

# 关于混合加密方案匿名性质的几个一般性结果

田 园 李明楚 陈治宇

(大连理工大学软件学院 辽宁 大连 116600)

**摘 要** 公钥加密方案的匿名性(亦称公钥隐密性)与数据保密性同样都具有重要应用价值. 文中首先建立关于公钥加密方案的两个通用的新概念, 即相对匿名性和相对保密性. 通过这些较弱的安全性概念, 证明了关于公钥加密方案匿名性质的两类一般性结果. 第一类结果建立了公钥加密方案的保密性与匿名性之间两个对偶式的普遍关系, 即相对匿名性(相对保密性)连同保密性(匿名性)蕴涵匿名性(保密性); 第二类结果给出两个典型的混合加密构造(即 Fujisaki-Okamoto 构造和 Okamoto-Pointcheval 构造(REACT))选择密文匿名的充分条件, 这些条件仅包括特定意义上的相对匿名性质和其它一些自然的弱保密性要求. 文中不仅用多个具体实例表明这些条件都是非常实用的判定准则, 而且还进一步应用这些普遍结果, 给出对某些具体公钥加密方案匿名性质的简化证明, 并证明了著名的 NESSIE 方案 PSEC-1/2/3 的选择密文匿名性质.

**关键词** 计算密码学; 匿名性; 可证明的安全性; 混合方案; 公钥隐密性

**中图法分类号** TP309

## Some General Results on Anonymity in Hybrid Encryption Schemes

TIAN Yuan LI Ming-Chu CHEN Zhi-Yu

(Software School of Dalian University of Technology, Dalian, Liaoning 116600)

**Abstract** Anonymity(key-privacy) as well as 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 weak security concepts some general results on anonymity in public-key encryption are proved, which fall in two categories. The first results are two general conjugate relations between anonymity and data-privacy, i. e., relevant anonymity(relevant data-privacy) together with data-privacy(anonymity) imply anonymity(data-privacy); the second are sufficient conditions for chosen-ciphertext anonymity in Fujisaki-Okamoto and Okamoto-Pointcheval(REACT) hybrid constructions respectively, only containing specific relevant anonymity and some naturally weak data-privacy requirements. As examples show, all these conditions are easy-to-check criterion in practice. These general consequences are applied to some specific schemes and, as a result, anonymity of some well-known schemes are re-established but in a simpler way. Furthermore, NESSIE scheme PSEC-1/2/3's chosen-ciphertext anonymity is proved as applications of these general results.

**Keywords** computational cryptography; anonymity; provable security; hybrid-scheme; key-privacy

# 1 引言

匿名性和保密性都是公钥加密方案的重要安全性质,两者都有广泛的应用价值.然而,对匿名性系统而严格的理论处理却较之保密性要晚得多,在这方面文献[1]是开创性的工作,它第一次建立了匿名性的精确的计算密码学概念,并严格证明了 ElGamal 方案、Cramer-Shoup 方案和 RAEP/RSA 方案的匿名性.直观地讲,匿名性(或称公钥隐密性, key-privacy)与保密性(data-privacy)是完全不同的性质,前者保证密文不泄露用来加密的公钥,后者则保证密文不泄露其明文.除了隐藏公钥,匿名性还是一个有用的工具,能用来达到复杂密码方案或协议的特殊功能目标,例如隐形检索方案中对关键字的保密<sup>[2]</sup>、组群加密方案中对接收方身份的保密<sup>①</sup>等.因此,同时具有匿名性和保密性的公钥加密方案有非常重要的应用价值.

混合加密方案(hybrid encryption scheme)复合公钥加密方案 and 对称加密方案,并且常能将仅有弱保密性的方案提升成为具有强保密性的方案(IND\_CCA 保密).较之纯粹的公钥加密方案,复合方案的一个优点是计算效率高.出于这些原因,混合加密方案无论在理论还是实际应用中都有重要作用,特别是作为构造选择密文保密(IND\_CCA)的公钥方案的一个通用方法(常借助于随机 oracle 模型),在这方面已经有较丰富的工作<sup>[3-5]</sup>.尽管如此,关于混合加密方案的匿名性质(甚至一般公钥方案的匿名性)至今研究很少,较之保密性,许多重要问题尚待回答,例如:许多常用的混合方案如 Fujisaki-Okamoto 方案是否也像其保密性那样能将仅有弱匿名性的基本组成方案提升为具有强匿名性的方案?什么样的弱匿名性质能被混合方案提升为最强的匿名性(ANO\_CCA 匿名性)?对这些问题的回答无疑将大大益于丰富混合方案的理论和应用范围.

本文工作将部分回答以上问题,特别是针对两种典型的混合加密方案,即 Fujisaki-Okamoto 方案<sup>[4]</sup>和 Okamoto-Pointcheval(React)方案<sup>[5]</sup>,肯定地回答了以上问题.本文建立关于公钥加密方案的几个通用的新概念,并基于这些概念建立关于混合公钥加密方案的匿名性条件.除普适性的理论结果之外,本文还给出这些概念和结论的具体应用,简化已有证明,并给出关于三个著名的 NESSIE 方案 PSEC-1/2/3<sup>[6]</sup>匿名性的证明.就作者目前所知,

这是关于 PSEC-1/2/3 的新结果.

## 1.1 本文主要贡献

本文结果分属三类.首先,我们建立关于公钥加密方案的两个一般性的新概念:相对匿名性和相对保密性,并通过这两个概念证明关于匿名性和保密性之间两个有趣而且很有用的普遍关系(定理 1 和 2).相对匿名性和相对保密性都严格弱于对应的匿名性和保密性概念,但正如例 1~5 所表明的,它们常常易于检验,从而使定理 1 和 2 能够用来大大简化某些方案的匿名性或保密性证明.

需要指出,Abdalla 等在文献[2]中针对基于身份的公钥加密方案(IBE/HIBE)的情形第一次给出了相对匿名性概念并基于这一概念证明了关于 IBE 方案匿名性的一个充分条件(但仅针对选择明文攻击),本文的定义 4 可以看作是 Abdalla 等人的定义在普通公钥方案上的移植和推广,本文的定理 1 也可以看作文献[2]中引理 4.3 的对应.更进一步,本文还给出相对保密性概念,这一概念及定理 2 可以看作是相对匿名性概念和定理 1 的对偶.相对匿名和相对保密性都是有利的分析工具,特别是相对匿名性,对本文工作是一个重要的工具.

本文第二类结果是关于两种典型的混合加密方案,即 Fujisaki-Okamoto 方案<sup>[4]</sup>和 Okamoto-Pointcheval 方案<sup>[5]</sup>(React)匿名性的充分条件.主要结论是:若基本的公钥方案在特定意义上相对匿名且满足某些其它自然的条件(与保证混合方案保密性的经典条件一致),则混合加密方案必是(抗适应性选择密文攻击)匿名的.结合文献[4-5]的经典结果,我们可以得出 Fujisaki-Okamoto 混合方案和 React 混合方案都具有非常好的性质:只要基本方案满足较弱的条件,混合方案将同时具有保密性和匿名性.

本文第三类结果是以上一般性理论结果的应用,特别是,前述定理分别应用于 NESSIE 方案 PSEC-1/2/3,(在随机 oracle 模型下)证明了这些方案的匿名性(命题 1、命题 3 和命题 5).

## 1.2 各节内容概要

第 2 节简要回顾基本概念;第 3 节建立相对匿名性和相对保密性概念,证明关于匿名性和保密性的两个普遍关系,并应用于 PSEC-1 等实例;第 4 节和第 5 节分别证明关于 Fujisaki-Okamoto 混合方

① Kiayias A, Tsiounis Y, Yung M. Group encryption, Cryptology eArchive 2007/015(eprint. iacr. org/2007/015).

案和 REACT 混合方案匿名性的充分条件,并分别应用于 PSEC-2/3;第 6 节总结全文.

## 2 基本概念与符号

本节回顾某些基本概念并给出符号约定.  $x \parallel y$  表示字  $x$  和  $y$  的联结,  $|x|$  表示字  $x$  的编码长度. 设  $X$  是一个集合, 记号  $a \leftarrow^{\$} X$  表示从  $X$  随机选取一个元素  $a$  ( $a$  在  $X$  上均匀分布). 正整数  $k$  的速降函数是指这样一类函数, 当  $k$  充分大时函数值下降得比任何多项式的倒数都要快. 文中所有算法均以伪 C 语言表达, 并以  $/ \cdots /$  给出算法中的注释. 给定某个特定的值  $a^*$ ,  $(a^*, \cdot)$  表示二元关系表中第一个字段的值等于  $a^*$  的表项 (这里句点 “.” 表示任意的、不加约定的值); 该符号可推广到任何  $n$  元关系表, 例如, 符号  $(a^*, b^*, \cdot, \cdot, \cdot)$  表示 5-元关系表中第一个字段的值等于  $a^*$  且第二个字段的值等于  $b^*$  的表项. 符号  $\perp$  用以表示异常或错误情况下的输出. 概率多项式算法简称为 P.P.T. 算法.

**定义 1** (公钥加密方案). 一个公钥加密方案  $\Pi = (KG, E, D)$  是一组 P.P.T. 算法  $KG, E$  和  $D$ . 设  $k$  是复杂度参数,  $KG$  是钥生成算法, 输出公钥/私钥对  $(pk, sk)$ ;  $E$  是加密算法, 以公钥  $pk$  和明文  $M$  为输入并输出密文  $y$ ;  $D$  是解密算法, 以私钥  $sk$  和密文  $y$  为输入, 输出明文  $M$ . 并且满足一致性关系: 对任意的  $k$  和  $M$  恒有  $P[(pk, sk) \leftarrow KG(k); y \leftarrow E(pk, M); D(sk, y) = M] = 1$ .

**定义 2** (保密性).  $\Pi = (KG, E, D)$  是一个公钥加密方案,  $k$  是复杂度参数.  $A = (A_1, A_2)$  是一个 P.P.T. 算法,  $ATK \in \{CPA, CCA\}$ ,  $Oracle$  是一个由  $ATK$  的值确定的 oracle. 考虑以下对抗实验:

$$\begin{aligned} &Exp_{\pi, A}^{IND\_ATK}(k); \\ &(pk, sk) \leftarrow KG(k); \\ &(M_0, M_1, St) \leftarrow A_1^{Oracle}(pk); \\ &b \leftarrow^{\$} \{0, 1\}; \\ &y^* \leftarrow E(pk, M_b); \\ &d \leftarrow A_2^{Oracle}(y^*, St); \\ &\text{if } d = b \text{ then } output(1) \text{ else } output(0); \end{aligned}$$

对  $ATK = CPA$ ,  $Oracle$  为空; 对  $ATK = CCA$ ,  $Oracle = D(sk, \cdot)$  且  $A$  不允许向其 oracle- $D(sk, \cdot)$  询问  $y^*$ .  $A$  的优势函数  $Adv_{\pi, A}^{IND\_ATK}$  定义为  $|2P[Exp_{\pi, A}^{IND\_ATK}(k) = 1] - 1|$ . 若对任何 P.P.T. 算法  $A$ ,  $Adv_{\pi, A}^{IND\_CPA}(Adv_{\pi, A}^{IND\_CCA})$  是  $k$  的速降函数, 则  $\Pi$  定义为抗适应性选择明文 (密文) 保密, 分别简称为 IND\_CPA 保密和 IND\_CCA

保密. 记  $Adv_{\pi}^{IND\_ATK}(k) \equiv \sup_{A \in \text{P.P.T.}} Adv_{\pi, A}^{IND\_ATK}(k)$ . 若需将这些函数视为计算时间上界  $t$  和 oracle 询问总数上界  $q$  的函数, 则用记号  $Adv_{\pi}^{IND\_ATK}(t, q)$  代替记号  $Adv_{\pi}^{IND\_ATK}(k)$ .

