Some Results on Anonymity in Hybrid Encryption

Tian Yuan[1+], Chen Zhi-Yu[1], Jin Yuee[1], Jin Feng[1], Ma Huihui[1]

[1](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

Anonymity(key-privacy) as well as security(data-privacy) are all important features in public-key encryption applications. In this paper two new and general concepts, named “relevant anonymity” and “relevant security”, are defined. Based-upon these concepts some general results on anonymity in public-key encryption are proved, which fall in three categories. The first results are two general relationships between anonymity and security; the second are a sufficient and necessary condition for chosen-plaintext anonymity in Fujisaki-Okamoto hybrid construction and a sufficient condition for its chosen-ciphertext anonymity; the third is a sufficient condition for chosen-ciphertext anonymity in Okamoto-Pointcheval hybrid construction (REACT). All these conditions are also easy-to-use criteria in practice. By examples such general consequences are applied to some specific schemes and as a result anonymity of some well-known schemes are re-established in a simpler way. Furthermore, NISSIE scheme PSEC-/1/2/3’s chosen-ciphertext anonymity are proved.

Key words: Computational Cryptography; Public-Key Anonymity; Provable Security; Hybrid-Scheme; Key-Privacy

1 Introduction

Anonymity as well as security are both widely-desired features in practical public-key encryption schemes, although the former comes to get a systematic theoretical treatment much later [3]. Intuitively, anonymity(key-privacy) guarantees that ciphertext can effectively hide public-key under which it is produced while security(data-privacy) guarantees that ciphertext can effectively hide the plaintext from which it is enciphered. In addition to key-privacy per se, anonymity is also an approach to some high level and complicated security objectives[1,2,10]. In general, security and anonymity are orthogonal each other and a scheme with both features are quite useful.

Although anonymity is a very general concept in all public-key cryptographic systems and its importance has been surfacing increasingly, it gets much fewer research than security. For example, we still have little knowledge on many well-known public-key encryption scheme's anonymity, although their security have been concretely established. Furthermore, because of wide requirements on both security and anonymity and difficulty of constructing efficient and provably secure public-key encryption schemes, it makes sense to investigate existed provably secure schemes' anonymity other than construct new ones from scratch.

Among existed public-key encryption constructions, hybrid schemes constructed from asymmetric and symmetric component encryption schemes are widely used in practice[8,10,11,12,15]. Not only better efficiency but also stronger security can be obtained by this construction, enhancing component encryption schemes which have only weak security to the strongest one. For instance, Fujisaki-Okamoto hybrid scheme[8] can provide provably adaptive chosen-ciphertext security (in random oracle) as long as its asymmetric and symmetric encryption components have comparatively very weak security features(one-way secure, γ-consistent and passive-attack-resistant), and a few other hybrid schemes also have such nice properties[10,11,12,15]. However, despite of practical importance and good understanding in hybrid schemes' security, so far there's few knowledge about their anonymity, e.g., whether a hybrid scheme can also enhance its component's weak anonymity to strong one, just like it does in security? If yes, to which degree can this enhancement reach? Answers to such questions are no doubt valuable in applications

In this paper we make a step in answering these questions, particularly with respect to two well-used hybrid constructions, i.e., Fujisaki-Okamoto and Okamoto-Pointcheval schemes[8,11]. A sequence of very general results are provably established with applications to some important examples, including some new specific anonymity results which are obtained for the first time with our knowledge.

1.1 Our Contributions

In this paper our contributions fall in three categories. Firstly, we present two new and generic concepts, named *relevant anonymity* and *relevant security*, and prove some general relationships between these new concepts and already well-established concepts of anonymity and security(theorem 3.1 and 3.2). Relevant anonymity/security are very weak and easy-to-verify properties in practice, however, by means of them some complicated security/anonymity proofs can be significantly simplified, as shown in examples 3.1-3.5. In these examples we re-establish some well-known anonymity consequences about specific schemes but in a easier way. In addition, some new and interesting results are also proved in these examples.

The concept of relevant anonymity was first introduced by Abdalla et al. in [1] in case of IBE (only the version against chosen-plaintext attacks was formally established in their innovative paper). Our definition 3.1 can be regarded as a transplant to traditional public-key encryption and our theorem 3.1 can be thought of as a counterpart to lemma 4.3 in [1]. However, the (conjugate) concept of relevant security and its relationship with anonymity are new and we believe all these are valuable tools in practice, just as we use in our works.

Secondly, based-on the concept of relevant anonymity we establish the strongest anonymity for two well-known hybrid encryption constructions: Fujisaki-Okamoto scheme and Okamoto-Pointcheval scheme(REACT hereafter). Both of them are used in PSEC-1/2/3 schemes proposed for NISSIE[9]. In case of Fujisaki-Okamoto scheme, we prove that the hybrid scheme is in the chosen-plaintext anonymity if and only if the component public-key encryption scheme is relevantly chosen-plaintext anonymous and one-way secure(theorem 4.1). Furthermore, if the component public-key scheme is relevantly strong anonymous(but not very strong as seen in examples) and one-way secure, the hybrid scheme can be in the strongest anonymity(against adaptive chosen-ciphertext attacks, theorem 4.2). In case of REACT, a similar consequence is proved(theorem 5.1). All consequences are established in style of concrete security. In combination with the original security results on these hybrid schemes, we can get quite weak and practical conditions to guarantee such schemes' anonymity and security at the same time.

Thirdly, as applications of these general consequences, we prove the famous PESC-1/2/3 schemes' anonymity against adaptive chosen-ciphertext attacks in oracle model(proposition 3.1,4.1 and 5.1). With our knowledge these are the first formal proofs about these schemes.

1.2 Outline of the Paper

After a brief overview of basic concepts, relevant anonymity/security concepts are defined and two general theorems are proved in section 3. Fujisaki-Okamoto hybrid scheme's anonymity and REACT's anonymity are investigated respectively in section 4 and 5. Section 6 concludes the paper and discusses some further works.

2 Preliminaries

In this section some basic concepts are recalled, together with some commonly-used notations. Let X be a set, we use $a \leftarrow^{\$} X$ to denote that a is randomly selected(with uniform distribution) from X. All algorithms are presented in pseudo-C with some comments in style of /*…*/. Given some specific value a*, such items as (a*, b) in a list of 2-tuples are simply denoted as (a*,.) (i.e., dot "." means some value we don't care), and similar notations are used for any list of n-tuples. For example, (a*,b*,.,.,.) denotes those items in a list of 5-tuples which first and second fields have the given specific values a* and b* respectively. A probabilistic polynomial-time algorithm is simply named P.P.T. algorithm.

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 a ciphertext y; 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(Security) Let Π=(KG,E,D) be a public-key encryption scheme, k be the complexity parameter, 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:

```
$Exp_{\pi,A}^{IND\_ATK}(k)$:
    (pk, sk)←KG(k);
    ($M_0$, $M_1$, St)←$A_1^{Oracle}$(pk);
    b$\xleftarrow{\$}${0,1};
    y*←E(pk, $M_b$);
    d←$A_2^{Oracle}$(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, .) and A is disallowed to query its oracle-D(sk, .) on the challenge ciphertext y*. The adversary's advantage $Adv_{\pi,A}^{IND\_ATK}$ is defined as $|2P[Exp_{\pi,A}^{IND\_ATK}(k)=1]-1|$. Π is said *secure against adaptive chosen-plaintext*(respectively, *chosen-ciphertext*) *attacks* if $Adv_{\pi,A}^{IND\_CPA}$ (respectively, $Adv_{\pi,A}^{IND\_CCA}$) is a negligible function in k for any P.P.T. adversary A. Denote the adversary's advantage $Adv_{\pi}^{IND\_ATK}(k) \equiv \max_{A\in P.P.T.} Adv_{\pi,A}^{IND\_ATK}(k)$, a function in k. Whenever the advantage is regarded as a function of computational time t and number of oracle queries q, we use the notation $Adv_{\pi}^{IND\_ATK}(t,q)$ instead of $Adv_{\pi}^{IND\_ATK}(k)$. Because we only concern about adaptive adversary hereafter, we will simply omit the adjective "adaptive" for brevity.

Definition 2.3(Anonymity)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:

```
$Exp_{\pi,A}^{ANO-ATK}(k)$:
    ($pk_0$, $sk_0$), ($pk_1$, $sk_1$)←KG(k); /*run KG(k) two times independently*/
    (M*, St)←$A_1^{Oracle}$($pk_0$, $pk_1$);
    b$\leftarrow^{\$}${0,1};
    y*←E($pk_b$, M*);
    d←$A_2^{Oracle}$(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 anyone of D(sk_0, .) and D(sk_1, .) on y*. The adversary's advantage $Adv_{\pi,A}^{ANO-ATK}$ is defined as $|2P[Exp_{\pi,A}^{ANO-ATK}(k)=1]-1|$. Π is said *anonymous against adaptive chosen-plaintext*(respectively, *chosen-ciphertext*) *attacks* if $Adv_{\pi,A}^{ANO-CPA}$ (respectively, $Adv_{\pi,A}^{ANO-CCA}$) is a negligible function in k for any P.P.T. adversary A. Denote $Adv_{\pi}^{ANO-ATK}(k) \equiv \max_{A \in P.P.T.} Adv_{\pi,A}^{ANO-ATK}(k)$, a function in k. Whenever the 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 $Adv_{\pi}^{ANO-ATK}(k)$, and we will simply omit the adjective "adaptive" for brevity.

3 Relationships Between Anonymity and Security

Abdalla et al presented the concept of *relevant anonymity* for identity-based encryption(IBE) scheme in [1] and used it as a sufficient condition for a secure IBE scheme to be anonymous[1]. Here we transplant this concept to traditional public-key schemes and prove a similar result. In addition to this, we also develop an conjugate concept, *relevant security*, and prove its sufficiency for a anonymous public-key encryption scheme to be secure. Relevant anonymity and relevant security are properties strictly weaker than their non-relevant counterparts but easy to check in practice. These results present some interesting and useful relationships between security and anonymity, which will be used as helpful tools frequently in our works.

