标准模型下一种实用的和可证明安全的 IBE 方案

徐 鹏[1)] 崔国华[1)] 雷凤宇[1)] 汤学明[1)] 陈 晶[2)]

[1)](华中科技大学计算机科学与技术学院信息安全实验室 武汉 430074)

[2)](武汉大学计算机学院 武汉 430072)

摘 要 组合公钥方案是一种用于基于身份密码体制中生成用户加密密钥和私钥的知名方案.针对组合公钥方案存在合谋攻击的问题,通过仅扩展该方案的私钥生成过程,实现了扩展方案的抗合谋攻击性.在此基础上构建标准模型下基于 Decisional Bilinear Diffie-Hellman 假设可证明安全的一种新的基于身份加密方案.最后,为了说明所构新方案的实用性,分析了扩展组合公钥方案的用户加密密钥抗碰撞性;对比了新方案和同类的 3 个知名方案在安全性证明的归约程度方面、加解密的时间复杂度方面和密文的长度方面的性能,表明了新方案在以上 3 点上具有目前最优的指标.因此新方案是相对较实用的.

关键词 组合公钥;合谋攻击;标准模型;Decisional Bilinear Diffie-Hellman 假设;基于身份加密

中图法分类号 TP309 **DOI 号**: 10.3724/SP.J.1016.2010.00335

An Efficient and Provably Secure IBE Scheme Under The Standard Model

XU Peng[1)] CUI Guo-Hua[1)] LEI Feng-Yu[1)] TANG Xue-Ming[1)] CHEN Jing[2)]

[1)](*Laboratory of Information Security, College of Computer Science, Huazhong University of Science and Technology, Wuhan* 430074)

[2)](*College of Computer Science, Wuhan University, Wuhan* 430072)

Abstract The Combined Public-Key scheme is a famous scheme which is commonly used to generate user's encryption-key and private-key in the identity-based encryption schemes. For overcoming the conspiracy attack on Combined Public-Key scheme, a new expanded scheme based on it is proposed in which the generation of private-key is an expansion of the corresponding part of combined public-key scheme. Based on the new expanded Combined Public-Key scheme, a new identity-based encryption scheme is proposed, and under the standard model it is provably secure based on Decisional Bilinear Diffie-Hellman Assumption. At last, by analyzing the collision of user's encryption-key and comparing the new proposed identity-based encryption scheme with three existed famously analogous schemes at the following three aspects: the tightness of reduction in security proof, the complexity of encryption and decryption and the binary length of ciphertext, it can be found that the new scheme is more efficient than them, so it is comparatively more useful.

Keywords combined public-key; conspiracy attack; standard model; Decisional Bilinear Diffie-Hellman Assumption; identity-based encryption

---

收稿日期:2007-12-24;最终修改稿收到日期:2009-04-29.本课题得到国家自然科学基金(60703048)、国家青年自然科学基金(60903196)及湖北省自然科学基金(2007ABA313,2009CDB379)资助.**徐 鹏**,男,1981 年生,博士研究生,主要研究领域为公钥密钥体制的可证明安全性理论、基于身份密码体制、椭圆曲线密码学. E-mail: xupeng0328@hotmail.com. **崔国华**(通信作者),男,1947 年生,教授,博士生导师,主要研究方向为访问控制、密码体制的安全性分析、代数数论. **雷凤宇**,女,1980 年生,博士研究生,主要研究方向为传感器网络的安全性研究、公钥密码体制的安全性分析. **汤学明**,男,1974 年生,博士,讲师,主要研究方向为密码学、数据库安全、网络安全. **陈 晶**,男,1981 年生,博士,讲师,主要研究方向为无线网络安全、路由协议安全与仿真.

1 引 言

1984 年,Shamir 创造性地提出了基于身份的加密体制(Identity-Based Encryption,IBE)的概念[1].和传统的公钥加密体制不同,它可以使用任意字符串作为用户的公钥,这样取消了传统公钥加密体制对在线密钥管理中心的需要,从而大大地提高了效率.虽然 IBE 的概念提出得很早,但直到 2001 年才由 Boneh 提出了第一个实用的 IBE 方案[2],并且该方案成功地在随机预言机模型(Random Oracle Model, RO Model)下将双线性计算难题 Bilinear Diffie-Hellman 问题(BDH 问题)的求解归约到其 IBE 方案的破解,因此是 RO 模型下可证明安全的.与此同时,Boneh 也提出了新的问题,即能否构建标准模型下可证明安全的 IBE 方案.

在标准模型下构建可证明安全的加密方案具有十分重要的实用意义.众所周知,RO 模型下的安全性证明中使用了随机预言机提供询问应答服务,而真实环境中并不存在随机预言机,因此一个 RO 模型下可证明安全的加密方案在实用中必须选取合适的 Hash 函数或伪随机函数等算法来代替方案中的随机预言机(即实例化随机预言机过程),这样对实例化后的方案是否安全和实用需要做进一步的评估[3].而在标准模型下可证明安全的加密方案通常只需要抗碰撞的 Hash 函数或伪随机函数或单向函数,甚至有的方案根本不需要此类函数,因此其可证明安全性更实用.当然,这些并不能说明标准模型绝对优于 RO 模型,因为成功实例化随机预言机后的加密方案并不一定比标准模型下可证明安全的方案的安全性和执行效率低,而且有的标准模型下可证明安全的加密方案很显然就是不实用的,例如,文献[4]中的 IBE 方案.由于在标准模型下构建可证明安全的加密方案比 RO 模型要难,而且其安全性证明更实用,因此近几年得到了广泛的重视,特别是构建标准模型下可证明安全的 IBE 方案.

在证明安全性的过程中,必须选取一个公认的难题(或称之为假设),并完成该难题的求解到加密方案破解的归约.这些难题可分为计算难题和判定难题.而要在标准模型下建立可证明安全的加密方案必须选取判定难题,因为在 RO 模型下安全性证明的归约过程中,计算难题的求解是依赖随机预言机的,而标准模型下由于不存在随机预言机,并且在安全性定义的攻击游戏中[2],仿真器不可能根据其与相应攻击者的交互信息求解计算难题,例如,IND-ID-CPA 安全性定义的攻击游戏中,攻击者告诉仿真器的只有身份信息、两个等长的明文信息和攻击结束时的一位猜测信息,而这些信息或者是仿真器已知的,或者和计算难题的求解无关,因此无法正确地归约并求解计算难题.由此可见,判定难题在标准模型中构建可证明安全的 IBE 方案是至关重要的.

