Some General Consequences on Chosen-ciphertext Anonymity in Public-Key Encryption

Tian Yuan[+]

(Software School, Dalian University of Technology, 116600, P.R.China)

+ Corresponding author: Phn: +86-0411-87571582, Fax: +86-0411-87571538, E-mail: tianyuan_ca@sina.com

Abstract

In applications of public-key encryption schemes, anonymity(key-privacy) as well as security(data-privacy) is useful and widely desired. In this paper some new and general concepts in public-key encryption, i.e., “master-key anonymity”, “relevant master-key anonymity” and “key-integrity”, are introduced(the former two are defined for IBE schemes and the latter one is for any public-key encryption scheme). By the concept of master-key anonymity, we prove that chosen-plaintext master-key anonymity is a sufficient condition for chosen-ciphertext anonymity in the recent elegant Canetti-Halevi-Katz and Boneh-Katz construction. By the concept of key-integrity, we prove it is(together with chosen-plaintext anonymity)a sufficient/necessary condition for chosen-ciphertext anonymity. In addition to these general consequences, some practical examples are also investigated to show such concepts’ easy-to-use in practice..

Key words: Computational Cryptography; Provable Security; Anonymity; Master-key Anonymity; Key-Integrity

1 Introduction

As one of the most important cryptographic primitives, public-key encryption schemes are widely used in modern security-sensitive applications. In various requirements not only security but also some additional features of the public-key encryption scheme are desired, among which anonymity(key-privacy) has been surfacing increasingly uptodate. Intuitively, anonymity guarantees that ciphertext can effectively hide its public-key under which the ciphertext is produced, in contrast data security guarantees that ciphertext can effectively hide the plaintext from which it is crafted. Therefore anonymity and security are quite different features from each other. It's no surprising that in high-level applications public-key encryption schemes with both such provable features will be more and more desired.

A precise theoretical treatment on public-key encryption scheme's anonymity (key-privacy) was established for the first time by Bellare et al in [2]. In that paper public-key encryption scheme's anonymity against adaptive chosen-plaintext and chosen-ciphertext attacks are established and some widely-used public-key schemes' anonymity(against specific types of attacks) are concretely proven. Furthermore, a new RSA-based public-key scheme RAEP-RSA is constructed to get around the well-known scheme OAEP-RSA's inanonymity. In some more recent work Abdalla et al [1] established the concept of anonymity in identity-based encryption(IBE) and hierarchical IBE(HIBE) schemes and proved that IBE's anonymity is critical to guarantee the security of the public-key encryption scheme with keyword search(PEKS) in BDOP construction [1,4]. In these work and some others, e.g., [10], public-key encryption scheme's anonymity is a helpful utility in constructing high-level cryptographic schemes or protocols and is fundamental to reach those cryptographic objectives.

According to [2] there are two types of anonymity properties: anonymity against adaptive chosen-plaintext attacks and that against adaptive chosen-ciphertext attacks, the former is strictly weaker than the latter. Just like security, the strongest anonymity(chosen-ciphertext anonymity) is widely desired in high-level cryptographic protocols and security-sensitive applications to resist capable active adversaries. On the other hand, constructing public-key encryption schemes with the strongest anonymity as well as the strongest security is comparatively more difficult than constructing those only with weak anonymity and security. Therefore, we can ask such questions that, in which additional condition(s) can a public-key encryption scheme which is known to be chosen-plaintext anonymous be chosen-ciphertext anonymous? What's the gap between the weak and strong anonymity? How to enhance a public-key encryption scheme only with weak anonymity to one with the strongest anonymity(just like successfully done by many hybrid encryption schemes for security[10-11,14])? Furthermore, for the elegant chosen-ciphertext secure public-key encryption scheme proposed by Canetti-Halevi-Katz[9] and Boneh-Katz[8] based-on IBE schemes, in which condition(s) can such constructions be also chosen-ciphertext anonymous? Obviously, answers to these questions should be very valuable in practice.

Our Contributions In this paper we introduce some new and generic concepts, "*master-key* *anonymity*", "*relevant master-key anonymity*" and "*key-integrity*", to make a step towards answering the above questions. Intuitively, master-key anonymity guarantees an IBE scheme's ciphertext can effectively hide its master public-key, and key-integrity violation models the capability for the adversary to craft new public key(s) and ciphertext(s) from existing ones so that decryptions on new and old cyphertext(s) with new and old secret key(s) respectively would have some adversary-desired relationships. Via these new concepts we prove two general consequences: firstly, Canetti-Halevi-Katz construction(CHK-construction hereafter) is chosen-ciphertext anonymous if the constituent IBE scheme is chosen-plaintext master-key anonymous(together with some other technical conditions, and a similar consequence is proven for BK-construction); secondly, a public-key encryption scheme is chosen-ciphertext anonymous if and only if it is both chosen-plaintext anonymous and chosen-ciphertext key-integral. Not only these consequences provide a different perspective to the strongest anonymity but also they can be used to investigate specific scheme's anonymity in practice. Some concrete examples are analyzed in this paper to give a deeper understanding about these new concepts.

In section 2 we briefly recall some basic concepts and notations. Section 3 introduces the concept of master-key anonymity and proves its sufficiency to CHK-construction's strongest anonymity. Its counterpart consequence for BK-construction is proven in section 4. In section 5 we first analyze a well-known public-key encryption scheme, ElGamal scheme, to see why it is only chosen-plaintext but not chosen-ciphertext anonymous, then we formalize the heuristics from example into the concept of key-integrity and prove its sufficiency/necessity(together with chosen-plaintext anonymity) to chosen-ciphertext anonymity.

2 Preliminaries

This section simply recalls some concepts fundamental to our work, together with some common notations. Let X be a set, we commonly use $a \leftarrow^{\$} X$ to denote that a is randomly selected(with uniform distribution) from X. Regarding other notations, || is a concatenating operator; ⊥ denotes a distinguished error signal which is neither in plaintext nor in ciphertext space; P.P.T. means "probabilistic polynomial time".

Definition 2.1(Public-Key Encryption Scheme) A public-key encryption scheme Π=(KG,E,D) is composed of three P.P.T. algorithms KG, E and D. Let k be complexity parameter, KG is the key generator which takes k as input and outputs public-key/secret-key pair (pk, sk); E is the encryption algorithm which takes public-key pk and plaintext M as input and outputs ciphertext; D is the decryption algorithm which takes secret-key sk and ciphertext y as input and outputs a message M. Additionally, P[(pk, sk)←KG(k); y←E(pk, M): D(sk, y)=M]=1 for any k and M.

Definition 2.2(Anonymity[2])Let Π=(KG,E,D) be a public-key encryption scheme, $A=(A_1,A_2)$ be an P.P.T. adversary, ATK∈{CPA, CCA} and Oracle be oracle determined by ATK. Consider the following game:

```
$Exp_{\pi,A}^{ANO\_ATK}(k)$:
    $(pk_0, sk_0), (pk_1, sk_1) \leftarrow KG(k)$; /*run KG(k) two times independently*/
    $(M^*, St) \leftarrow A_1^{Oracle}(pk_0, pk_1)$;
    $b \xleftarrow{\$} \{0,1\}$;
    $y^* \leftarrow E(pk_b, M)$;
    $d \leftarrow A_2^{Oracle}(y^*, St)$;
    if d=b then output 1 else output 0.
```

In case of ATK=CPA, Oracle is empty; in case of ATK=CCA, Oracle=(D(sk_0, .), D(sk_1, .)) and A is disallowed to query its Oracle on y*. The adversary's advantage $Adv_{\pi,A}^{ANO-ATK}$ is defined as $|2P[Exp_{\pi,A}^{ANO-ATK}(k)=1]-1|$ or equivalently |P[d=0|b=0]-P[d=0|b=1]|. Π is called *anonymous against adaptive chosen-plaintext*(respectively, *adaptive chosen-ciphertext*) *attacks* if $Adv_{\pi,A}^{ANO\_CPA}$ (respectively, $Adv_{\pi,A}^{ANO\_CCA}$) is a negligible function in k. Hereafter we simply omit "adaptive" and denote $\max\limits_{A \in P.P.T.} Adv_{\pi,A}^{ANO-ATK}(k)$ as $Adv_{\pi}^{ANO-ATK}(k)$. Whenever the adversary's advantage is regarded as a function of computational time t and number of oracle queries q, we use the notation $Adv_{\pi}^{ANO\_ATK}(t,q)$ instead of $Adv_{\pi}^{ANO\_ATK}(k)$. For shorthand, we also use the term *ANO_CPA* and *ANO_CCA anonymity* respectively.

Definition 2.3(Relevant Anonymity[15]) Let Π=(KG, E, D) be a public-key encryption scheme, A=(A_1,A_2) be a P.P.T. adversary, ATK∈{CPA, CCA} and Oracle be oracle determined by ATK. Consider the following game:

```
$Exp_{\pi,A}^{RE\_ANO\_ATK}(k)$:
    $(pk_0, sk_0), (pk_1, sk_1) \leftarrow KG(k)$; /*run KG(k) two times independently*/
    $(M^*, St) \leftarrow A_1^{Oracle}(pk_0, pk_1)$;
    $M \xleftarrow{\$} \{0,1\}^{|M^*|}$; /*randomly generate a valid message M in the same size as M*.*/
    $b \xleftarrow{\$} \{0,1\}$;
    $y^* \leftarrow E(pk_b, M)$;
    $d \leftarrow A_2^{Oracle}(y^*, St)$;
    if d=b then output 1 else output 0.
```

In case of ATK=CPA, Oracle is empty; in case of ATK=CCA, Oracle=(D(sk_0, .), D(sk_1, .)). In contrast to the concept of (non-relevant) anonymity, A is allowed to query its oracles D(sk_0, .) and D(sk_1, .) on the challenge ciphertext y*. The adversary's advantage $Adv_{\pi,A}^{RE\_ANO\_ATK}$ is defined as $|2P[Exp_{\pi,A}^{RE\_ANO\_ATK}(k)=1]-1|$ or equivalently |P[d=0|b=0]-P[d=0|b=1]|. We say that Π is *relevantly anonymous against chosen-plaintext*(respectively, *chosen-ciphertext*) *attacks* if $Adv_{\pi,A}^{RE\_ANO\_CPA}$ (respectively, $Adv_{\pi,A}^{RE\_ANO\_CCA}$) is a negligible function in k for any P.P.T. adversary A. We denote $\max_{A\in P.P.T.} Adv_{\pi,A}^{RE\_ANO\_ATK}$ as $Adv_{\pi}^{RE\_ANO\_ATK}$. Whenever the advantage is regarded as a function of computational time t and number of oracle queries q, we use the notation $Adv_{\pi}^{RE\_ANO\_ATK}(t,q)$ instead of $Adv_{\pi}^{RE\_ANO\_ATK}(k)$, and we simply omit the adjective "adaptive" for brevity.

Its easy to prove that Π's anonymity implies its corresponding relevant anonymity, i.e., relevant anonymity is weaker than anonymity. On the other hand, as the following theorem states, relevant anonymity in combination with security can imply (strong) anonymity, which is a very powerful tool for anonymity proof(for self-containment, theorem 2.1's proof is presented in appendix A).