3.1 Relevant anonymity and its relationship with security

Definition 3.1(Relevant Anonymity) 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

[1] [1] Only gives the concept in case of chosen-plaintext attacks which is adequate for their objectives.

determined by ATK. Consider the following game:

```
$Exp_{\pi,A}^{RE\_ANO\_ATK}(k)$:
    ($pk_0$, $sk_0$), ($pk_1$, $sk_1$)←KG(k); /*run KG(k) two times independently*/
    (M*, St)←$A_1^{Oracle}$($pk_0$, $pk_1$);
    M$\xleftarrow{\$}\{0,1\}^{|M^*|}$; /*randomly generate a valid message M in the same size as M*.*/
    b$\xleftarrow{\$}\{0,1\}$;
    y*←E($pk_b$, M);
    d←$A_2^{Oracle}$(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, relevant anonymity in combination with security can imply (strong) anonymity, which is exactly presented in the following theorem.

Theorem 3.1. *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.

Proof. 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:

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

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

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

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

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

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

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

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

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

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

In practice theorem 3.1 is an easy-to-check sufficient condition for a secure public-key encryption scheme to be anonymous, and can be used to simplify anonymity proofs based-upon already known security consequences.

Example 3.1(ElGamal scheme's anonymity against chosen-plaintext attacks) ElGamal scheme is provably secure against chosen-plaintext attacks under the assumption of decisional Diffie-Hellman problem's hardness[7]. Furthermore, its anonymity can be derivedfrom its security and theorem 3.1.

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

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

It's straightforward to observe that for any adversary A in $Exp_{\pi,A}^{RE\_ANO\_CPA}(k)$ when A_2 is provided with the challenge ciphertext (Y, W), where W=TM and M is selected at random and independent of the message M* output by $A_1(pk_0,pk_1)$(the only relationship is that |M|=|M*|), X_0^r M and X_1^rM have exactly the same distribution from A_2's perspective. As a result, $Adv_{\pi,A}^{RE\_ANO\_CPA}(k)$ =0. Applying theorem 3.1 to this observation we get ElGamal scheme's anonymity against chosen-plaintext attacks under the assumption of decisional Diffie-Hellman problem's hardness. The same result was directly proven in [3].

An interesting aspect of ElGamal scheme is that it is NOT anonymous against chosen-ciphertext attacks . We'll have an explanation for this in next subsection.

Example 3.2(Cramer-Shoup scheme's anonymity against chosen-ciphertext attacks) Cramer-Shoup scheme is provably secure against chosen-ciphertext attacks under the assumption of decisional Diffie-Hellman problem's hardness [6]. Its anonymity against chosen-ciphertext attacks can be also derived from its proven security and theorem 3.1 via an analysis very similar as example 3.1.

Before we proceed to analyze Cramer-Shoup scheme's anonymity, we explicitly present a convention that we regard K, g_1 and g_2(fig.2) only as public parameters instead of public-key components. This means that anonymity in Cramer-Shoup scheme only concerns c,d and h. This convention is reasonable because g_1,g_2 and K are shared by all users of this scheme and only c,d and h are independently generated and designated to each individual. In fact, the original proof in [2](refer to the adversary's construction in [2]'s appendix B.1) was also carried out implicitly in this opinion. We'll follow this convention in other examples and in each example we will explicitly point out the public (shared) parameters and (individual) public-keys.

Coming back to Cramer-Shoup scheme's anonymity, the critical point is that for any adversary A in $Exp_{\pi,A}^{RE\_ANO\_CCA}(k)$ when A_2 is provided with the challenge ciphertext $Y^*=(u_1,u_2,e,v)$, where $e=h^rM$ and M is selected at random and independent of the message M* output by $A_1(pk_0,pk_1)$(the only relationship is that |M|=|M*|), (u_1,u_2,e,v) in case of pk_0 and pk_1 have exactly the same distribution from A_2's perspective, even if A_2 queries its decryption oracles $D(sk_0,.)$ and $D(sk_1,.)$ on Y*(recall that in $Exp_{\pi,A}^{RE\_ANO\_CCA}(k)$ the adversary A is allowed to query its decryption oracle on the challenge ciphertext). As a result, $Adv_{\pi,A}^{RE\_ANO\_CCA}(k)=0$ and the anonymity against chosen-ciphertext attacks follows.

```
Key generator KG(q,g_1,g_2,K):
    $g_1 \leftarrow g$;
    $x_1,x_2,y_1,y_2, z \xleftarrow{\$} Z_q$;
    $c \leftarrow g_1^{x1} g_2^{x2}$; $d \leftarrow g_1^{y1} g_2^{y2}$;
    $h \leftarrow g_1^{z}$;
    $pk \leftarrow (c,d,h)$;
    $sk \leftarrow (x_1,x_2,y_1,y_2, z)$;
    return(pk, sk)
```

```
Encryption algorithm E(pk, M),
M∈G:
        $r \xleftarrow{\$} Z_q$;
        $u_1 \leftarrow g_1^{r}$; $u_2 \leftarrow g_2^{r}$;
        $e \leftarrow Mh^{r}$;
        $T \leftarrow H_K(u_1,u_2,e)$;
        $v \leftarrow c^{r} d^{rT}$;
        return($u_1,u_2,e, v$)
```

```
Decryption algorithm D(sk,Y):

        Parse Y as ($u_1,u_2,e, v$)
        $T \leftarrow H_K(u_1,u_2,e)$;
        If   $v=u_1^{x1+Ty1} u_2^{x2+Ty2}$;
        Then   $M \leftarrow e/u_1^{z}$;
        Else   $M \leftarrow \perp$;
        return(M)
```

Figure 2 Crammer-Shoup Scheme: G is a prime-order(q) group with generator g.

The above examples just repeat some already-known anonymity consequences in public-key encryption but regain them in a simple way. In example 3.3 we'll obtain a new anonymity result(with our knowledge so far)on a well-known scheme, PSEC-1, proposed for NISSIE[9].

Example 3.3(PSEC-1 scheme's anonymity against chosen-ciphertext attacks) PSEC-1 public-key encryption scheme is provably secure(in random oracle model)against chosen-ciphertext attacks under the assumption of decisional Diffie-Hellman problem's hardness on elliptic curves. In this scheme(fig.3), it's reasonable to consider the curve E/F_q, p, q and point P as (shared) public parameters and W as the real public-key (each individual has distinct W).

Key generator $KG(E/F_q,p,q,P)$:

```
s←Z_p;
W←sP;
pk←W;
sk←s;
return(pk, sk)
```

Encryption algorithm E(pk, M), $M\in\{0,1\}^k$:

```
r←$ Z_p;
t←H(M||r); /*r used as a string*/
Q←tW;
C_1←tP;
C_2←(M||r) ⊕ x(Q);
return(C_1,C_2)
```

Decryption algorithm D(sk,Y):

```
Parse Y as (C_1,C_2)
Q←sC_1;
u←C_2 ⊕ x(Q);
parse u as M||r;
if   C_1=H(u)P
Then   return(M);
Else   return(⊥);
```

Figure 3 PSEC-1 encryption Scheme: E/F_q is the group of an elliptic curve over field F_q . P is a point on E/F_q with (prime) order p. x(Q) is the x-coordinate of curve point Q. H is a random oracle.

For any adversary A in $Exp_{\pi,A}^{RE\_ANO\_CCA}(k)$, A_2 is provided with the challenge ciphertext $Y^*=(C_1,C_2)$, which equals $(tP, R\oplus x(tW_0))$ or $(tP, R\oplus x(tW_1))$ respectively in case of pk_0 or pk_1 where R=M||r and M is selected at random and independent of the message M* output by $A_1(pk_0,pk_1)$(the only relationship is that |M|=|M*|). Note that for any $b\in\{0,1\}$ we have $(tP, R\oplus x(tW_b))=(tP, R'\oplus x(tW_{1-b}))$ where $R'=R\oplus x(tW_0)\oplus x(tW_1)$, i.e., R and R' have exactly the same distribution from A_2's perspective even if A_2 can get the plaintexts (R and R' respectively) via querying its decryption oracle $D(sk_0,.)$ and $D(sk_1,.)$ on Y*. This implies that $Adv_{\pi,A}^{RE\_ANO\_CCA}(k)$ =0 unconditionally and the anonymity against chosen-ciphertext attacks follows.

Proposition 3.1 PSEC-1 *is both secure and anonymous in random oracle model against chosen-ciphertext attacks under the assumption of decisional Diffie-Hellman problem's hardness on elliptic curves.* □

3.2 Relevant security and its relationship with anonymity

In this section we develop a concept conjugate to relevant anonymity, which is not only useful in our works but also independently valuable in practice.

Definition 3.2(Relevant Security) 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(Note: to emphasize that two public/secret key pairs in this game are generated under the same public parameters, we use *sp* to explicitly represent this fact in all necessary places. This cumbersome representation will be omitted hereafter):

```
$Exp_{\pi,A}^{RE\_IND\_ATK}(k)$:

    (pk*, sk*)←KG(sp, k); /*sp is public (shared) parameters, refer to example 3.2 */
    ($M_0$*, $M_1$*, St)←$A_1^{Oracle}$(sp, pk*);
    (pk, sk)←KG(sp, k); /*randomly generate another public-secret key pair (pk, sk)
                          under the same parameter sp.*/
    b$\xleftarrow{\$}$ {0,1};
    y*←E(sp, pk, $M_b$*);
    d←$A_2^{Oracle}$(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*, .), Similar to the case of relevant anonymity, A is allowed to query its Oracle on the challenge ciphertext y*. The adversary's advantage $Adv_{\pi,A}^{RE\_IND\_ATK}$ is defined as $|2P[Exp_{\pi,A}^{RE_IND_ATK}(k)=1]-1|$or equivalently |P[d=0|b=0]-P[d=0|b=1]|. We say that Π is *relevant secure against adaptive chosen-plaintext*(respectively, *chosen-ciphertext*) *attacks* if $Adv_{\pi,A}^{RE\_IND\_CPA}$(respectively, $Adv_{\pi,A}^{RE\_IND\_CCA}$) is negligible in k for any P.P.T. adversary A. We notate $\max_{A\in P.P.T.} Adv_{\pi,A}^{RE\_IND\_ATK}$ as $Adv_{\pi,A}^{RE\_IND\_ATK}$ and have similar conventions as those for $Adv_{\pi,A}^{RE\_ANO\_ATK}$.