2004 年,Boneh 等人[5]提出了第一个标准模型下可证明安全的 IBE 方案,即在相对较弱的安全性定义下(即非适应性选择挑战 ID 和选择明文攻击下的语义不可区分性,简称为 IND-sID-CPA 安全性)成功地实现了 Decisional Bilinear Diffie-Hellman 问题(Decisional BDH 问题)的求解到该方案破解的归约.但是在相对较强的安全性定义下(即适应性选择挑战 ID 和选择明文攻击下的语义不可区分性,简称为 IND-ID-CPA 安全性),该 IBE 方案的归约十分"松散",具体地说该归约是指数级的归约,因而在实用中为了保证 IND-ID-CPA 安全性会选取一个很大的安全参数,但这使得该 IBE 方案不具有实用性.同年,Boneh 等人[4]提出了另一个标准模型下可证明安全的 IBE 方案,虽然该方案实现了 IND-ID-CPA 安全性下 Decisional BDH 问题的求解到 IBE 方案破解相对有效的归约,但其方案中密文的长度与用户 ID 的长度有关,因而密文较长,同时也增加了加解密的时间复杂度,从而降低了实用性.2005 年,Waters[6]提出了第 1 个标准模型下可证明安全的且综合来说较实用的 IBE 方案,即该方案不仅具有固定长度的密文(安全参数的 3 倍),同时实现了 IND-ID-CPA 安全性下 Decisional BDH 问题的求解到 IBE 方案破解相对有效的归约.2006 年,Gentry[7]提出了另一个标准模型下可证明安全的 IBE 方案,该方案不仅减少了公开参数的个数,提高了性能,并且实现了更紧的归约,但是该归约是基于一个更强的问题,即判定的双线性 Diffie-Hellman 指数的扩展问题(Decisional Augmented Bilinear Diffie-Hellman Exponent Problem,Decisional ABDHE Problem),因而该方案的性能和安全性并不一定比前述方案优秀[7],因此其实用性是否真的提高还有待研究.

通过研究发现,采用组合公钥方案[8](Combined Public-Key Scheme,CPK)可以构建更高效的 IBE 方案,并且若不考虑 CPK 本身的安全性问题,该方案是标准模型下可证明安全的,而且具有目前同类方案[4-6]中最优的 Decisional BDH 问题的求解到 IBE 方案破解的归约有相对最优的加解密时间

复杂度和密文长度. 但是众所周知，CPK 存在合谋攻击问题[9]，即令 CPK 中私钥种子矩阵为 $m\times h$ 阶，则若有 $m\times h$ 个合法用户参与合谋即可计算出私钥种子矩阵. 目前，现有的防范该攻击的方法[9]都是不合理的，例如，要求合法用户的总数小于 $m\times h$，很明显这和 CPK 的设计宗旨是相违背；通过加强管理使得合谋用户数量小于 $m\times h$，这种方法是不具有说服力的. 因而，本文提出的新 IBE 方案首先继承 CPK 的优点及加密密钥和私钥的生成方法，通过扩展私钥的生成过程实现根本上的抗合谋攻击性；再由该扩展 CPK 方案构建标准模型下可证明安全的 IBE 方案；最后通过与前述的同类方案对比归约程度、加解密执行效率、密文长度来说明该方案具有相对较好的实用性. 另外，在标准模型下可证明安全的 IBE 方案中，要求不同用户的加密密钥具有抗碰撞性(通常由输入为用户 ID 的某个抗碰撞的 Hash 函数实现)，因此为了说明扩展 CPK 方案生成的用户加密密钥具有抗碰撞性，本文将详细分析新方案中加密密钥种子矩阵的规模(即 $m\times h$ 的大小)对抗碰撞性的影响，得出具有某种程度的抗碰撞性所需要的矩阵规模，而且由于扩展 CPK 方案和原 CPK 方案的加密密钥的生成方法相同，因此该结论也适用于原 CPK 方案.

为了方便理解，本文将一些重要的预备知识集中在下一节中描述，并进行简要的分析.

2　预备知识

本章将简要介绍与可证明安全的 IBE 方案有关的重要基础知识，分别是 IBE 方案的核心构件——单向函数“双线性映射”；安全性归约中基于的难题；安全性证明所要达到的安全目标，即安全性定义.

2.1　双线性映射

双线性映射是对修正后的 Weil 对和 Tate 对的总结和抽象，是第一个实用的 IBE 方案[2]之所以成功的关键，因而在 2001 年后的大部分 IBE 方案中都得到了应用.

定义 1.　令 G_1 和 G_2 分别是两个大素数 q 阶加法循环群和乘法循环群. 称满足以下条件的映射 $\hat{e}$：$G_1\times G_1\to G_2$ 为双线性映射，条件如下：

(1) 双线性性. 对 $\forall P,Q\in G_1$ 和 $a,b\in \boldsymbol{Z}$，有 $\hat{e}(aP,bQ)=\hat{e}(P,Q)^{ab}$ 成立.

(2) 非退化性. 若 P 为群 G_1 的生成元，则 $\hat{e}(P,P)$ 是 G_2 的生成元.

(3) 可计算性. 对 $\forall P,Q\in G_1$，映射 $\hat{e}(P,Q)$ 在有效时间内可计算.

一个具体的双线性映射可以参考文献[2].

2.2　Computational Diffie-Hellman 假设

定义 2[10].　令 G_1 为素数 q 阶加法群，P 为该群的一个生成元. 群 G_1 上的 CDH 问题(CDHP)为：给定 P,aP,bP，计算 abP，其中 a,b 在 $\boldsymbol{Z}_q^*$ 中随机选取. 若有效时间内，任意概率多项式时间算法的求解优势可忽略，则称群 G_1 上 CDH 假设成立.

2.3　Decisional Bilinear Diffie-Hellman 假设

Decisional BDH 问题的提出是因为在具有双线性映射的群中，判定 Diffie-Hellman(DDH)问题是易解的，即 DDH 假设不成立，因此 Boneh 在双线性映射群中扩展了 DDH 问题，即得到 Decisional BDH 问题，并提出了研究热点，即若 Decisional BDH 假设成立如何在标准模型下构建基于该假设的可证明安全的 IBE 方案.

定义 3.　令 G_1 和 G_2 是两个大素数 q 阶加法循环群和乘法循环群，且存在双线性映射 $\hat{e}:G_1\times G_1\to G_2$，$P$ 为群 G_1 的生成元. Decisional BDH 问题定义如下.

Decisional BDH 问题. 给定一个具有若干形如 $\langle P,aP,bP,cP,abcP\rangle$ 的 Diffie-Hellman 分组的分布 D 和一个具有若干形如 $\langle P,aP,bP,cP,rP\rangle$ 的随机分组的分布 R，区分这两个分布，其中 a,b,c,r 在范围 $\boldsymbol{Z}_q^*$ 中随机选取.

若不存在有效的统计测试算法能在概率多项式时间 T 内，以至少 ε' 的优势解 Decisional BDH 问题，则称为 (T,ε')-Decisional BDH 假设，即 Decisional BDH 假设成立.

总的来说，判定难题属于不可区分性问题，而不可区分性问题又分为：计算不可区分性问题和统计不可区分性问题. 到目前为止，绝大多数基于判定问题可证明安全的公钥加密方案中，其判定问题均是计算不可区分性问题，例如：著名的 Cramer-Shoup 方案[11]；还有本文第 1 节中介绍的所有标准模型下可证明安全的 IBE 方案[4,6-7]. 关于统计不可区分性的定义可以参考文献[12].

2.4　IND-ID-CPA 安全性

IND-ID-CPA 安全性指的是适应性选择挑战 ID 和选择明文攻击下的语义不可区分性，是目前可证明安全的 IBE 方案中最受重视的安全性定义，因为凡是具有该安全性的 IBE 方案均可由 Canetti 等人[13]、Boneh 等人[14]和 Boyen 等人[15]分别提出的通用方法有效地扩展为具有 IND-ID-CCA 安全性

(适应性选择挑战 ID 和选择密文攻击下的语义不可区分性)的 IBE 方案,因此一般只证明某 IBE 方案具有 IND-ID-CPA 安全性.但是实现 IND-ID-CPA 安全性并不容易,有些方案只在较弱的安全性定义 IND-sID-CPA 下才具有相对较实用的安全性归约,而在 IND-ID-CPA 安全性下的归约完全不实用[5],因此这也是标准模型下构建可证明安全的 IBE 方案的难点.下面给出 IND-ID-CPA 攻击的通用定义,再根据该攻击给出 IND-ID-CPA 安全性的定义.