Theorem 2.1[15] *Let* Π=(KG, E, D) *be a public-key encryption scheme which is secure against chosen-plaintext (respectively, chosen-ciphertext) attacks. If* Π *is also relevant anonymous against chosen-plaintext(respectively, chosen-ciphertext) attacks, then* Π *is anonymous against chosen-plaintext(respectively, chosen-ciphertext) attacks. Concretely, we have*

$$Adv_{\pi}^{ANO\_CPA}(t) \le Adv_{\pi}^{RE\_ANO\_CPA}(t) + 2Adv_{\pi}^{IND\_CPA}(t)$$

$$Adv_{\pi}^{ANO\_CCA}(t,q) \le Adv_{\pi}^{RE\_ANO\_CCA}(t,q) + 2Adv_{\pi}^{IND\_CCA}(t+O(qT_d),q)$$

where T_d is computational time of decryption algorithm D. □

Definition 2.4(Identity-based Encryption Scheme: IBE[7]) An IBE scheme Π=(Setup, UKG, E, D) is composed of P.P.T. algorithms Setup, UKG, E and D. Let k be complexity parameter. Setup() is the master-key generator producing master public-key and master secret-key pair (mpk, msk) on input k; UKG() is the user's secret-key generator which takes msk and user identity *a* as input and outputs user's secret-key usk(*a*); E is the encryption algorithm which takes master public-key mpk, user ID *a* and plaintext M as inputs and outputs ciphertext y; D is the decryption algorithm which takes mpk, user's secret-key usk(*a*) and ciphertext y as inputs and outputs a message M. Additionally, P[(mpk,msk)←Setup(k); usk(*a*)←UKG(msk,*a*); y←E(mpk, *a*, M): D(mpk, usk(*a*), y)=M]=1 for any k, *a* and M.

Definition 2.5(Encapsulation Scheme[8]) Encapsulation scheme EC=(P,S,R) is composed of three P.P.T. algorithms, where P takes complexity parameter k as input and outputs a string pub; S takes pub as input and outputs a string r||cmt||dec where |r|=k, cmt is called public commitment string and dec is called de-commitment string; R takes pub, cmt, dec as inputs and outputs(recoveries) r, i.e., P[pub←P(k); r||cmt||dec←S(pub); r*←R(pub, cmt, dec): r*=r]=1 for any value of k.

3 Anonymity in Canetti-Halevi-Katz Construction

3.1 construction

Canetti, Halevi and Katz proposed an elegant and very general public-key encryption scheme(*CHK-construction* hereafter) constructed from an IBE scheme and a one-time signature scheme[9]. Let Π=(Setup, UKG, E, D) be a IBE scheme where constituent algorithms are described in definition 2.3, Sign=(G, Sig, Vf) be a one-time signature scheme where G, Sig, Vf are verification/signature key-pair generating algorithm, signing algorithm and verification algorithm respectively. Furthermore, suppose all scheme Sign's verification keys fall within the set of IBE scheme Π's identifiers[1]. Let k be the complexity parameter. A public-key encryption scheme $\hat{\Pi} = (K\hat{G}, \hat{E}, \hat{D})$ is constructed as follows:

```
$K\hat{G}$(k): (mpk, msk)←Setup(k); set mpk to be public-key and msk to be secret-key;
$\hat{E}$(mpk, M): (svk, ssk)←G(k); y←E(mpk, svk, M); σ←Sig(ssk, y); output(svk||y||σ);
$\hat{D}$(msk, y): parse y as svk||y||σ;
          if   Vf(svk, y, σ)=0   then output($\perp$);
          else   usk←UKG(msk, vsk);
                 M←D(mpk, usk, y);
                 output(M)
```

Compared with all previous chosen-ciphertext secure public-key encryption scheme constructions, CHK-construction is simple, efficient and chosen-ciphertext secure in standard model. In addition, the underlying IBE scheme is only required to be chosen-plaintext secure which is weak and easily to achieve in practice, avoiding any non-interactive proofs of well-formedness which underlies all previously-known constructions. Such security property can be precisely presented in the following:

Proposition 3.1[9] $\hat{\Pi} = (K\hat{G}, \hat{E}, \hat{D})$ *is a public-key encryption scheme constructed as above from the IBE scheme* Π *and one-time signature scheme* Sign. *If* Π *is secure against selective-id, chosen-plaintext attacks and* Sign *is strongly unforgeable*, *then* $\hat{\Pi}$ *is secure against adaptive chosen-ciphertext attacks*. *Concretely, we have*

$$Adv_{\hat{\pi}}^{IND\_CCA}(t,q) \le Adv_{\pi}^{SID\_IN\_CPA}(t + q(T_{Vf} + T_D), q) + 2\,Adv_{Sign}^{SUF\_1}(\mathrm{k}). \qquad \square$$

3.2 Chosen-Plaintext Master-key Anonymity in IBE scheme and its Relationship with Chosen-Ciphertext Anonymity in CHK-construction

In order to investigate $\hat{\Pi}$'s anonymity, we introduce a new and general concept for IBE

[1] More generally, we can assume the existence of a collision-free hash function H mapping the set of Sign's verification keys to the set of IBE scheme Π's identifiers. All results on security and anonymity in CHK-construction remain true in this case, which proofs are almost verbatim of those proofs in CHK's original paper and here.

scheme, named master-key anonymity(or master-key privacy), which is formalized as follows.

Definition 3.1(Master-key Anonymity against Adaptive Chosen-Plaintext Attacks)Let Π=(Setup, UKG, E, D) be a IBE scheme, A=(A_1,A_2) be an P.P.T. adversary, k be complexity parameter. Consider the following game:

$Exp_{\pi,A}^{MPK\_ANO\_CPA}(k)$:

(mpk$_0$, msk$_0$), (mpk$_1$, msk$_1$)←Setup(k); /*run Setup(k) two times independently*/

(*a**, M*, St)← $A_1^{UKG(msk_0,.),UKG(msk_1,.)}$ (mpk$_0$, mpk$_1$);

b$\leftarrow^{\$}${0,1};

y*←E(mpk$_b$, *a**, M*);

d← $A_2^{UKG(msk_0,.),UKG(msk_1,.)}$(y*, St);

if d=b then output 1 else output 0.

In the above game A is disallowed to query *a** of either oracle-UKG(msk$_0$,.) or oracle-UKG(msk$_1$,.). The adversary's advantage $Adv_{\pi,A}^{MPK\_ANO\_CPA}$ is defined as $|2P[Exp_{\pi,A}^{MPK\_ANO\_CPA}(k)=1]-1|$ or equivalently |P[d=0|b=0]- P[d=0|b=1]|. Π is called *master-key anonymous against adaptive chosen-plaintext attacks* (*MPK_ANO_CPA anonymous* for shorthand) if $Adv_{\pi,A}^{MPK\_ANO\_CPA}$ is a negligible function in k. Hereafter we simply omit "adaptive" and denote $\max_{A\in P.P.T.} Adv_{\pi,A}^{MPK\_ANO\_CPA}(k)$ as $Adv_{\pi}^{MPK\_ANO\_CPA}(k)$. Whenever the adversary's advantage is regarded as a function of computational time t and number of oracle queries q, we use the notation $Adv_{\pi}^{MPK\_ANO\_CPA}(t,q)$ instead of $Adv_{\pi}^{MPK\_ANO\_CPA}(k)$.

Via the concept of chosen-plaintext master-key anonymity, we can prove a sufficient condition for CHK-construction's strong anonymity.

Theorem 3.1 $\hat{\Pi}=(K\hat{G},\hat{E},\hat{D})$ *is a CHK public-key encryption scheme constructed from the IBE scheme* Π *and one-time signature scheme* Sign. *If* Π *is MPK_ANO_CPA anonymous and* Sign *is strongly unforgeable*, *then* $\hat{\Pi}$ *is ANO_CCA anonymous*. *Concretely,*

$$Adv_{\hat{\pi}}^{ANO\_CCA}(t,q)\le Adv_{\pi}^{MPK\_ANO\_CPA}(t+q(T_{Vf}+T_D),q)+2\,Adv_{Sign}^{SUF\_1}(k).$$

where T_{vf} *and* T_D *are computational time of* Sign*'s algorithm Vf and* Π*'s decryption algorithm D.*

Proof Let k be complexity parameter, A=(A_1,A_2) be an P.P.T. adversary to break $\hat{\Pi}$'s ANO_CCA anonymity. We construct a P.P.T. adversary B=(B_1,B_2) to break Π's MPK_ANO_CPA anonymity. Consider the following game:

```
$Exp_{\pi,B}^{MPK\_ANO\_CPA}(k)$:
    (mpk$_0$, msk$_0$), (mpk$_1$, msk$_1$)←Setup(k); /*run Setup(k) two times independently*/
    ($a$*, M*, St)← $B_1^{UKG(msk_0,.),UKG(msk_1,.)}$(mpk$_0$, mpk$_1$), where B$_1$ is implemented as:
                    (svk*, ssk*)←G(k);
                    $a$*←svk*;
                    (M*, St$_A$)← $A_1^{\hat{D}(msk_0,.),\hat{D}(msk_1,.)}$(mpk$_0$, mpk$_1$);
                    St←St$_A$||$a$*||M*||ssk*;
                    return($a$*, M*, St);
    b$\leftarrow^{\$}${0,1};
    y*←E(mpk$_b$, $a$*, M*);
    d← $B_2^{UKG(msk_0,.),UKG(msk_1,.)}$(y*, St), where B$_2$ is implemented as:
                    parse St as St$_A$||$a$*||M*||ssk*;
                    σ*←Sig(ssk*, y*);
                    d← $A_2^{\hat{D}(msk_0,.),\hat{D}(msk_1,.)}$($a$*||y*||σ*, St$_A$);
                    return(d);
    if d=b then output 1 else output 0.
```

B simulates A's oracle-$\hat{D}$(msk$_i$,.)'s (i=0,1) computation on $\hat{y}$=a||y||σ as follows:

```
    if Vf($a$, y, σ)=0
    then return(⊥)
    else if $a \neq a$*
        then usk←UKG(msk$_i$, $a$); /*query $a$ of B's own oracle-UKG(msk$_i$,.)*/
            return(D(mpk$_i$, usk, y))
        else /* $\hat{y}$=$a$*||y||σ and Vf($a$*, y, σ)=1*/
            halt
```

It's very clear that on valid outputs(i.e., non-⊥) the simulation is perfect, while in the event of *halt* A just produces a ciphertext $\hat{y}$=a*||y||σ where Vf(a*, y, σ)=1. Because (by definition) A doesn't query a*||y*||σ* on its oracle $\hat{D}$(msk$_i$,.) for any i∈{0,1}, we have y||σ≠y*||σ*, which means（y, σ）is a strongly forged message-signature pair for the one-time signature scheme Sign(with verification/signing key instance (a*,ssk*)). As a result, P[halt]≤$Adv_{Sign,A}^{SUF\_1}$(k).

