不含双线性对的无证书签密方案安全性分析与改进

王电钢[1] 丁雪峰[2] 黄 昆[1]
(四川省电力公司智能电网信息技术实验室 成都 610041)[1] (四川大学信息管理中心 成都 610065)[2]

摘 要 无证书密码体制能同时解决传统公钥密码体制证书管理问题和基于身份密码体制中密钥分发的问题,而受到学者们的关注。基于双线性对的无证书签密,因需要大量开销用于双线性对运算而性能不佳。研究不基于双线性对的无证书签密方案,发现Selvi等人的不基于双线性对的无证书签密方案不是标准的无证书签密方案,因为用户在使用时必须先验证对方的公钥,这不仅与无证书公钥体制相背,而且增加了用户的开销。分析了其他3个不基于双线性对的无证书签密方案,发现这3个方案都不满足不可伪造性和机密性。为解决这些安全性问题,提出一个新的不基于双线性对的无证书签密方案,并在随机预言机模型下证明了其安全性。

关键词 无证书公钥密码体制,签密,双线性对,椭圆曲线,随机预言机模型
中图法分类号 TP918.1 **文献标识码** A

Security Analysis and Improvement of Strongly Secure Certificateless Key Agreement Protocol

WANG Dian-gang[1] DING Xue-feng[2] HUANG Kun[1]
(Smart Grid Information Technology Laboratory of Sichuan Electric Power and Communication Corporation, Chengdu 610041, China)[1]
(Information Management Center, Sichuan University, Chengdu 610065, China)[2]

Abstract The certificateless public key cryptography (CLPKC) has attracted wide attention since it could solve the certificate management problem in the traditional public cryptography and the key escrow problem in the ID-based cryptography. Many certificateless signcryption (CLSC) schemes using pairing have been proposed. The pairing operation is a very complicated operation. So the performance of these schemes is not very good. In this paper, we study the CLSC schemes without pairing, and find that Selvi et al. Is scheme is not a standard CLSC scheme since the user must verify the public key before using it. This not only inverses the thought of the CLPKS but also increases the user's computational cost. To solve the problem, three new CLSC schemes without pairing have been proposed. In this paper, we will show the three CLSC schemes provide neither unforgeability property nor confidentiality property. To improve security, we also propose a new CLSC scheme without pairing and demonstrate it is provably secure in the random oracle model.

Keywords CLPKC signcryption scheme, Bilinear pairings, Elliptic curve, Random oracle model

1 引言

为解决传统公钥密码体制中的证书管理问题,1984年Shamir[1]提出了基于身份密码体制的概念。在基于身份的公钥密码中,用户的公钥为他的身份信息,因此不需要证书。然而,用户的私钥是由密钥生成中心(KGC)生成的,因此基于身份的PKC具有密钥分发的问题,即KGC知道所有用户的私钥。为解决此问题,Al-Riyami等人[2]提出无证书公钥密码体制(CLPKC)的概念。在CLPKC中,用户的私钥由KGC计算的部分私钥和用户自己选择的秘密值组成。因此,CLPKC解决了密钥分发问题。此后很多基于CLPKC的密码方案相继被提出。

在很多应用中,我们想同时实现加密和签名的安全目标。1997年,Zheng[3]提出了签密的概念。签密方案能同时实现加密和签名,因此签密方案与传统的签名-加密方法比较具有低计算开销和低通信开销的优点。基于离散对数难题,Zheng提出了一个完整的签密方案,然而他们没有形式化证明该签密方案的安全性。An等人[4]系统地研究了签密方案的各种性质。进而,Malone-Lee[5]提出了基于身份签密的概念,并且定义了关于隐私性和不可伪造性的安全模型。在2008年,Barbosa等人[6]给出了无证书签密的概念,并提出了第一个无证书签密方案。为了改进性能,Wu等人[7]提出了一个新的无证书签密方案。然而Selvi等人[8]指出他们的方案是不安全的。为解决安全问题,Xie等人[9]提出了一个无证书签密方案,可是Selvi等人[10]仍发现该方案不能抵抗类型1敌手的攻击。2010年,Liu等人[11]提出第一个标准模型下的无证书签密方案。此后,Weng等人[12]指出Liu的方案对于恶意且被动KGC是不安全的。

从理论分析[13]和实验结果[14,15]发现双线性对的计算量大约比椭圆曲线标量乘法运算量高出20倍。因此,不含双线

本文受四川省科技计划支撑项目(2013GZ0004),四川省科研计划项目(2012GZ0001)资助。
王电钢(1973—),男,博士,高级工程师,主要研究方向为信息安全,E-mail:2887770@qq.com;丁雪峰(1974—),男,博士,高级工程师,主要研究方向为信息安全,E-mail:dingxf@scu.edu.cn(通信作者);黄 昆(1977—),女,硕士,高级工程师,主要研究方向为信息安全。