定义 4. IND-ID-CPA 攻击由如下几个阶段构成.

初始化阶段.挑战者生成公开参数和秘密参数,并将公开参数传递给攻击者.

私钥查询阶段 1.攻击者可以向挑战者多次查询任意用户的私钥.

挑战阶段.攻击者提交等长的明文 m_0,m_1 和要挑战的用户身份 ID_{ch} 给挑战者,其中要求攻击者没有询问过 ID_{ch} 的私钥;挑战者随机选取 $d\in\{0,1\}$,并利用 ID_{ch} 的加密密钥加密 m_d 生成挑战密文 C;最后返回 C 给攻击者.

私钥查询阶段 2.除了攻击者不能询问 ID_{ch} 的私钥外,该阶段的执行和私钥查询阶段 1 相同.

猜测阶段.攻击者向挑战者提交对 d 的猜测 d',则完成了一次 IND-ID-CPA 攻击.

定义 5. 称一个 IBE 方案 θ 是 (T,q_{ID},ε)-IND-ID-CPA 安全的,若在时间 T 内对任意一个 IND-ID-CPA 攻击者 A 在进行最多 q_{ID} 次私钥查询后,其破解方案 θ 的优势 $Adv_{\theta,A}<\varepsilon$.

IND-sID-CPA 攻击和 IND-ID-CPA 攻击的差别仅在于:前者的攻击者在初始化阶段必须提交给挑战者其准备挑战的用户身份 ID_{ch},而后者的攻击者在挑战阶段才提交其挑战的用户身份 ID_{ch}.显然,IND-ID-CPA 攻击中的攻击者具有更强的攻击能力.

3 基于扩展 CPK 方案的 IBE 方案

本方案首先对 CPK 方案进行扩展,实现抗合谋攻击性,即所有的合法用户合谋也不可能求出私钥种子矩阵;再基于该扩展 CPK 构建 IBE 方案.明确地说,这项研究的难点就在于不仅可以实现扩展 CPK 方案的完全抗合谋攻击性,同时可以基于该扩展 CPK 方案构建标准模型下可证明安全的 IBE 方案.本文将以上两个过程合为一体作为一个完整的 IBE 方案来描述,并不单独描述扩展 CPK 方案.

基于扩展 CPK 方案的 IBE 方案由 4 个算法组成:系统初始化算法 Setup、用户公私钥生成算法 Extract、加密算法 Encrypt、解密算法 Decrypt.令 $\eta(k)$ 为 Decisional BDH 假设的参数生成算法,其中 k 为安全参数.各算法具体如下.

Setup 算法. 输入系统安全参数 k,密钥管理中心进行如下初始化过程:

1.运行算法 $\eta(k)$ 生成两个大素数 q 阶加法循环群 G_1 和 q 阶乘法循环群 G_2、双线性映射 $\hat{e}$:$G_1\times G_1\to G_2$,G_1 的生成元 P.

2.随机选取 $a,b\in\boldsymbol{Z}_q^*$,计算 $g_1=aP$ 和 $g_2=bP$.

3.(生成 CPK 的所有参数)生成 $m\times h$ 阶私钥种子矩阵 ***PriKSM***:

$$\begin{pmatrix} r_{1,1} & \cdots & r_{1,h} \\ \vdots & \ddots & \vdots \\ r_{m,1} & \cdots & r_{m,h} \end{pmatrix},$$其中 $r_{i,j}$ 在 $\boldsymbol{Z}_q^*$ 内随机选取.

生成相应的 $m\times h$ 阶加密密钥种子矩阵 ***PubKSM***:

$$\begin{pmatrix} r_{1,1}P & \cdots & r_{1,h}P \\ \vdots & \ddots & \vdots \\ r_{m,1}P & \cdots & r_{m,h}P \end{pmatrix}.$$

选取 h 个不同的伪随机函数(或带密钥的 Hash 函数)组成函数集 $F=\{f_1,f_2,\cdots,f_h\}$,且满足对 $\forall i\in[1,h]$ 和 $ID\in\{0,1\}^*$ 有 $f_i(ID)\in[1,m]$.

4.保密私钥种子矩阵 ***PriKSM*** 和 $\boldsymbol{a}$;公开系统参数 $params=\langle q,G_1,G_2,\hat{e},P,g_1,g_2,F,\boldsymbol{PubKSM}\rangle$,其中 G_2 也为明文空间.

Extract 算法. 给定用户 $ID\in\{0,1\}^*$;令用户的私钥为 SK_{ID},密钥管理中心随机选取 $\sigma\in\boldsymbol{Z}_q^*$,并计算用户私钥 $SK_{ID}=(a\cdot g_2+\sigma\cdot SK'_{ID}\cdot P,\sigma\cdot P)$,其中 $SK'_{ID}=(r_{f_1(ID),1}+\cdots+r_{f_h(ID),h})\bmod q\in\boldsymbol{Z}_q^*$,$r_{f_i(ID),i}\in\boldsymbol{PriKSM}$.显然:$SK'_{ID}$ 的计算和 CPK 方案的私钥计算完全一样.扩展 CPK 方案只是在 SK'_{ID} 的基础上额外进行了形如 $(a\cdot g_2+\sigma\cdot SK'_{ID}\cdot P,\sigma\cdot P)$ 的计算,并将其作为用户的私钥,记为 SK_{ID}.

Encrypt 算法. 给定用户 ID 和明文 $m\in G_2$;加密过程如下:

1.计算该用户的加密密钥 $PK_{ID}=(r_{f_1(ID),1}P+\cdots+r_{f_h(ID),h}P)\in G_1^*$,其中 $r_{f_i(ID),i}P\in\boldsymbol{PubKSM}$.

2.随机选取 $t\in\boldsymbol{Z}_q^*$,计算密文 $c=\langle\hat{e}(g_1,g_2)^t\cdot m,t\cdot P,t\cdot PK_{ID}\rangle$.

Decrypt 算法. 给定密文 $c=\langle c_1,c_2,c_3\rangle$;令私钥 $SK_{ID}=(a\cdot g_2+\sigma\cdot SK'_{ID}\cdot P,\sigma\cdot P)$,解密过程如下:$m=c_1\cdot\dfrac{\hat{e}(c_3,\sigma\cdot P)}{\hat{e}(c_2,a\cdot g_2+\sigma\cdot SK'_{ID}\cdot P)}$.加解密算法的一致性验证如下:令 $c_2=t\cdot P$,$c_3=t\cdot PK_{ID}$,由于 $\dfrac{\hat{e}(t\cdot PK_{ID},\sigma\cdot P)}{\hat{e}(t\cdot P,a\cdot g_2+\sigma\cdot SK'_{ID}\cdot P)}=$

$$\frac{\hat{e}(t\cdot SK'_{ID}\cdot P,\sigma\cdot P)}{\hat{e}(t\cdot P,a\cdot g_2)\cdot\hat{e}(t\cdot P,\sigma\cdot SK'_{ID}\cdot P)}=\frac{1}{\hat{e}(g_1,g_2)^t},$$

又有 $c_1=\hat{e}(g_1,g_2)^t\cdot m$，所以显然有一致性成立，即解密过程正确.

