_2) \ge \frac{1}{2} + \frac{1}{2}\Pr(E_1) - \frac{3}{2}\Pr(E_2).$$

(Proof)

$$\begin{aligned}\Pr(E_1 \wedge \neg E_2) + \frac{1}{2}\Pr(\neg E_1 \wedge \neg E_2) &\ge \Pr(E_1) - \Pr(E_2) + \frac{1}{2}(\Pr(\neg E_1) - \Pr(E_2)) \\ &= \Pr(E_1) + \frac{1}{2}(1 - \Pr(E_1)) - \frac{3}{2}\Pr(E_2)) \\ &= \frac{1}{2} + \frac{1}{2}\Pr(E_1) - \frac{3}{2}\Pr(E_2).\end{aligned}$$

Q.E.D.

Let B be a type 0 adversary attacking $\mathcal{H}^n$ with time-complexity at most t'. We will design a type 0 adversary D_B for $\mathcal{PE}^n$, where D_B has time complexity at most t''.

B behaves as follows. Remember that $N = \{1, \cdots, n\}$ is the set of all recpients.

1. B sends N, M_0 and M_1 to the encryption oracle of $\mathcal{H}^n$.
2. The encryption oracle chooses a random bit c and gives a challenge ciphertext $\mathcal{E}^n_{\underline{pk}}(N, r^*)||M_c \oplus G(r^*)$ to B, where r^* is a random element.
3. B finally outputs $\tilde{c}$.

If B does not query r^* to the random oracle G, B has no advantage in distinguishing M_0 and M_1. Therefore,

$$\Pr(c = \tilde{c} \mid r^* \text{ is not queried}) = 1/2.$$

Then from lemma D.1 and eq.(3), we have that

$$\Pr(r^* \text{ is queried}) \geq 2\Pr(c = \tilde{c}) - 1 = \mathtt{AdvTO}^{n\text{-cpa}}_{\mathcal{H}^n, I}(B). \tag{23}$$

Now let the input to D_B be $\underline{pk}$. Then D_B first gives $\underline{pk}$ to B. Next D_B behaves as follows.

1. D_B chooses r_0 and r_1 randomly. It sends $N, (r_0, \cdots, r_0)$ and $(r_1, \cdots, r_1)$ to the encryption oracle of $\mathcal{PE}^n$.

2. Then the encryption oracle chooses a random bit b and gives a challenge ciphertext $Z = \mathcal{E}^n_{\underline{pk}}(N, r_b)$ to D_B.

3. D_B chooses a random element α. It will be used as $G(r_b) = G(r_{1-b}) = \alpha$.

4. D_B runs B as follows.

4-1. If B queries $r \in \{r_0, r_1\}$ to G, then D_B returns α as the value of $G(r)$. Otherwise, D_B simulates the random oracle G in the natural way. (It flips coins to answer queries and makes a set $Q = \{r, G(r)\}$, where r is the query made by B and $G(r)$ is the answer of D_B.)

4-2. Suppose that B sends N, M_0 and M_1 to the encryption oracle of $\mathcal{H}^n$. Then D_B chooses a random bit c and returns a ciphertext of M_u such that $Z||M_u \oplus \alpha$ to B.

5. Suppose that B stops. Then D_B outputs $\tilde{b}$ such that

$$\tilde{b} = \begin{cases} 0 & \text{if } r_0 \in Q \text{ and } r_1 \notin Q \\ 1 & \text{if } r_1 \in Q \text{ and } r_0 \notin Q \\ random & \text{otherwise} \end{cases}$$

D_B fails to simulate G if B queries r_{1-b}. However, B has no information on r_{1-b} through the whole experiment. Therfore, this probability is bounded by

$$\Pr(D_B \text{ fails to simulate}) = \Pr(r_{1-b} \in Q) = q_G/2^l$$

because r_{1-b} is randomly chosen by D_B. Hence,

$$\Pr(r_b \in Q) \geq \mathtt{AdvTO}^{n\text{-cpa}}_{\mathcal{H}^n, I}(B) - q_G/2^{l-1}$$

from eq.(23). Now from lemma D.2, we have that

$$\begin{aligned}
\Pr(\tilde{b}=b) &= \Pr(r_b \in Q \text{ and } r_{1-b} \notin Q) + \frac{1}{2}\Pr(r_b \notin Q \text{ and } r_{1-b} \notin Q) \\
&= \frac{1}{2} + \frac{1}{2}\Pr(r_b \in Q) - \frac{3}{2}\Pr(r_{1-b} \in Q) \\
&\geq \frac{1}{2} + \frac{1}{2}\left(\mathtt{AdvTO}^{n\text{-cpa}}_{\mathcal{H}^n,I}(B) - \frac{q_g}{2^l}\right) - \frac{3}{2}\frac{q_G}{2^l} \\
&= \frac{1}{2} + \frac{1}{2}\mathtt{AdvTO}^{n\text{-cpa}}_{\mathcal{H}^n,I}(B) - \frac{q_G}{2^{l-2}}
\end{aligned}$$