Its easy to prove that Π's security implies its corresponding relevant security, i.e., relevant security is weaker than security. Similar as the case of relevant anonymity, relevant security in combination with anonymity can imply (strong) security, which is exactly presented in the following theorem.

Theorem 3.2. *Let* Π=(KG, E, D) *be a public-key encryption scheme which is anonymous against chosen-plaintext*(*respectively, chosen-ciphertext*) *attacks. If* Π *is relevant secure against chosen-plaintext*(*respectively, chosen-ciphertext*) *attacks, then* Π *is secure against chosen-plaint*(*respectively, chosen-ciphertext*) *attacks. Concretely, we have*

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

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

where T_d is computational time of decryption algorithm D.

Proof. For the same reason as in the proof of theorem 3.1, we only prove the (comparatively more complicated)case of chosen-ciphertext attack. Suppose A=(A_1,A_2) is an P.P.T. adversary cracking Π's chosen-ciphertext security. We construct an P.P.T adversary B^A=(B_1,B_2) cracking Π's chosen-ciphertext anonymity as the following. Consider the game:

```
$Exp_{\pi,B}^{ANO\_CCA}(k)$:
    ($pk_0$, $sk_0$), ($pk_1$, $sk_1$)←KG(sp, k); /*sp is the public (shared) parameter.*/
    (M*, St)←$B_1^{D(sk0,.), D(sk1,.)}$(sp, $pk_0$, $pk_1$) where $B_1$ is implemented as:
            ($M_0$*, $M_1$*, St)←$A_1^{D(sk0,.)}$(sp, $pk_0$);
            M*←$M_0$;
            return(M*, St);
    b←$^\$${0,1};
    y*←E(sp, $pk_b$, M*);
    d←$B_2^{D(sk0, .), D(sk1,.)}$(y*, St) where $B_2$ is implemented as:
            d←$A_2^{D(sk0,.)}$(y*, St);
            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 such simulation is obviously perfect.

It's straightforward to verify that $Exp_{\pi,B}^{ANO\_CCA}(k)$ in case of b=0 is equivalent to $Exp_{\pi,A}^{IND\_CCA}(k)$ in case of b=0 and $Exp_{\pi,B}^{ANO\_CCA}(k)$ in case of b=1 is equivalent to $Exp_{\pi,A}^{RE\_IND\_CCA}(k)$ 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 anonymity in a very similar way as that of B^A, with the only difference that $C_1^{D(sk0, .)}$(pk_0, pk_1) calls A_1 in the way of $A_1^{D(sk1,.)}$(sp, pk_1)(correspondingly C simulates A's oracle D(sk_1,.) with its oracle D(sk_1,.)) and set M* to M_1*. As a result, $Exp_{\pi,C}^{ANO\_CCA}(k)$ in case of b=0 is equivalent to $Exp_{\pi,A}^{RE\_IND\_CCA}(k)$ in case of b=1 and $Exp_{\pi,C}^{ANO\_CCA}(k)$ in case of b=1 is equivalent to $Exp_{\pi,A}^{IND\_CCA}(k)$ in case of b=1. Therefore:

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

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

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

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

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

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

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

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

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

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

Alike theorem 3.1, theorem 3.2 presents an easy-to-check sufficient condition for a anonymous public-key encryption scheme to be secure, which can be used to simplify security proofs based-upon already known anonymous consequences. The concept of relevant security can be also ported to IBE schemes and theorem 3.2 is still true in that case.

Example 3.4(Example 3.1 continued): ElGamal scheme is not anonymous against chosen-ciphertext attacks. In fact an analysis very similar as in example 3.2(for Cramer-Shoup scheme)can derive that $Adv_{\pi,A}^{RE\_IND\_CCA}(k)$ =0 for any adversary A. If ElGamal scheme is really anonymous against chosen-ciphertext attacks, by theorem 3.2 it would be secure against chosen-ciphertext attaks, however, the consequence is actually false because of ElGamal scheme’s malleability. This contradiction shows that ElGamal scheme is anonymous only against chosen-plaintext but not chosen-ciphertext attacks.

Example 3.5(Example 3.2 continued) It’s not hard to observe that in Cramer-Shoup scheme $Adv_{\pi,A}^{RE\_IND\_CCA}(k)$ =0 for any adversary A. Since this scheme’s anonymity against chosen-ciphertext attacks is provably true [3], we can derive its security against chosen-ciphertext attacks under the same computational hardness assumption by combining the consequence in [3] and our theorem 3.2. In the style, some complicated proofs can be saved. The same thing holds for PSEC-1 too.

4 Anonymity of Fujisaki-Okamoto Hybrid Scheme

4.1 Fujisaki-Okamoto Hybrid Scheme

Fujisaki-Okamoto hybrid scheme[8] Π=(KG, E, D, G, H) is constructed from public-key encryption scheme Π^a=(KG^a, E^a, D^a), symmetric encryption scheme Π^s=(KG^s, E^s, D^s) and two random oracles G, H. KG=KG^a. The encryption algorithm is defined as E(pk,M)=E^a(pk, σ; H(σ||M))||E^s(G(σ),M) where σ is randomly selected and H(σ||M) plays the role of random seed in encryption computation. The decryption algorithm D(sk,y) woks as the following:

```
parse y as $y_1||y_2$;
$\sigma \leftarrow D^a(sk,y_1)$;
$M \leftarrow D^s(G(\sigma),y_2)$;
if $y_1=E^a(pk,\sigma; H(\sigma||M))$ then output(M) else output($\perp$)
```

To proceed with our discussion we need one more concept related to the hybrid construction. A *plaintext-checking* oracle PCA$_{sk}$(.) takes plaintext-ciphertext pair (M,y) as input, outputs 1 if M=D(sk,y) and 0 otherwise. Let ATK$\in${CPA,PCA, CCA}, Oracle be oracle determined by ATK, which is empty for CPA, PCA$_{sk}$(.) for PCA and D$_{sk}$(.) for CCA. Consider the following game:

```
$Exp_{\pi^a,J}^{OWE\_ATK}(k)$:
    (pk, sk)←KG(k);
    Randomly select σ* from $\Pi^a$'s message space;
    y*←E (pk, σ*);
    $\sigma^0 \leftarrow J^{Oracle}$(pk, y*);
    if($\sigma^0$=σ* ) then output 1 else output 0.
```

In case of ATK=CCA, J is disallowed to query on its challenge ciphertext y*(but in case of PCA, this event is allowed). Public-key scheme Π^a is said *one-way secure against chosen-plaintext, chosen plaintext-checking or chosen-ciphertext attacks* respectively if for any P.P.T. adversary J the corresponding game can output 1 only with a negligible probability in k. Such probability is notated as $Adv_{\pi,J}^{OWE-ATK}(k)$ and $Adv_{\pi}^{OWE\_ATK}(k) \equiv \max_{J \in P.P.T.} Adv_{\pi,J}^{OWE\_ATK}(k)$. In this whole section only one-way security against chosen-plaintext attacks is needed so we simply name it "one-way secure" as shorthand.

Fujisaki-Okamoto hybrid scheme can strongly enhance its component schemes' security, which is exactly proved in their original paper[8](In our following work the asymmetric scheme's γ-uniformity and symmetric scheme's find-and-guess security are not used, so no explanations on them are given in this paper).

Fujisaki-Okamoto Theorem Let Π=(KG, E, D, G, H) *be Fujisaki-Okamoto hybrid public-key encryption scheme constructed from public-key encryption scheme* Π^a=(KG^a, E^a, D^a) *and symmetric encryption scheme* Π^s=(KG^s, E^s, D^s). If Π^a *is one-way secure and γ–uniform where γ is negligible in k,* Π^s *is secure in sense of Find-and-Guess, then* Π *is secure against chosen-ciphertext attacks.*

4.2 A Sufficient and Necessary Condition for Anonymity against Chosen-plaintext Attacks

Before exactly presenting our results we need to specify a property of well-constructed public-key encryption schemes.

Definition 4.1(regular encryption)A public-key encryption scheme Π=(KG, E, D) is defined as *regular* if for any message-pair (M_0,M_1) the probability $\delta_{\pi^a}(k)$≡P[(pk_0, sk_0),(pk_1, sk_1)←KG(k): E(pk_0,M_0)=E(pk_1, M_1)] is negligible in complexity parameter k.

Regularity is a good property possessed by almost all practical public-key schemes, e.g., ElGamal and Cramer-Shoup schemes(for instance of ElGamal scheme, E(pk_0,M_0)=E(pk_1, M_1) iff $g_0^r \| g_0^{rx_0} M_0 = g_1^{r'} \| g_1^{r'x_1} M_1$.Since r and r' are selected at random and independently, $\delta_{ElGamal}(k)$=P[$g_0^r \| g_0^{rx_0} M_0 = g_1^{r'} \| g_1^{r'x_1} M_1$]≤P[$g_0^r = g_1^{r'}$]=1/q which is obviously negligible in complexity parameter k(=$\log_2$q). The same analysis is also true for Cramer-Shoup scheme).

Theorem 4.1 *Let* Π=(KG, E, D, G, H) *be Fujisaki-Okamoto hybrid public-key encryption scheme constructed from regular public-key scheme* Π^a=(KG^a, E^a, D^a) *and symmetric encryption scheme* Π^s=(KG^s, E^s, D^s). Π *is anonymous against chosen-plaintext attacks if and only if* Π^a *is relevant anonymous against chosen-plaintext attacks and one-way secure.*

Remarks: Conditions in the theorem only concerns the component public-key scheme Π^a's weak anonymity(RE_ANO_CPA) and its weak security(OWE). As Fujiksaki-Okamoto theorem states, OWE(together with other weak properties) leads to the hybrid scheme's strong security, i.e., IND_CCA(in fact even stronger than that: plaintext-aware in random oracle model as shown in their original paper). Therefore, for applications where both anonymity and security are desired conditions in theorem 4.1 is weak and practical.

In the following proof, the adversary's advantage is denoted as $Adv_\pi^{\{RE\_ANO\_CPA,ANO\_CPA\}}(q_g, q_h, t)$ or $Adv_\pi^{\{RE\_ANO\_CCA,ANO\_CCA\}}(q_g, q_h, q_d, t)$ where q_g, q_h, q_d are number of queries to G, H and decryption oracles respectively. Theorem 4.1 comes from the following three lemmas.

Lemma 4.1 *If* Π *is relevantly anonymous against chosen-plaintext attacks, then* Π^a *is also relevant anonymous against chosen-plaintext attacks. Concretely,*

$$Adv_{\pi^a}^{RE\_ANO\_CPA}(t) \le Adv_{\pi}^{RE\_ANO\_CPA}(0,0,t)\ .$$

Proof Suppose A=(A_1,A_2) is an P.P.T. chosen-plaintext adversary cracking Π^a's relevant anonymity, we construct a P.P.T chosen-plaintext adversary B^A=(B_1,B_2) cracking Π's relevant anonymity. B has access to random oracles G and H. Consider the following game:

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

    ($pk_0$, $sk_0$), ($pk_1$, $sk_1$)←KG(k);
    (M*, St)←$B_1^{G,H}$($pk_0$, $pk_1$) where $B_1$ is implemented as:
            ( σ *, $St_A$)←$A_1$($pk_0$, $pk_1$);
            randomly select M* from Π 's message space;
            return(M*, St);
    b$\xleftarrow{\$}$\{0,1\};
    randomly select M from Π 's message space and in the same size of M*: |M|=|M*|;
    randomly select  σ from  $\Pi^a$'s message space;
      /* σ is used in the hybrid encryption and comes from the same space in which σ *
         resides. In particular, |σ|=|σ*|.*/
    y*←$E^a$($pk_b$, σ , H( σ ||M))|| $E^s$(G(σ),M);
    d←$B_2^{G,H}$(y*, St) where $B_2$ is implemented as:
            parse y* as $y^a$||$y^s$;
            d←$A_2$ ($y^a$, St);
            return(d);
    if d=b then output 1 else output 0.
```