Furthermore, it's quite straightforward to see that $Exp_{\pi,B}^{MPK\_ANO\_CPA}(k)$ in case of ∼*halt* is exactly equivalent to $Exp_{\hat{\pi},A}^{ANO\_CCA}(k)$ (since in event of ∼*halt* all simulations on A's queries which are valid cyphertexts are perfect), so

$$\mathrm{P}[Exp_{\pi,B}^{MPK\_ANO\_CPA}(k)=1] \geq \mathrm{P}[Exp_{\pi,B}^{MPK\_ANO\_CPA}(k)=1|\sim\mathrm{halt}]\,\mathrm{P}[\sim\mathrm{halt}]$$

= P[$Exp_{\hat{\pi},A}^{ANO\_CCA}(k)$ =1] P[～halt]

= P[$Exp_{\hat{\pi},A}^{ANO\_CCA}(k)$ =1](1-P[halt])

≥ P[$Exp_{\hat{\pi},A}^{ANO\_CCA}(k)$ =1]-P[halt]

≥ P[$Exp_{\hat{\pi},A}^{ANO\_CCA}(k)$ =1]- $Adv_{Sign,A}^{SUF\_1}$ (k)

Namely $Adv_{\hat{\pi},A}^{ANO\_CCA}(k) \le Adv_{\pi,B}^{MPK\_ANO\_CPA}(k)$ +2 $Adv_{Sign,A}^{SUF\_1}$ (k). The computational complexity can be directly verified and the theorem's inequality is immediately derived from the above. □

3.3 A More Practical Consequence

In last subsection we have proven the concept of MPK_ANO_CPA's sufficiency to CHK-construction's strongest anonymity(ANO_CCA). However, MPK_ANO_CPA property is not always easy to prove for IBE schemes. Fortunately, by means of the ideals of *relevant anonymity* and its relationship with security and (strong) anonymity[1,12] the sufficient condition for CHK-construction's anonymity can be significantly weakened to a very easy-to-check property which is named *relevant chosen-plaintext master-key anonymity*(RE_MPK_ANO_CPA for shorthand).

Definition 3.2(Relevant Master-key Anonymity against Chosen-Plaintext Attacks)Let Π=(Setup, UKG, E, D) be a IBE scheme, A=(A$_1$,A$_2$) be an P.P.T. adversary, k be complexity parameter. Consider the following game:

```
$Exp_{\pi,A}^{RE\_MPK\_ANO\_CPA}(k)$ :

    ($mpk_0$, $msk_0$), ($mpk_1$, $msk_1$)←Setup(k); /*run Setup(k) two times independently*/
    ($a$*, M*, St)← $A_1^{UKG(msk_0,.),UKG(msk_1,.)}$ ($mpk_0$, $mpk_1$);
    $M \xleftarrow{\$} \{0,1\}^{|M^*|}$; /*randomly generate a valid message M in the same size as M*.*/
    $b \xleftarrow{\$} \{0,1\}$;
    y*←E($mpk_b$, $a$*, M);
    d← $A_2^{UKG(msk_0,.),UKG(msk_1,.)}$ (y*, St);
    if d=b then output 1 else output 0.
```

In contrast to the concept of (non-relevant) master-key anonymity, in the above game A is allowed to query a* of both oracle-UKG(msk$_0$,.) and oracle-UKG(msk$_1$,.). The adversary's advantage $Adv_{\pi,A}^{RE\_MPK\_ANO\_CPA}$ is defined as $|\,2P[Exp_{\pi,A}^{RE\_MPK\_ANO\_CPA}(k)=1]-1\,|$ or equivalently |P[d=0|b=0]-P[d=0|b=1]|. Π is called *relevant master-key anonymous against adaptive chosen-plaintext attacks* (*RE_MPK_ANO_CPA anonymous* for shorthand) if $Adv_{\pi,A}^{RE\_MPK\_ANO\_CPA}$ is a negligible function in k. Hereafter we simply omit "adaptive" and denote $\max_{A \in P.P.T.} Adv_{\pi,A}^{RE\_MPK\_ANO\_CPA}(k)$ as $Adv_{\pi}^{RE\_MPK\_ANO\_CPA}(k)$. Whenever the adversary's advantage is regarded as a function of computational time t and number of oracle queries q, we use the notation $Adv_{\pi}^{RE\_MPK\_ANO\_CPA}(t,q)$ instead of $Adv_{\pi}^{RE\_MPK\_ANO\_CPA}(k)$.

It's easy to see that relevant master-key anonymity is weaker than its non-relevant counterpart(definition 3.1). To show RE_MPK_ANO_CPA is easy-to-check in practice, we show in the following example that the well-known Boneh-Franklin IBE scheme is RE_MPK_ANO_CPA.

Example 3.1(Boneh-Franklin IBE scheme[7]) Let (q, P, G, G_T, e:G×G→G_T) be a bilinear pairing configuration on which the BCDH(bilinear computational Diffie-Hellman) problem is computationally hard. Furthermore, H_1: $\{0,1\}^*$→G_1, H_2: G_2→$\{0,1\}^n$ are random oracles where n is the size of plaintext and k is the complexity parameter. Boneh-Franklin scheme works as follows:

```
Setup(k):   $s \leftarrow^{\$} Z^*_q$; mpk←sP; msk←s; return(mpk, msk)
UKG(msk, $a$), where $a \in \{0,1\}^+$ is the user's ID and msk=s:
            usk←$sH_1(a)$; return(usk);
E(mpk, $a$, M):
            $r \leftarrow^{\$} Z^*_q$; T←M⊕$H_2(e(H_1(a), mpk)^r)$; y←rP||T; return(y)
D(mpk, usk, y):
            Parse y as $y_0$||T; M←T⊕$H_2(e(usk, y_0))$
```

It's quite straightforward to see that in $Exp_{B-F,A}^{RE\_MPK\_ANO\_CPA}(k)$ when M is selected at random by the challenger, in particular independent of the adversary's choice M*, the challenge ciphertext y=rP||(M⊕$H_2(e(H_1(a), mpk_0)^r)$) has exactly the same (uniform) distribution in both cases of b=0 and b=1 from the adversary's perspective(because H_1 is random oracle, even accesses to oracle-UKG's doesn't help to distinguish these cases). As a result, $Adv_{B-F,A}^{RE\_MPK\_ANO\_CPA}$=0 unconditionally holds. □

The strength of RE_MPK_ANO_CPA is manifested in the following theorem.

Theorem 3.2 $\hat{\Pi}=(K\hat{G},\hat{E},\hat{D})$ *is a CHK public-key encryption scheme constructed from the IBE scheme* Π *and one-time signature scheme* Sign. *If* Π *is RE_MPK_ANO_CPA anonymous, then* $\hat{\Pi}$ *is relevant anonymous against chosen-ciphertext attacks (RE_ANO_CCA). Concretely,*

$$Adv_{\hat{\pi}}^{RE\_ANO\_CCA}(t,q) \leq Adv_{\pi}^{RE\_MPK\_ANO\_CPA}(t+q(T_{Vf}+T_D),q)$$

where T_{vf} *and* T_D *are computational time of* Sign*'s algorithm Vf and* Π*'s decryption algorithm D.*

Proof The proof is almost verbatim from the proof of theorem 3.1, except that (1)A and B are adversaries respectively to break $\hat{\Pi}$ and Π's RE_ANO_CPA and RE_MPK_ANO_CPA anonymity; (2)games $Exp_{\pi,B}^{MPK\_ANO\_CPA}$ and $Exp_{\hat{\pi},A}^{ANO\_CPA}$ are replaced with $Exp_{\pi,B}^{RE\_MPK\_ANO\_CPA}$ and $Exp_{\hat{\pi},A}^{RE\_ANO\_CPA}$ respectively; (3) the challenge ciphertext to B is the encryption of a randomly generated plaintext M independent of B_1's choice M*; (4)because both $Exp_{\pi,B}^{RE\_MPK\_ANO\_CPA}$ and $Exp_{\hat{\pi},A}^{RE\_ANO\_CPA}$ respectively allow their adversaries querying the challenge identity *a** and challenge ciphertext y* of their oracles, scheme-Sign's strongly unforgeability is not required in this proof. □

In combination with theorem 3.2(constituent IBE scheme's RE_MPK_ANO_CPA anonymity implies CHK-construction's RE_ANO_CCA anonymity), Proposition 3.1 (CHK-construction is IND_CCA under some conditions) and theorem 2.1(IND_CCA security plus RE_ANO_CCA anonymity implies ANO_CCA anonymity), it's easy to get the following consequence:

Corollary 3.1 $\hat{\Pi} = (K\hat{G}, \hat{E}, \hat{D})$ *is a CHK public-key encryption scheme constructed from the IBE scheme* Π *and one-time signature scheme* Sign. *If* Π *is SID_IND_CPA secure, RE_MPK_ANO_CPA anonymous and* Sign *is strongly unforgeable*, *then* $\hat{\Pi}$ *is both secure and anonymous against chosen-ciphertext attacks* (i.e., *both IND_CCA and ANO_CCA*). □

Remark A noticeable fact is that although corollary 3.1 seems stronger than theorem 3.1, the latter's consequence does not depend on the constituent IBE's security property, i.e., even the constituent IBE scheme is not SID_IND_CPA the CHK-construction can be still ANO_CCA. Therefore, theorem 3.1 may be of its own values.

3.4 More Examples on Master-Key Anonymity

Theorem 3.2(and theorem 4.1 in next section) reduces anonymous CHK-constructions(or BK-construction in next section) to RE_MPK_ANO_CPA anonymous IBE schemes. To get more understanding about this new concept, we investigate more typical IBE schemes' RE_MPK_ANO_CPA anonymity in this section.