Finally, from eq.(3), we obtain that

$$\begin{aligned}
\mathtt{AdvTO}^{n\text{-cpa}}_{\mathcal{PE}^n,I}(D_B) &\geq \mathtt{AdvTO}^{n\text{-cpa}}_{\mathcal{H}^n,I}(B) - \frac{q_G}{2^{l-3}} \\
\mathtt{AdvTO}^{n\text{-cpa}}_{\mathcal{H}^n,I}(B) &\leq \mathtt{AdvTO}^{n\text{-cpa}}_{\mathcal{PE}^n,I}(D_B) + \frac{q_G}{2^{l-3}} \\
\mathtt{AdvTO}^{n\text{-cpa}}_{\mathcal{H}^n,I}(t) &\leq \mathtt{AdvTO}^{n\text{-cpa}}_{\mathcal{PE}^n,I}(t') + \frac{q_G}{2^{l-3}}.
\end{aligned}$$

It is easy to see that $t'' = t' + O(q_G) + O(n)$.

E Proof of Lemma 6.2

Let B be a type 0 adversary attacking $\mathcal{HY}^n$ with time-complexity at most t'. We will design a type 0 adversary A_B for $\mathcal{PE}^n$, where A_B has time complexity at most t''.

B behaves as follows. Remember that $N = \{1, \cdots, n\}$ is the set of all recpients.

1. B sends N, M_0 and M_1 to the encryption oracle of $\mathcal{HY}^n$.
2. The encryption oracle chooses a random bit u and gives a challenge ciphertext $C_N = c_1||c_2||c_3$ to B, where

$$c_1 = M_u \oplus G(r^*),\ c_2 = H(r^*||M_u),\ c_3 = \mathcal{E}^n_{\underline{pk}}(N, \underline{r^*})$$

and r^* is a random element.

3. B finally outputs $\tilde{u}$.

Let Y be the event that B queries r^* to the random oracle G or $r^*||M$ to the random oracle H for some M. Then it is easy to see that B has no information on u if Y does not occur. Therefore,

$$\Pr(\tilde{u} = u \mid \neg Y) = 1/2.$$

Hence from lemma D.1 and eq.(3), we have

$$\Pr(Y) \geq 2\Pr(\tilde{u} = u) - 1 = \mathtt{Adv}^{n\text{-cca}}_{\mathcal{HY}^n, I}(B). \tag{24}$$

Now let the input to A_B be $\underline{pk}$. Then A_B first gives $\underline{pk}$ to B. Next A_B behaves as follows.

1. A_B chooses r_0 and r_1 randomly. It sends $N, (r_0, \cdots, r_0)$ and $(r_1, \cdots, r_1)$ to the encryption oracle of $\mathcal{PE}^n$.

2. Then the encryption oracle chooses a random bit b and gives a challenge ciphertext $Z = \mathcal{E}^n_{\underline{pk}}(N, r_b)$ to A_B.

3. A_B chooses two random elements α and β. They will be used as

$$G(r_b) = G(r_{1-b}) = \alpha, \quad H(r_b||M_u) = H(r_{1-b}||M_u) = \beta.$$

4. A_B runs B as follows.

4-1. Suppose that B sends N, M_0 and M_1 to the encryption oracle of $\mathcal{HY}^n$. Then A_B chooses a random bit u and returns a ciphertext of M_u such that

$$C_N = M_u \oplus \alpha||\beta||Z$$

to B.

4-2. Supose that $r \in \{r_0, r_1\}$. If B queries r to G, then A_B returns α and if B queries $r||M_u$ to H, then A_B returns β.

4-3. Otherwise, A_B simulates G and H in the natural way. That is, it flips coins to answer the queries and makes the sets $Q_G = \{r, G(r)\}$ and $Q_H = \{r||M, H(r||M)\}$.

4-4. A_B simulates the decryption oracles of $\mathcal{HY}^n$ as follows. Suppose that B asks $C' = c_1'||c_2'||c_3'$ to D_{sk_i}. If $c_3' \neq TAKE_i(Z)$, then A_B can ask c_3' to D_{sk_i}. Hence, A_B can decrypt it properly.