**定义 3** (匿名性).  $\Pi = (KG, E, D)$  是一个公钥加密方案,  $A = (A_1, A_2)$  是 P.P.T. 算法,  $ATK \in \{CPA, CCA\}$ ,  $Oracle$  是一个由  $ATK$  的值确定的 oracle. 考虑以下对抗实验:

$$\begin{aligned} &Exp_{\pi, A}^{ANO\_ATK}(k); \\ &(pk_0, sk_0), (pk_1, sk_1) \leftarrow KG(k); \\ &\quad / \text{ * 独立运行 } KG(k) \text{ 两次 * } / \\ &(M^*, St) \leftarrow A_1^{Oracle}(pk_0, pk_1); \\ &b \leftarrow^{\$} \{0, 1\}; \\ &y^* \leftarrow E(pk_b, M^*); \\ &d \leftarrow A_2^{Oracle}(y^*, St); \\ &\text{if } d = b \text{ then } output(1) \text{ else } output(0). \end{aligned}$$

对  $ATK = CPA$ ,  $Oracle$  为空; 对  $ATK = CCA$ ,  $Oracle = (D(sk_0, \cdot), D(sk_1, \cdot))$  且  $A$  不允许向该 oracle 询问  $y^*$ .  $A$  的优势函数  $Adv_{\pi, A}^{ANO\_ATK}$  定义为  $|2P[Exp_{\pi, A}^{ANO\_ATK}(k) = 1] - 1|$ . 若对任何 P.P.T. 算法  $A$ ,  $Adv_{\pi, A}^{ANO\_CPA}(Adv_{\pi, A}^{ANO\_CCA})$  是  $k$  的速降函数, 则  $\Pi$  定义为抗适应性选择明文 (密文) 匿名, 今后分别简称为 ANO\_CPA 匿名和 ANO\_CCA 匿名. 记  $Adv_{\pi}^{ANO\_ATK}(k) \equiv \sup_{A \in \text{P.P.T.}} Adv_{\pi, A}^{ANO\_ATK}(k)$ . 若需将这些函数视为计算时间上界  $t$  和 oracle 询问总数上界  $q$  的函数, 则用记号  $Adv_{\pi}^{ANO\_ATK}(t, q)$  代替记号  $Adv_{\pi}^{ANO\_ATK}(k)$ .

## 3 匿名性和保密性之间的两个普遍关系

Abdalla 等针对 IBE 的情形引入了所谓相对匿名性概念<sup>[2]</sup>, 并以此建立了一个关于 IBE 加密方案匿名性的充分条件 (针对其具体应用, 他们仅考虑了抗选择明文攻击). 这里我们将这一概念移植到传统的公钥加密方案并证明更一般的结果. 不仅如此, 我们还进一步建立一个对偶的概念——相对保密性, 并以此建立一个关于保密性的充分条件. 正如本节各种例子所显示的, 虽然相对匿名性和相对保密性都严格弱于对应的 (非相对) 匿名性和保密性, 但在具体应用中它们往往很容易判别, 因此这些充分条件实际上都是很实用的判定准则, 特别是在以后各节中作为重要的工具.

### 3.1 相对匿名性及其与保密性的关系

定义 4(相对匿名). 设  $\Pi = (KG, E, D)$  是公钥加密方案,  $A = (A_1, A_2)$  是 P.P.T. 算法,  $ATK \in \{CPA, CCA\}$ ,  $Oracle$  是由  $ATK$  的值决定的 oracle. 考虑以下对抗实验:

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

$(pk_0, sk_0), (pk_1, sk_1) \leftarrow KG(k)$ ;  
 /\* 独立运行  $KG(k)$  两次 \*/  
 $(M^*, St) \leftarrow A_1^{Oracle}(pk_0, pk_1)$ ;  
 $M \leftarrow \$ \{0, 1\}^{|M^*|}$ ; /\* 随机选取与  $M^*$  相同长度的消息  $M^*$  \*/  
 $b \leftarrow \$ \{0, 1\}$ ;  
 $y^* \leftarrow E(pk_b, M)$ ;  
 $d \leftarrow A_2^{Oracle}(y^*, St)$ ;  
 if  $d = b$  then  $output(1)$  else  $output(0)$ ;

对  $ATK = CPA$ ,  $Oracle$  为空; 对  $ATK = CCA$  有  $Oracle = (D(sk_0, \cdot), D(sk_1, \cdot))$ , 但与定义 3 的(非相对)匿名性概念不同, 这里允许  $A$  向其 oracle- $(D(sk_0, \cdot), D(sk_1, \cdot))$  询问  $y^*$ .  $A$  的优势函数  $Adv_{\pi, A}^{RE\_ANO\_ATK}$  定义为  $|2P[Exp_{\pi, A}^{RE\_ANO\_ATK}(k) = 1] - 1|$  或等价的表达式  $|P[d = 0 | b = 0] - P[d = 0 | b = 1]|$ . 若对任何 P.P.T. 算法  $A$ ,  $Adv_{\pi, A}^{RE\_ANO\_CPA}(Adv_{\pi, A}^{RE\_ANO\_CCA})$  是  $k$  的速降函数, 则  $\Pi$  定义为抗适应性选择明文(密文)相对匿名, 今后分别简称为 RE\_ANO\_CPA 匿名和 RE\_ANO\_CCA 匿名. 记  $Adv_{\pi}^{RE\_ANO\_ATK}(k) \equiv \sup_{A \in P.P.T.} Adv_{\pi, A}^{RE\_ANO\_ATK}(k)$ . 若需要将这些函数视为计算时间上界  $t$  和对其 oracle 询问的总数上界  $q$  的函数, 则用记号  $Adv_{\pi}^{RE\_ANO\_ATK}(t, q)$  代替记号  $Adv_{\pi}^{RE\_ANO\_ATK}(k)$ .

不难验证匿名性蕴涵相对匿名性. 另一方面, 以下定理表明相对匿名性与保密性相结合蕴涵匿名性, 从而能够借助于已经证明的保密性结果和方案的相对匿名性(这一点常容易判定), 推出方案的匿名性. 定理 1 是对这一事实的精确陈述, 后续的例子给出其具体应用.

定理 1.  $\Pi = (KG, E, D)$  是 IND\_CPA(IND\_CCA) 保密的公钥加密方案. 若  $\Pi$  也是 RE\_ANO\_CPA(RE\_ANO\_CCA) 匿名的, 则  $\Pi$  必 ANO\_CPA(ANO\_CCA) 匿名. 具体有不等式

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

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

其中  $T_d$  是解密算法  $D$  的计算时间.

证明. 这里仅给出对 CCA 情形的证明, CPA

情形的证明本质相同但更简单, 不再赘述. 设  $A = (A_1, A_2)$  是破译  $\Pi$  的 ANO\_CCA 匿名性的 P.P.T. 算法, 以下基于  $A$  构造一个 P.P.T. 算法  $B^A = (B_1, B_2)$  来破译  $\Pi$  的 IND\_CCA 保密性. 考虑以下对抗实验及算法  $B$  的实现:

$Exp_{\pi, B}^{IND\_CCA}(k)$ :

$(pk_0, sk_0) \leftarrow KG(k)$ ;  
 $(M_0, M_1, St) \leftarrow B_1^{D(sk_0, \cdot)}(pk_0)$ , 其中  $B_1$  实现如下:  
 $(pk_1, sk_1) \leftarrow KG(k)$ ;  
 $(M^*, St_A) \leftarrow A_1^{D(sk_0, \cdot), D(sk_1, \cdot)}(pk_0, pk_1)$ ;  
 $M_0 \leftarrow M^*$ ;  $M_1 \leftarrow \$ \{0, 1\}^{|M^*|}$ ;  
 $St \leftarrow St_A \parallel pk_1 \parallel sk_1$ ;  
 return  $(M_0, M_1, St)$ ;  
 $b \leftarrow \$ \{0, 1\}$ ;  
 $y^* \leftarrow E(pk_b, M_b)$ ;  
 $d \leftarrow B_2^{D(sk_0, \cdot)}(y^*, St)$ , 其中  $B_2$  实现如下:  
 parse  $St$  as  $St_A \parallel pk_1 \parallel sk_1$ ;  
 $d \leftarrow A_2^{D(sk_0, \cdot), D(sk_1, \cdot)}(y^*, St_A)$ ;  
 return  $(d)$ ;  
 if  $d = b$  then  $output(1)$  else  $output(0)$ .

$B$  以其自身的 oracle- $D(sk_0, \cdot)$  仿真  $A$  的 oracle- $D(sk_0, \cdot)$ ; 又由于  $B$  已知  $sk_1$ , 故  $B$  能完全实现对  $A$  的 oracle- $D(sk_1, \cdot)$  的仿真. 显然这两种仿真都是完美的(perfect).

根据以上构造, 不难直接验证  $b = 0$  情形的  $Exp_{\pi, B}^{IND\_CCA}(k)$  恰等价于  $b = 0$  情形的  $Exp_{\pi, A}^{ANO\_CCA}(k)$ , 而  $b = 1$  情形的  $Exp_{\pi, B}^{IND\_CCA}(k)$  恰等价于  $b = 0$  情形的  $Exp_{\pi, A}^{RE\_ANO\_CCA}(k)$ . 另一方面, 可以构造  $\Pi$  的另一个 IND\_CCA 破译算法  $C^A = (C_1, C_2)$ ,  $C$  与  $B$  的唯一差别是  $C_1^{D(sk_0, \cdot)}(pk_0)$  以  $A_1^{D(sk_0, \cdot), D(sk_1, \cdot)}(pk_1, pk_0)$  的形式调用  $A_1$ , 即对换  $pk_0$  和  $pk_1$  的角色, 从而  $b = 0$  情形的  $Exp_{\pi, C}^{IND\_CCA}(k)$  恰等价于  $b = 1$  情形的  $Exp_{\pi, A}^{ANO\_CCA}(k)$ , 而  $b = 1$  情形的  $Exp_{\pi, C}^{IND\_CCA}(k)$  恰等价于  $b = 1$  情形的  $Exp_{\pi, A}^{RE\_ANO\_CCA}(k)$ . 因此,

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

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

且

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

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

两式相加得

$$\begin{aligned} Adv_{\pi,B}^{IND\_CCA}(k) + Adv_{\pi,C}^{IND\_CCA}(k) \geq \\ |P[Exp_{\pi,A}^{ANO\_CCA}(k) = 1 | b=0] - \\ P[Exp_{\pi,A}^{RE\_ANO\_CCA}(k) = 1 | b=0]| + \\ |P[Exp_{\pi,A}^{ANO\_CCA}(k) = 1 | b=1] - \\ P[Exp_{\pi,A}^{RE\_ANO\_CCA}(k) = 1 | b=1]| \geq \\ Adv_{\pi,A}^{ANO\_CCA}(k) - Adv_{\pi,A}^{RE\_ANO\_CCA}(k), \end{aligned}$$

即

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

从这一不等式立即导出待证的不等式;从算法  $B, C$  的构造不难直接验证相应的计算复杂度. 证毕.