Example 3.2(Boyen-Waters scheme [4]) Let k be complexity parameters. Boyen-Waters IBE scheme's constituent algorithms are defined respectively as follows.

```
Setup(k):
        randomly select a bilinear pairing configuration ($G_1$,$G_2$,p,$e$) where |$G_1$|=|$G_1$|=p and p is prime in size of k-bits;
        g, $g_0$, $g_1$←$G_1$;   ω, $t_1$, $t_2$, $t_3$, $t_4$$\leftarrow^{\$}Z_p$;   $\Omega \leftarrow e(g, g)^{t1t2\omega}$;
        $v_1 \leftarrow g^{t1}$; $v_2 \leftarrow g^{t2}$; $v_3 \leftarrow g^{t3}$; $v_4 \leftarrow g^{t4}$;
        mpk←($G_1$,$G_2$,p,$e$, Ω, g, $g_0$, $g_1$, $v_1$, $v_2$, $v_3$, $v_4$);
        msk←(mpk, ω, $t_1$, $t_2$, $t_3$, $t_4$);
        return(mpk, msk);
```

```
UKG(msk, $a$) where $a \in Z_p$
        $r_1, r_2 \xleftarrow{\$} Z_p$;
        usk($a$)$\leftarrow$( $g^{r_1 t_1 t_2 + r_2 t_3 t_4}, g^{-\varpi t_2}(g_0 g_1{}^{a})^{-r_1 t_2}, g^{-\varpi t_1}(g_0 g_1{}^{a})^{-r_1 t_1}, (g_0 g_1{}^{a})^{-r_2 t_4}, (g_0 g_1{}^{a})^{-r_2 t_3}$ );
        return(usk($a$));
E(mpk, $a$, M) where $M \in G_2$
        $s, s_1, s_2 \xleftarrow{\$} Z_p$;
        y$\leftarrow$($\Omega^s$M, $(g_0 g_1{}^{a})^{s}$, $v_1{}^{s-s1}$, $v_2{}^{s1}$, $v_3{}^{s-s2}$, $v_4{}^{s2}$);
        return(y);
D(mpk, usk($a$), y)
        Parse y as ($y_{00}$, $y_0$, $y_1$, $y_2$, $y_3$, $y_4$) and usk($a$) as ($d_0$, $d_1$, $d_2$, $d_3$, $d_4$);
        T$\leftarrow$$e(d_0, y_0)e(d_1, y_1)e(d_2, y_2)e(d_3, y_3)e(d_4, y_4)$;
        return($y_{00}$/T);
```

In [4](refer to its section 4, lemma 2 and 3) it is proven under the assumption of decisional linear problem's hardness that (Ω^sM, $(g_0 g_1{}^{a})^{s}$, $v_1{}^{s-s1}$, $v_2{}^{s1}$, $v_3{}^{s-s2}$, $v_4{}^{s2}$) is computationally distinguishable from (R, $(g_0 g_1{}^{a})^{s}$, R_1, $v_2{}^{s1}$, R_3, $v_4{}^{s2}$) where R, R_1 and R_3 are selected randomly and independently. Since s, s_1 and s_2 are selected randomly and independently each other and so are g_0, g_1, v_2 and v_4, all components of (R, $(g_0 g_1{}^{a})^{s}$, R_1, $v_2{}^{s1}$, R_3, $v_4{}^{s2}$) are at random and probabilistically independent each other. As a result, for the MPK_ANO_CPA adversary the challenge ciphertext's distributions in both cases of b=0 and b=1 are computationally indistinguishable from a purely random ciphertext (R, R_0, R_1, R_2, R_3, R_4). therefore, Boyen-Waters scheme is MPK_ANO_CPA anonymous(in fact also IBE_ANO_CCA anonymous, refer the concept of IBE_ANO_CPA anonymity to appendix B) under the assumption of decisional linear problem's hardness. □

Example 3.3(Waters scheme [16]) Let k be complexity parameters and n be a polynomial of k. Waters IBE scheme's constituent algorithms are defined respectively as follows.

```
Setup(k):
        randomly select a bilinear pairing configuration ($G_1$,$G_2$,p,$e$) where
    |$G_1$|=|$G_1$|=p and p is prime in size of k-bits;
        P, Q$\xleftarrow{\$}G_1$;  $\alpha \xleftarrow{\$} Z_p$;  $P_1 \leftarrow \alpha P$;  $Q_1 \leftarrow \alpha Q$;
        U[0..n]$\xleftarrow{\$}G^{n+1}$;  E$\leftarrow$$e$(P, Q);
        mpk$\leftarrow$($G_1$,$G_2$,p,$e$,P, $P_1$,U,E);
        msk$\leftarrow$(mpk,$Q_1$);
        return(mpk, msk);
UKG(msk, $a$) where $a$=$a$(1)…$a$(n)$\in\{0,1\}^n$
        Parse msk as (($G_1$,$G_2$,p,$e$,P, $P_1$,U,E), $Q_1$);
        $r \leftarrow^{\$} Z_p$;   $V \leftarrow U[0]+\sum_{i=1}^{n} a(i)U[i]$;
        usk($a$)$\leftarrow$($Q_1$+rV, rP);
        return(usk($a$));
    E(mpk, $a$, M) where $M \in G_2$
        Parse msk as (($G_1$,$G_2$,p,$e$,P, $P_1$,U,E), $Q_1$);
        $V \leftarrow U[0]+\sum_{i=1}^{n} a(i)U[i]$;
        $t \leftarrow^{\$} Z_p$;   $T \leftarrow E^t$;
        y$\leftarrow$(TM, tP, tV);
        return(y);
    D(mpk, usk($a$), y)
        Parse y as ($y_1$, $y_2$, $y_3$) and usk($a$) as ($s_1$, $s_2$);
        T$\leftarrow$$e$($s_1$, $y_2$)/$e$($s_2$, $y_3$);
        return($y_1$/T);
```

The critical point is that e(P, y_3)=e(y_2, V(a)) holds for any valid ciphertext y=(y_1, y_2, y_3) with master public key mpk=(G_1,G_2,p,e,P, P_1,U,E). Because pairing e is non-degenerate, such equation can easily derive a RE_MPK_ANO_CPA attack on this scheme(in fact the same equation can also derive an IBE_ANO_CPA attack. Refer the concept of IBE_ANO_CPA anonymity to appendix B). As a result, Waters scheme is neither RE_MPK_ANO_CPA anonymous(so of course neither MPK_ANO_CPA anonymous) nor IBE_ANO_CPA anonymous. □

4 Anonymity in Boneh-Katz Construction

Boneh and Katz[8] proposed another public-key encryption scheme construction based-on IBE which is not only provably chosen-ciphertext secure but also more computationally efficient than CHK-construction. In this section we prove a consequence on Boneh-Katz construction's ANO_CCA anonymity which is very similar as that on CHK-construction. As a result, both CHK-construction and BK-construction have very fine features in practice.

Let Π=(Setup, UKG, E, D) be a IBE scheme where constituent algorithms are described in definition 2.3, EC=(P, S, R) be an encapsulation scheme as described in definition 2.5 where P, S, R are key-generating, secret commitment and recovery algorithms respectively, and MAC=(G, Mac, Vf) be a message authentication scheme where G, Mac, Vf are key generating, message authenticating and verifying algorithms respectively. Furthermore, suppose all scheme EC's commitment strings fall within the set of Π's identifiers and MAC's authentication keys. Let k be the complexity parameter. A public-key encryption scheme $\hat{\Pi} = (K\hat{G}, \hat{E}, \hat{D})$ is constructed as follows:

```
$K\hat{G}$(k):
        (mpk, msk)←Setup(k); pub←P(k);
        set mpk||pub to be public-key and msk||pub to be secret-key;
$\hat{E}$ (mpk||pub, M):
        r||cmt||dec←S(pub);
        y←E(mpk, cmt, M||dec); /* use cmd as ID. */
        σ←Mac(r, y);
        output(cmt||y||σ);
$\hat{D}$ (msk||pub, $\hat{y}$ ): parse $\hat{y}$ as cmt||y||σ;
        usk←UKG(msk, cmt);
        M||dec←D(mpk, usk, y);
        r←R(pub, cmt, dec);
        if  Vf(r, y, σ)=0 then output( ⊥) else output(M)
```

BK-construction's security is proved in the following theorem:

Proposition 4.1[8] $\hat{\Pi} = (K\hat{G}, \hat{E}, \hat{D})$ *is a public-key encryption scheme constructed as above from the IBE scheme* Π, *encapsulation scheme* EC *and message authentication scheme* MAC. *If* Π *is secure against selective-id, chosen-plaintext attacks,* EC *is secure encapsulated and* MAC *is strongly unforgeable against one-time chosen-message attacks*[2], *then* $\hat{\Pi}$ *is secure against adaptive chosen-ciphertext attacks.* □

Similar as in the case of CHK-construction, RE_MPK_ANO_CPA anonymity is critical for BK-construction's chosen-ciphertext anonymity.

Theorem 4.1 $\hat{\Pi} = (K\hat{G}, \hat{E}, \hat{D})$ *is a BK public-key encryption scheme constructed from the IBE scheme* Π, *encapsulation scheme* EC *and message authentication scheme* MAC *as above. If* Π *is RE_MPK_ANO_CPA anonymous*, *then* $\hat{\Pi}$ *is relevant anonymous against chosen-ciphertext attacks* (*RE_ANO_CCA*). *Concretely,*

$$Adv_{\hat{\pi}}^{RE\_ANO\_CCA}(t,q) \le 2\, Adv_{\pi}^{RE\_MPK\_ANO\_CPA}(t + q(T_R + T_{Vf} + T_D), q)$$

where T_R , T_{Vf} *and* T_D *are computational time of* EC*'s algorithm R*, *MAC's verifying algorithm Vf and* Π*'s decryption algorithm D respectively.*

Proof Let k be complexity parameter, A=(A$_1$,A$_2$) be an P.P.T. adversary to break $\hat{\Pi}$'s RE_ANO_CCA anonymity. We construct a P.P.T. adversary B^A=(B$_1$,B$_2$) to break Π's RE_MPK_ANO_CPA anonymity. Consider the following game:

```
$Exp_{\pi,B}^{RE\_MPK\_ANO\_CPA}(k)$ :
        (mpk$_0$, msk$_0$), (mpk$_1$, msk$_1$)←Setup(k); /*run Setup(k) two times independently*/
```

[2] The concepts of secure encapsulation and unforgeability against one-time chosen-message attacks are omitted since they are not used in this paper.

```
($a$*, M*, St)← $B_1^{UKG(msk_0,.),UKG(msk_1,.)}$ (k, $mpk_0$, $mpk_1$), where $B_1$ is implemented as:
        $pub_0$, $pub_1$←P(k); /*run two times independently.*/
        $pk_0$←$mpk_0||pub_0$; $pk_1$←$mpk_1||pub_1$; /* $sk_i$=$msk_i||pub_i$ for i=0,1*/
        $r_0||cmt_0||dec_0$←S($pub_0$); $r_1||cmt_1||dec_1$←S($pub_1$);
        $a$*←$cmt_0$;
        (m*, $St_A$)← $A_1^{\hat{D}(sk_0,.),\hat{D}(sk_1,.)}$ ($pk_0$, $pk_1$);
        M*←m*||$dec_0$;
        St←$St_A$||m*||$r_0||cmt_0||dec_0||$ $r_1||cmt_1||dec_1$;
        return($a$*, M*, St);
M$\xleftarrow{\$}$$\{0,1\}^{|M*|}$; /*randomly generate a valid message M in the same size as M*.*/
b$\xleftarrow{\$}$$\{0,1\}$;
y*←E($mpk_b$, $a$*, M);
d← $B_2^{UKG(msk_0,.),UKG(msk_1,.)}$ (y*, St), where $B_2$ is implemented as:
        parse St as $St_A$||m*||$r_0||cmt_0||dec_0||$ $r_1||cmt_1||dec_1$;
        σ*←Mac($r_0$, y*);
        d← $A_2^{\hat{D}(sk_0,.),\hat{D}(sk_1,.)}$ ($cmt_0$||y*||σ*, $St_A$);
        return(d);
if d=b then output 1 else output 0.
```

B simulates A's oracle-$\hat{D}$ ($msk_i||pub_i$,.)'s (i=0,1) computation on $\hat{y}$ =a||y||σ as follows:

```
usk←UKG($msk_i$, $a$); /* call B's own oracle-U($msk_i$, .) */
M||dec←D($mpk_i$, usk, y);
r←R($pub_i$, $a$, dec);
if  Vf(r, y, σ)=0 then output(⊥) else output(M)
```