Note that in $Exp_{\pi,B}^{RE\_ANO\_CPA}(k)$ for any b∈{0,1} the challenge ciphertext y^a= E^a(pk_b, σ , H(σ ||M)) as input to A_2 has exactly the same distribution as that in $Exp_{\pi^a,A}^{RE\_ANO\_PA}(k)$ in the same case of b. Therefore, $Adv_{\pi,B}^{RE\_ANO\_CPA}(k)$ = $|2\ P[Exp_{\pi,B}^{RE\_ANO\_CPA}(k)=1]\ \text{-}1|$ = $|2\ P[Exp_{\pi^a,A}^{RE\_ANO\_CPA}(k)=1]\ \text{-}1|$ = $Adv_{\pi^a,A}^{RE\_ANO\_CPA}(k)$. The theorem's inequality can be directly derived from this result. □

Lemma 4.2 *If* Π *is anonymous against chosen-plaintext attacks and* Π^a *is regular, then* Π^a *is one-way secure. Concretely,*

$$Adv_{\pi^a}^{OWE\_CPA}(t) \le Adv_{\pi}^{ANO\_CPA}(q_g, q_h, O(t+T_{E^a})) + \delta_{\pi^a}(k)$$

where q_g=0, q_h≤2, T_{E^a} is Π^a's computation time of its encryption algorithm.

Proof Suppose J is an P.P.T. adversary cracking Π^a's one-way security, we construct a P.P.T chosen-plaintext adversary $A^J=(A_1,A_2)$ cracking Π's anonymity. A has access to random oracles G and H. Consider the following game:

```
$Exp_{\pi,A}^{ANO-CPA}(k)$:
    $(pk_0, sk_0), (pk_1, sk_1) \leftarrow KG(k)$;
    $(M^*, St) \leftarrow A_1^{G,H}(pk_0, pk_1)$ where $A_1$ is implemented as:
            randomly select M* from Π's message space;
            $St \leftarrow M^* \| pk_0 \| pk_1$;
            return(M*, St);
    $b \overset{\$}{\leftarrow} \{0,1\}$;
    randomly select $\sigma^*$ from $\Pi^a$'s message space;
    $y^* \leftarrow E^a(pk_b,\sigma^*; H(\sigma^* \| M^*)) \| E^s(G(\sigma^*),M^*)$;
    $d \leftarrow A_2^{G,H}(y^*, St)$ where $A_2$ is implemented as:
            parse $y^*$ as $y^a \| y^s$; parse St as $M^* \| pk_0 \| pk_1$;
            $\sigma_0 \leftarrow J(pk_0, y^a)$;   $\sigma_1 \leftarrow J(pk_1, y^a)$;
            if  $E^a(pk_0,\sigma_0; H(\sigma_0 \| M^*))=y^a$
            then  $d \leftarrow 0$;
            else  if  $E^a(pk_1,\sigma_1, H(\sigma_1 \| M^*))=y^a$
                then  $d \leftarrow 1$;
                else  $d \overset{\$}{\leftarrow} \{0,1\}$;
            return(d);
    if d=b then output 1 else output 0.
```

Denote the probability in $Exp_{\pi,A}^{ANO-CPA}(k)$ as $P_A[]$ and the probability in $Exp_{\pi,J}^{OWE}(k)$ as $P_J[]$.

By A's specification we have

$$\begin{aligned}
P_A[d=0|b=0]&=P_A[E^a(pk_0,\sigma_0;H(\sigma_0\|M^*))=y^a|\ y^a\in E^a(pk_0,\sigma^*)]+\\
&\quad+(1/2)\ P_A[E^a(pk_0,\sigma_0;H(\sigma_0\|M^*))\neq y^a\wedge E^a(pk_1,\sigma_1;H(\sigma_1\|M^*))\neq y^a\ |\ y^a\in E^a(pk_0,\sigma^*)]\\
&=P_J[y^a\in E^a(pk_0,\sigma^*):\ J(pk_0,y^a)=D^a(sk_0,y^a)]\\
&\quad+(1/2)\ P_J[J(pk_0,y^a)\neq D^a(sk_0,y^a)\wedge J(pk_1,y^a)\neq D^a(sk_1,y^a)\ |\ y^a\in E^a(pk_0,\sigma^*)]
\end{aligned}$$

$$\begin{aligned}
P_A[d=0|b=1]&=P_A[E^a(pk_0,\sigma_0;H(\sigma_0\|M^*))=y^a|\ y^a\in E^a(pk_1,\sigma^*)]\\
&\quad+(1/2)\ P_A[E^a(pk_0,\sigma_0;H(\sigma_0\|M^*))\neq y^a\wedge E^a(pk_1,\sigma_1;H(\sigma_1\|M^*))\neq y^a\ |\ y^a\in E^a(pk_1,\sigma^*)]\\
&=P[(pk_0,sk_0),(pk_1,sk_1)\text{ are randomly selected: }E^a(pk_0,\sigma_0;H(\sigma_0\|M^*))=E^a(pk_1,\sigma^*;H(\sigma^*\|M^*))]\\
&\quad+(1/2)\ P_J[J(pk_0,y^a)\neq D^a(sk_0,y^a)\wedge J(pk_1,y^a)\neq D^a(sk_1,y^a)\ |\ y^a\in E^a(pk_1,\sigma^*)]\\
&\leq\delta_{\pi^a}(k)+(1/2)\ P_J[J(pk_0,y^a)\neq D^a(sk_0,y^a)\wedge J(pk_1,y^a)\neq D^a(sk_1,y^a)\ |\ y^a\in E^a(pk_1,\sigma^*)]
\end{aligned}$$

where $\delta_{\pi^a}(k)$ is Π^a's regularity advantage(since H is a random oracle). Note that (pk_0, sk_0) and (pk_1, sk_1) are randomly and independently generated so $P_J[J(pk_0,y^a)\neq D^a(sk_0,y^a)\wedge J(pk_1, y^a)\neq D^a(sk_1,y^a)\ |\ y^a\in E^a(pk_0,\sigma^*)]=P_J[J(pk_0,y^a)\neq D^a(sk_0,y^a)\wedge J(pk_1, y^a)\neq D^a(sk_1,y^a)\ |\ y^a\in E^a(pk_1,\sigma^*)]$. Therefore:

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

$=|\ P_J[y^a \in E^a(pk_0,\sigma^*)\text{: } J(pk_0, y^a)=D^a(sk_0, y^a)|]\ \text{-}\ \delta_{\pi^a}(k)\ |$

$\geq Adv^{OWE\_CPA}_{\pi^a,J}(k)\ \text{-}\ \delta_{\pi^a}(k)$. namely

$$Adv^{OWE\_CPA}_{\pi^a,J}(k) \leq Adv^{ANO\_CPA}_{\pi,A}(k) + \delta_{\pi^a}(k)$$

which derives the lemma's inequality and the time complexity can be directly verified according to A's specification. □

Lemma 4.1 and lemma 4.2 proves the necessity of Π^a's one-way security and relevant anonymity against chosen-plaintext attacks. Next lemma proves its sufficiency.