定理 1 是一个有力的工具,能用来大大简化某些公钥加密方案的匿名性证明. 以下给出一些具体的实例.

**例 1**(ElGamal 方案的 ANO\_CPA 匿名性). 在判定性 Diffie-Hellman 问题的难解性假设下已经证明 ElGamal 方案是 IND\_CPA 保密的<sup>[8,11]</sup>. 进一步分析 ElGamal 方案(图 1),注意到在相对匿名对抗实验  $Exp_{\pi,A}^{RE\_ANO\_CPA}(k)$  中攻击算法  $A_2$  接受挑战密文(challenge-ciphertext)  $y^* = (Y, W)$ , 其中  $W = TM, M$  是随机选择的群元素(但  $M$  的编码长度等于  $A_1(pk_0, pk_1)$  输出消息  $M^*$  的编码长度),在  $b=0$  和  $b=1$  两种情形下,  $y^*$  对  $A_2$  有完全相同的概率分布( $Y$  的值均为  $g^r, W$  的值分别为  $X_0^r M$  和  $X_1^r M$ ), 从而  $Adv_{\pi,A}^{RE\_ANO\_CPA}(k) = 0$ , 即 ElGamal 方案无条件 RE\_ANO\_CPA 匿名. 根据其 IND\_CPA 保密性结论和以上分析,应用定理 1 立得 ElGamal 方案在判定性 Diffie-Hellman 问题难解性假设下 ANO\_CPA 匿名,这正是文献[1]用直接方法证明的结论.

钥生成算法 $KG(q, g)$ : $x \leftarrow \mathbb{Z}_q$ ; $X \leftarrow g^x$ ; $pk \leftarrow (q, g, X)$ ; $sk \leftarrow (q, g, x)$ ; return $(pk, sk)$ ;	加密算法 $E(pk, M), M \in G$ : $r \leftarrow \mathbb{Z}_q$ ; $Y \leftarrow g^r$ ; $T \leftarrow X^r$ ; $W \leftarrow TM$ ; return $(Y, W)$ ;	解密算法 $D(sk, (Y, W))$ : $T \leftarrow Y^x$ ; $M \leftarrow WT^{-1}$ ; return $(M)$ ;
--	---	--

图 1 ElGamal 方案(其中  $G$  是素阶( $q$  阶)群,生成子为  $g$ )

一个更进一步的结论是 ElGamal 方案并非 ANO\_CCA 匿名,这一点将在下一小节证明定理 2 后予以解释.

**例 2**(Cramer-Shoup 方案 ANO\_CCA 匿名). 在判定性 Diffie-Hellman 问题的难解性假设下已经证明 Cramer-Shoup 方案是 IND\_CCA 保密的<sup>[9]</sup>. 文献[1]直接证明了该方案的 ANO\_CCA 匿名性. 这里我们应用与例 1 类似的方法对此给出一个高度简化的证明.

在具体分析之前我们先说明一个区分. 对 Cramer-Shoup 方案(图 2),实际上我们仅将  $(c, d, h)$  视为公钥而不包括  $K, g_1$  和  $g_2$ . 这是因为  $K, g_1$  和  $g_2$

实际上是公共参数,被应用此方案的系统中的所有用户所共享,而每个用户单独持有的、各不相同的变量实质上只是  $c, d$  和  $h$ . 因此 Cramer-Shoup 方案的匿名性并不涉及  $K, g_1$  和  $g_2$ ,将其视为全局性的共享参数是合理的(事实上,在文献[1]对其匿名性的直接证明中也隐含了这一点,这从其证明中对判定性 Diffie-Hellman 问题的变形构造中可以看出来). 区分真正的公钥和共享参数对保密性证明无关紧要,但对匿名性的分析却是必要的. 在以下分析具体例子时我们都将明确区分开真正的公钥和共享参数,但在证明一般性结论时为避免行文繁琐往往不在符号上特别区分.

钥生成算法 $KG(q, g_1, g_2, K)$ : $g_1 \leftarrow g$ ; $x_1, x_2, y_1, y_2, z \leftarrow \mathbb{Z}_q$ ; $c \leftarrow g_1^{x_1} g_2^{x_2}$ ; $d \leftarrow g_1^{y_1} g_2^{y_2}$ ; $h \leftarrow g_1^z$ ; $pk \leftarrow (c, d, h)$ ; $sk \leftarrow (x_1, x_2, y_1, y_2, z)$ ; return $(pk, sk)$ ;	加密算法 $E(pk, M), M \in G$ : $r \leftarrow \mathbb{Z}_q$ ; $u_1 \leftarrow g_1^r$ ; $u_2 \leftarrow g_2^r$ ; $e \leftarrow Mh^r$ ; $T \leftarrow H_K(u_1, u_2, e)$ ; $v \leftarrow c^r d^{rT}$ ; return $(u_1, u_2, e, v)$ ;	解密算法 $D(sk, Y)$ : parse $Y$ as $(u_1, u_2, e, v)$ $T \leftarrow H_K(u_1, u_2, e)$ ; if $v = u_1^{x_1 + Ty_1} u_2^{x_2 + Ty_2}$ ; then $M \leftarrow e/u_1^z$ ; else $M \leftarrow \perp$ ; return $(M)$ ;
---	--	---

图 2 Crammer-Shoup 方案(其中  $G$  是素阶( $q$  阶)群,生成子为  $g$ )

对 Cramer-Shoup 方案,注意到在  $Exp_{\pi,A}^{RE\_ANO\_CCA}(k)$  中  $A_2$  被给予的挑战密文  $y^* = (u_1, u_2, e, v)$  (其中  $e =$

$h^r M, M$  随机生成,特别是  $M$  与  $A_1$  输出的消息  $M^*$  独立,唯一约束是两者编码长度相同),即使  $A_2$  就  $y^*$

向其  $\text{oracle}-(D(sk_0, \cdot), D(sk_1, \cdot))$  询问并获取响应 (参见定义 4), 在  $b=0$  和  $b=1$  两种情形下,  $A_2$  所获取的全部信息 (包括输入信息和 oracle 响应) 有完全相同的概率分布, 从而无条件成立  $\text{Adv}_{\text{CS}, A}^{\text{RE\_ANO\_CCA}}(k) = 0$ . 应用定理 1 立得在判定性 Diffie-Hellman 问题难解性假设下 Cramer-Shoup 方案 ANO\_CCA 匿名.

除简化已有的证明之外, 定理 1 也能用来导出关于匿名性的新结果. 例 3 应用定理 1 证明著名的 NESSIE 方案的匿名性质. 这是关于 NESSIE 方案

的新结果, 三个 NESSIE 公钥方案 PSEC-1/2/3 的保密性证明见文献[7].

**例 3** (PSEC-1 公钥加密方案 ANO\_CCA 匿名). 在椭圆曲线上的判定性 Diffie-Hellman 问题难解性假设和随机 oracle 模型之下, PSEC-1 方案 (图 3) IND\_CCA 保密. 对 PSEC-1, 将曲线  $E/F_q$ 、素数  $p$  和  $q$ 、曲线上的基点  $P$  以及随机函数  $H$  视为共享参数, 而将  $W$  视为公钥.

钥生成算法 $KG(E/F_q, p, q, P)$ : $s \leftarrow \mathbb{Z}_p$ ; $W \leftarrow sP$ ; $pk \leftarrow W$ ; $sk \leftarrow s$ ; return $(pk, sk)$ ;	加密算法 $E(pk, M), M \in \{0, 1\}^k$ : $r \leftarrow \$ \mathbb{Z}_p$ ; $t \leftarrow H(M \parallel r)$ ; /* $r$ 这时用作字符串 */ $Q \leftarrow tW$ ; $C_1 \leftarrow tP$ ; $C_2 \leftarrow (M \parallel r) \oplus x(Q)$ ; return $(C_1, C_2)$ ;	解密算法 $D(sk, Y)$ : parse $Y$ as $(C_1, C_2)$ $Q \leftarrow sC_1$ ; $u \leftarrow C_2 \oplus x(Q)$ ; parse $u$ as $M \parallel r$ ; if $C_1 = H(u)P$ then return $(M)$ ; else return $(\perp)$ ;
---	---	---

图 3 PSEC-1 加密方案 ( $E/F_q$  是椭圆曲线上的点群,  $F_q$  是有限域,  $P$  是  $E/F_q$  上的  $p$  阶点; 对  $E/F_q$  上的点  $Q$ ,  $x(Q)$  表示  $Q$  的  $x$ -坐标.  $H$  是随机 oracle)

在  $\text{Exp}_{\text{PSEC-1}, A}^{\text{RE\_ANO\_CCA}}(k)$  中,  $A_2$  被给予的挑战密文  $y^*$  在  $b=0$  和  $b=1$  两种情形下分别为  $(tP, R \oplus x(tW_0))$  和  $(tP, R \oplus x(tW_1))$ , 其中  $R = M \parallel r$  且  $M$  与  $A_1$  生成的消息  $M^*$  独立 (唯一约束是两者编码长度相同). 即使  $A_2$  就  $y^*$  向其  $\text{oracle}-(D(sk_0, \cdot), D(sk_1, \cdot))$  询问并获取响应 (参见定义 4), 注意到对任何  $b \in \{0, 1\}$  有  $(tP, R \oplus x(tW_b)) = (tP, R' \oplus x(tW_{1-b}))$ , 其中  $R' = R \oplus x(tW_0) \oplus x(tW_1)$  和  $R$  有相同的概率分布 (对  $A_2$  而言), 从而  $A_2$  所获取的全部信息 (包括输入信息和 oracle 响应) 在  $b=0$  和  $b=1$  两种情形下有着完全相同的概率分布, 这导致  $\text{Adv}_{\text{PSEC-1}, A}^{\text{RE\_ANO\_CCA}}(k) = 0$  无条件成立. 应用文献[8]已经证明的保密性结论和定理 1, 立得在椭圆曲线上的判定性 Diffie-Hellman 问题难解性假设下 PSEC-1 方案 ANO\_CCA 匿名. 总结以上分析, 我们可以给出关于 PSEC-1 的较之文献[7]更强的结论.

**命题 1.** 假设椭圆曲线上的判定性 Diffie-Hellman 问题难解,  $H$  是随机 oracle, 则 PSEC-1 既是 IND\_CCA 保密的, 也是 ANO\_CCA 匿名的.

### 3.2 相对保密性及其与匿名性的关系

这一节建立相对匿名性的对偶概念: 相对保密性. 与相对匿名性一样, 相对保密性虽然是一个较弱的保密性概念, 但对许多具体方案很容易验证. 基于下面的定理 2, 这一概念能够成为证明保密性质的一个非常有用的工具.