It's very clear that on valid queires the simulation is perfect, because both $Exp_{\pi,B}^{RE\_MPK\_ANO\_CPA}$ and $Exp_{\hat{\pi},A}^{RE\_ANO\_CPA}$ allow their adversaries querying the challenge identity a* and challenge ciphertext y* of their oracles respectively. Furthermore, note that $Exp_{\pi,B}^{RE\_MPK\_ANO\_CPA}$ in case of b=0 is exactly equivalent to $Exp_{\hat{\pi},A}^{RE\_ANO\_CPA}$ in cased of b=0, so $Adv_{\pi,B}^{RE\_MPK\_ANO\_CPA}$(k)

= |P[$Exp_{\pi,B}^{RE\_MPK\_ANO\_CPA}$(k)=1|b=0]-P[$Exp_{\pi,B}^{RE\_MPK\_ANO\_CPA}$(k)=1|b=1]|

= |P[$Exp_{\hat{\pi},A}^{RE\_ANO\_CPA}$(k)=1|b=0]-P[$Exp_{\pi,B}^{RE\_MPK\_ANO\_CPA}$(k)=1|b=1]|

On the other hand, we can construct another P.P.T. adversary C^A=(C_1,C_2) to break Π's RE_MPK_ANO_CPA anonymity, which specification is almost the same as B^A with the only differences that (1) in C_1 the statements a*←cmt_0 and M*←m*||dec_0 are replaced with a*←cmt_1 and M*←m*||dec_1 respectively; (2) in C_2 statements σ*←Mac(r_0, y*) and d← $A_2^{\hat{D}(sk_0,.),\hat{D}(sk_1,.)}$ (cmt_0||y*||σ*, St_A) are replaced with σ*←Mac(r_1, y*) and d← $A_2^{\hat{D}(sk_0,.),\hat{D}(sk_1,.)}$ (cmt$_1$||y*||σ*, St$_A$) respectively. By the same observation we have

$$Adv_{\pi,C}^{RE\_MPK\_ANO\_CPA}(k)$$
$$= |P[Exp_{\pi,C}^{RE\_MPK\_ANO\_CPA}(k)=1|b=0]-P[Exp_{\pi,C}^{RE\_MPK\_ANO\_CPA}(k)=1|b=1]|$$
$$= |P[Exp_{\pi,C}^{RE\_MPK\_ANO\_CPA}(k)=1|b=0]-P[Exp_{\hat{\pi},A}^{RE\_ANO\_CPA}(k)=1|b=1]|$$

A further observation tells that $Exp_{\pi,B}^{RE\_MPK\_ANO\_CPA}$ in case of b=1 is exactly equivalent to $Exp_{\pi,C}^{RE\_MPK\_ANO\_CPA}$ in case of b=0 from A's perspective in terms of probabilistic distribution, therefore

$$Adv_{\pi,B}^{RE\_MPK\_ANO\_CPA}(k) + Adv_{\pi,C}^{RE\_MPK\_ANO\_CPA}$$
$$= |P[Exp_{\hat{\pi},A}^{RE\_ANO\_CPA}(k)=1|b=0]-P[Exp_{\pi,B}^{RE\_MPK\_ANO\_CPA}(k)=1|b=1]|+$$
$$|P[Exp_{\pi,C}^{RE\_MPK\_ANO\_CPA}(k)=1|b=0]-P[Exp_{\hat{\pi},A}^{RE\_ANO\_CPA}(k)=1|b=1]|$$
$$\geq |P[Exp_{\hat{\pi},A}^{RE\_ANO\_CPA}(k)=1|b=0]-P[Exp_{\hat{\pi},A}^{RE\_ANO\_CPA}(k)=1|b=1]|$$
$$= Adv_{\hat{\pi},A}^{RE\_ANO\_CCA}(k)$$

The computational complexity can be directly verified and the theorem's inequality is immediately derived from the above. □

In combination with theorem 4.1(constituent IBE scheme's RE_MPK_ANO_CPA anonymity implies BK-construction's RE_ANO_CCA anonymity), Proposition 4.1 (BK-construction is IND_CCA secure under some conditions) and theorem 2.1(IND_CCA security plus RE_ANO_CCA anonymity implies ANO_CCA anonymity in general), it's easy to get the following consequence:

Corollary 4.1 $\hat{\Pi}=(K\hat{G},\hat{E},\hat{D})$ *is a BK public-key encryption scheme constructed from constituent IBE scheme* Π, *encapsulation scheme* EC *and message authentication scheme* MAC *as above*. *If* Π *is both SID_IND_CPA secure and RE_MPK_ANO_CPA anonymous,* EC *is secure encapsulated and* MAC *is strongly unforgeable against one-time chosen-message attacks*, *then* $\hat{\Pi}$ *is both secure and anonymous against chosen-ciphertext attacks* (i.e., *both IND_CCA and ANO_CCA*). □

5 Key-Integrity: The Gap between Weak and Strong Anonymity

In this section we introduce another new and general concept, "key-integrity", to connect the concept of chosen-plaintext anonymity and that of chosen-ciphertext anonymity. Firstly a heuristic example is investigated to get some observations on why a chosen-plaintext anonymous scheme is not chosen-ciphertext anonymous; secondly the observation is formalized and a sufficient/necessary condition to fill the gap between ANO_CPA and ANO_CCA anonymity is proved; thirdly one more complicated example is investigated to show the concept of key-integrity is actually orthogonal with the well-known concept of anonymity(key-privacy).

5.1 A Heuristic Example: ElGamal Scheme

In [2] ElGamal scheme is proven anonymous against chosen-plaintext attacks under the assumption of decisional Diffie-Hellman problem's hardness. This scheme is presented in figure 1. However, ElGamal scheme is not anonymous against chosen-ciphertext attacks. Firstly we observe that if (Y,W) is a valid ElGamal ciphertext produced by public-key X, then for arbitary z in Z_q, (Y,Y^zW) is also a valid ciphertext produced by public-key Xg^z. Furthermore, let x be X's secret-key then $D(x, (Y,Y^zW))=Y^zD(x,(Y,W))$. Based-on this fact, a chosen-ciphertext adversary $A=(A_1,A_2)$ can work in this way to break its anonymity: $A_1(X_0,X_1)$ randomly generate a message M from group G; then A_2(taking challenge ciphertext (Y,W) as its input) randomly selects a non-zero element z in Z_q, gets $M_0\leftarrow D(x_0, (Y,Y^zW))$ and $M_1\leftarrow D(x_1, (Y,Y^zW))$ via its decryption oracle $D(x_0,.)$ and $D(x_1,.)$, and makes decision on b=0 or 1 respectively according to $M_0=Y^zM$ or $M_1=Y^zM$. It's easy to verify that the adversary's advantage $Adv_{\pi,A}^{ANO-CCA}(t,q)=1$ where q=2 and t is obviously a polynomial in k.

```
Key generator KG(q,g):
    $x \leftarrow^{\$} Z_q$;
    $X \leftarrow g^x$;
    $pk \leftarrow (q,g,X)$;
    $sk \leftarrow (q,g,x)$;
    return(pk,sk)
```

```
Encryption algorithm E(pk, M), M∈G:
    $r \leftarrow^{\$} Z_q$;
    $Y \leftarrow g^r$;
    $T \leftarrow X^r$;
    $W \leftarrow TM$;
    return(Y, W)
```

```
Decryption algorithm D(sk, (Y,W)):
    $T \leftarrow Y^x$;
    $M \leftarrow W/T$;
    return(M)
```

Figure 1: ElGamal Scheme. G is a prime-order(q) group with generator g.

The critical point for the above attacker's success is that given a public key $pk_0=X_0$ and valid ciphertext y=(Y,W)(but the corresponding secret key sk_0 is unknown), there can be found another public key $pk_1=g^zX_0$, a function h and new valid ciphertext $y^*=(Y,Y^zW)$ such that decryptions on y* and y respectively with secret keys sk_1 and sk_0 have some relationship: $D(sk_1, y^*)=h(D(sk_0,y^*),y)$, or more concretely in the above attack: $D(x_1, (Y,Y^zW))=Y^{-z}D(x_0, (Y,Y^zW))$. In next section we'll carefully generalize this observation to find a sufficient and necessary condition for a chosen-plaintext anonymous scheme to be anonymous against chosen-ciphertext attacks.

5.2 Key-integrity as a Sufficient and Necessary Condition for Chosen-ciphertext Anonymity

In this subsection we formalize the heuristics on the attack to ElGamal scheme's chosen-ciphertext anonymity into a general concept, "key-integrity", and then prove its sufficiency and necessity for chosen-ciphertext anonymity.

Definition 5.1(key-integrity) Let Π=(KG, E, D) be a public-key encryption scheme, $U=(U_1,U_2)$ be an P.P.T. adversary, ATK∈{CPA, CCA} and Oracle be oracle determined by

ATK. Consider the following game:

```
$Exp_{\pi,A}^{KINT\_ATK}(k)$:
        ($pk_0$, $sk_0$)←KG(k);
        (M, St)←$U_1^{Oracle}$($pk_0$);
        y←E($pk_0$, M);
        ($pk_1$, h, ψ)←$U_2^{Oracle}$(y, St), such that $pk_0$≠$pk_1$ and
                      h, ψ are P.P.T. algorithms and ψ≠E;
        y*←ψ($pk_1$, y) such that y* is not independent of y.
                      (i.e., ψ is really a function on y);
        if D($sk_1$, y*)=h(D($sk_0$,y*),y)
        then output 1;
        else output 0.
```

In case of ATK=CPA, Oracle is empty; in case of ATK=CCA, Oracle=D(sk_0, .) and A is disallowed to query its Oracle on y*. The adversary's advantage $Adv_{\pi,A}^{KINT\_ATK}$ is defined as $P[Exp_{\pi,A}^{KINT\_ATK}(k)=1]$. Whenever it is considered as a function of computation time t and number of oracle queries q, we also use the notation $Adv_{\pi,A}^{KINT\_ATK}(t,q)$ instead of $Adv_{\pi,A}^{KINT\_ATK}(k)$. We say that Π is of *key-integrity against adaptive chosen-plaintext*(*respectively, chosen-ciphertext*) *attacks* if $Adv_{\pi,A}^{KINT\_CPA}(k)$ (respectively, $Adv_{\pi,A}^{KINT\_CCA}(k)$) is a negligible function in k for any P.P.T. adversary A. Hereafter we notate $\max_{A\in P.P.T.} Adv_{\pi,A}^{KINT\_ATK}$ as $Adv_{\pi}^{KINT\_ATK}$ and usually omit the adjective "adaptive" .

Some remarks about the notion:

(1) ψ is disallowed to be Π's encryption algorithm E, otherwise the adversary can trivially win the game via simply generating (pk_1, sk_1)←KG(k) and setting h(x,y)=y. In this case y*=ψ(pk_1, y)=E(pk_1, y) so D(sk_1, y*)=y=h(D(sk_0,y*),y), i.e., the adverrsary always wins.