Lemma 4.3 *If* Π^a *is one-way secure and relevantly anonymous against chosen-plaintext attacks, then* Π *is anonymous against chosen-plaintext attacks. Concretely,*

$$Adv^{ANO\_CPA}_{\pi}(q_g, q_h, t) \leq Adv^{RE\_ANO\_CPA}_{\pi^a}(t) + (q_g+q_h)\, Adv^{OWE\_CPA}_{\pi^a}(t)$$

Proof Suppose $A=(A_1,A_2)$ is an P.P.T. chosen-plaintext adversary cracking Π's anonymity, we construct a P.P.T chosen-plaintext adversary $B^A=(B_1,B_2)$ cracking Π^a's relevant anonymity. A needs access to random oracles G and H. Consider the following game:

```
$Exp^{RE\_ANO\_CPA}_{\pi^a,B}(k)$:
    $(pk_0, sk_0), (pk_1, sk_1) \leftarrow KG(k)$;
    $(\sigma^0, St) \leftarrow B_1(pk_0, pk_1)$ where $B_1$ is implemented as:
            Both G-list and H-list are initialized to be empty;
            Randomly select $\sigma^0$ from $\Pi^a$'s message space;
            Randomly select $g^0$ from $\Pi^S$'s key space;
            $(M^*, St_A) \leftarrow A_1^{G,H}(pk_0, pk_1)$;
            $St \leftarrow St_A||M^*||\sigma^0||g^0$;
            Return($\sigma^0$, St);
    $b \xleftarrow{\$} \{0,1\}$;
    Randomly select h* from $\Pi^a$'s coin space;
    Randomly select $\sigma^*$ from $\Pi^a$'s message space; /*It's the same space as
      from which $\sigma^0$ is generated. In particular, $|\sigma^*|=|\sigma^0|$.*/
    $y^* \leftarrow E^a(pk_b,\sigma^*; h^*)$
    $d \leftarrow B_2(y^*, St)$ where $B_2$ is implemented as:
            parse St as $St_A||M^*||\sigma^0||g^0$;
            $v^* \leftarrow E^S(g^0, M^*)$;
            $d \leftarrow A_2^{G,H}(y^*||v^*, St_A)$;
            return(d);
    if d=b then output 1 else output 0.
```

B carries out simulation as follows.

```
On each query  σ from A to oracle G(.), B does:
        If there exists (σ,g) in G-list
        Then return(g)
        Else randomly select g from $\Pi^{s}$'s key space;
            Insert (σ,g) in G-list;
            Return(g);

On each query (σ,m) from A to oracle H(.), B does:
        If there exists (σ,m,h) in H-list
        Then return(g)
        Else randomly select h from $\Pi^{a}$'s coin space;
            Insert (σ,m,h) in H-list;
            Return(h);
```

Define an event Z as that there exists an item (σ*,.) in G-list or (σ*,.,.) in H-list. Let p_0 be P[Z]. According to B's specification we have P[$Exp^{RE\_ANO\_CPA}_{\pi^a,B}(k)$ =1| ∼ Z] =P[$Exp^{ANO\_CPA}_{\pi,A}(k)$=1], so P[$Exp^{RE\_ANO\_CPA}_{\pi^a,B}(k)$=1] ≥ P[$Exp^{RE\_ANO\_CPA}_{\pi^a,B}(k)$=1|∼Z]P[∼Z] = P[$Exp^{RE\_ANO\_CPA}_{\pi^a,B}(k)$=1|∼Z](1-$p_0$) ≥P[$Exp^{ANO\_CPA}_{\pi,A}(k)$=1]-$p_{0,}$ hence

$$P[Exp^{ANO\_CPA}_{\pi,A}(k)=1] \leq P[Exp^{RE\_ANO\_CPA}_{\pi^a,B}(k)=1] + p_{0.}$$

Furthermore, p_0 can be estimated by constructing two P.P.T. adversaries J_0 and J_1 based-on A to crack Π^a's one-way security. Consider the game:

```
$Exp^{OWE\_CPA}_{\pi^a,J0}(k)$:
    ($pk_0$, $sk_0$)←KG(k);
    Randomly select σ* from  $\Pi^{a}$'s message space;
    y*←$E^a$($pk_0$, σ*);
    $\sigma^0$←$J_0$($pk_0$, y*) where $J_0$ is implemented as:
            cnt←0;
            ($pk_1$, $sk_1$)←KG(k);
            Randomly select g* from  $\Pi^{S}$'s key space;
            (M, St)←$A_1^{G,H}$($pk_0$, $pk_1$);
            $v^0$←$E^s$(g*, M);
            d←$A_2^{G,H}$(y*||$v^0$, St);
            i← $^\$$ {1,2,…,cnt};
            /* w.o.l.g., all σ's queried by A for G and H are distinct and
               indexed as $\sigma_1$,…, $\sigma_{cnt}$.*/
            output($\sigma_i$).
```

On each query σ or (σ,m) from A to its oracle G(.) or H(.) respectively, J_0 simulates G and H as B does in the above; Additionally, every query from A is counted by J_0 via the variable cnt. Note that $Exp_{\pi^a,J0}^{OWE\_CPA}(k)$ is just $Exp_{\pi,A}^{ANO\_CPA}(k)$ in case of b=0. Denoting the probability of the event occurring in $Exp_{\pi,A}^{ANO\_CPA}(k)$ as $P_A[.]$, we have

$$Adv_{\pi^a,J0}^{OWE\_CPA}(k)=P[Exp_{\pi^a,J0}^{OWE\_CPA}(k)=1]\geq(1/cnt)P_A[Z|b=0]\geq P_A[Z|b=0]/(q_g+q_h)$$

On the other hand, we can construct another adversary J_1 in a similar way as that of J_0 with the only difference that J_1 calls A_1 in the form of (M, St)←$A_1^{G,H}(pk_1, pk_0)$, i.e., exchanging pk_0 and pk_1's roles. As a result, $Exp_{\pi^a,J1}^{OWE\_CPA}(k)$ is just $Exp_{\pi,A}^{ANO\_CPA}(k)$ in case of b=1 and we have

$$Adv_{\pi^a,J1}^{OWE\_CPA}(k)=P[Exp_{\pi^a,J1}^{OWE\_CPA}(k)=1]\geq P_A[Z|b=1]/(q_g+q_h)$$

So p_0≡P[Z]=(1/2)(P_A[Z|b=1]+P_A[Z|b=0])≤(cnt/2)($Adv_{\pi^a,J0}^{OWE\_CPA}(k)$ + $Adv_{\pi^a,J1}^{OWE\_CPA}(k)$) ≤((q_g+q_h)/2)($Adv_{\pi^a,J0}^{OWE\_CPA}(k)$ + $Adv_{\pi^a,J1}^{OWE\_CPA}(k)$). In combination with the inequality $Exp_{\pi,A}^{ANO\_CPA}(k)\leq$ P[$Exp_{\pi^a,B}^{RE\_ANO\_CPA}(k)=1$] + p_0 we got before, we have:

$$P[Exp_{\pi,A}^{ANO\_CPA}(k)=1]$$

$$\leq P[Exp_{\pi^a,B}^{RE\_ANO\_CPA}(k)=1]+(1/2(q_g+q_h))(Adv_{\pi^a,J0}^{OWE\_CPA}(k)+Adv_{\pi^a,J1}^{OWE\_CPA}(k))$$

and the lemma's final inequality can be derived directly. □

4.3 A Sufficient Condition for Anonymity against Chosen-ciphertext Attacks

Theorem 4.1 shows that Fujisaki-Okamoto's hybrid scheme also has a good enhancement in anonymity, although not as good as its enhancement in security. A further question is that which kind of anonymity of the component public-key scheme can be enhanced to the strongest one, i.e., anonymity against chose-ciphertext attacks? Theorem 4.2 presents such a condition and this theorem can be regarded as a generalization of lemma 4.3 to the case of chosen-ciphertext attacks. Its proof logic is somewhat like that of lemma 4.3 and its special difficulty comes from how to simulate Π's decryption oracle by $Π^a$'s one-way security cracker, which is solved essentially by Π's knowledge extractor.[2] As remarks on theorem 4.1, conditions in theorem 4.2 are weak and practical for applications where both security and anonymity of the hybrid scheme is desired.

[2] The same idea was originally used by Fujisaki and Okamoto to prove that their hybrid scheme is in fact plaintext-aware(in oracle model). The decryption simulation in our proof is essentially the same as that in [8].

Theorem 4.2 *If* Π^a *is one-way secure*(*against chosen-plaintext attacks*) *and relevantly anonymous against chosen-ciphertext attacks, then* Π *is anonymous against chosen-ciphertext attacks. Concretely,* $Adv_{\pi}^{ANO\_CCA}(q_g, q_h, q_d, t) \le$

$$Adv_{\pi^a}^{RE\_ANO\_CCA}(q_d, t+O(q_d)) + (q_g+q_h)\, Adv_{\pi^a}^{OWE\_CPA}(t+O(q_g+q_h)q_d)$$

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 B^A=(B_1,B_2) cracking Π^a's relevant anonymity. Consider the following game:

```
$Exp_{\pi^a,B}^{RE\_ANO\_CCA}(k)$:
    ($pk_0$, $sk_0$), ($pk_1$, $sk_1$)←KG(k);
    ($\sigma^0$, St)← $B_1^{D^a(sk_0,.),D^a(sk_1,.)}(pk_0, pk_1)$   where $B_1$ is implemented as:
            Both G-list and H-list are initialized to be empty;
            Randomly select $\sigma^0$ from $\Pi^a$'s message space;
            Randomly select $g^0$ from $\Pi^s$'s key space;
            ($M^0$, $St_A$)← $A_1^{G,H,D(sk_0,.),D(sk_1,.)}(pk_0, pk_1)$;
            St←$St_A$||$M^0$||$\sigma^0$||$g^0$;
            Return($\sigma^0$, St);
    b←$^\$${0,1};
    Randomly select h* from $\Pi^a$'s coin space;
    Randomly select σ* from $\Pi^a$'s message space; /*it's the same space as
          from which $\sigma^0$ is generated. In particular, |$\sigma^0$|=|σ*|.*/
    y*←$E^a$($pk_b$,σ*; h*);
    d← $B_2^{D^a(sk_0,.),D^a(sk_1,.)}(y^*, St)$   where $B_2$ is implemented as:
            parse St as $St_A$||$M^0$||$\sigma^0$||$g^0$;
            v*←$E^s$($g^0$, $M^0$);
            d← $A_2^{G,H,D(sk_0,.),D(sk_1,.)}(y^* \| v^*, St_A)$;
            return(d);
    if d=b then output 1 else output 0.
```

```
B carries out simulations as follows.
(1)On each query σ from A to oracle G(.), B does:
        If there exists (σ,g) in G-list
        Then return(g);
        Else randomly select g from $\Pi^s$'s key space;
            Insert (σ,g) in G-list;
            Return(g);
```

```
(2)On each query (σ,m) from A to oracle H(.), B does:
        If there exists (σ,m,h) in H-list
        Then return(h);
        Else randomly select h from Π^a's coin space;
            Insert (σ,m,h) in H-list;
            Return(h);
```