**定义 5** (相对保密). 设  $\Pi = (KG, E, D)$  是公

钥加密方案,  $A = (A_1, A_2)$  是 P.P.T. 算法,  $\text{ATK} \in \{\text{CPA}, \text{CCA}\}$ ,  $\text{Oracle}$  是依  $\text{ATK}$  而定的 oracle. 考虑以下对抗实验 (注意: 为强调实验中的两对密钥  $(pk^*, sk^*)$  和  $(pk, sk)$  的生成是基于相同的共享参数, 凡需要共享参数的地方都以符号  $sp$  显式地予以表达. 除定理 2 的证明之外, 今后只要不影响理解, 将不再使用这种繁琐的记号):

$\text{Exp}_{\pi, A}^{\text{RE\_IND\_ATK}}(k)$ :

$(pk^*, sk^*) \leftarrow KG(sp, k)$ ;

/\*  $sp$  是共享参数, 参见例 2 中的解释 \*/

$(M_0^*, M_1^*, St) \leftarrow A_1^{\text{Oracle}}(sp, pk^*)$ ;

$(pk, sk) \leftarrow KG(sp, k)$ ;

/\* 基于同一共享参数  $sp$  随机生成另一对公钥/私钥  $(pk, sk)$  \*/

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

$y^* \leftarrow E(sp, pk, M_b^*)$ ;

$d \leftarrow A_2^{\text{Oracle}}(y^*, St)$ ;

if  $d=b$  then output(1) else output(0);

对  $\text{ATK} = \text{CPA}$ ,  $\text{Oracle}$  为空; 对  $\text{ATK} = \text{CCA}$  有  $\text{Oracle} = D(sk^*, \cdot)$  并且与定义 4 (相对匿名性) 类似, 允许  $A$  向其  $\text{oracle} = D(sk^*, \cdot)$  询问  $y^*$ .  $A$  的优势函数  $\text{Adv}_{\pi, A}^{\text{RE\_IND\_ATK}}$  定义为  $|2P[\text{Exp}_{\pi, A}^{\text{RE\_IND\_ATK}}(k) = 1] - 1|$  或等价的表达式  $|P[d=0|b=0] - P[d=0|b=1]|$ . 若对任何 P.P.T. 算法  $A$ ,  $\text{Adv}_{\pi, A}^{\text{RE\_IND\_CPA}}(\text{Adv}_{\pi, A}^{\text{RE\_IND\_CCA}})$  是  $k$  的速降函数, 则  $\Pi$  定义为抗适应性选择明文 (密文) 相对保密, 今后分别简称为 RE\_IND\_CPA

保密和 RE\_IND\_CCA 保密. 记  $Adv_{\pi}^{\text{RE\_IND\_ATK}}(k) \equiv \sup_{A \in \text{P.P.T.}} Adv_{\pi,A}^{\text{RE\_IND\_ATK}}(k)$ . 若需要将这些函数视为计算时间上界  $t$  和对其 oracle 询问的总数上界  $q$  的函数, 则用记号  $Adv_{\pi}^{\text{RE\_IND\_ATK}}(t, q)$  代替记号  $Adv_{\pi}^{\text{RE\_IND\_ATK}}(k)$ . 相对保密性概念的工具作用体现为以下定理.

**定理 2.**  $\Pi = (KG, E, D)$  是 ANO\_CPA(ANO\_CCA) 匿名的公钥加密方案. 若  $\Pi$  也是 RE\_IND\_CPA(RE\_IND\_CCA) 保密的, 则  $\Pi$  必 IND\_CPA(IND\_CCA) 保密. 具体地, 有以下不等式:

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

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

其中  $T_d$  是解密算法  $D$  的计算时间.

证明. 这里仅给出抗选择密文攻击情形的证明, 抗选择明文攻击情形的证明本质相同但更简单, 不再赘述. 设  $A = (A_1, A_2)$  是破译  $\Pi$  的 IND\_CCA 保密性的 P.P.T. 算法, 以下基于  $A$  构造一个 P.P.T. 算法  $B^A = (B_1, B_2)$  来破译  $\Pi$  的 ANO\_CCA 匿名性. 考虑以下对抗实验及算法  $B$  的实现:

$Exp_{\pi,B}^{\text{ANO\_CCA}}(k):$   
 $(pk_0, sk_0), (pk_1, sk_1) \leftarrow KG(sp, k);$   
 $\quad \quad \quad / * sp \text{ 是共享参数 } */$   
 $(M^*, St) \leftarrow B_1^{D(sk_0, \cdot), D(sk_1, \cdot)}(pk_0, pk_1),$  其中  $B_1$  实现如下:  
 $(M_0^*, M_1^*, St) \leftarrow A_1^{D(sk_0, \cdot)}(sp, pk_0);$   
 $M^* \leftarrow M_0^*;$   
 $\text{return}(M^*, St);$   
 $b \leftarrow \$\{0, 1\};$   
 $y^* \leftarrow E(sp, pk_b, M^*);$   
 $d \leftarrow B_2^{D(sk_0, \cdot), D(sk_1, \cdot)}(y^*, St),$  其中  $B_2$  实现如下:  
 $d \leftarrow A_2^{D(sk_0, \cdot)}(y^*, St);$   
 $\text{return}(d);$   
 $\text{if } d=b \text{ then } output(1) \text{ else } output(0);$

$B$  以自身的 oracle- $D(sk_0, \cdot)$  仿真  $A$  的 oracle- $D(sk_0, \cdot)$ , 显然该仿真是完美的.

由以上构造不难看出  $b=0$  情形的  $Exp_{\pi,B}^{\text{ANO\_CCA}}(k)$  恰是  $b=0$  情形的  $Exp_{\pi,A}^{\text{IND\_CCA}}(k)$ ,  $b=1$  情形的  $Exp_{\pi,B}^{\text{ANO\_CCA}}(k)$  恰是  $b=0$  情形的  $Exp_{\pi,A}^{\text{RE\_IND\_CCA}}(k)$ . 另一方面, 还可以构造另一个破译  $\Pi$  的 ANO\_CCA 匿名性的 P.P.T. 算法  $C^A = (C_1, C_2)$ ,  $C$  与  $B$  的差别仅在于:  $C_1^{D(sk_0, \cdot), D(sk_1, \cdot)}(pk_0, pk_1)$  以形式  $A_1^{D(sk_1, \cdot)}(sp, pk_1)$  调用  $A_1$ , 置消息  $M^*$  为  $M_1^*$  且相应地以其 oracle- $D(sk_1, \cdot)$  仿真  $A$  的 oracle- $D(sk_1, \cdot)$ . 于是  $b=0$  情形

的  $Exp_{\pi,C}^{\text{ANO\_CCA}}(k)$  恰是  $b=1$  情形的  $Exp_{\pi,A}^{\text{RE\_IND\_CCA}}(k)$ , 而  $b=1$  情形的  $Exp_{\pi,C}^{\text{ANO\_CCA}}(k)$  恰是  $b=1$  情形的  $Exp_{\pi,A}^{\text{IND\_CCA}}(k)$ , 因此,

$$\begin{aligned} Adv_{\pi,B}^{\text{ANO\_CCA}}(k) &= |P[Exp_{\pi,B}^{\text{ANO\_CCA}}(k)=1|b=0] - \\ &\quad P[Exp_{\pi,B}^{\text{ANO\_CCA}}(k)=1|b=1]| \\ &= |P[Exp_{\pi,A}^{\text{IND\_CCA}}(k)=1|b=0] - \\ &\quad P[Exp_{\pi,A}^{\text{RE\_IND\_CCA}}(k)=1|b=0]| \end{aligned}$$

且

$$\begin{aligned} Adv_{\pi,C}^{\text{ANO\_CCA}}(k) &= |P[Exp_{\pi,C}^{\text{ANO\_CCA}}(k)=1|b=0] - \\ &\quad P[Exp_{\pi,C}^{\text{ANO\_CCA}}(k)=1|b=1]| \\ &= |P[Exp_{\pi,A}^{\text{RE\_IND\_CCA}}(k)=1|b=1] - \\ &\quad P[Exp_{\pi,A}^{\text{IND\_CCA}}(k)=1|b=1]|. \end{aligned}$$

两式相加得

$$\begin{aligned} Adv_{\pi,B}^{\text{ANO\_CCA}}(k) + Adv_{\pi,C}^{\text{ANO\_CCA}}(k) &\geq \\ &|P[Exp_{\pi,A}^{\text{IND\_CCA}}(k)=1|b=0] - \\ &P[Exp_{\pi,A}^{\text{RE\_IND\_CCA}}(k)=1|b=0]| + \\ &|P[Exp_{\pi,A}^{\text{RE\_IND\_CCA}}(k)=1|b=1] - \\ &P[Exp_{\pi,A}^{\text{IND\_CCA}}(k)=1|b=1]| \geq \\ &Adv_{\pi,A}^{\text{IND\_CCA}}(k) - Adv_{\pi,A}^{\text{RE\_IND\_CCA}}(k), \end{aligned}$$

即

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

从这一不等式立即导出待证的不等式且从算法  $B, C$  的构造不难直接验证相应的计算复杂度.

证毕.

下面的例子表明如何借助于定理 2 简化保密性证明或得出新的结果.

**例 4(例 1 续)**<sup>[1]</sup>. 已经证明 ElGamal 方案是 ANO\_CPA 匿名的(例 1 给出另一种证明), 但该方案并非 ANO\_CCA 匿名. 事实上, 运用与例 2 完全类似的分析(Cramer-Shoup 方案的密文结构实际上包含 ElGamal 密文)可以得出对任何  $A$  无条件地有  $Adv_{\pi, A}^{\text{RE\_IND\_CCA}}(k) = 0$ ; 假若 ElGamal 方案 ANO\_CCA 匿名, 则由定理 2 立得该方案是 IND\_CCA 保密的. 但实际上该方案密文可塑(malleable), 因此结论显然不真, 从而该方案并非 ANO\_CCA 匿名. 最后注意到通过与例 2 类似的分析还可以得出  $Adv_{\pi, A}^{\text{RE\_ANO\_CCA}}(k) = 0$  无条件成立, 这说明相对匿名性严格弱于匿名性.

**例 5(例 2 续).** 对 Cramer-Shoup 方案不难验证: 对任何算法  $A$  都有  $Adv_{\pi, A}^{\text{RE\_IND\_CCA}}(k) = 0$ . 由于文献[1]已经证明该方案的 ANO\_CCA 匿名性, 故由定理 2 立得其 IND\_CCA 保密. 如此, 我们从匿名性

的证明导出了保密性证明,并且不难从定理 2 的不等式及文献[1]验证这种方法与原始保密性证明文献[9]中所得出的保密强度及计算复杂度的估计相同.同样的论证对 PSEC-1 方案也适用.

以上例子表明,对某些特殊方案,相对匿名和相对保密性概念可以用来大大简化保密性或匿名性的证明.不仅如此,相对匿名性这一较弱的条件也能够导致某些混合加密方案的(强)匿名性,下两节将考察典型混合加密方案的匿名性质.

## 4 Fujisaki-Okamoto 混合加密方案的匿名性质

混合加密方案较之纯粹的公钥方案具有通用(消息长度不限)和计算高效的特点,是构造具有选择密文保密性公钥方案的一个有效方法<sup>[3-7,11]</sup>.然而,目前虽然对各类混合构造方法的保密性已经有很好的理解,但对其匿名性则研究很少.本节就广泛应用的高效混合方案之一,即 Fujisaki-Okamoto 方案建立匿名条件并给出证明.