通过以上新 IBE 方案的描述可以看出：系统初始化阶段引入了 Decisional BDH 假设的参数生成算法；加密密钥和私钥的生成过程在继承 CPK 方案的基础上进行了扩展，使得私钥变成一个随机化的值；加密的密文长度为固定长度. 这些为该方案的安全性证明和实用性提供了必要的条件.

4　新方案的安全性证明

本章分两个部分分别证明扩展 CPK 方案的抗合谋攻击性和新 IBE 方案在标准模型下 IND-ID-CPA 安全性.

4.1　扩展 CPK 方案的抗合谋攻击性

扩展 CPK 方案由新 IBE 方案的 Extract 算法、Encrypt 算法中接收方加密密钥的生成算法及其相应的系统参数共同组成. 本节将根据合谋攻击的直观含义和 IBE 体制的特点，即攻击者有可能预先知道某些合法用户的私钥，给出具有针对性的合谋攻击的定义. 并在此基础上，基于 CDH 假设证明扩展 CPK 方案的抗合谋攻击性.

定义 6.　IBE 体制中针对私钥的合谋攻击. IBE 体制中针对私钥的合谋攻击由以下阶段组成.

初始化阶段. 挑战者执行 IBE 体制的 Setup 算法，但仅生成与计算加密密钥和私钥相关的公开参数和秘密参数，并将公开参数发送给攻击者.

私钥查询阶段. 输入用户身份信息，攻击者可以向挑战者询问任意合法用户的私钥.

私钥生成阶段. 攻击者根据获取的用户私钥，生成并输出某合法用户的身份信息及其私钥，且攻击者在私钥查询阶段未询问过该用户的私钥.

根据上述定义，若有效时间内，在私钥生成阶段攻击者输出的私钥为该用户的合法私钥，即满足 IBE 体制的私钥的结构，则称为 IBE 体制中一次成功的私钥合谋攻击.

由于原 CPK 方案和扩展 CPK 方案的合谋攻击均是仅针对私钥的攻击，因此上述定义的初始化阶段并不要求生成完整的 IBE 体制的公开参数和秘密参数，而仅仅生成与计算加密密钥和私钥有关的参数.

定理 1.　假设新 IBE 方案中，群 G_1 上 CDH 假设成立，则其扩展 CPK 方案抗 IBE 体制中针对私钥的合谋攻击.

证明.　假设新 IBE 方案中存在成功的针对私钥的合谋攻击者 A′，则可以构造有效的仿真算法 B′实现一次 A′和 B′间合谋攻击的有效仿真，且最终仿真算法 B′求解出 CDH 问题.

令 $\eta'(k)$ 为 CDH 问题的参数生成算法，其中 k 为安全参数.

仿真算法 B′如下：

初始化阶段. 由算法 $\eta'(k)$ 生成 CDH 问题实例 $\langle q,G_1,P,aP,bP\rangle$；根据新 IBE 方案的生成针对私钥的合谋攻击所需要的公开参数 $\langle q,G_1,P,g_1,g_2,F,\boldsymbol{PubKSM}\rangle$ 和秘密参数 $\boldsymbol{PriKSM}$，其中 $g_1=aP$，$g_2=bP$，$F=\{f_1,f_2,\cdots,f_h\}$，

$$\boldsymbol{PubKSM}=\begin{pmatrix} r_{1,1}P & \cdots & r_{1,h-1}P & (r_{1,h}-b)P\\ \vdots & \ddots & \vdots & \vdots\\ r_{m-1,1}P & \cdots & r_{m-1,h-1}P & (r_{m-1,h}-b)P\\ r_{m,1}P & \cdots & r_{m,h-1}P & r_{m,h}P \end{pmatrix},$$

$$\boldsymbol{PriKSM}=\begin{pmatrix} r_{1,1} & \cdots & r_{1,h}\\ \vdots & \ddots & \vdots\\ r_{m,1} & \cdots & r_{m,h} \end{pmatrix},$$

各 $r_{i,j}$ 均在 $\boldsymbol{Z}_q^*$ 中随机选取（该阶段也是扩展 CPK 方案的实例化过程）.

私钥查询阶段. 合谋攻击者 A′可以询问任意合法用户的私钥. 令查询的用户身份信息为 $\langle ID\rangle$，若 $f_h(ID)=m$ 则仿真算法 B′停止并退出；否则仿真算法随机选取 $\sigma\in\boldsymbol{Z}_q^*$，计算并返还私钥

$$SK_{ID}=\langle\sigma\cdot SK'_{ID}\cdot P-\sigma\cdot b\cdot P+a\cdot SK'_{ID}\cdot P,\sigma\cdot P+a\cdot P\rangle,$$

其中，SK'_{ID} 的计算与新 IBE 方案的 Extract 算法相同. 显然 SK_{ID} 可有效计算，且易证

$$SK_{ID}=\langle a\cdot g_2+(\sigma+a)\cdot(SK'_{ID}-b)\cdot P,(\sigma+a)P\rangle.$$

由于 a 为随机选取，且 SK_{ID} 和新 IBE 方案的 Extract 算法生成的算法具有相同的结构，因此合谋攻击者 A′在有效时间内无法区分仿真算法 B′和新 IBE 方案的 Extract 算法的输出，即仿真算法 B′为有效仿真.

私钥生成阶段. 攻击者生成并输出某合法用户的有效的私钥，令输出为 $\langle ID^*,SK_{ID^*}\rangle$，且在私钥查询阶段攻击者没有询问过 ID^* 的私钥. 若 $f_h(ID)\neq m$ 则仿真算法 B′停止并退出.

仿真算法 B′由 $\langle ID^*,SK_{ID^*}\rangle$ 求解 CDH 问题：由于 SK_{ID^*} 为有效私钥，即 $SK_{ID^*}=\langle a\cdot g_2+\sigma'\cdot SK'_{ID}\cdot P,\sigma'P\rangle$，其中 $\sigma'\in\boldsymbol{Z}_q^*$；与新 IBE 方案的 Extract 算法相同，由 ID^* 计算 SK'_{ID^*}；由于已知 $SK'_{ID^*},\sigma'P,a\cdot g_2+\sigma'\cdot SK'_{ID}\cdot P$，易求 $a\cdot g_2$；由于 $a\cdot g_2=abP$，因此仿真算法 B′成功求解 CDH 问题.

最后计算仿真算法 B′在私钥查询阶段和私钥生成阶段不会停止并退出的概率. 令该事件为 $\overline{Abort}$、合谋攻击者 A′询问用户私钥的次数为 q'_{ID}，

则显然有 $Pr[\overline{Abort}]=\frac{1}{m}\left(1-\frac{1}{m}\right)^{q'_{ID}}$.

综上所述,可以得出:若新 IBE 方案中存在针对私钥的合谋攻击者 A′,且仿真算法 B′不会中途停止并退出,则以概率"1"求解 CDH 问题;又由于合谋攻击者 A′的询问必须在有效时间内完成,因此其询问次数 q'_{ID} 必是关于安全参数 k 的多项式,则令 $m=q'_{ID}$,显然可以看出 $Pr[\overline{Abort}]$ 的值为不可忽略数.结合以上两点可以看出,仿真算法 B′求解 CDH 问题的概率不可忽略,而和群 G_1 上 CDH 假设成立相矛盾,因此新 IBE 方案不存在针对私钥的有效的合谋攻击,即扩展 CPK 方案具有抗合谋攻击性.

证毕.