(3)On each query y from A to its oracle D(sk_j,.), j=0,1, B simulates D(sk_j,y) as follows(note that oracle-D(sk_j,.) may access G and H from inside and such accesses are also processed by B in the afore-specified way):

```
        Parse y as $y^a||y^s$;
        $σ \leftarrow D^a(sk_j,y^a)$;    /* $D^a(sk_j,.)$ is B's decryption oracle and recall that $y^a$ is allowed
              to be y* in defition.*/
        Find the item (σ, g) in G-list;
        If there is no item (σ, . ) in G-list
        Then    randomly select g from Π^s's key space;
                Insert (σ, g) into G-list;
        $m \leftarrow D^s(g,y^s)$;
        Find the item (σ, m, h) in H-list;
        If there is no item (σ, m, . ) in H-list
        Then    randomly select h from Π^a's coin space;
                Insert (σ, g, h) into H-list;
        If    $y^a=E^a(pk_j, σ; h)$
        Then    return(m);
        Else     return( ⊥ )
```

Define an event Z as that there exists an item (σ*,.) in G-list or item (σ*,.,.) in H-list. Let p_0 be P[Z]. According to B's specification we have P[$Exp_{\pi^a,B}^{RE\_ANO\_CCA}(k)$=1|∼Z] =P[$Exp_{\pi,A}^{ANO\_CCA}(k)$=1] because in event of ∼Z decryption operations simulated by B on all queries from A is perfect, so

$$P[Exp_{\pi^a,B}^{RE\_ANO\_CCA}(k)=1] \geq P[Exp_{\pi^a,B}^{RE\_ANO\_CCA}(k)=1|\sim Z]\ P[\sim Z]$$

$$=P[Exp_{\pi^a,B}^{RE\_ANO\_CCA}(k)=1|\sim Z](1-p_0) \geq P[Exp_{\pi,A}^{ANO\_CCA}(k)=1]-p_0$$

hence $Exp_{\pi,A}^{ANO\_CCA}(k) \leq P[Exp_{\pi^a,B}^{RE\_ANO\_CCA}(k)=1]+p_0$.

Furthermore p_0 can be estimated by constructing two P.P.T. adversaries J_0 and J_1 based-on A to crack Π^a's one-way security. Consider the game:

```
$Exp_{\pi^a,J0}^{OWE\_CPA}(k)$:
        $(pk_0, sk_0) \leftarrow KG(k)$;
        Randomly select σ* from  Π^a's message space;
```

```
$y^a*$←$E^a(pk_0, σ*)$;
$σ^0$←$J_0(pk_0, y^a*)$ where $J_0$ is implemented as:
        cnt←0;
        $(pk_1, sk_1)$←KG(k);
        Randomly select g* from Π$^s$'s key space;
        (M, St)← $A_1^{G,H,D(sk_0,.),D(sk_1,.)}(pk_0, pk_1)$;
        $v^*$←$E^s$(g*, M);
        d← $A_2^{G,H,D(sk_0,.),D(sk_1,.)}(y^a * \| v*, St)$;
        i← $^\$$ {1,2,…,cnt};
        /* w.o.l.g., all σ's queried by A for G and H are distinct and
           indexed as $σ_1$,…, $σ_{cnt}$.*/
        output($σ_i$).
```

J_0 carries out simulations as follows.

(1)On each query σ or (σ, m) from A to its oracle G(.) or H(.) respectively, J_0 simulates G or H as B does in the above; Additionally, every query from A is counted by J_0 via cnt.

(2)On each query y from A to its oracle-D(sk_1,.), J_0 simulates D(sk_1,y) via directly applying Π's decipher algorithm with its complete knowledge of secret key sk_1(when D(sk_1,.) needs to access G and H from inside, such accesses are also processed by B in the afore-specified way):

(3) On each query y from A to its oracle-D(sk_0,.), J_0 simulates D(sk_0,y) as follows:

```
    Parse y as $y^a \| y^s$;
    If   There exist an item (σ, g) in G-list and item (σ, m, h) in H-list
         such that $y^a$=$E^a$($pk_0$, σ; h)
    Then   return(m);
    Else /*y is not produced by A via explicitly encrypting some plaintext.*/
         If   there exists (σ, m, h) in H-list such that $y^a$=$E^a$($pk_0$, σ; h)
              /*but no (σ, .) in G-list */
         Then randomly select g from Π$^s$'s key space;
                Insert (σ, g) into G-list;
                m←$D^s$(g, $y^s$);
                Return(m);
          Else
                Randomly select m from Π$^s$'s message space;
                Return(m)
```

Because $y^a*\|v*$ is disallowed to query and G,H are random oracles, this simulation is perfect. Furthermore, note that $Exp_{\pi^a,J0}^{OWE-CPA}(k)$ is just $Exp_{\pi\ ,A}^{ANO-CCA}(k)$ in case of b=0.

Denoting the probability of the event occurring in $Exp_{\pi\ ,A}^{ANO\_CCA}(k)$ as $P_A[.]$, we have

$$Adv_{\pi^a,J0}^{OWE\_CPA}(k)\text{=P[}Exp_{\pi^a,J0}^{OWE\_CPA}(k)\text{=1]}\geq 1/(q_g+g_h)P_A[Z|b=0]$$

On the other hand, we can construct another adversary J_1 in a similar way as that of J_0 with the only difference that J_1 calls A_1 in the form of (M, St)← $A_1^{G,H,D(sk_1,.),D(sk_0,.)}(pk_1,pk_0)$, i.e., exchanging pk_0 and pk_1's roles. As a result, $Exp_{\pi^a,J1}^{OWE\_CPA}(k)$ is just $Exp_{\pi\ ,A}^{ANO\_CCA}(k)$ in case of b=1 and we have

$$Adv_{\pi^a,J1}^{OWE\_CPA}(k)\text{=P[}Exp_{\pi^a,J1}^{OWE\_CPA}(k)\text{=1]}\geq 1/(q_g+g_h)P_A[Z|b=1]$$

So p_0≡P[Z]=(1/2)(P_A[Z|b=1]+P_A[Z|b=0])≤(1/2(q_g+q_h))($Adv_{\pi^a,J0}^{OWE\_CPA}(k)+Adv_{\pi^a,J1}^{OWE\_CPA}(k)$).

In combination with the inequality $Exp_{\pi,A}^{ANO\_CCA}(k)$≤P[$Exp_{\pi^a,B}^{RE\_ANO\_CCA}(k)$ =1]+p_0 we got before, we have P[$Exp_{\pi,A}^{ANO\_CCA}(k)$ =1]

$$\leq\text{P[}Exp_{\pi^a,B}^{RE\_ANO\_CCA}(k)\text{ =1]+(1/2(}q_g+q_h\text{))(}Adv_{\pi^a,J0}^{OWE\_CPA}(k)+Adv_{\pi^a,J1}^{OWE\_CPA}(k)\text{)}$$

and the lemma's final inequality can be derived directly and the time/query complexity can be directly verified. □

Corollary 4.1 Let Π=(KG, E, D, G, H) *be Fujisaki-Okamoto hybrid public-key encryption scheme constructed from public-key encryption scheme* Π^a=(KG^a, E^a, D^a) *and symmetric encryption scheme* Π^s=(KG^s, E^s, D^s). If Π^a *is one-way secure, γ–uniform where γ is negligible in k and relevantly anonymous against chosen-ciphertext attacks;* Π^s *is secure in sense of Find-and-Guess, then* Π *is secure and anonymous, both are against chosen-ciphertext attacks.*

Theorem 4.2 shows that in many reasonable cases the component public-key scheme's weak anonymity(i.e.,relevant anonymity against chosen-ciphertext attacks) can be enhanced by Fujisaki-Okamoto construction to the strongest anonymity. Theorem 4.2 can be applied to lots of concrete hybrid schemes(e.g.,ElGamal-based and Okamoto-Uchiyama-based schemes in [8]'s section 6) to prove their anonymity against chosen-ciphertext attacks. Here we apply this theorem to PSEC-2, an provably secure elliptic curve encryption scheme proposed for NISSIE[9].

Example 4.1(PSEC-2's anonymity against chosen-ciphertext attacks) PSEC-2 public-key encryption scheme is provably secure(in random oracle model)against chosen-ciphertext attacks under the assumption of decisional Diffie-Hellman problem's hardness on elliptic curves and some additional weak security assumptions on its symmetric encryption component. In this scheme(fig.4), just like in PSEC-1 it's reasonable to consider (E/F_q, p, q, P) as (shared) public parameters and W as the real public-key (each individual has distinct W).