### 4.1 Fujisaki-Okamoto 混合加密方案

Fujisaki-Okamoto 混合加密方案<sup>[4]</sup>  $\Pi = (KG, E, D, G, H)$  由一个公钥加密方案  $\Pi^a = (KG^a, E^a, D^a)$  和一个对称加密方案  $\Pi^s = (KG^s, E^s, D^s)$  复合而成,其中  $G$  和  $H$  是随机 oracle;  $KG = KG^a$ , 即  $\Pi$  的公钥和私钥分别是  $\Pi^a$  的公钥和私钥;加密算法  $E(pk, M) = E^a(pk, \sigma; H(\sigma \parallel M)) \parallel E^s(G(\sigma), M)$ , 其中  $\sigma$  从  $\Pi^a$  的明文空间中随机生成,  $H(\sigma \parallel M)$  用作随机算法  $E^a$  中的随机数;解密算法  $D(sk, y)$  定义如下:

parse  $y$  as  $y_1 \parallel y_2$ ;

$\sigma \leftarrow D^a(sk, y_1)$ ;

$M \leftarrow D^s(G(\sigma), y_2)$ ;

if  $y_1 = E^a(pk, \sigma; H(\sigma \parallel M))$  then  $output(M)$   
else  $output(\perp)$ ;

为下文需要,首先回顾几个基本概念<sup>[4-5,11]</sup>.明文验证 (plaintext-checking)-oracle  $PCA_{sk}(\cdot)$  是这样的一个 oracle:对输入  $(M, y)$ ,  $PCA_{sk}(M, y)$  输出为 1 当且仅当  $M = D(sk, y)$ , 否则输出为 0. 对  $ATK \in \{CPA, PCA, CCA\}$ , Oracle 是由  $ATK$  确定的 oracle:对  $ATK = CPA$ , Oracle 为空;对  $ATK = PCA$ , Oracle 为  $PCA_{sk}(\cdot)$ ;对  $ATK = CCA$ , Oracle 为  $D_{sk}(\cdot)$ . 考虑以下对抗实验:

$Exp_{\Pi^a, J}^{OWE\_ATK}(k)$ :

$(pk, sk) \leftarrow KG(k)$ ;

$\sigma^* \leftarrow \$_{\Pi^a}$  的明文空间;

$y^* \leftarrow E(pk, \sigma^*)$ ;

$\sigma^0 \leftarrow J^{Oracle}(pk, y^*)$ ;

if  $\sigma^0 = \sigma^*$  then  $output(1)$  else  $output(0)$ ;

对  $ATK = CCA$  的情形,  $J$  不允许向其 oracle- $D_{sk}(\cdot)$  询问  $y^*$  (但对情形  $ATK = PCA$ ,  $A$  允许向其 oracle- $PCA_{sk}(\cdot)$  询问  $y^*$ ). 公钥方案  $\Pi^a$  分别定义为抗选择明文单向、抗选择明文验证单向和抗选择密文单向 (one-way secure against chosen-plaintext attacks, chosen plaintext-checking attacks, chosen-ciphertext attacks), 若对任何 P.P.T. 算法  $J$  相应对抗实验输出为 1 的概率是复杂度参数  $k$  的速降函数. 相应的概率记做  $Adv_{\Pi, J}^{OWE\_ATK}(k)$  且  $Adv_{\Pi}^{OWE\_ATK}(k) \equiv \sup_{J \in \text{P.P.T.}} Adv_{\Pi, J}^{OWE\_ATK}(k)$ , 以后分别简称其为 OWE\_CPA 单向、OWE\_PCA 单向和 OWE\_CCA 单向. 本节仅用到 OWE\_CPA 单向性, 下节将应用其他单向性质.

关于 Fujisaki-Okamoto 混合方案的保密性有以下定理成立 (其表述中所涉及的  $\gamma$ -一致性和 Find-and-Guess 保密性与我们的工作无关, 因此略去其详细解释).

**Fujisaki-Okamoto 定理<sup>[4]</sup>.** 设  $\Pi = (KG, E, D, G, H)$  是由公钥加密方案  $\Pi^a$  和对称加密方案  $\Pi^s$  复合而成的 Fujisaki-Okamoto 方案. 若  $\Pi^a$  OWE\_CPA 单向且  $\gamma$ -一致,  $\gamma$  是  $k$  的速降函数,  $\Pi^s$  Find-and-Guess 保密, 则  $\Pi$  必 IND\_CCA 保密.

这表明 Fujisaki-Okamoto 方法可以将只具备很弱保密性的公钥方案  $\Pi^a$  和对称方案  $\Pi^s$  增强为具有最强保密性的加密方案. 一个自然的问题是, Fujisaki-Okamoto 方法是否也能增强公钥方案  $\Pi^a$  的匿名性质? 结果是肯定的, 下一小节将给出精确的表述和证明.

### 4.2 ANO\_CCA 匿名性的一个充分条件

本节主要结论是以下定理.

**定理 3.**  $\Pi^a$  是 OWE\_CPA 单向且 RE\_ANO\_CCA 匿名的公钥加密方案,  $\Pi^s$  是对称加密方案,  $\Pi$  是基于  $\Pi^a$  和  $\Pi^s$  的 Fujisaki-Okamoto 混合方案, 则  $\Pi$  必 ANO\_CCA 匿名. 具体有以下不等式:

$$Adv_{\Pi}^{ANO\_CCA}(q_g, q_h, q_d, t) \leq Adv_{\Pi^a}^{RE\_ANO\_CCA}(q_d, t + O(q_d)) +$$

$$(q_g + q_h) Adv_{\Pi^a}^{OWE\_CPA}(t + O(q_g + q_h)q_d),$$

其中,  $q_d, q_g, q_h$  分别是攻击算法对解密 oracle、oracle-G 和 oracle-H 询问次数的上界.

在证明定理之前先对这一结论做几点解释.



虽然  $\Pi$  是混合方案,但在以上定理中仅涉及公钥方案  $\Pi^a$  的性质,并不涉及对称加密方案  $\Pi^s$ ;在对  $\Pi^a$  所要求的两个性质(充分条件)中,RE\_ANO\_CCA 匿名实际是一个很弱的匿名性质,例如(参见例 4),ElGamal 方案甚至无条件 RE\_ANO\_CCA 匿名,但其并非 ANO\_CCA 匿名;对  $\Pi^a$  所要求的另一性质即 OWE\_CPA 单向性本质上是一个保密性质,它之所以出现在匿名性的充分条件中是由 Fujisaki-Okamoto 混合方案的结构特点决定的.实际上可以证明 Fujisaki-Okamoto 混合方案  $\Pi$  的匿名性必然蕴涵  $\Pi^a$  的 OWE\_CPA 单向性,甚至可以证明关于  $\Pi$  的 ANO\_CPA 匿名性的以下充分必要条件(限于篇幅,我们不给出其证明而直接证明更有用的定理 3):

$\Pi$  是基于  $\Pi^a$  和  $\Pi^s$  的 Fujisaki-Okamoto 混合方案,则  $\Pi$  是 ANO\_CPA 匿名的当且仅当  $\Pi^a$  OWE\_CPA 单向且 RE\_ANO\_CPA 匿名.具体有以下估计式:

$$\begin{aligned} Adv_{\pi^a}^{\text{RE\_ANO\_CPA}}(t) &\leq Adv_{\pi^a}^{\text{RE\_ANO\_CPA}}(0,0,t) \\ &\leq Adv_{\pi^a}^{\text{ANO\_CPA}}(0,0,t), \\ Adv_{\pi^a}^{\text{OWE\_CPA}}(t) &\leq Adv_{\pi^a}^{\text{ANO\_CPA}}(q_g, q_h, O(t+T_E)) + \delta_{\pi^a}(k), \\ Adv_{\pi^a}^{\text{ANO\_CPA}}(q_g, q_h, t) &\leq Adv_{\pi^a}^{\text{RE\_ANO\_CPA}}(t) + \\ &\quad (q_g + q_h) Adv_{\pi^a}^{\text{OWE\_CPA}}(t), \end{aligned}$$

其中,  $\delta_{\pi^a}(k) \equiv P[(M_0, M_1) \leftarrow \$ \Pi^a \text{ 的明文空间}; (pk_0, sk_0), (pk_1, sk_1) \leftarrow KG(k); E(pk_0, M_0) = E(pk_1, M_1)]$  度量  $\Pi^a$  的所谓适应性. 对许多实用的公钥方案,  $\delta_{\pi^a}(k)$  是  $k$  的速降函数,例如不难验证  $\delta_{\text{ElGamal}}(k) = P[M_0, M_1 \leftarrow \$ \text{明文空间}; x_0, x_1 \leftarrow \$ Z_q; g_0, g_1 \leftarrow \$ G; r, r' \leftarrow \$ Z_q; g_0^r \| g_0^{r'x_0} M_0 = g_1^r \| g_1^{r'x_1} M_1] \leq P[r, r' \leftarrow \$ Z_q; g_0^r = g_1^{r'}] = 1/q < 2^{-k}$ .

最后注意到,  $\Pi^a$  的 OWE\_CPA 单向性也是保证  $\Pi$  的保密性的充分条件之一(见上一小节的 Fujisaki-Okamoto 定理),因此定理 3 中的条件非常自然,特别是从定理 3 立得关于 Fujisaki-Okamoto 方案的以下结论.

**命题 2.** 设  $\Pi$  是由公钥加密方案  $\Pi^a$  和对称加密方案  $\Pi^s$  复合而成的 Fujisaki-Okamoto 方案. 若  $\Pi^a$  RE\_ANO\_CCA 匿名、OWE\_CPA 单向且  $\gamma$ -一致,  $\gamma$  是  $k$  的速降函数,  $\Pi^s$  Find-and-Guess 保密,则  $\Pi$  必 IND\_CCA 保密且 ANO\_CCA 匿名.

这表明 Fujisaki-Okamoto 方案是一个非常好的通用混合方案.

定理 3 的证明.

设  $A = (A_1, A_2)$  是破译  $\Pi$  的 ANO\_CCA 匿名性的 P.P.T. 算法,我们构造一个 P.P.T. 算法  $B^A =$

$(B_1, B_2)$  以破译  $\Pi^a$  的 RE\_ANO\_CCA 匿名性. 考虑以下对抗实验及  $B$  的实现:

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

$(pk_0, sk_0), (pk_1, sk_1) \leftarrow KG(k);$   
 $/ * KG(k)$  独立运行两次  $*/$   
 $(\sigma^0, St) \leftarrow B_1^{G^a(sk_0, \cdot), D^a(sk_1, \cdot)}(pk_0, pk_1)$ , 其中  $B_1$  实现如下:

$G\text{-list}$  和  $H\text{-list}$  均初始化为空;  
 $\sigma^0 \leftarrow \$ \Pi^a$  的明文空间;  
 $g^0 \leftarrow \$ \Pi^a$  的密钥空间;  
 $(M^0, St_A) \leftarrow A_1^{G, H, D(sk_0, \cdot), D(sk_1, \cdot)}(pk_0, pk_1);$   
 $St \leftarrow St_A \| M^0 \| \sigma^0 \| g^0;$   
 $\text{return}(\sigma^0, St);$   
 $b \leftarrow \$ \{0, 1\};$   
 $h^* \leftarrow \$ \Pi^a$  的随机数空间;  
 $\sigma^* \leftarrow \$ \Pi^a$  的明文空间;  $/ * \text{特别地, } \sigma^0 \text{ 与 } \sigma^* \text{ 编码长度相同} */$   
 $y^* \leftarrow E^a(pk_b, \sigma^*; h^*);$   
 $d \leftarrow B_2^{D^a(sk_0, \cdot), D^a(sk_1, \cdot)}(y^*, St)$   $B_2$  实现如下:

$\text{parse } St \text{ as } St_A \| M^0 \| \sigma^0 \| g^0;$   
 $v^* \leftarrow E^s(g^0, M^0);$   
 $d \leftarrow A_2^{G, H, D(sk_0, \cdot), D(sk_1, \cdot)}(y^* \| v^*, St_A);$   
 $\text{return}(d);$

if  $d=b$  then  $\text{output}(1)$  else  $\text{output}(0)$ ;

$B$  对  $A$  的诸 oracle 分别仿真如下.