(2) y* must depend on y, otherwise the adversary can trivially win the game by simply generating (pk_1, sk_1)←KG(k) , setting ψ(x,y) to be a constant a_0 which is selected at random and setting h(x,y)=D(sk_1, a_0).

(3) If there exists a function φ such that y*=ψ(pk_1, y)=E(pk_1, φ(M)), i.e., ψ(pk_1, E(pk_0,M))=E(pk_1, φ(M)) for any pk_0, pk_1 and M, then D(sk_1, y*)=h(D(sk_0,y*),y) implies φ(M)= h(D(sk_0,y*),y), as a result Π is not key-integral. Some schemes, e.g., ElGamal scheme, have this feature and that's why(according to theorem 4.1) they are not anonymous against chosen-ciphertext attacks.

(4) In $Exp_{\pi,A}^{KINT\_ATK}(k)$ the functional equation D(sk_1, y*)=h(D(sk_0,y*),y) can be replaced with a more generic relationship such as H(D(sk_1, y*), D(sk_0,y*),y))=1 where H is a P.P.T

predicate associated with a P.P.T. algorithm F such that P[F(v,w)=u: H(u,v,w)=1] is non-negligible. All the following theorems can be proven in this more generic cases, however, for simplicity we only consider the functional forms in definition 5.1.

Theorem 5.1 *A public-key encryption scheme* Π *is anonymous against chosen-ciphertext attacks iff* Π *is both anonymous against chosen-plaintext attacks and key-integral against chosen-ciphertext attacks*. □

Because anonymity against chosen-ciphertext attacks strictly implies anonymity against chosen-plaintext attacks(as ElGamal scheme shows), key-integrity against chosen-ciphertext attacks exactly specifies the gap between the two types of anonymity properties. From this viewpoint, theorem 4.1 can be equivalently stated as:

Theorem 5.2 *Let* Π *be a public-key encryption scheme which is anonymous against chosen-plaintext attacks. Then* Π *is anonymous against chosen-ciphertext attacks iff it is key-integral against chosen-ciphertext attacks.* □

The proof of theorem 5.1 comes from next two lemmas.

Lemma 5.1 *Let* Π *be a public-key encryption scheme* which is *anonymous against chosen-ciphertext attacks. Then* Π *is key-integral against chosen-ciphertext attacks.* Concretely,

$$Adv_{\pi}^{KINT\_CCA}(t,q) \le Adv_{\pi}^{ANO\_CCA}(t+O(T_d+T_e),q+2)$$

where T_d, T_e are respectively computational time of Π's decryption and encryption algorithms.

Proof Suppose U=(U_1,U_2) is an P.P.T. chosen-ciphertext adversary cracking Π's key-integrity, we construct a P.P.T chosen-ciphertext adversary A^U=(A_1,A_2) cracking Π's anonymity. Consider the following game:

```
$Exp_{\pi,A}^{ANO\_CCA}(k)$:
    $(pk_0, sk_0), (pk_1, sk_1) \leftarrow KG(k)$;
    $(M, St) \leftarrow A_1^{D(sk_0,.),D(sk_1,.)}(pk_0, pk_1)$  where $A_1$ is implemented as:
        $(M_0, St_0) \leftarrow U_1^{D(sk_0,.)}(pk_0)$; $(M_1, St_1) \leftarrow U_1^{D(sk_1,.)}(pk_1)$;
        $t \leftarrow^{\$} \{0,1\}$; $M \leftarrow M_t$; $St \leftarrow t || pk_0 || pk_1 || M_0 || M_1 || St_0 || St_1$;
        return(M, St).
    $b \leftarrow^{\$} \{0,1\}$;
    $y \leftarrow E(pk_b, M)$;
    $d \leftarrow A_2^{D(sk_0,.),D(sk_1,.)}(y, St)$  where $A_2$ is implemented as
        parse St as $t || pk_0 || pk_1 || M_0 || M_1 || St_0 || St_1$;
        $(pk_0^*, h_0, \psi_0) \leftarrow U_2^{D(sk_0,.)}(y, St_0)$; $(pk_1^*, h_1, \psi_1) \leftarrow U_2^{D(sk_1,.)}(y, St_1)$;
        $y_0^* \leftarrow \psi_0(pk_0^*, y)$;  $y_1^* \leftarrow \psi_1(pk_1^*, y)$;
        $M_0^* \leftarrow h_0(D_{sk_0}(y_0^*), y)$;  $M_1^* \leftarrow h_1(D_{sk_1}(y_1^*), y)$;
          /*This is done via A's decryption oracle. */
        If  $E(pk_0^*, M_0^*) = y_0^* \wedge t=0$  Then  $d \leftarrow 0$;
        Else  if  $E(pk_1^*, M_1^*) = y_1^* \wedge t=1$
                Then  $d \leftarrow 1$;
                Else  $d \xleftarrow{\$} \{0,1\}$;
        Return(d);
    If d=b the output 1 else output 0.
```

A simulates U's decryption oracle via its own corresponding decryption oracle, which is obviously a perfect simulation.

For j=0,1, set event Z_j: (pk_j^*, h_j, ψ_j) output by $U_2^{D(skj,.)}(y, St_j)$ satisfies the constraints and $D(sk_j^*, y_j^*) = h_j(D(sk_j, y_j^*), y)$, or equivalently $E(pk_j^*, M_j^*) = y_j^*$. Denote the probability of an event occurring in $Exp_{\pi,A}^{ANO\_CCA}(k)$ as $P_A[]$ and that occurring in $Exp_{\pi,U}^{KINT\_CCA}(k)$ as $P_U[]$. According to A's specification, we have $P_A[d=0|b=t=0 \wedge Z_0]=1$. Observe that Z_j, b are independent, so

$$
\begin{aligned}
& P_A[d=0|b=t=0] \\
&= P_A[d=0|b=t=0\wedge Z_0]P_A[Z_0] + P_A[d=0|b=t=0\wedge \sim Z_0]P_A[\sim Z_0] \\
&= P_A[Z_0] + P_A[d=0|b=t=0\wedge \sim Z_0]P_A[\sim Z_0] \\
&= P_A[Z_0] + P_A[d=0|b=t=0\wedge \sim Z_0](1-P_A[Z_0])
\end{aligned}
$$

Note that $P_A[Z_0]=P_U[Exp_{\pi,U}^{KINT\_CCA}(k)=1]=Adv_{\pi,U}^{KINT\_CCA}(k)$ and

$$
\begin{aligned}
& P_C[d=0|b=t=0\wedge \sim Z_0] = P_A[E(pk_0^*, M_0^*) = y_0^* \wedge t=0 | y=E(pk_0, M) \wedge E(pk_0^*, M_0^*) \neq y_0^*] \\
& \quad + P_A[d=0 \mid y=E(pk_0, M_0) \wedge t=0 \wedge E(pk_0^*, M_0^*) \neq y_0^*] = 0+1/2 = 1/2.
\end{aligned}
$$

We have $P_A[d=0|b=t=0]=(1/2)(1+Adv_{\pi,U}^{KINT\_CCA}(k))$. The same analysis also derives $P_A[d=1|b=t=1]=(1/2)(1+Adv_{\pi,U}^{KINT\_CCA}(k))$.

On the other hand, when b≠t, i.e., b=1-t, we have $y=E(pk_b, M_{1-b})$ for any $b\in\{0,1\}$. According to A_2's specification, obviously $P_A[d=0|b=0\wedge t=1] = P_A[d=1|b=1\wedge t=0]=1/2$. Combining all the results, finally we have:

$$Adv_{\pi,A}^{ANO\_CCA}(k) = |2P_A[d=b]-1|$$

$$= \left|\sum_{i=0}^{1} P_A[d=b|\ b=i]-1\right| = \left|\sum_{i=0}^{1}\sum_{j=0}^{1}\frac{1}{2} P_A[d=b|b=i\wedge t=j]-1\right| = Adv_{\pi,U}^{KINT\_CCA}(k).$$

As a result, the lemma's inequality can be directly derived from this equation and time/query complexity can be directly verified. □

Lemma 5.2 *Let* Π *be a public-key encryption scheme which is anonymous against chosen-plaintext attacks. If* Π *is key-integral against chosen -ciphertext attacks then* Π *is anonymous against chosen-ciphertext attacks*. *Concretely*,

$$Adv_{\pi}^{ANO\_CCA}(\text{ t,q})\leq Adv_{\pi}^{ANO\_CPA}(\text{t})+2\text{q}\,Adv_{\pi}^{KINT\_CCA}(\text{ t+O(q}T_d\text{), q})$$

where q is the number of queries to decryption oracle and T_d is computation time of Π's decryption algorithm.

Proof Suppose $A=(A_1,A_2)$ is an P.P.T. chosen-ciphertext adversary cracking Π's anonymity, we construct a P.P.T chosen-ciphertext adversary $U^A=(U_1,U_2)$ cracking Π's key-integrity. Consider the following game:

```
$Exp_{\pi,U}^{KINT\_CCA}(k)$:
        $(pk_0, sk_0)\leftarrow KG(k)$;
        $(M, St)\leftarrow U_1^{D(sk0,.)}(pk_0)$ where $U_1$ is implemented as:
                $(pk_1, sk_1)\leftarrow KG(k)$;
                $(M, St_A)\leftarrow A_1^{D(sk_0,.),D(sk_1,.)}(pk_0, pk_1)$;
                $St\leftarrow pk_0||pk_1||sk_1||St_A$;
                return(M, St).
        $y\leftarrow E(pk_0, M)$;
        $(pk_1, h, \psi)\leftarrow U_2^{D(sk0,.)}(y, St)$, where $U_2$ is implemented as:
                Parse St as $pk_0||pk_1||sk_1||St_A$;
                $d\leftarrow A_2^{D(sk_0,.),D(sk_1,.)}(y, St_A)$;
                $Q_A\leftarrow\{y_i^*: \ y_i^*$'s are queried by A to its decryption
                  oracle and their replies are distinct each other, i.e.
                  $D_{sk}(y_i^*)\neq D_{sk}(y_j^*)$ for $i\neq j$ and $sk\in\{sk_0,sk_1\}$.}
                $\Psi_A(pk_1, y)\leftarrow\{y_i^*: \ y_i^*\in Q_A\}$;
                $H_A(y)\leftarrow\{(y_i^*,u_i,v_i): \ y_i^*\in Q_A\wedge u_i=D_{sk0}(y_i^*)\wedge v_i=D_{sk1}(y_i^*)\}$;
                Specify algorithm $\psi(pk_1, y)$ as:
                        $i\leftarrow^{\$}\{1,\ldots, |Q_A|\}$; return($y_i^*$);
                Specify algorithm h(u,y) as:
                        if there exists ($y_i^*$,$u_i$, $v_i$): in $H_A(y)$ such that $u=u_i$
                        then return($v_i$)
                        else return($\perp$)
                return($pk_1$, h, $\psi$);
        $y^*\leftarrow\psi(pk_1, y)$;
        if $D(sk_1, y^*)=h(D(sk_0,y^*),y)$ then output 1; else output 0.
```

U Simulates A's oracle $D_{sk0}(.)$ and $D_{sk1}(.)$ respectively via its own oracle $D_{sk0}(,.)$ and the its completely known secret key sk_1. Obviously this simulation is perfect.