4.2 新方案的 IND-ID-CPA 安全性

新 IBE 方案的 IND-ID-CPA 安全性的证明:将某难题的求解归约到某方案的破解,从而推出矛盾(难题通常认为是不可解的),并证明该方案的安全性.针对本文提出的新 IBE 方案和安全性目标,即 IND-ID-CPA 安全性,该方案的安全性证明主要在于如何有效地仿真各用户私钥,并在某些条件下生成有效的挑战密文(具体条件见下文).本节将先提出安全性定理并详细证明.

定理 2. 假设新 IBE 方案中,群 G_1 上 $\left(T+O(q_{ID}T_E),\frac{1}{m}\left(1-\frac{1}{m}\right)^{q_{ID}}\varepsilon\right)$-Decisional BDH 假设成立,则该方案的实例 θ 是 (T,q_{ID},ε)-IND-ID-CPA 安全的,其中 T_E 是群 G_1 中一次模幂运算的最大时间.

证明. 假设存在 IND-ID-CPA 攻击者 A 在时间 T 内以不可忽略的优势 $Adv_{\theta,A}=\varepsilon$ 攻破新 IBE 方案 θ,本文将构建仿真器 B 实现一次 A 与 B 间的 IND-ID-CPA 攻击的有效仿真,并通过多次该仿真完成一次统计测试过程,最终以压倒性概率求解 Decisional BDH 问题.

从 Decisional BDH 问题的分布 D 和 R 中,任意取定一个分布,并从中随机选取一个分组,且令该分组为 $\langle P,aP,bP,cP,Z\rangle$.输入分组 $\langle P,aP,bP,cP,Z\rangle$ 到仿真器 B,并仿真新 IBE 方案的实例,过程如下:

1. 初始化阶段.继承 Decisional BDH 问题的系统参数 $\langle q,G_1,G_2,\hat{e},P\rangle$;根据新 IBE 方案的 Setup 算法生成系统参数 $\langle q,G_1,G_2,\hat{e},P,g_1,g_2,F\rangle$,其中 $g_1=aP$,$g_2=bP$,$F=\{f_1,f_2,\cdots,f_h\}$;选取私钥种子矩阵 $\boldsymbol{PriKSM}=\begin{pmatrix} r_{1,1} & \cdots & r_{1,h} \\ \vdots & \ddots & \vdots \\ r_{m,1} & \cdots & r_{m,h} \end{pmatrix}$;为了实现私钥查询阶段和挑战密文阶段的有效仿真,计算加密密钥种子矩阵 $\boldsymbol{PubKSM}=\begin{pmatrix} r_{1,1}P & \cdots & r_{1,h-1}P & (r_{1,h}-b)P \\ \vdots & \ddots & \vdots & \vdots \\ r_{m-1,1}P & \cdots & r_{m-1,h-1}P & (r_{m-1,h}-b)P \\ r_{m,1}P & \cdots & r_{m,h-1}P & r_{m,h}P \end{pmatrix}$,且由于 $\boldsymbol{PriKSM}$ 中各元素和 b 均是随机选取,所以该加密密钥种子矩阵和真实的新 IBE 方案的加密密钥种子矩阵不可区分;保密私钥种子矩阵 $\boldsymbol{PriKSM}$,公开系统参数 $\langle q,G_1,G_2,\hat{e},P,g_1,g_2,F,\boldsymbol{PubKSM}\rangle$.

2. 私钥查询阶段 1.攻击者 A 可以向仿真器 B 多次询问任意用户的私钥.令私钥查询为 $\langle ID\rangle$,仿真器 B 的私钥生成过程如下:

2.1. 若 $f_h(ID)=m$,则 B 随机输出"1"或"0",并提前结束该次仿真.

2.2. 否则,与新方案的 Extract 算法相同,根据私钥种子矩阵 $\boldsymbol{PriKSM}$ 和函数集 F 计算 SK'_{ID}.

2.3. 选取随机数 $\sigma\in\boldsymbol{Z}_q^*$,计算该用户私钥如下:

$$SK_{ID}=(\sigma\cdot SK'_{ID}\cdot P-\sigma\cdot b\cdot P+a\cdot SK'_{ID}\cdot P,\sigma\cdot P+a\cdot P).$$

根据初始化阶段的已知参数,上式显然可计算;(用户私钥的有效性分析)根据私钥生成方式,有如下等式成立:

$$\sigma\cdot SK'_{ID}\cdot P-\sigma\cdot b\cdot P+a\cdot SK'_{ID}\cdot P=\sigma\cdot SK'_{ID}\cdot P-\sigma\cdot b\cdot P+a\cdot SK'_{ID}\cdot P-a\cdot b\cdot P+a\cdot b\cdot P=a\cdot g_2+(\sigma+a)\cdot(SK'_{ID}-b)\cdot P,$$

即私钥 $SK_{ID}=(a\cdot g_2+(\sigma+a)\cdot(SK'_{ID}-b)\cdot P,(\sigma+a)\cdot P)$.又根据初始化阶段的加密密钥种子矩阵,显然有该用户的加密密钥 $PK_{ID}=(SK'_{ID}-b)\cdot P$.对比新 IBE 方案和仿真器 B 可以发现,由于 σ,a,b 和私钥种子矩阵的元素均是随机选取,因此这两种方式生成的加密密钥和私钥不可区分,即仿真器 B 生成的私钥有效.

2.4. 返回查询结果 SK_{ID} 给 A.

3. 挑战阶段.攻击者 A 结束私钥查询阶段 1 后,提交等长的明文 m_0,m_1 和要挑战的用户身份 ID_{ch} 给仿真器 B,其中 A 没有询问过 ID_{ch} 的私钥.B 生成挑战密文过程如下:

3.1. 若 $f_h(ID)\neq m$,则 B 随机输出"1"或"0",并提前结束该次仿真.

3.2. 否则,随机选取 $d\in\{0,1\}$,并根据分组 $\langle P,aP,bP,cP,Z\rangle$ 生成 m_d 的挑战密文 $C=\langle\hat{e}(P,Z)\cdot m_d,c\cdot P,SK'_{ID_{ch}}\cdot c\cdot P\rangle$,由于 B 已知 $SK'_{ID_{ch}}$,所以挑战密文可计算.

3.3. 将挑战密文 C 返回给 A.

4. 私钥查询阶段 2.除了攻击者 A 不能询问 ID_{ch} 的私钥外,该阶段的执行和私钥查询阶段 1 相同.

5. 猜测阶段.攻击者 A 向仿真器 B 提交对 d 的猜测 d'.若 $d'=d$,则 B 输出"1";若 $d'\neq d$,则 B 输出"0".最后结束该次仿真.

以上过程即为一次完整的 IND-ID-CPA 攻击的仿真,而且由于仿真不提前结束时,系统参数和私钥查询的结果和真实环境不可区分,因此是一次有效的仿真.若能证明当仿真器的输入分组来自不同

的分布时，攻击者 A 将以不可忽略的优势成功猜测 d，则此时 B 也将以不可忽略的优势输出“1”，那么就可以通过执行多次以上仿真（每次仿真器的输入分组在取定的分布中随机选取）构成一次统计测试求解 Decisional BDH 问题（具体的求解方法将在后面描述）. 因此，通过以下两个引理的证明，最终可以证明定理 2.

引理 1.　当仿真器的输入分组$\langle P, aP, bP, cP, Z\rangle$来自分布 D，并且仿真不提前结束时，攻击者 A 所看到的和 d 的联合分布与真实环境统计不可区分.