(1) 对来自  $A$ 、针对 oracle-G 的询问  $\sigma$ ;

if there exists  $(\sigma, g)$  in  $G\text{-list}$   
then  $\text{return}(g)$ ;  
else  $g \leftarrow \$ \Pi^a$  的密钥空间;  
insert  $(\sigma, g)$  in  $G\text{-list}$ ;  
 $\text{return}(g)$ .

(2) 对来自  $A$ 、针对 oracle-H 的询问  $(\sigma, m)$ ;

if there exists  $(\sigma, m, h)$  in  $H\text{-list}$   
then  $\text{return}(h)$ ;  
else  $h \leftarrow \$ \Pi^a$  随机数空间;  
insert  $(\sigma, m, h)$  in  $H\text{-list}$ ;  
 $\text{return}(h)$ .

(3) 对来自  $A$ 、针对 oracle-D( $sk_j, \cdot$ ) 的询问  $y$ ,  $j=0, 1$  (注意 oracle-D( $sk_j, \cdot$ ) 可能从其内部访问  $G$  和  $H$ , 对这类访问  $B$  如上处理):

$\text{parse } y \text{ as } y^a \| y^s;$   
 $\sigma \leftarrow D^a(sk_j, y^a);$   
 $/ * \text{这里 } B \text{ 调用自己的 oracle-} D^a(sk_j, \cdot). \text{ 根据相对匿名性的定义, 这里的 } y^a \text{ 允许等于 } y^* * /$

find the item  $(\sigma, g)$  in  $G\text{-list}$  ;  
 if there is no item  $(\sigma, \cdot)$  in  $G\text{-list}$   
 /\* 符号 $(\sigma, \cdot)$ 的涵义参见第2节第一段的说明 \*/  
 then  $g \leftarrow {}^{\$} \Pi^s$  的密钥空间;  
     insert  $(\sigma, g)$  into  $G\text{-list}$  ;  
 $m \leftarrow D^s(g, y^s)$  ;  
 find the item  $(\sigma, m, h)$  in  $H\text{-list}$  ;  
 if there is no item  $(\sigma, m, \cdot)$  in  $H\text{-list}$   
 then  $h \leftarrow {}^{\$} \Pi^a$  随机数空间;  
     insert  $(\sigma, g, h)$  into  $H\text{-list}$  ;  
 if  $y^a = E^a(pk_j, \sigma; h)$   
 then return  $(m)$  ;  
 else return  $(\perp)$  .

定义事件  $Z$ : 存在  $(\sigma^*, \cdot) \in G\text{-list}$  或  $(\sigma^*, \cdot, \cdot) \in H\text{-list}$  ;  
 记  $p_0 = P[Z]$ . 注意到在情形  $\sim Z$  下  $B$  的以上仿真均为完美仿真, 故有

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

因此

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

即

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

下面估计  $p_0$ . 构造两个 P.P.T. 算法  $J_0$  和  $J_1$  破译  $\Pi^a$  的 OWE\_CPA 单向性, 考虑对抗实验及  $J_0$  的实现如下:

$Exp_{\pi^*, J_0}^{\text{OWE\_CPA}}(k)$  :  
 $(pk_0, sk_0) \leftarrow KG(k)$  ;  
 $\sigma^* \leftarrow {}^{\$} \Pi^a$  明文空间;  
 $y^{a*} \leftarrow E^a(pk_0, \sigma^*)$  ;  
 $\sigma^0 \leftarrow J_0(pk_0, y^{a*})$ ,  $J_0$  实现如下:  
      $cnt \leftarrow 0$  ;  $G\text{-list}$  和  $H\text{-list}$  均初始化为空;  
      $(pk_1, sk_1) \leftarrow KG(k)$  ;  
      $g^* \leftarrow {}^{\$} \Pi^s$  密钥空间;  
      $(M, St) \leftarrow A_1^{G, H, D(sk_0, \cdot), D(sk_1, \cdot)}(pk_0, pk_1)$  ;  
      $v^* \leftarrow E^s(g^*, M)$  ;  
      $d \leftarrow A_2^{G, H, D(sk_0, \cdot), D(sk_1, \cdot)}(y^{a*} \parallel v^*, St)$  ;  
      $i \leftarrow {}^{\$} \{1, 2, \dots, cnt\}$  ;  
     /\* 不失一般性, 设在所有询问中出现过的  
         $\sigma$  互不相同且编号为  $\sigma_1, \dots, \sigma_{cnt}$  \*/  
     output  $(\sigma_i)$  ;

$J_0$  对  $A$  的诸 oracle 分别仿真如下.

(1) 对来自  $A$  的、针对 oracle- $G$  的询问  $\sigma$  或针对 oracle- $H$  的询问  $(\sigma, m)$ ,  $J_0$  的行为分别与前面  $B$

对  $G$  或  $H$  的仿真完全相同, 并且对每次询问以变量  $cnt$  计数.

(2) 对来自  $A$  的、针对 oracle- $D(sk_1, \cdot)$  的询问  $y$ , 因为  $J_0$  持有  $sk_1$  故可以直接计算出  $D(sk_1, y)$  并响应  $A$ .

(3) 对来自  $A$  的、针对 oracle- $D(sk_0, \cdot)$  的询问  $y$ :  
 parse  $y$  as  $y^a \parallel y^s$  ;  
 if 若存在  $(\sigma, g) \in G\text{-list}$  和  $(\sigma, m, h) \in G\text{-list}$   
     使  $y^a = E^a(pk_0, \sigma; h)$   
 then return  $(m)$  ;

else

if 若存在  $(\sigma, m, h) \in G\text{-list}$ , 使  $y^a = E^a(pk_0, \sigma; h)$   
 /\* 这时没有  $(\sigma, \cdot) \in G\text{-list}$  \*/

then  $g \leftarrow {}^{\$} \Pi^s$  的密钥空间;  
     insert  $(\sigma, g)$  into  $G\text{-list}$  ;  
      $m \leftarrow D^s(g, y^s)$  ;  
     return  $(m)$  ;

else

$m \leftarrow {}^{\$} \Pi^s$  的明文空间;  
     return  $(m)$  ;

由于  $y^a \parallel v^*$  不能用来询问  $A$  的解密 oracle 且  $G$ 、 $H$  是随机 oracle, 以上仿真是完美的. 进一步注意到  $Exp_{\pi^*, J_0}^{\text{OWE\_CPA}}(k)$  恰是  $b=0$  情形下的  $Exp_{\pi^*, A}^{\text{ANO\_CCA}}(k)$ , 将  $Exp_{\pi^*, A}^{\text{ANO\_CCA}}(k)$  中发生的事件的概率记为  $P_A[\cdot]$ , 则有

$$Adv_{\pi^*, J_0}^{\text{OWE\_CPA}}(k) = P[Exp_{\pi^*, J_0}^{\text{OWE\_CPA}}(k) = 1] \geq 1/(q_g + g_h) P_A[Z|b=0],$$

同理构造  $J_1$ ,  $J_1$  与  $J_0$  的差别仅在于以形式  $(M, St) \leftarrow A_1^{G, H, D(sk_1, \cdot), D(sk_0, \cdot)}(pk_1, pk_0)$  调用  $A_1$ , 即交换  $pk_0$  和  $pk_1$  的角色, 于是  $Exp_{\pi^*, J_1}^{\text{OWE\_CPA}}(k)$  恰是  $b=1$  情形下的  $Exp_{\pi^*, A}^{\text{ANO\_CCA}}(k)$ , 从而

$$Adv_{\pi^*, J_1}^{\text{OWE\_CPA}}(k) = P[Exp_{\pi^*, J_1}^{\text{OWE\_CPA}}(k) = 1] \geq 1/(q_g + g_h) P_A[Z|b=1],$$

于是有

$$p_0 \equiv P[Z] = (1/2)(P_A[Z|b=1] + P_A[Z|b=0]) \leq ((q_g + q_h)/2)(Adv_{\pi^*, J_0}^{\text{OWE\_CPA}}(k) + Adv_{\pi^*, J_1}^{\text{OWE\_CPA}}(k)).$$

将此式与前面已经得到的不等式  $Exp_{\pi^*, A}^{\text{ANO\_CCA}}(k) \leq P[Exp_{\pi^*, B}^{\text{RE\_ANO\_CCA}}(k) = 1] + p_0$  相结合, 立得

$$P[Exp_{\pi^*, A}^{\text{ANO\_CCA}}(k) = 1] \leq P[Exp_{\pi^*, B}^{\text{RE\_ANO\_CCA}}(k) = 1] + ((q_g + q_h)/2)(Adv_{\pi^*, J_0}^{\text{OWE\_CPA}}(k) + Adv_{\pi^*, J_1}^{\text{OWE\_CPA}}(k)),$$

由此得出定理的不等式. 对计算复杂度的估计不难根据  $B$ 、 $J_0$  和  $J_1$  的构造直接验证. 证毕.

定理 3 是一个有力的结论, 能用来证明许多方

案的 ANO\_CCA 匿名性,例如可以证明 Fujisaki-Okamoto 在文献[4]中给出的分别基于 ElGamal 和 Okamoto-Uchiyama 方案的混合构造都是 ANO\_CCA 匿名的. 这里我们将定理 3 应用于 NESSIE 方案 PSEC-2<sup>[8]</sup>, 证明其匿名性质.

**例 6**(PSEC-2 ANO\_CCA 匿名). 图 4 是 PSEC-2

公钥加密方案,文献[7]已经证明若椭圆曲线上的判定性 Diffie-Hellman 问题难解且对称加密方案 Find-and-Guess 保密,则 PSEC-2 在随机 oracle 模型下 IND\_CCA 保密. 与 PSEC-1 类似,这里  $(E/F_q, p, q, P)$  是共享参数,  $W$  是公钥.