Since i≠j implies $y_i^* \neq y_j^*$ and then $u_i=D(sk_0, y_i^*) \neq D(sk_0, y_j^*)=u_j$, so for any u there is at most one $(y_i^*, u_i, v_i) \in H_A(y)$ such that $u=u_i$. As a result, h(u,y) is a well-defined function. According to ψ's and h's specification, it is trivially true that $D(sk_1, y^*)=h(D(sk_0,y^*),y)$ for any $y^*=\psi(pk_1, y)$.

Set the event **Z**: all y_i^*'s are probabilistically independent of y. Observe that $Exp_{\pi,U}^{KINT\_CCA}(k)$ is equivalent to $Exp_{\pi,A}^{ANO\_CCA}(k)$ with b=0. Denote the probability of an event occurring in $Exp_{\pi,A}^{ANO\_CCA}(k)$ as $P_A[]$, that of event occurring in $Exp_{\pi,U}^{KINT\_CCA}(k)$ as $P_U[]$ and denote $|Q_A|$ as q, we have

$P_A[d=0|b=0]=P_U[d=0\wedge Z|b=0]+P_U[d=0\wedge\sim Z|b=0]$

$= P_U[d=0\wedge Z|b=0]+P_U[d=0|\sim Z\wedge b=0]P_U[\sim Z]$ (b, Z are independent)

$\leqq P_U[d=0\wedge Z|b=0]+P_U[\sim Z]$

$\leqq P_U[d=0\wedge Z|b=0]+qP[Exp_{\pi,U}^{KINT\_CCA}(k)=1]$

$= P_U[d=0\wedge Z|b=0]+q\, Adv_{\pi,U}^{KINT\_CCA}(k)$

On the other hand we can construct another chosen-ciphertext adversary $V^A=(V_1,V_2)$ cracking Π's key-integrity which is almost the same as U, with the only difference that V_1 calls A_1 by $(M, St_A)\leftarrow A_1^{D(sk_1,.),D(sk_0,.)}(pk_1, pk_0)$, i.e., exchanging roles of pk_0 and pk_1. As a result, $Exp_{\pi,V}^{KINT\_CCA}(k)$ is equivalent to $Exp_{\pi,A}^{ANO\_CCA}(k)$ with b=1 and we have $P_A[d=1|b=1]\leqq P_V[d=1\wedge Z|b=1]+q\, Adv_{\pi,V}^{KINT\_CCA}(k)$ by the almost the same analysis as above. Hence

$Adv_{\pi,A}^{ANO\_CCA}(k)=|2P_A[d=b]-1|=|P_A[d=0|b=0]+P_A[d=1|b=1]-1|$

$\leqq |P_U[d=0\wedge Z|b=0]+P_V[d=1\wedge Z|b=1]-1| + q(Adv_{\pi,U}^{KINT\_CCA}(k)+Adv_{\pi,V}^{KINT\_CCA}(k))$

In event of Z, i.e., if all y_j^*'s are independent of y, $Exp_{\pi,U}^{KINT\_CCA}(k)$ is actually equivalent to $Exp_{\pi,A}^{ANO\_CPA}(k)$ with b=0: recall that y_j^*'s are ciphertexts issued by A to guess the public-key in challenge ciphertext y. If y_j^*'s are all independent of y, we can simply craft a adversary A* which behaves exactly as A does, however, A* doesn't need to resort decryption oracle. At any time when A needs to query its decipher oracle on some ciphertext, say y_j^*, A* randomly(particularly independent of y) generates some plaintext x_j, makes an encryption on x_j, keeps the ciphertext $E(pk_0, x_j)$ and simply uses x_j as the answer from the oracle(since y_j^*'s are independent of y, these $E(pk_0, x_j)$'s have exactly the same distribution as y_j^*'s.). As a result, we have $P_U[d=0\wedge Z|b=0]= P[Exp_{\pi,A}^{ANO\_CPA}(k)=1|b=0]$. By the same analysis we can have $P_V[d=1\wedge Z|b=1]= P[Exp_{\pi,A}^{ANO\_CPA}(k)=1|b=1]$, therefore

$Adv_{\pi,A}^{ANO\_CCA}(k)\leqq |P[Exp_{\pi,A}^{ANO\_CPA}(k)=1|b=0]+P[Exp_{\pi,A}^{ANO\_CPA}(k)=1|b=1]-1|$

$+ q(Adv_{\pi,U}^{KINT\_CCA}(k)+Adv_{\pi,V}^{KINT\_CCA}(k))$

$= Adv_{\pi,A}^{ANO\_CPA}(k)+q(Adv_{\pi,U}^{KINT\_CCA}(k)+Adv_{\pi,V}^{KINT\_CCA}(k))$

The lemma's inequality can be directly derived and time/query complexity can be easily verified according to U's and V's constructions. □

5.3 A More Complicated Example: RSAP-RSA Scheme

ElGamal scheme(in 4.1)is an example which is anonymous against chosen-plaintext attacks but not key-integral under chosen-ciphertext attacks. Here we show another well-known public-key encryption scheme, OAEP-RSA, is key-integral against chosen-ciphertext attacks but not anonymous under chosen-plaintext attacks. These two examples show that anonymity against chosen-plaintext attacks and key-integrity against chosen-ciphertext attacks are orthogonal each other. Therefore(as proved in section 4.2) to get anonymity against chosen-ciphertext attacks, both properties are required.

OAEP-RSA is a provably secure and widely used public-key encryption scheme [3]. However, it is not anonymous even against chosen-plaintext attacks [2](so of course not anonymous under chosen-ciphertext attacks). The interesting fact is that it is key-integral against chosen-ciphertext attacks. This fact can be shown via the proven anonymity of its variant scheme RAEP-RSA.

Bellare et al in [2] constructed RAEP-RAS scheme which is a variant of OAEP-RSA but is both secure and anonymous against chosen-ciphertext attacks. According to the consequence in [2] and our theorem 4.1, RAEP-RSA must be key-integral against chosen-ciphertext attacks. This fact in combination with next proposition immediately derives OAEP-RSA's key-integrity against chosen-ciphertext attacks.

Let k be complexity parameter, k_0 and k_1 are integers satisfying $k_0+k_1<k$ and let $n(k)=k-k_0-k_1$. RAEP-RSA's key generation algorithm KG(k) produces RSA family public-secret key pair ((N,e),(N,d)), set pk to be (N,e,k,k_0,k_1) and sk to be (N,d,k_0,k_1). G and H are random oracles. The encryption and decryption algorithms are presented in figure 2.

```
Encryption Algorithm $E^{*G, H}(pk,x)$
  Ctr= -1;
  repeat
     $Ctr \leftarrow Ctr+1$;
     $r \xleftarrow{\$} \{0,1\}^{k0}$;
     $s \leftarrow (x||0^{k1}) \oplus G(r)$;
     $t \leftarrow r \oplus H(s)$;
     $v \leftarrow (s||t)^e \bmod N$;
  untill $(v<2^{k-2}) \vee (Ctr=k_1)$;
  if $Ctr=k_1$ then $y \leftarrow 10^{k0+k1}||x$
  else $y \leftarrow 0||v$;
  return(y)
```

```
Decryption Algorithm $D^{*G, H}(sk,y)$
  Parse y as b||v where b is a bit;
  If b=1 then
     parse v as w||x where $|x|=n(k)$;
     if $w=0^{k0+k1}$ then $z \leftarrow x$;
     else $z \leftarrow \perp$ ;
  else
     $(s||t) \leftarrow v^d \bmod N$; /*$|s|=k_1+n$, $|t|=k_0$*/
     $r \leftarrow t \oplus H(s)$;
     $(x||p) \leftarrow s \oplus G(r)$; /*$|x|=n$, $|p|=k_1$*/
     If $p=0^{k1}$ then $z \leftarrow x$;
     Else $z \leftarrow \perp$ ;
  Return(z)
```

Figure 2: RAEP-RSA public-key encryption scheme

Proposition 5.1 *If OAEP-RSA scheme* $\Pi=(KG,E,D)$ *is non-key-integral under chosen-ciphertext attacks, then RAEP-RSA scheme* $\Pi^*=(KG^*,E^*,D^*)$ *is non-key-integral under chosen-ciphertext attacks either.*

Proof Let U=(U_1,U_2) be OAEP-RSA's KINT-CCA adversary, we construct RAEP-RSA's KINT-CCA adversery V=(V_1,V_2). Consider the game:

```
$Exp^{KINT\_CCA}_{RAEP-RSA,V}(k)$

        ($pk_0$, $sk_0$)←KG*(k);
        (M, St)←$V_1^{D^*(sk0,.)}$($pk_0$) where $V_1$ is implemented as:
                (M, St)←$U_1^{D(sk0,.)}$($pk_0$);
                return(M, St);
        y←E*($pk_0$, M);
        ($pk_1$, h*, ψ*)←$V_2^{D^*(sk0,.)}$(y, St) where $V_2$ is implemented as:
              Parse y as b||$y_1$, where b is a bit;
              If b=1 then halt;
              ($pk_1$, h, ψ)←$U_2^{D(sk0,.)}$($y_1$, St)
              Specify algorithm ψ*(pk,y) as:
                  If y=0||$y_1$ then return(ψ(pk,$y_1$)) else return(⊥).
              Specify algorithm h*(v,y) as:
                  If y=0||$y_1$ then return(h(v,$y_1$)) else return(⊥).
              ($pk_1$, h*, ψ*);
        y*←ψ($pk_1$, y);
        if D*($sk_1$, y*)=h*(D*($sk_0$,y*),y) then output 1 else output 0.
```

V simulates U's OAEP-RSA decipher oracle via its RAEP-RSA decipher oracle: on query y from U, V sets z←0||y, queries its own RAEP-RSA decipher oracle on z and returns the answer to U.

Note that (1)if h, ψ are P.P.T. algorithms and ψ≠E, then h*, ψ* are P.P.T. algorithms and ψ*≠E*. (2)In event of ～halt, U's success in D(sk_1, y_1*)=h(D(sk_0,y_1*),y_1) implies V's success in D*(sk_1, y*)=h*(D*(sk_0,y*),y) where y*=0||y_1* and y=0||y_1. (3)If h and ψ satisfies the requirements imposed by $Exp^{KINT\_CCA}_{OAEP-RSA,U}(k)$ then h* and ψ* will satisfy the requirements imposed by $Exp^{KINT\_CCA}_{RAEP-RSA,V}(k)$.(4)P[～halt]=P[E*(pk_0, M)=0||y_1]≥1/4. As a result of all these facts, we have

$$Adv^{KINT\_CCA}_{RAEP-RSA,V}(k)=P[Exp^{KINT\_CCA}_{RAEP-RSA,V}(k)=1]$$

$$\geq P[Exp^{KINT\_CCA}_{RAEP-RSA,V}(k)=1|\sim halt]P[\sim halt]$$

$$\geq (1/4)P[Exp^{KINT\_CCA}_{OAEP-RSA,U}(k)=1]=(1/4)Adv^{KINT\_CCA}_{OAEP-RSA,U}(k)$$

which is exactly the lemma's conclusion. □

References

[1] M. Abdalla, M. Bellare, D. Catalano, et al. *Searchable Encryption Revisited: Consistency Properties*, *Relation to Anonymous IBE, and Extensions*. In: V. Shoup ed, Advances in Cryptology - Crypto 2005 Proceedings, Lecture Notes in Computer Science Vol. 3621, Sata Babara, California: Springer-Verlag, 2005, 205-222.