证明.　根据以上仿真过程，当仿真不提前结束时，显然有攻击者 A 所看到的和 d 的联合部分只在挑战密文阶段有效，因此只需证明该阶段的统计不可区分性.

已知分组$\langle P, aP, bP, cP, Z\rangle$来自分布 D，则 $Z=abcP$. 根据挑战密文的生成方式，挑战密文 $C=\langle \hat{e}(g_1, g_2)^c \cdot m_d, c \cdot P, SK'_{ID_{ch}} \cdot c \cdot P\rangle$. 由于 c 是随机选取，并且挑战密文的生成形式和真实的新 IBE 方案相同，因此在一次仿真中，攻击者 A 所看到的和 d 的联合分布与真实环境不可区分.

又因为由多次 IND-ID-CPA 攻击的仿真构成的统计测试中，每次仿真器的输入分组均是随机选取，且每个分布中的分组是均匀的和随机生成的，所以每次仿真所生成的挑战密文是均匀的和相互独立的. 因此攻击者 A 所看到的和 d 的联合部分与真实环境是统计不可区分的. 引理 1 得证.　　证毕.

引理 2.　当仿真器的输入分组$\langle P, aP, bP, cP, Z\rangle$来自分布 R，并且仿真不提前结束时，攻击者 A 所看到的和 d 的分布相互独立.

证明.　与引理 1 相同，只需证明挑战密文阶段攻击者 A 所看到的和 d 的分布相互独立.

已知分组$\langle P, aP, bP, cP, Z\rangle$来自分布 R，则 $Z=rP$. 根据挑战密文的生成方式，挑战密文 $C=\langle \hat{e}(P, P)^r \cdot m_d, c \cdot P, SK'_{ID_{ch}} \cdot c \cdot P\rangle$. 由于 r 是随机选取并且和 a, b, c 无关，更进一步的说，r 和 A 所看到的无关，因此 $\hat{e}(P, P)^r \cdot m_d$ 是一次完美填充，即攻击者 A 所看到的和 d 的分布相互独立. 引理 2 得证.　证毕.

一方面，综合引理 1 和 2，可以看出：当仿真器的输入分组$\langle P, aP, bP, cP, Z\rangle$来自分布 D 并且仿真不提前结束时，一次仿真中攻击者 A 在时间 T 内以优势 $Adv_{\theta, A}=\varepsilon$ 使得 $d'=d$；当仿真器的输入分组$\langle P, aP, bP, cP, Z\rangle$来自分布 R 并且仿真不提前结束时，一次仿真中攻击者 A 在时间 T 内以优势 $Adv_{\theta, A}=0$ 使得 $d'=d$. 又根据仿真过程中，函数集 F 的选取方式，可以估算出一次仿真不提前结束的概率. 令 $Abort$ 表示一次仿真提前结束事件，则 $Pr[\overline{Abort}]=\frac{1}{m}\left(1-\frac{1}{m}\right)^{q_{ID}}$. 因此，仿真器 B 的输入来自不同分布时，B 输出“1”的优势为：$|Pr[B(\langle P, aP, bP, cP, abcP\rangle)=1]-Pr[B(\langle P, aP, bP, cP, rP\rangle)=1]|=\left|\left(\frac{1}{2}+\varepsilon \cdot Pr(\overline{Abort})\right)-\frac{1}{2}\right|=\frac{1}{m}\left(1-\frac{1}{m}\right)^{q_{ID}}\varepsilon$. 与文献[12]的定理 3.1 相类似，可以构建由若干次以上仿真组成的一次统计测试，并且若统计测试结果中 B 输出“1”的次数多于输出“0”的次数，则 B 的输入分组来自分布 D；若统计测试结果中 B 输出“1”的次数等于输出“0”的次数，则 B 的输入分组来自分布 R，从而实现以压倒性的概率求解 Decisional BDH 问题.

另一方面，易计算仿真器 B 的时间复杂度约为 $O(q_{ID}T_E)$. 又因为攻击者 A 的时间约束为 T，所以一次仿真中 B 利用 A 求解 Decisional BDH 问题的时间约束为 $T+O(q_{ID}T_E)$.

综合以上两方面可以得出，Decisional BDH 问题在时间 $T+O(q_{ID}T_E)$ 内以不小于 $\frac{1}{m}\left(1-\frac{1}{m}\right)^{q_{ID}}\varepsilon$ 的优势被 B 破解. 因此和已知中$\left(T+O(q_{ID}T_E), \frac{1}{m}\left(1-\frac{1}{m}\right)^{q_{ID}}\varepsilon\right)$-Decisional BDH 假设成立相矛盾，所以上述新 IBE 方案 θ 是(T, q_{ID}, ε)-IND-ID-CPA 安全的. 定理 2 得证.　　证毕.

综上所述，新 IBE 方案在标准模型下具有可证明的 IND-ID-CCA 安全性，即在标准模型下有效地实现了 Decisional BDH 问题到新 IBE 方案的 IND-ID-CPA 攻击者的归约.

5　新方案的实用性分析

众所周知，用户加密密钥的抗碰撞性是一个重要的安全性和实用性指标. 由于扩展 CPK 方案和其它的 IBE 方案的加密密钥生成过程不同，因此需要单独讨论其抗碰撞性. 本节还将通过与同类方案的归约程度和时空复杂度对比，讨论新 IBE 方案的实用性.

5.1　扩展 CPK 方案的加密密钥抗碰撞分析

根据扩展 CPK 方案的加密密钥种子矩阵可以看出，共存在两种可能的碰撞：(1) 两用户的 ID 对应不同索引值时，即 $\exists f_i \in F$ 使得两用户的 $f_i(ID)$ 值不同时，对应的加密密钥相同；(2) 两用户的 ID 对应的索引值相同，则加密密钥相同. 本节将分别讨

论以上两种情况.

情况 1. 由于私钥种子矩阵的元素是随机选取,且加密密钥种子矩阵基于素数阶循环群,因此任意用户对应的加密密钥种子矩阵中元素的组合也是循环群中的随机元. 由于 $m\times h$ 阶加密密钥种子矩阵可以产生 m^h 种组合,因此 m^h 种组合不发生碰撞的概率 Pr_1 为 $Pr_1=\left(1-\frac{1}{q}\right)\left(1-\frac{2}{q}\right)\cdots\left(1-\frac{m^h-1}{q}\right)=\prod_{i=1}^{m^h-1}\left(1+\frac{-i}{q}\right)\approx\prod_{i=1}^{m^h-1}e^{-i/q}=e^{-(m^h-1)m^h/q}$. 以 32×32 的加密密钥种子矩阵为例,$Pr_1\approx e^{-2^{320}/O(2^{1024})}$,可见此时不发生碰撞的概率极高. 虽然根据 Pr_1 的计算公式可以看出:不发生碰撞的概率 Pr_1 随 $m\times h$ 增大而减小,但是在实际应用中显然较小的 $m\times h$ 已经满足应用,例如 32×32 的加密密钥种子矩阵具有大约 10^{48} 种组合. 因此在实际应用中,第 1 种情况几乎不会发生.

情况 2. 由于目前对所有实用中的 Hash 函数很难精确地刻画其抗碰撞概率,因此本文无法精确地计算出该情况下扩展 CPK 方案发生碰撞的概率. 但是从实用角度出发,可以通过存在性证明的方法得出,当加密密钥种子矩阵的规模达到一定时,存在某种方法使其该情况下碰撞发生的概率和某实用 Hash 函数相同,具体的过程见定理 3.