密钥生成算法 $KG(E/F_q, p, q, P)$ :	加密算法 $E(pk, M), M \in \{0, 1\}^+$ :	解密算法 $D(sk, Y)$ :
$s \leftarrow \$Z_p$ ;	$r \leftarrow \$Z_p$ ;	parse $Y$ as $(C_1, C_2, C_3)$
$W \leftarrow sP$ ;	$t \leftarrow H(r \parallel M)$ ;	$Q \leftarrow sC_1$ ;
$pk \leftarrow W$ ;	$Q \leftarrow tW$ ;	$u \leftarrow C_2 \oplus x(Q)$ ;
$sk \leftarrow s$ ;	$C_1 \leftarrow tP$ ;	$M \leftarrow \text{SymDec}(G(u), C_3)$ ;
return $(pk, sk)$ ;	$C_2 \leftarrow r \oplus x(Q)$ ;	if $C_1 = H(u \parallel M)P$
	$C_3 \leftarrow \text{SymEnc}(G(r), M)$ ;	then return $(M)$ ;
	return $(C_1, C_2, C_3)$ ;	else return $(\perp)$ ;

图 4 PSEC-2 加密方案  $(E/F_q)$  是域  $F_q$  上的椭圆曲线的点群,  $P$  是  $E/F_q$  上的一个固定点, 阶为素数  $p$ . 对曲线上的点  $Q, x(Q)$  表示  $Q$  的  $x$ -坐标.  $(\text{SymEnc}, \text{SymDec})$  是对称加密方案,  $G: Z_p \rightarrow \{0, 1\}^k$  和  $H: \{0, 1\}^+ \rightarrow Z_p$  是随机 oracle

不难看出 PSEC-2 是一个 Fujisaki-Okamoto 混合构造, 其中的公钥方案  $\Pi^a$  如图 5 所示. 基于与例 3 (PSEC-1) 类似的分析, 对  $\Pi^a$  无条件地成立  $\text{Adv}_{\pi^a, A}^{\text{RE\_ANO\_CCA}}(k) = 0$ . 进一步注意到 Fujisaki-Oka-

moto 定理所要求的所有条件  $\Pi^a$  都满足<sup>[8]</sup>, 特别是  $\Pi^a$  OWE\_CPA 单向. 结合所有以上事实并应用定理 3, 我们得出比文献[7]更佳的结论.

密钥生成算法 $KG^a(E/F_q, p, q, P)$ :	加密算法 $E^a(pk, \sigma), \sigma \in \{0, 1\}^+$ :	解密算法 $D^a(sk, Y)$ :
$s \leftarrow \$Z_p$ ;	$t \leftarrow \$Z_p$ ;	parse $Y$ as $(C_1, C_2)$
$W \leftarrow sP$ ;	$Q \leftarrow tW$ ;	$Q \leftarrow sC_1$ ;
$pk \leftarrow W$ ;	$C_1 \leftarrow tP$ ;	$\sigma \leftarrow C_2 \oplus x(Q)$ ;
$sk \leftarrow s$ ;	$C_2 \leftarrow \sigma \oplus x(Q)$ ;	return $(\sigma)$ ;
return $(pk, sk)$ ;	return $(C_1, C_2)$ ;	

图 5 构成 PSEC-2 的公钥加密方案  $\Pi^a$

**命题 3.** 若对称加密方案 Find-and-Guess 保密、椭圆曲线上的判定性 Diffie-Hellman 问题难解, 则 PSEC-2 在随机 oracle 模型下 IND\_CCA 保密且 ANO\_CCA 匿名.

## 5 Okamoto-Pointcheval 混合加密方案的匿名性质

Okamoto-Pointcheval 在文献[5]中建立的 REACT 方案是另一类高效的混合加密方案并且已被证明 IND\_CCA 保密. REACT 方案  $\Pi = (KG, E, D, G, H)$  由公钥加密方案  $\Pi^a = (KG^a, E^a, D^a)$  和对称加密方案  $\Pi^s = (KG^s, E^s, D^s)$  按以下方式复合而成:  $G, H$  是随机 oracle,  $KG = KG^a$ ; 加密算法  $E(pk, M) = E^a(pk, R; u) \parallel E^s(G(R), M) \parallel H(R, m, y_1, y_2)$ , 其中  $R$  是随机选取的明文,  $u$  是加密算法  $E^a$  中的随机数,  $y_1 = E^a(pk, R; u)$ ,  $y_2 = E^s(G(R), M)$ ; 解密算法  $D(sk, y)$  定义如下:

parse  $y$  as  $y_1 \parallel y_2 \parallel h$ ;  
 $R \leftarrow D^a(sk, y_1)$ ;  
 $M \leftarrow D^s(G(R), y_2)$ ;  
if  $h = H(R, M, y_1, y_2)$  then  $\text{output}(M)$  else  
 $\text{output}(\perp)$ ;

**Okamoto-Pointcheval 定理<sup>[5]</sup>.**  $\Pi$  是基于公钥加密方案  $\Pi^a$  和对称加密方案  $\Pi^s$  构造的 REACT 混合方案, 若  $\Pi^a$  OWE\_PCA 单向、 $\Pi^s$  Find-and-Guess 保密, 则  $\Pi$  必 IND\_CCA 保密.

关于明文验证 (PCA) 和 PCA 攻击的概念参见 4.1 节. 基于 4.1 节定义的明文验证 oracle, 不难仿照定义 3 和定义 4 建立相应的匿名性和相对匿名性概念, 并定义相应的优势函数  $\text{Adv}_{\pi, A}^{\text{ANO\_PCA}}(k)$  和  $\text{Adv}_{\pi, A}^{\text{RE\_ANO\_PCA}}(k)$ . 我们在此省去这些繁琐的定义, 以后分别简称其为 ANO\_PCA 匿名和 RE\_ANO\_PCA 匿名. 对 REACT 混合构造也有类似定理 3 的结果.

**定理 4.** 若  $\Pi^a$  OWE\_PCA 单向且 RE\_ANO\_PCA

PCA 匿名, 则 REACT 混合方案  $\Pi$  必 ANO\_CCA 匿名. 具体有不等式:

$$Adv_{\pi}^{\text{ANO\_CCA}}(q_g, q_h, q, t) \leq Adv_{\pi^a}^{\text{RE\_ANO\_PCA}}(q, t + O(q)) + (q_g + q_h) Adv_{\pi^a}^{\text{OWE\_PCA}}(t + O(q_g + q_h)q),$$

其中  $q, q_g, q_h$  分别是攻击算法对解密-oracle、oracle-G 和 oracle-H 询问次数的上界.

证明. 设  $A = (A_1, A_2)$  是破译  $\Pi$  的 ANO\_CCA 匿名性的 P.P.T. 算法, 我们构造一个破译  $\Pi^a$  的 RE\_ANO\_PCA 匿名性的 P.P.T. 算法  $B^A = (B_1, B_2)$ . 考虑以下对抗实验和  $B$  的实现:

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

$(pk_0, sk_0), (pk_1, sk_1) \leftarrow KG(k)$ ;

$(R^0, St) \leftarrow B_1^{PCA^a(sk_0, \cdot), PCA^a(sk_1, \cdot)}(pk_0, pk_1)$ ,

$B_1$  实现如下:

$G\text{-list}$  和  $H\text{-list}$  均初始化为空;

$R^0 \leftarrow \$ \Pi^a$  的明文空间;

$g^0 \leftarrow \$ \Pi^a$  的密钥空间;

$(M^0, St_A) \leftarrow A_1^{G, H, D(sk_0, \cdot), D(sk_1, \cdot)}(pk_0, pk_1)$ ;

$St \leftarrow St_A \parallel M^0 \parallel R^0 \parallel g^0$ ;

return  $(R^0, St)$ ;

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

$R^* \leftarrow \$ \Pi^a$  的明文空间;

/\* 特别地, 有  $|R^0| = |R^*|$  \*/

$y_1^* \leftarrow E^a(pk_b, R^*)$ ;

$d \leftarrow B_2^{PCA^a(sk_0, \cdot), PCA^a(sk_1, \cdot)}(y_1^*, St)$ ,  $B_2$  实现如下:

parse  $St$  as  $St_A \parallel M^0 \parallel R^0 \parallel g^0$ ;

$y_2^* \leftarrow E^s(g^0, M^0)$ ;

$h^* \leftarrow \$ H$  的值域;

$d \leftarrow A_2^{G, H, D(sk_0, \cdot), D(sk_1, \cdot)}(y_1^* \parallel y_2^* \parallel h^*, St_A)$ ;

return  $(d)$ ;

if  $d=b$  then  $output(1)$  else  $output(0)$ .

$B$  对  $A$  的各个 oracle 分别仿真如下.

(1) 对来自  $A$ 、针对 oracle-G 的询问  $R$ :

if 存在  $(R, g) \in G\text{-list}$

then return  $(g)$ ;

else  $g \leftarrow \$ \Pi^a$  的密钥空间;

insert  $(R, g)$  in  $G\text{-list}$ ;

return  $(g)$ ;

(2) 对来自  $A$ 、针对 oracle-H 的询问  $(R, m,$

$y_1, y_2)$ :

if 存在  $((R, m, y_1, y_2), h) \in H\text{-list}$

then return  $(h)$ ;

else  $h \leftarrow \$ H$  的值域;

insert  $((R, m, y_1, y_2), h)$  in  $H\text{-list}$ ;

return  $(h)$ ;

(3) 对来自  $A$ 、针对 oracle- $D(sk_j, \cdot)$  的询问  $y, j=0, 1$  (若 oracle- $D(sk_j, \cdot)$  从其内部询问  $G$  或  $H$ ,  $B$  按照上面定义的行为予以响应):

parse  $y$  as  $y_1 \parallel y_2 \parallel h$ ;

if 存在  $(R, K) \in G\text{-list}$  使  $PCA^a(sk_j, R, y_1) = 1$

/\* 显然这样的项  $(R, K)$  至多一个 \*/

then if 存在  $(R, M, y_1, y_2, h) \in H\text{-list}$

then return  $(M)$ ;

else  $M \leftarrow D^s(K, y_2)$ ;

insert  $(R, M, y_1, y_2, h)$  into  $H\text{-list}$ ;

return  $(M)$ ;

else /\* 对每项  $(R, K) \in G\text{-list}$  都有

$PCA^a(sk_j, R, y_1) = 0$  \*/

return  $(\perp)$ ;

定义事件  $Z$ : 存在  $(R^*, \cdot) \in G\text{-list}$  或  $((R^*, \cdot, \cdot, \cdot), \cdot) \in H\text{-list}$ ; 记  $p_0 \equiv P[Z]$ . 注意到在  $\sim Z$  的情形下  $B$  的仿真是完美的, 故

$$P[Exp_{\pi, B}^{\text{RE\_ANO\_PCA}}(k) = 1 | \sim Z] = P[Exp_{\pi, A}^{\text{ANO\_CCA}}(k) = 1].$$

从而

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

即

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

以下通过构造两个破译  $\Pi^a$  的 OWE\_PCA 单向性的 P.P.T. 算法  $J_0$  和  $J_1$  来进一步估计  $p_0$ . 考虑以下对抗实验和  $J_0$  的实现:

$Exp_{\pi^a, J_0}^{\text{OWE\_PCA}}(k)$ :

$(pk_0, sk_0) \leftarrow KG(k)$ ;

$R^* \leftarrow \$ \Pi^a$  的明文空间;

$y_1^* \leftarrow E(pk_0, R^*)$ ;

$\sigma^0 \leftarrow J_0^{PCA(sk_0, \cdot)}(pk_0, y_1^*)$ ,  $J_0$  实现如下:

$cnt \leftarrow 0$ ;

$(pk_1, sk_1) \leftarrow KG(k)$ ;

$K^* \leftarrow \$ \Pi^a$  的密钥空间;

$(M, St) \leftarrow A_1^{G, H, D(sk_0, \cdot), D(sk_1, \cdot)}(pk_0, pk_1)$ ;

$v^* \leftarrow E^s(K^*, M)$ ;

$d \leftarrow A_2^{G, H, D(sk_0, \cdot), D(sk_1, \cdot)}(y_1^* \parallel v^*, St)$ ;

$i \leftarrow \$ \{1, 2, \dots, cnt\}$ ;

/\* 不失一般性, 设在所有询问中出现过的

$R$  互不相同且编号为  $R_1, \dots, R_{cnt}$  \*/

return  $(R_i)$ ;

$J_0$  对  $A$  的 oracle 仿真如下.