Note that PSEC-2 is actually a Fujisaki-Okamoto construction from asymmetric scheme Π^a and symmetric scheme (SymEnc,SymDec) where Π^a=(KG^a, E^a, D^a) is defined in fig.5。

With the same analysis as in example 3.3 for PSEC-1, it holds unconditionally that $Adv_{\pi^a,A}^{RE\_ANO\_CCA}(k)$=0. In addition, all conditions in Fujisaki-Okamoto theorem are satisfied by Π^a [9], in particular Π^a is one-way secure (against chosen-plaintext attacks). Combining these facts and our theorem 4.2, we have the following consequence on PSEC-2.

```
Key generator KG(E/F_q,p,q,P):
    s ←$ Z_p;
    W ← sP;
    pk ← W;
    sk ← s;
    return(pk, sk)

Encryption algorithm E(pk, M), M∈{0,1}^+:
    r ←$ Z_p;
    t ← H(r||M); /*r used as a string*/
    Q ← tW;
    C_1 ← tP;
    C_2 ← r ⊕ x(Q);
    C_3 ← SymEnc(G(r), M);
    return(C_1,C_2, C_3)

Decryption algorithm D(sk,Y):
    Parse Y as (C_1,C_2,C_3)
    Q ← sC_1;
    u ← C_2 ⊕ x(Q);
    M ← SymDec(G(u), C_3);
    if  C_1=H(u||M)P
    Then  return(M);
    Else  return(⊥);
```

Figure 4 PSEC-2 encryption Scheme: E/F_q is the group of an elliptic curve over field F_q. P is a point on E/F_q with (prime) order p. x(Q) is the x-coordinate of curve point Q. (SymEnc, SymDec) is a symmetric encryption scheme. $G:Z_p \rightarrow \{0,1\}^k$ and H: $\{0,1\}^+ \rightarrow Z_p$ are random oracles.

```
Key generator KG^a(E/F_q,p,q,P):
    s ←$ Z_p;
    W ← sP;
    pk ← W;
    sk ← s;
    return(pk, sk)

Encryption algorithm E^a(pk, σ), σ∈{0,1}^+:
    t ←$ Z_p;
    Q ← tW;
    C_1 ← tP;
    C_2 ← σ ⊕ x(Q);
    return(C_1,C_2)

Decryption algorithm D^a(sk,Y):
    Parse Y as (C_1,C_2)
    Q ← sC_1;
    σ ← C_2 ⊕ x(Q);
    return(σ);
```

Figure 5 PSEC-2's asymmetric component encryption scheme Π^a

Proposition 4.1 If the component symmetric encryption scheme is Find-and-Guess secure, then PSEC-2 *is both secure and anonymous in random oracle model against chosen-ciphertext attacks under the assumption of decisional Diffie-Hellman problem's hardness on elliptic curves.* □

5 Anonymity of Okamoto-Pointcheval Hybrid Scheme: REACT

REACT[11] is another highly efficient hybrid scheme Π=(KG, E, D, G, H) constructed from a public-key encryption scheme Π^a=(KG^a, E^a, D^a), a symmetric encryption scheme Π^s=(KG^s, E^s, D^s) and two random oracles G, H. Alike Fujisaki-Okamoto scheme, KG=KG^a. The encryption algorithm is defined as E(pk,M)=E^a(pk,R;u) ||E^s(G(R),M)||H(R,m,y_1,y_2), where u is random seed in encryption computation, y_1= E^a(pk,R;u) and y_2=E^s(G(R),M). The decryption algorithm D(sk,y) woks as the following:

```
parse y as $y_1||y_2||h$;
R←$D^a(sk,y_1)$;
M←$D^s(G(R),y_2)$;
if h=H(R,M, $y_1$,$y_2$) then output(M) else output(⊥)
```

Alike Fujisaki-Okamoto hybrid scheme, REACT can also strongly enhance its component schemes' security, which is exactly proved in [11].

Okamoto-Pointcheval Theorem Let Π=(KG, E, D, G, H) *be REACT hybrid public-key encryption scheme constructed from public-key encryption scheme* Π^a=(KG^a, E^a, D^a) *and symmetric encryption scheme* Π^s=(KG^s, E^s, D^s). If Π^a *is one-way secure against plaintext-checking attacks*, Π^s *is secure in sense of Find-and-Guess, then* Π *is secure against chosen-ciphertext attacks.*

Similar results as theorem 4.1 can be proved for REACT, however, we only present the strongest result in the following which is most useful in practice.

Theorem 5.1 *If* Π^a *is one-way secure and relevantly anonymous, both are against plaintext-checking attacks, then* Π *is anonymous against chosen-ciphertext attacks. Concretely,* $Adv_{\pi}^{ANO\_CCA}(q_g, q_h, q_d, t)$

$$\le Adv_{\pi^a}^{RE\_ANO\_PCA}(q_d, t + O(q_d)) + (q_g+q_h)\, Adv_{\pi^a}^{OWE\_PCA}(t + O(q_g + q_h)q_d)$$

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 plaintext-checking adversary B^A=(B_1,B_2) cracking Π^a's relevant anonymity. Consider the following game:

$Exp_{\pi^a,B}^{RE\_ANO\_PCA}(k)$:

(pk_0, sk_0), (pk_1, sk_1)←KG(k);

(R^0, St)← $B_1^{PCA^a(sk_0,.),PCA^a(sk_1,.)}(pk_0, pk_1)$ where B_1 is implemented as:

Both G-list and H-list are initialized to be empty;
Randomly select R^0 from Π^a's message space;
Randomly select g^0 from Π^s's key space;

```
            $(M^0, St_A) \leftarrow A_1^{G,H,D(sk_0,.),D(sk_1,.)}(pk_0, pk_1)$;
            $St \leftarrow St_A||M^0||R^0||g^0$;
            return($R^0$, St);
    $b \xleftarrow{\$} \{0,1\}$;
    Randomly select R* from $\Pi^a$'s message space; /*the same space as that
        from which $R^0$ is generated. In particular, $|R^0|=|R^*|$.*/
    $y_1^* \leftarrow E^a(pk_b, R^*)$;
    $d \leftarrow B_2^{PCA^a(sk_0,.),PCA^a(sk_1,.)}(y_1^*, St)$ where $B_2$ is implemented as:
            parse St as $St_A||M^0||R^0||g^0$;
            $y_2^* \leftarrow E^s(g^0, M^0)$;
            Randomly select h* from H's image space;
            $d \leftarrow A_2^{G,H,D(sk_0,.),D(sk_1,.)}(y_1^* || y_2^* || h^*, St_A)$;
            return(d);
    if d=b then output 1 else output 0.
```

B carries out simulation as follows.

```
(1)On each query R from A to oracle G(.), B does:
        If there exists (R,g) in G-list
        Then return(g)
        Else randomly select g from $\Pi^s$'s key space;
            Insert (R,g) in G-list;
            Return(g);
```

```
(2)On each query $(R,m, y_1, y_2)$ from A to oracle H(.), B does:
        If there exists $((R,m, y_1, y_2),h)$ in H-list
        Then return(h)
        Else randomly select h from H's image space;
            Insert $((R,m, y_1, y_2),h)$ in H-list;
            Return(h);
```

(3)On query y from A to its oracle $D(sk_j,.)$, j=0,1, B simulates $D(sk_j,y)$ as follows(note that oracle-$D(sk_j,.)$ may access G and H from inside and such accesses are also processed by B in the afore-specified way):

```
        Parse y as $y_1||y_2||h$;
        if there exists (R,K) in G-list s.t. $PCA^a(sk_j,R,y_1)=1$
          /*note that there is at most one such (R,K).*/
        then if there exits $(R,M,y_1,y_2,h)$ in H-list
            then   return(M)
            else   $M \leftarrow D^s(K,y_2)$;
                   insert $(R,M,y_1,y_2,h)$ into H-list
                   return(M);
        else /*For any (R,K) in G-list, it has $PCA^a(sk_j,R,y_1)=0$*/
                return(⊥)
```

Define an event Z as that there exists an item (R*,.) in G-list or item ((R*,.,.,.),.) in H-list. Let p_0 be P[Z]. According to B's specification, we have P[$Exp_{\pi^a,B}^{RE\_ANO\_PCA}(k)=1$|~Z]=P[$Exp_{\pi,A}^{ANO\_CCA}(k)=1$] because in event of ~Z decryption oracle simulated by B on all queries from A is perfect, so

$$P[Exp_{\pi^a,B}^{RE\_ANO\_PCA}(k)=1] \geq P[Exp_{\pi^a,B}^{RE\_ANO\_PCA}(k)=1|\sim Z]P[\sim Z]$$

$$= P[Exp_{\pi,A}^{ANO\_CCA}(k)=1](1-p_0) \geq P[Exp_{\pi,A}^{ANO\_CCA}(k)=1]-p_0$$

hence $Exp_{\pi,A}^{ANO\_CCA}(k) \leq P[Exp_{\pi^a,B}^{RE\_ANO\_PCA}(k)=1]+p_0$.

Furthermore, p_0 can be estimated by constructing two P.P.T. adversaries J_0 and J_1 based-on A to crack Π^a's one-way security under plaintext-checking attack. Consider the game:

```
$Exp_{\pi^a,J0}^{OWE\_PCA}(k)$:
        $(pk_0, sk_0) \leftarrow KG(k)$;
        Randomly select R* from $\Pi^a$'s message space;
        $y_1^* \leftarrow E(pk_0, \sigma^*)$;
        $\sigma^0 \leftarrow J_0^{PCA(sk0,.)}(pk_0, y^{a*})$ where $J_0$ is implemented as:
                cnt←0;
                $(pk_1, sk_1) \leftarrow KG(k)$;
                Randomly select K* from $\Pi^s$'s key space;
                (M, St)← $A_1^{G,H,D(sk_0,.),D(sk_1,.)}(pk_0, pk_1)$;
                $v^* \leftarrow E^s(K^*, M)$;
                d← $A_2^{G,H,D(sk_0,.),D(sk_1,.)}(y_1^* \| v^*, St)$;
                i← $^{\$}$ {1,2,…,cnt};
                /* w.o.l.g., all R's queried by A for G and H are distinct and
                   indexed as $R_1$,…, $R_{cnt}$.*/
                output($R_i$).
```

(1)On each query R or (R, m,y_1,y_2) from A to its oracle G(.) or H(.) respectively, J_0 simulates G or H as B does in the above; Additionally, every query from A is counted by J_0 via increasing cnt by 1 on each query.