定理 3. 若扩展 CPK 方案的 $m\times h$ 阶加密密钥种子矩阵满足 $m\geq2^{\lceil\frac{160}{h}\rceil}$ 时,存在某种方法使其不同用户的索引值发生碰撞的概率不大于 Hash 函数 SHA-1.

证明. 本文通过构造具体的方法证明该定理. 已知 Hash 函数 *SHA*-1 的输出为 160 位. 因此分为以下两种情况分别证明:

(1) 当 $h|160$ 时,构造用户 ID 的加密密钥生成方式为:计算用户 ID 的 Hash 值 *SHA*-1(*ID*);将该值依次分为等长的 h 份并依次对应扩展 CPK 方案加密密钥种子矩阵的 h 列,每份的值对应相应列的行号;依次提取 h 列的相应行值作为该用户的加密密钥种子组合,并计算加密密钥. 由于每份长为 $\frac{160}{h}$ 位,因此当 $m\geq2^{\frac{160}{h}}$ 时,均存在某个行号和该份的值相同. 而且此时不同用户的索引值发生碰撞的概率不大于 *SHA*-1.

(2) 当 $h\nmid160$ 时,构造用户 ID 的加密密钥生成方式为:计算用户 ID 的 Hash 值 *SHA*-1(*ID*);将该值依次分为 h 份,其中二进制长度为 $\left\lfloor\frac{160}{h}\right\rfloor$ 的有 X 份、二进制长度为 $\left\lceil\frac{160}{h}\right\rceil$ 的有 Y 份,并且满足方程组 $\begin{cases}\left\lfloor\frac{160}{h}\right\rfloor\times X+\left\lceil\frac{160}{h}\right\rceil\times Y=160\\X+Y=h\end{cases}$,即 $\begin{cases}X=\left\lceil\frac{160}{h}\right\rceil h-160\\Y=160-\left\lfloor\frac{160}{h}\right\rfloor h\end{cases}$;将 h 份依次对应扩展 CPK 方案加密密钥种子矩阵的 h 列,每份的值对应相应列的行号;依次提取 h 列的相应行值作为该用户的加密密钥种子组合,并计算加密密钥. 由于每份的长小于等于 $\left\lceil\frac{160}{h}\right\rceil$ 位,因此当 $m\geq2^{\lceil\frac{160}{h}\rceil}$ 时,均存在某个行号和该份的值相同. 而且此时不同用户的索引值发生碰撞的概率不大于 *SHA*-1. 综合 1、2,定理 3 得证. 证毕.

根据定理 3 可知,当扩展 CPK 方案的加密密钥种子矩阵达到 32×32 阶以上时,必然存在某种方法使其不同用户索引值发生碰撞的概率不大于 Hash 函数 *SHA*-1. 同理,当扩展 CPK 方案的加密密钥种子矩阵达到 16×32 阶以上时,必然存在某种方法使该碰撞的发生概率不大于 Hash 函数 MD5.

进一步可以看出,与情况 1 相反,情况 2 不发生碰撞的概率随 $m\times h$ 增大而增大,但是通过以上分析可见存在很多种加密密钥种子矩阵规模使以上两种情况发生的概率很小. 另外,由于原 CPK 方案和扩展 CPK 方案的加密密钥生成方式相同,因此上述用户加密密钥的碰撞分析同样适用于前者.

5.2 新方案与同类方案的归约程度对比

可证明安全性的归约程度是衡量一个密码体制安全性和实用性的重要指标. 总的来说,基于同一个困难假设(不仅假设的文字描述相同,且安全性的量化也相同)的不同密码体制的可证明安全性,归约程度越"紧"(具体的含义见下文)则密码体制越安全;换句话说,基于同一类困难假设(假设的文字描述相同,但安全性的量化不同),且具有相同安全性量化的不同密码体制,归约程度越"紧"则密码体制的安全参数越小,计算效率更高. 本节将对比新 IBE 方案和 3 个知名的基于同一个困难假设的 IBE 方案[4,6-7]在可证明安全性中的归约程度,从而得出新 IBE 方案在归约程度方面的实用性.

由于文献[4-6]中各 IBE 方案的安全性定理的描述方式不同,为了方便进行归约程度的比较,本文将各安全性定理等价转换为同一种描述形式,即假设 (T',ε')-Decisional BDH 假设在群 G_1 中成立时,各 IBE 方案的 IND-ID-CPA 安全性,并且对结论进行了优化(选取适当参数使归约达到最"紧"),具体结论见表 1(称文献[4-6]中的 IBE 体制分别为 BB04a、BB04b、W05).

表 1　4 种 IBE 方案的 IND-ID-CPA 安全性对比

IBE 方案名称	IND-ID-CPA 安全性	备注
BB04a	$(T'-O(q_{ID}T_E),q_{ID},2^N\varepsilon')$	N 为系统允许的 ID 的二进制长度(下同)
BB04b	$(T',q_{ID},eq_{ID}\varepsilon'))$	通过适当取系统参数使归约达到最“紧”时的近似值;$e=2.71$(下同)
W05	$(T'-O(\varepsilon'^{-2}\ln(\varepsilon'^{-1})\lambda^{-1}\ln(\lambda^{-1})),q_{ID},32(N+1)q_{ID}\varepsilon')$	$\lambda=\frac{1}{8(N+1)q_{ID}}$
新 IBE 方案	$(T'-O(q_{ID}T_E),q_{ID},eq_{ID}\varepsilon')$	通过适当取 m 使归约达到最“紧”时的近似值($m=q_{ID}$)

归约程度越“紧”指的是:若可以证明基于(T',ε')-HA 假设,密码体制是$(T'-T_R,\varepsilon)$-SD 安全的,其中 HA 表示某难题(例如,Decisional BDH 难题等等)、SD 表示某安全性定义(例如,IND-ID-CPA 安全性等等)、T_R表示归约的时间复杂度,那么 ε 和 ε'越接近,归约程度越“紧”.根据表 1 可以看出,基于同一个困难假设的新 IBE 方案和 BB04b 方案具有目前同类方案中最“紧”的归约,换句话说,当以上 4 个方案具有相同的安全参数时,新 IBE 方案和 BB04b 方案的安全性最高.另一方面,虽然难题和密码方案的破解难度与时间有关,即时间越长破解优势越高,但是由于实用中安全的密码方案和难题通常是指在相当长的时间内它们的破解优势可忽略,因此基于难题的时间参数 T'很大,而又因为归约过程是有效时间内可完成的(否则证明过程无意义),即 T_R最多为多项式时间复杂度,所以不考虑表 1 中 4 个 IBE 方案的 IND-ID-CPA 安全性因时间参数的不同对安全性的影响.由此可见,在归约程度上新 IBE 方案具有相对较好的实用性.

5.3　新方案与同类方案的时空复杂度对比

除了归约程度外,由于较长时间的加解密过程会降低密码方案的应用范围,较长的密文会消耗更多的传输资源,因此加解密时间复杂度和密文长度是衡量密码方案的另一个重要指标.与上一节相同,本节将对比表 1 中 4 个 IBE 方案的加解密时间复杂度和密文的长度,具体数据见表 2.