(1) 对来自  $A$ 、分别针对 oracle- $G$  或  $H$  的询问  $R$  或  $(R, m, y_1, y_2)$ :  $J_0$  的行为与前面  $B$  的行为相同, 且以变量  $cnt$  对询问计数.

(2) 对来自  $A$ 、针对 oracle- $D(sk_1, \cdot)$  的询问  $y$ , 由于  $J_0$  持有私钥  $sk_1$  故能直接计算出  $D(sk_1, y)$ .

(3) 对来自  $A$ 、针对 oracle- $D(sk_0, \cdot)$  的询问  $y$ ,  $J_0$  (其本身带有 oracle- $PCA(sk_0, \cdot, \cdot)$ ) 按照前面定义的  $B$  的行为仿真  $D(sk_0, y)$ .

注意到  $Exp_{\pi^a, J_0}^{OWE\_PCA}(k)$  恰是  $b=0$  情形下的  $Exp_{\pi, A}^{ANO\_CCA}(k)$ , 以  $P_A[\cdot]$  表示  $Exp_{\pi, A}^{ANO\_CCA}(k)$  中事件的概率, 则

$$\begin{aligned} Adv_{\pi^a, J_0}^{OWE\_PCA}(k) &= P[Exp_{\pi^a, J_0}^{OWE\_PCA}(k)=1] \\ &\geq (1/cnt) P_A[Z|b=0] \\ &\geq 1/(q_g + g_h) P_A[Z|b=0]. \end{aligned}$$

同理构造  $J_1, J_1$  与  $J_0$  的差别仅在于  $J_1$  以形式  $(M, St) \leftarrow A_1^{G, H, D(sk_1, \cdot), D(sk_0, \cdot)}(pk_1, pk_0)$  调用  $A_1$ , 即交换  $pk_0$  和  $pk_1$  的角色, 于是  $Exp_{\pi^a, J_1}^{OWE\_PCA}(k)$  恰是  $b=1$  情形下的  $Exp_{\pi, A}^{ANO\_CCA}(k)$ , 从而

$$\begin{aligned} Adv_{\pi^a, J_1}^{OWE\_PCA}(k) &= P[Exp_{\pi^a, J_1}^{OWE\_PCA}(k)=1] \\ &\geq 1/(q_g + g_h) P_A[Z|b=1], \end{aligned}$$

故

$$\begin{aligned} p_0 &\equiv P[Z] = (1/2)(P_A[Z|b=1] + P_A[Z|b=0]) \\ &\leq (q_g + q_h)(Adv_{\pi^a, J_0}^{OWE\_PCA}(k) + Adv_{\pi^a, J_1}^{OWE\_PCA}(k))/2. \end{aligned}$$

结合前面已经导出的不等式  $Exp_{\pi, A}^{ANO\_CCA}(k) \leq P[Exp_{\pi^a, B}^{RE\_ANO\_PCA}(k)=1] + p_0$  立得

$$P[Exp_{\pi, A}^{ANO\_CCA}(k)=1] \leq P[Exp_{\pi^a, B}^{RE\_ANO\_PCA}(k)=1] + (q_g + q_h)(Adv_{\pi^a, J_0}^{OWE\_PCA}(k) + Adv_{\pi^a, J_1}^{OWE\_PCA}(k))/2.$$

由此立得定理的不等式, 且不难根据  $B, J_0$  和  $J_1$  的构造直接验证计算复杂度. 证毕.

结合 Okamoto-Pointcheval 定理和以上定理, 立得 REACT 混合构造也有非常良好的性质.

**命题 4.**  $\Pi$  是由公钥加密方案  $\Pi^a$  和对称加密方案  $\Pi^s$  复合而成的 REACT 方案, 若  $\Pi^a$  OWE\_PCA 单向且 RE\_ANO\_PCA 匿名,  $\Pi^s$  Find-and-Guess 保密, 则  $\Pi$  必 IND\_CCA 保密且 ANO\_CCA 匿名.

**例 7** (PSEC-3 方案 ANO\_CCA 匿名)<sup>[7]</sup>. 已经证明若椭圆曲线上的 Gap-Diffie-Hellman 问题<sup>[10]</sup>难解、对称加密方案 Find-and-Guess 保密, 则公钥方案 PSEC-3 在随机 oracle 模型下 IND\_CCA 保密. PSEC-3 方案如图 6 所示. 与 PSEC-1 和 PSEC-2 类似, 这里  $(E/F_q, p, q, P)$  是共享参数,  $W$  是公钥.

钥生成算法 $KG(E/F_q, p, q, P)$ : $s \leftarrow \$Z_p$ ; $W \leftarrow sP$ ; $pk \leftarrow W$ ; $sk \leftarrow s$ ; return $(pk, sk)$	加密算法 $E(pk, M), M \in \{0, 1\}^+$ : $t \leftarrow \$Z_p$ ; $u \leftarrow \$\{0, 1\}^k$ ; $C_1 \leftarrow tP$ ; $Q \leftarrow tW$ ; $C_2 \leftarrow u \oplus x(Q)$ ; $C_3 \leftarrow \text{SymEnc}(G(u), M)$ ; $C_4 \leftarrow H(u, M, C_1, C_2, C_3)$ ; return $(C_1, C_2, C_3, C_4)$	解密算法 $D(sk, Y)$ : Parse $Y$ as $(C_1, C_2, C_3, C_4)$ $Q \leftarrow sC_1$ ; $u \leftarrow C_2 \oplus x(Q)$ ; $M \leftarrow \text{SymDec}(G(u), C_3)$ ; if $C_4 = H(u, M, C_1, C_2, C_3)$ then return $(M)$ ; else return $(\perp)$ ;
--	---	---

图 6 PSEC-3 加密方案 ( $E/F_q$  是有限域  $F_q$  上的椭圆曲线的点群,  $P$  是曲线  $E/F_q$  上的一个固定点, 阶为素数  $p$ .  $x(Q)$  表示曲线上的点  $Q$  的  $x$ -坐标;  $(\text{SymEnc}, \text{SymDec})$  是对称加密方案,  $G, H$  是随机 oracle)

不难看出 PSEC-3 是一个 REACT 混合构造, 其公钥方案  $\Pi^a$  与 PSEC-2 的公钥方案相同, 特别是  $Adv_{\pi^a, A}^{RE\_ANO\_CCA}(k)=0$ , 从而更有  $Adv_{\pi^a, A}^{RE\_ANO\_PCA}(k)=0$ . 既然  $\Pi^s$  满足 Okamoto-Pointcheval 定理和定理 4 所要求的所有条件, 故有比文献<sup>[7]</sup>更强的结论.

**命题 5.** 若对称加密方案 Find-and-Guess 保密、椭圆曲线上的 Gap-Diffie-Hellman 问题难解, 则 PSEC-3 在随机 oracle 模型下 IND\_CCA 保密且 ANO\_CCA 匿名.

## 6 总 结

本文建立了公钥加密方案的相对匿名性概念和

相对保密性概念, 基于这两个普遍的弱安全性概念证明了匿名性和保密性之间的两个普遍关系, 并且以相对匿名性为工具, 进一步研究了 Fujisaki-Okamoto 混合加密方案和 REACT 混合加密方案的匿名性质, 得出这两类混合方案相当良好的结果: 只要基本的公钥方案满足较弱的保密性和相对匿名性条件, 混合方案就能具有最强的保密性和匿名性. 作为这些一般性结果的具体应用, 证明了三个 NESSIE 方案 PSEC-1/2/3 抗选择密文攻击意义下的匿名性. 下一步自然的工作是考察其它混合加密方案的匿名性, 例如非常高效的 GEM 混合方案等. 此外, Canetti-Halevi-Katz 和 Boneh 等人最近给出基于弱安全的 IBE 方案构造抗选择密文攻击的普通公

钥加密方案的方法,以相对匿名性为工具考察这类构造的匿名性质,将是另一类很有意义的工作.

参 考 文 献

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

[2] Abdalla M, Bellare M, Catalano D et al. Searchable encryption revisited: Consistency properties, relation to anonymous IBE, and extensions//Shoup V ed. Advances in Cryptology—Crypto 2005 Proceedings. Lecture Notes in Computer Science 3621. Sata Babara, California: Springer-Verlag, 2005: 205-222

[3] Coron J-S, Handschuh H, Joye M et al. GEM: A generic chosen-ciphertext secure encryption method//Preneel B ed. Topics in Cryptology—CT-RSA 2002. Lecture Notes in Computer Science 2271. 2002: 263-276

[4] Fujisaki E, Okamoto T. Secure integration of asymmetric and symmetric encryption schemes//Wiener M ed. Advances in Cryptology 1999—Crypto 1999 Proceedings. Lecture Notes in Computer Science 1666. Berlin: Springer-Verlag, 1999: 535-554

[5] Okamoto T, Pointcheval D. REACT: Rapid enhanced-security asymmetric cryptosystem transform//Proceedings of the CT-RSA'2001. Lecture Notes in Computer Science 2020. Berlin: Soringen-Verlag, 2001: 159-175

[6] Okamoto T, Pointcheval D. RSA-REACT: An alternative to RSA-OAEP//Proceedings of the 2nd NESSIE Workshop. Egham, UK, 2001: 76-92

[7] Fujisaki E, Kobatashi T, Morita H et al. PSEC: Provably secure elliptic encryption schemes (Submission to NESSIE by NTT Corp.)//Proceedings of the 1st NESSIE Workshop. Leuven, Belgium, 2000: 1-20

[8] ElGamal T. A public-key cryptosystem and signature scheme based-on discrete logarithms. IEEE Transactions on Information, 1985, 31(5): 469-472

[9] Cramer R, Shoup V. A practical public-key cryptosystem provably secure against adaptive chosen-ciphertext attacks//Krawczyk H ed. Proceedings of the Advances in Cryptology—Crypto'98. Lecture Notes in Computer Science 1462. 1998: 97-109

[10] Okamoto T, Pointcheval D. The gap problems: A new class of problems for security of cryptographic systems//Kim K ed. Proceedings of the Public-Key Cryptography 2001. Berlin: Springer-Verlag, 2001: 104-118

[11] Pointcheval D. Provable security for public-key schemes//Advanced Courses in Contemporary Cryptology. Berlin: Springer-Verlag, 2005: 123-189



**TIAN Yuan**, born in 1966, Ph. D. , associate professor. His main research interests include computer cryptography and applications in network security.

**LI Ming-Chu**, born in 1962, Ph. D. , professor, Ph. D. supervisor. His main research interests include theoretical computer science and computer cryptography.

**CHEN Zhi-Yu**, born in 1984, M. S. candidate. His main research interests focus on network security.

Background

Cryptographic scheme's anonymity(not only limited to public-key encryption scheme) is a very useful utility to high-level cryptographic protocols design, however, this topic is far less investigated by researchers in comparison with data-privacy properties. In this and some following papers hybrid encryption schemes' anonymity will be systematically investigated. Such research is part of a project supported by NFS about how to implement trusted computation in a totally un-

trustable environment(stealthy computing). One of the authors' approaches is to construct IBE/HIBE-like schemes as a general transformation to deform cryptographic data structures, in which anonymity plays a critical role. This is a very interesting, potentially valuable but pretty new field where there is plenty of new ideas and consequences to be explored ahead.