(2)On each query y from A to its oracle-D(sk_1,.), J_0 simulates D(sk_1,y) via directly applying Π's decipher algorithm with its complete knowledge of the secret key sk_1(when D(sk_1,.) needs to access G and H from inside, such accesses are also processed by B in the afore-specified way).

(3) On each query y from A to its oracle-D(sk_0,.), J_0 (with its PCA-oracle) simulates D(sk_0,y) in the same way as B does in the above.

Note that $Exp_{\pi^a,J0}^{OWE\_PCA}(k)$ is just $Exp_{\pi\ ,A}^{ANO\_CCA}(k)$ in case of b=0. Denoting the probability of the event occurring in $Exp_{\pi\ ,A}^{ANO\_CCA}(k)$ as P_A[.], we have

$$Adv_{\pi^a,J0}^{OWE\_PCA}(k) = \text{P}[\,Exp_{\pi^a,J0}^{OWE\_PCA}(k) = 1\,] \geq (1/\text{cnt})P_A[Z|b=0] \geq 1/(q_g+g_h)P_A[Z|b=0]$$

On the other hand, we construct another adversary J_1 in a similar way as that of J_0 with the only difference that J_1 calls A_1 in the form of (M, St)← $A_1^{G,H,D(sk_1,.),D(sk_0,.)}(pk_1, pk_0)$, i.e., exchanging pk_0 and pk_1's roles. As a result, $Exp_{\pi^a,J1}^{OWE\_PCA}(k)$ is just $Exp_{\pi\ ,A}^{ANO\_CCA}(k)$ in case of b=1 and we have

$$Adv_{\pi^a,J1}^{OWE\_PCA}(k) = \text{P}[\,Exp_{\pi^a,J1}^{OWE\_PCA}(k) = 1\,] \geq 1/(q_g+g_h)P_A[Z|b=1]$$

So p_0=P[Z]=(1/2)(P_A[Z|b=1]+P_A[Z|b=0])≤(q_g+q_h)($Adv_{\pi^a,J0}^{OWE\_PCA}(k) + Adv_{\pi^a,J1}^{OWE\_PCA}(k)$)/2. In combination with the inequality $Exp_{\pi,A}^{ANO\_CCA}(k)$≤P[$Exp_{\pi^a,B}^{RE\_ANO\_PCA}(k) = 1$]+$p_0$ we got before, we have

$$\text{P}[\,Exp_{\pi,A}^{ANO\_CCA}(k) = 1\,] \leq \text{P}[\,Exp_{\pi^a,B}^{RE\_ANO\_PCA}(k) = 1\,] + 4(q_g+q_h)(\,Adv_{\pi^a,J0}^{OWE\_PCA}(k) + Adv_{\pi^a,J1}^{OWE\_PCA}(k)\,)$$

and the final inequality can be derived directly and the time and query complexity can be directly verified. □

Corollary 5.1 Let Π=(KG, E, D, G, H) *be REACT hybrid public-key encryption scheme constructed from public-key encryption scheme* Π^a=(KG^a, E^a, D^a) *and symmetric encryption scheme* Π^s=(KG^s, E^s, D^s). If Π^a *is one-way secure and relevantly anonymous, both are against plaintext-checking attacks*; Π^s *is secure in sense of Find-and-Guess*, *then* Π *is secure and anonymous , both are against chosen-ciphertext attacks.* □

Example 5.1(PSEC-3's anonymity against chosen-ciphertext attacks) PSEC-3 public-key encryption scheme is provably secure(in random oracle model)against chosen-ciphertext attacks under the assumption of Gap-Diffie-Hellman problem's hardness [13] on elliptic curves and some additional weak security assumptions on its symmetric encryption component. In this scheme(fig.6), just like in PSEC-1/2 it's reasonable to consider the curve E/F_q, p, q and point P as (shared) public parameters and W as the real public-key (each individual has distinct W).

Note that PSEC-3 is actually a REACT scheme constructed from Π^a and (SymEnc,SymDec) where Π^a=(KG^a, E^a, D^a) is defined in fig. 7.
In fact this Π^a is just that asymmetric component encryption scheme in PSEC-2(example 4.1), particularly $Exp_{\pi^a,A}^{RE\_ANO\_PCA}(k)$ =0(implied by $Exp_{\pi^a,A}^{RE\_ANO\_CCA}(k)$=0). In addition, all conditions in Okamoto-Pointcheval theorem are

satisfied by Π^a (as proved in t1he original proposal [9]), in particular Π^a is one-way secure against plaintext-checking attacks. Combining all these facts and our theorem 5.1, we have the following consequence on PSEC-3:

Proposition 5.1 If the component symmetric encryption scheme is Find-and-Guess secure, then PSEC-3 *is both secure and anonymous in random oracle model against chosen-ciphertext attacks under the assumption of Gap-Diffie-Hellman problem's hardness on elliptic curves.* □

```
Key generator KG($E/F_q$,p,q,P):
    $s \leftarrow^{\$} Z_p$;
    $W \leftarrow sP$;
    $pk \leftarrow W$;
    $sk \leftarrow s$;
    return(pk, sk)
```

```
Encryption algorithm E(pk, M),
$M \in \{0,1\}^+$:
    $t \leftarrow^{\$} Z_p$;
    $u \leftarrow^{\$} \{0,1\}^k$;
    $C_1 \leftarrow tP$;
    $Q \leftarrow tW$;
    $C_2 \leftarrow u \oplus x(Q)$;
    $C_3 \leftarrow$ SymEnc(G(u), M);
    $C_4 \leftarrow$ H(u, M, $C_1$,$C_2$, $C_3$);
    return($C_1$,$C_2$, $C_3$, $C_4$)
```

```
Decryption algorithm D(sk,Y):
    Parse Y as ($C_1$,$C_2$, $C_3$, $C_4$)
    $Q \leftarrow sC_1$;
    $u \leftarrow C_2 \oplus x(Q)$;
    $M \leftarrow$ SymDec(G(u), $C_3$);
    if  $C_4$=H(u, M, $C_1$,$C_2$, $C_3$ )
    then  return(M);
    else   return( $\perp$ );
```

Figure 6: PSEC-3 encryption Scheme. E/F_q is the group of an elliptic curve over field F_q. P is a point on E/F_q with (prime) order p. x(Q) is the x-coordinate of curve point Q. (SymEnc, SymDec) is a symmetric encryption scheme. G and H are random oracles.

```
Key generator $KG^a$($E/F_q$,p,q,P):
    $s \leftarrow^{\$} Z_p$;
    $W \leftarrow sP$;
    $pk \leftarrow W$;
    $sk \leftarrow s$;
    return(pk, sk)
```

```
Encryption algorithm $E^a$(pk, R),
$R \in \{0,1\}^+$:
    $t \leftarrow^{\$} Z_p$;
    $Q \leftarrow tW$;
    $C_1 \leftarrow tP$;
    $C_2 \leftarrow R \oplus x(Q)$;
    return($C_1$,$C_2$)
```

```
Decryption algorithm $D^a$(sk,Y):
    Parse Y as ($C_1$,$C_2$)
    $Q \leftarrow sC_1$;
    $R \leftarrow C_2 \oplus x(Q)$;
    return(R);
```

Figure 7: PSEC-3's asymmetric component encryption scheme Π^a

6 Summary

In this paper some general results on anonymity in two well-known hybrid encryption constructions, i.e., Fujisaki-Okamoto and REACT schemes are proved, based-upon new and general concept of relevant anonymity. The main results are quite positive, and as applications well-known NISSIE schemes PSEC-1/2/3's chosen-ciphertext anonymity is proved. Further work naturally along this way is to investigate more other hybrid schemes, e.g, the very efficient GEM proposed recently by Coron et al.. Another interesting work is to investigate anonymity in other strong secure constructions, e.g., the IBE-based chosen-ciphertext secure public-key encryption's construction recently proposed by Canetti-Halevi-Katz and Boneh-Katz. Because of practical usefulness of anonymity, such results will be valuable in cryptographic applications.

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. Abdalla, M. Bellare, P.rogaway. *DHAES: An Encryption Scheme based-on Diffie-Hellman problem*. Submission to IEEE P1363: Asymmetric Encryption, 1998.

[3] 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.

[4] 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.

[5] 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.

[6] R.Cramer and V.Shoup, *A Practical Public-Key Cryptosystem Provably Secure against Adaptive Chosen-ciphertext Attacks*, In:H.Krawczyk ed, Advances in Cryptology – Crypti'98, Lecture Notes in Computer Science Vol.1462, 1998.

[7] T.ElGamal, *A Public-key Cryptosystem and Signature Scheme based-on Discrete Logarithms*, IEEE Transactions on Information, 1985:31(5), 469-472.

[8] 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.

[9] E.Fujisaki, T.Kobatashi, H.Morita et al., *PSEC: Provably Secure Elliptic Encryption Scheme*(Submission to NESSIE), Technical Report, NTT Lab, 1999.

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

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

[12] T.Okamoto and D.Pointcheval, *RSA-REACT: An Alternative to RSA-OAEP*, In: 2nd NESSIE Workshop, 2001, Egham, UK, 2001

[13] T.Okamoto and D.Pointcheval, *The Gap Problems: A New Class of problems for Security of Cryptographic Systems*, Manuscript, 2000.

[14] D.Pointcheval, *Provable Security for Public-Key Schemes*, In: Advanced Courses in Contemporary Cryptology, Berlin:Springer-Verlag, 2005, 123-189.

[15] V.Shoup *Using Hash Functions as a Hedge against Chosen-ciphertext Attack*, in: B.Preneel ed, Advances in Cryptology, Lecture Notes in Computer Science Vol 1807, Berlin:Springer-Verlag, 2000, 275-288.