表 2　4 个 IBE 方案的加解密时间复杂度和密文长度对比

IBE 方案的名称	加密时间复杂度		解密时间复杂度			密文长度	
	群 G_1的模幂运算/次	群 G_2的模幂运算/次	双线性对运算/次	群 G_2的模乘运算/次	群 G_2的求逆运算/次	群 G_1的元素/个	群 G_2的元素/个
BB04a	3	1	2	2	1	2	1
BB04b	$N+1$	1	$N+1$	$N+2$	1	$N+1$	1
W05	2	1	2	2	1	2	1
新 IBE 方案	2	1	2	2	1	2	1

根据表 2 显然可以看出,虽然 BB04b 和新 IBE 方案具有目前最优的归约程度,但是 BB04b 方案的加解密时间复杂度和密文长度是 4 个方案中最差的,相反新 IBE 方案和 W05 方案具有目前最优的加解密时间复杂度和密文长度.综合以上两点可以得出,新 IBE 方案不仅具有目前最优的归约程度,同时具有目前最优的加解密时间复杂度和密文长度,是相对比较实用的加密方案.

6　总结与展望

针对 CPK 方案存在合谋攻击的缺陷,本文在完全继承 CPK 方案的基础上,对其私钥生成过程进行了扩展,使得扩展 CPK 方案具有可证明的抗合谋攻击性.

CPK 方案是一种用于给基于身份密码体制生成加密密钥和私钥的方案,其最终意义还是要运用在某基于身份密码体制中,因此构建可证明安全的基于扩展 CPK 方案的 IBE 方案具有重要意义.本文基于扩展 CPK 方案提出了一个在标准模型下基于 Decisional BDH 假设可证明安全的新 IBE 方案.

最后,为了说明扩展 CPK 方案具有基本的实用性,即用户加密密钥的抗碰撞性,本文分析了加密密钥种子矩阵的规模对该碰撞性的影响.另一方面,本文对比了目前知名的 3 个同类方案和新 IBE 方案的 3 个重要的实用性指标,即安全性证明中的归约程度、加解密时间复杂度、密文长度,并得出新 IBE 方案在以上三点上具有目前最优的性能,因此新 IBE 方案是相对较实用的.

目前,研究在标准模型下基于 Decisional BDH 假设具有更“紧”归约的可证明安全的 IBE 方案仍然是一个公开的问题[7].

致　谢　感谢华中科技大学计算机学院信息安全实验室的郑明辉博士、粟栗博士对可证明安全性理论的前期指导和对文章有价值的讨论!

参　考　文　献

[1] Shamir A. Identity-based cryptosystems and signature

schemes//Blankley G T, Chaum D eds. //Proceedings of the CRYPTO'84. LNCS 196, Springer-Verlag, 1985: 48-53

[2] Boneh D, Franklin M. Identity-based encryption from the weil pairing//Proceedings of the Cryptology-Crypto 2001. LNCS 2139, Springer-Verlag, 2001: 231-229

[3] Bellare M, Boldyreva A, Palacio A. An uninstantiable random-oracle-model scheme for a hybrid-encryption problem//Proceedings of the Cryptology-EUROENCRYPT' 2004. LNCS 3027, Springer-Verlag, 2004: 171-188

[4] Boneh D, Boyen X. Secure identity based encryption without random oracles//Proceedings of the Cryptology-Crypto 2004. LNCS 3152, Springer-Verlag, 2004: 443-459

[5] Boneh D, Boyen X. Efficient selective-ID identity based encryption without random oracles//Proceedings of the Cryptology-EUROENCRYPT'2004. LNCS 3027, Springer-Verlag, 2004: 223-238

[6] Waters B. Efficient identity-based encryption without random oracles//Proceedings of the Cryptology-EUROENCRYPT'2005. LNCS 3494, Springer-Verlag, 2005: 114-127

[7] Gentry C. Practical identity-based encryption without random oracles//Proceedings of the Cryptology-EUROENCRYPT'2006. LNCS 4004, Springer-Verlag, 2006: 445-464

[8] Zhong Xu, Lu Lang-Ru, Nan Xiang-Hao. A project designed by IBE encryption system based on SPK. Microcomputer Information, 2005, 21(4): 226-227(in Chinese)
(钟旭,陆浪如,南湘浩. 一种基于种子密钥 SPK 的 IBE 加密体制设计方案. 微计算机信息, 2005, 21(4): 226-227)

[9] Chen Hua-Ping, Guan Zhi. Some questions explained about CPK. Information Security and Communication Privacy, 2007, 160(9): 47-49(in Chinese)
(陈华平, 关志. 关于 CPK 若干问题的说明. 信息安全与通讯保密, 2007, 160(9): 47-49)

[10] Xu Peng, Cui Guo-Hua, Lei Feng-Yu. An efficient and provably secure IBE scheme without bilinear map. Journal of Computer Research and Development, 2008, 45(10): 1687-1695(in Chinese)
(徐鹏, 崔国华, 雷凤宇. 非双线性映射下一种实用的和可证明安全的 IBE 方案. 计算机研究与发展, 2008, 45(10): 1687-1695)

[11] Cramer R, Shoup V. A practical public key cryptosystem provably secure against adaptive hosen Ciphertext//Proceedings of the Cryptology-Crypto'98. LNCS 1462, Springer-Verlag, 1998: 13-25

[12] Boneh D. The decision diffie-hellman problem//Proceeding of the 3rd Algorithmic Number Theory Symposium, LNCS 1423, Springer-Verlag, 1998: 48-63

[13] Canetti R, Halevi S, Katz J. Chosen-Ciphertext security from identity-based encryption//Proceedings of the Cryptology-EUROENCRYPT'2004. LNCS 3027, Springer-Verlag, 2004: 207-222

[14] Boneh D, Katz J. Improved efficiency for CCA-secure cryptosystems built using identity-based encryption//Proceedings of the CT-RSA 2005, LNCS 3376, Springer-Verlag, 2005: 87-103

[15] Boyen X, Mei Q, Waters B. Direct chosen ciphertext security from identity-based techniques//Proceedings of the 12th ACM CCS, 2005: 320-329

XU Peng, born in 1981, Ph. D. candidate. His research interests include the provable security of public-key cryptosystem, identity-based cryptosystem, elliptic curve cryptosystem.

CUI Guo-Hua, born in 1947, professor, Ph. D. supervisor. His main research interests include access control, the security analysis of cryptosystem, algebra number theory.

LEI Feng-Yu, born in 1980, Ph. D. candidate. Her main research interests include the security research of sensor net, the security analysis of public-key cryptosystem.

TANG Xue-Ming, born in 1974, Ph. D., lecturer. His main research interests include cryptography, data based security, and network security.

CHEN Jing, born in 1981, Ph. D., lecturer. His main research interests include wireless network routing protocol security and simulation.

Background

The Combined Public Key (referred to as CPK) scheme, which was firstly proposed by professor Nan Xianghao, is a new method to contrive the management of keys. But as well as we known, this scheme also contains some flaws. For overcoming the conspiracy attack of the CPK scheme, the authors fully researched the reasons, which can make this attack happening, and then improved the process of private key generation of this scheme, at last successfully solved this flaw. Furthermore, based on the improved CPK scheme, the authors proposed a new provably secure Identity-based Encryption (referred to as IBE) scheme under the standard model.

In addition, the research of the efficient and provably secure IBE scheme recently is a hot field. Furthermore, the problem that how to propose a provably secure IBE scheme, under the standard model, has more efficient degree of reduction in the security proof, is the most important problem (in this aspect, the scholars from the Stanford made some great contributions). By compared with some well known IBE scheme in three important aspects of the security and efficiency, the authors reasonably explain that the new IBE scheme based on the improved CPK scheme is more efficient in some aspects.