[2] M. Bellare, A. Boldyreva, A. Desai and D. Pointcheval. *Key-privacy in public-key encryption*. In: C. Boyd ed, Advances in Cryptology - Asiacrypt 2001 Proceedings, Lecture Notes in Computer Science Vol. 2248, Goldcoast Australia:Springer-Verlag, 2001, 566-582.

[3] M.Bellare and P.Rogaway, *Optimal Asymmetric Encryption: How to Encrypt with RSA*, In: L. Guillou and J. Quisquater ed, Advances in Cryptology - Eurocrypt 1995 Proceedings, Lecture Notes in Computer Science Vol. 921, Springer-Verlag, 1995.

[4] X. Boyen, B.Waters, *Anonymous Hierarchical Identity-based Encryption without Random Oracles*, eprint.iacr.org/2006/085.

[5] D. Boneh, X.Boyen and Eu-Jin Goh, *Hierarchical Identity-based Encryption withConstant Size Ciphertext*, In: R.Cramer ed, Advances in Cryptology – CRYPTO'05, Lecture Notes in Computer Science Vol.3494, Aarhus, Denmark:Springer-Verlag, 2005, 440-456.

[6] D Boneh, G.Di Crescenzo, R.Ostrovski et al. *Public key Encryption with Keyword Search*, In: C.Cachin and J.Camenisch ed, Advances in Cryptology – EUROCRYPT'04, Lecture Notes in Computer Science Vol.3027, Interlaken, Switzerland:Springer-Verlag, 2004, 506-522.

[7]D.Boneh, M.Franklin, Identity-based Encryption from Weil Pairing, In: Advances in Cryptology, Lecture Notes in Computer Science Vol. 2139, Springer-Verlag, 2001, 213-229.

[8]D.Boneh, J.Katz. *Improved Efficiency for CCA-Secure Cryptosystems Built using Identity-Based Encryption*, eprint.iacr.org/2005/185

[9]R.Canetti, S.Halevi and J. Katz, *Chosen-ciphertext Security from Identity-Based Encryption*, In: Advances in Cryptology, Lecture Notes in Computer Science Vol.3027, 2004, 207-222.

[10] J-S. Coron, H.Handschuh, M.Joye et al, *GEM: a Generic Chosen-ciphertext Secure Encryption Method*, In: B.Preneel ed, Topics in Cryptology – CT-RSA 2002, Lecture Notes in Computer Science Vol.2271, 2002, 263-276.

[11] E. Fujisaki, T. Okamoto, *Secure Integration of Asymmetric and Symmetric Encryption Schemes*, In: M.Wiener ed, Advances in Cryptology 1999 – Crypto 1999 Proceedings, Lecture Notes in Computer Science Vol 1666, Springer-Verlag, 1999, 535-554.

[12] O.Goldreich *Foundations of Cryptography: Basic Applications*, Cambridge University Press 2004.

[13] A. Kiayias, Y. Tsiounis and M. Yung *Group Encryption*, eprint.iacr.org/2007/015

[14] T.Okamoto and D.Pointcheval, *REACT: Rapid Enhanced-security Asymmetric Cryptosystem Transform*, In: CT-RSA'2001, Lecture Notes in Computer Science Vol.2020, Springer-Verlag, 159-175, 2001.

[15]Y.Tian, *Some Results on Anonymity in Hybrid Encryption Schemes*, eprint.iacr.org/2007/130.

[16]B.Waters *Efficient Identity-based Encryption without Random Oracles*, In:R.Cramer ed, Advances in Cryptology, Lecture Notes in Computer Science Vol. 3494, Springer-Verlag, 114-127, 2005.

Appendix A: Concept of Relevant Anonymity and Proof of Theorem 2.1[15]

We only prove the case of chosen-ciphertext attack. The case of chosen-plaintext attack can be done following almost exactly the same logic(but more easily). Suppose A=(A_1,A_2) is an P.P.T. adversary cracking Π's chosen-ciphertext anonymity. We construct an P.P.T adversary B^A=(B_1,B_2) cracking Π's chosen-ciphertext security as the following. Consider the game:

```
$Exp_{\pi,B}^{IND-CCA}(k)$:

    $(pk_0, sk_0) \leftarrow KG(k)$;
    $(M_0, M_1, St) \leftarrow B_1^{D(sk0,\ .)}(pk_0)$ where $B_1$ is implemented as:
            $(pk_1, sk_1) \leftarrow KG(k)$;
            $(M^*, St_A) \leftarrow A_1^{D(sk0,.),\ D(sk1,.)}(pk_0, pk_1)$;
            $M_0 \leftarrow M^*$; $M_1 \leftarrow^{\$} \{0,1\}^{|M^*|}$; $St \leftarrow St_A||pk_1||sk_1$;
            return$(M_0, M_1, St)$;
    $b \leftarrow^{\$} \{0,1\}$;
    $y^* \leftarrow E(pk_0, M_b)$;
    $d \leftarrow B_2^{D(sk0,\ .)}(y^*, St)$ where $B_2$ is implemented as:
            parse St as $St_A||pk_1||sk_1$;
            $d \leftarrow A_2^{D(sk0,.),\ D(sk1,.)}(y^*, St_A)$;
            return(d).
    if d=b then output 1 else output 0.
```

In this game, B simulates oracle D(sk_0, .) via its own oracle and simulates oracle D(sk_1,.) via direct decipher computation based-on its possession of sk_1. Such simulation is obviously perfect.

It's straightforward to verify that $Exp_{\pi,B}^{IND-CCA}(k)$ in case of b=0 is just equivalent to $Exp_{\pi,A}^{ANO-CCA}(k)$ in case of b=0, and $Exp_{\pi,B}^{IND-CCA}(k)$ in case of b=1 is equivalent to $Exp_{\pi,A}^{RE-ANO-CCA}(k)$ in case of b=0. On the other hand, we can construct another P.P.T. adversary C^A=(C_1,C_2) cracking Π's chosen-ciphertext security in very similar way as that of B^A, with the only difference that $C_1^{D(sk0,\ .)}$(pk_0) calls A_1 in the way of $A_1^{D(sk1,.),\ D(sk0,.)}$ (pk_1, pk_0), i.e. exchanging the roles of pk_0 and pk_1. As a result, $Exp_{\pi,C}^{IND-CCA}(k)$ in case of b=0 is equivalent to $Exp_{\pi,A}^{ANO-CCA}(k)$ in case of b=1 and $Exp_{\pi,C}^{IND-CCA}(k)$ in case of b=1 is equivalent to $Exp_{\pi,A}^{RE-ANO-CCA}(k)$ in case of b=1. Therefore:

$$Adv_{\pi,B}^{IND-CCA}(k) = |P[Exp_{\pi,B}^{IND-CCA}(k)=1 \mid b=0] - P[Exp_{\pi,B}^{IND-CCA}(k)=1 \mid b=1]|$$

$$= |P[Exp_{\pi,A}^{ANO-CCA}(k)=1 \mid b=0] - P[Exp_{\pi,A}^{RE-ANO-CCA}(k)=1 \mid b=0]|$$

$$Adv_{\pi,C}^{IND-CCA}(k) = |P[Exp_{\pi,C}^{IND-CCA}(k)=1 \mid b=0] - P[Exp_{\pi,C}^{IND-CCA}(k)=1 \mid b=1]|$$

$$=|\, P[Exp_{\pi,A}^{ANO\_CCA}(k)=1\,|\,b=1] - P[Exp_{\pi,A}^{RE\_ANO\_CCA}(k)=1\,|\,b=1]\,|$$

Then $Adv_{\pi,B}^{IND\_CCA}(k)+Adv_{\pi,C}^{IND\_CCA}(k)$

$$\geq |\, P[Exp_{\pi,A}^{ANO\_CCA}(k)=1\,|\,b=0] - P[Exp_{\pi,A}^{RE\_ANO\_CCA}(k)=1\,|\,b=0]\,|$$

$$+\big|\, P[Exp_{\pi,A}^{ANO\_CCA}(k)=1\,|\,b=1] - P[Exp_{\pi,A}^{RE\_ANO\_CCA}(k)=1\,|\,b=1]\,\big|$$

$\geq Adv_{\pi,A}^{ANO\_CCA}(k) - Adv_{\pi,A}^{RE\_ANO\_CCA}(k)$, namely,

$$Adv_{\pi,A}^{ANO\_CCA}(k) \leq Adv_{\pi,A}^{RE\_ANO\_CCA}(k)+Adv_{\pi,B}^{IND\_CCA}(k)+Adv_{\pi,C}^{IND\_CCA}(k)$$

The theorem’s inequality can be derived directly and the adversary’s time complexity can be easily verified. □

Appendix B: IBE’s Chosen-Plaintext Anonymity[1]

Let Π=(Setup, UKG,E,D) be an IBE encryption scheme, A=(A$_1$,A$_2$) be an P.P.T. adversary. Consider the following game:

```
$Exp_{\pi,A}^{IBE\_ANO\_CPA}(k)$:
    (mpk, msk)←Setup(k);
    ($a_0$*, $a_1$*, M*, St)←$A_1^{UKG(msk,.)}$(mpk);
    b←$^\$${0,1};
    y*←E(mpk, $a_b$*, M*);
    d←$A_2^{UKG(msk,.)}$(y*, St);
    if d=b then output 1 else output 0.
```

In the above game A is disallowed to query any one of a_0* and a_1* of its oracle-UKG(msk,.). The adversary’s advantage $Adv_{\pi,A}^{IBE\_ANO\_CPA}$ is defined as $|\,2P[Exp_{\pi,A}^{IBE\_ANO\_CPA}(k)=1]-1\,|$ or equivalently |P[d=0|b=0]- P[d=0|b=1]|. Π is called *anonymous against adaptive chosen-plaintext attacks* (*ANO_CPA anonymous* for shorthand) if $Adv_{\pi,A}^{IBE\_ANO\_CPA}$ is a negligible function in k. Hereafter we simply omit “adaptive” and denote $\max_{A\in P.P.T.} Adv_{\pi,A}^{IBE\_ANO\_CPA}(k)$ as $Adv_{\pi}^{IBE\_ANO\_CPA}(k)$. Whenever the adversary’s advantage is regarded as a function of computational time t and number of oracle queries q, we use the notation $Adv_{\pi}^{IBE\_ANO\_CPA}(t,q)$ instead of $Adv_{\pi}^{IBE\_ANO\_CPA}(k)$.

To distinguish the anonymity defined in the above from chosen-plaintext master-key anonymity defined in definition 3.1, we call this concept as IBE scheme’s “identity anonymity”.