If $c_3' = TAKE_i(Z)$, then A_B cannot ask c_3' to D_{sk_i}. However, we know that c_3' is a ciphertext of r_0 or r_1 in this case. Therefore, if C' is a legal ciphertext, then the plaintext must be $M' \stackrel{\text{def}}{=} c_1' \oplus \alpha$. From this observation, A_B answers as follows.

(a) A_B returns M' to B if $r_0||M' \in Q_H$ and $c_2' = H(r_0||M')$ or if $r_1||M' \in Q_H$ and $c_2' = H(r_1||M')$.

(b) Otherwise, A_B returns *reject* to B.

5. Suppose that B stops. Let Y_0 be the event that $r_0 \in Q_G$ or $r_0||M \in Q_H$ for some M. Let Y_1 be the event that $r_1 \in Q_G$ or $r_1||M \in Q_H$ for some M. Then D_B outputs $\tilde{b}$ such that

$$\tilde{b} = \begin{cases} 0 & \text{if } Y_0 \text{ occurs and } Y_1 \text{ does not occur} \\ 1 & \text{if } Y_1 \text{ occurs and } Y_0 \text{ does not occur} \\ random & \text{otherwise} \end{cases}$$

A_B fails to simulate the real world if

1. Y_{1-b} occurs.
2. At step 4-3 (b), A_B returns *reject* for a legal ciphertext queried by B.

Note that B as no information on r_{1-b} since r_{1-b} is randomly chosen by A_B. Therefore, it holds that

$$\Pr(Y_{1-b} \text{ occurs}) = (q_G + q_H)/2^l.$$

Further, B makes at most nq_d queries in total to the decryption oracles. Hence, we have that

$$p_f \stackrel{\text{def}}{=} \Pr(A_B \text{ fails to simulate the real world}) \leq \frac{q_G + q_H}{2^l} + \frac{nq_d}{2^h}.$$

Then form eq.(24), we obtain that

$$\Pr(Y_b \text{ occurs}) \geq \mathtt{Adv}^{n\text{-cca}}_{\mathcal{HY}^n,I}(B) - p_f.$$

Now from lemma D.2, we have that

$$\Pr(\tilde{b} = b) \quad \geq \quad \Pr(Y_b \text{ and } \neg Y_{1-b}) + \frac{1}{2}\Pr(\neg Y_b \text{ and } \neg Y_{1-b}))$$

$$
\begin{aligned}
&= \frac{1}{2} + \frac{1}{2}\Pr(Y_b) - \frac{3}{2}\Pr(Y_{1-b}) \\
&\geq \frac{1}{2} + \frac{1}{2}(\mathtt{Adv}^{n\text{-cca}}_{\mathcal{HY}^n,I}(B) - p_f) - \frac{3}{2}\frac{q_G + q_H}{2^l} \\
&= \frac{1}{2} + \frac{1}{2}(\mathtt{Adv}^{n\text{-cca}}_{\mathcal{HY}^n,I}(B) - \sigma),
\end{aligned}
$$

where

$$
\sigma = p_f + 3\frac{q_G + q_H}{2^l} = \frac{q_G + q_H}{2^{l-2}} + \frac{nq_d}{2^h}
$$

From eq.(3), we obtain that

$$
\begin{aligned}
\mathtt{Adv}^{n\text{-cca}}_{\mathcal{PE}^n,I}(A_B) &\geq (\mathtt{Adv}^{n\text{-cca}}_{\mathcal{HY}^n,I}(B) - \sigma) \\
\mathtt{Adv}^{n\text{-cca}}_{\mathcal{HY}^n,I}(B) &\leq \mathtt{Adv}^{n\text{-cca}}_{\mathcal{PE}^n,I}(A_B) + \sigma,
\end{aligned}
$$

Therefore,

$$
\begin{aligned}
\mathtt{Adv}^{n\text{-cca}}_{\mathcal{HY}^n,I}(B) &\leq \mathtt{Adv}^{n\text{-cca}}_{\mathcal{PE}^n,I}(A_B) + \sigma \\
\mathtt{AdvTO}^{n\text{-cca}}_{\mathcal{HY}^n,I}(t, q_d) &\leq \mathtt{AdvTO}^{n\text{-cca}}_{\mathcal{PE}^n,I}(t', q_d) + \sigma,
\end{aligned}
$$

It is easy to see that $t'' = t' + O(q_G) + O(q_H) + O(q_d) + O(n)$.