性对的无证书签密方案更有效。2008 年，Barreto 等人[16]提出第一个不含双线性对的无证书签密方案。然而 Selvi 等人[17]指出该方案不能抵抗类型 1 敌手的攻击，不满足机密性。为改进安全性，Selvi 等人[17]提出一个改进的不含双线性对的无证书签密方案。Xie 等人[18]也提出了一个不含双线性对的无证书签密方案。该方案[17,18]比以前的方案[6,7,9,11]更为高效，因为在方案[17,18]中不需要计算双线性对。然而这两个方案必须验证公钥，这不仅增加了用户的负担，而且与无证书签密的思想相违背。为改进性能，Zhu 等人[19]、Liu 等人[20]、Jing 等人[21]分别提出了无证书签密方案。通过具体的攻击表明，Jing 等人[21]的方案既不满足不可伪造性，也不满足机密性。我们的攻击对于 Zhu 等人[19]和 Liu 等人[20]的方案都是有效的。为了改进安全性，我们提出一个新的不含双线性对的无证书签密方案，并在随机预言机模型下证明了方案的安全性。

本文第 2 节给出一些背景知识；第 3 节回顾了 Jing 等人的无证书签密方案；第 4 节提出我们的无证书签密方案；第 5 节和第 6 节给出安全性形式化分析和性能比较；最后总结全文。

2 背景知识

2.1 计算困难问题

定义 1(离散对数问题(DLP)) 令 p 和 q 为素数，满足 $q|p-1$，令 g 是 Z_p 中的 q 阶元素。给定 $y=g^x$ 和 g，离散对数问题的任务是求满足等式的 $x\in Z_q^*$。

定义 2(计算 Diffie-Hellman 问题(CDHP)) 令 p 和 q 是素数，且满足 $q|p-1$。令 g 是 Z_p 中的 q 阶元素。对于未知的 $a,b\in Z_q^*$，给定 g^a 和 g^b，计算 Diffie-Hellman 问题的任务是计算 g^{ab} 的值。

2.2 无证书签密模型

一个无证书签密方案(CLSC)由以下 6 个多项式时间算法构成：

Setup：算法输入安全参数 k，KGC 运行该算法，产生系统公开参数 *params* 和主密钥 *mk*。

PartialPrivateKeyExtract：输入 *params*，*mk* 和用户的身份信息 ID_U，KGC 执行该算法并返回该用户的部分私钥 D_U。

SetSecretValue：输入安全参数 k 和系统参数，用户执行该算法，并返回秘密值 sk_U。

SetPrivateKey：输入用户的秘密值 sk_U 和部分私钥 D_U，用户执行该算法并返回用户私钥 SK_U。

SetPublicKey：输入系统参数 *params* 和用户的秘密值 sk_U，用户执行该算法并产生其公钥 PK_U。

Signcrypt：输入系统参数 *params*、消息 m、发送者身份信息 ID_A、私钥 SK_A、公钥 PK_A、接收者的身份信息 ID_B 和公钥 PK_B，发送者执行该算法并产生签密密文 σ。

Unsigncrypt：输入密文 σ、接收者私钥 SK_B、发送者的身份信息 ID_A、公钥 PK_A，接收者执行该算法并返回 m 或错误标识 $\perp$。

2.3 敌手模型

CLPKC 有两类敌手[2]，即类型 1 敌手 $\mathcal{A}_1$ 和类型 2 敌手 $\mathcal{A}_2$。敌手 $\mathcal{A}_1$ 不能得到系统主密钥，但能替换用户的公钥；敌手 $\mathcal{A}_2$ 代表恶意 KGC，他能产生用户的部分私钥，得到系统主密钥，但不能替换用户的公钥。Barbosa 等人[6]定义了 CLSC 形式化安全概念。敌手 $\mathcal{A}(\mathcal{A}\in\{\mathcal{A}_1,\mathcal{A}_2\})$ 可以做如下询问。

Public-Key-Request：收到对于用户 ID_U 的询问，则计算用户的私钥 SK_U 和公钥 PK_U，返回 PK_U 给 $\mathcal{A}$。

Partial-Pirvate-Key-Extract：收到对于用户 ID_U 的询问，则返回用户的部分私钥 D_U 给 $\mathcal{A}$。

Secret-Value-Extract：收到对于用户 ID_U 的询问，则返回用户的秘密值 sk_U 给 $\mathcal{A}$。

Public-Key-Replace：收到对于用户身份信息和公钥的询问，则产生一个新的公钥替换原有的公钥。

Signcrypt：收到对于消息 m、发送者身份信息 ID_A、私钥 SK_A、公钥 PK_A、接收者的身份信息 ID_B 和公钥 PK_B 的询问，则返回签密密文 σ。

Unsigncrypt：收到对于密文 σ、接收者的私钥 SK_B、发送者身份 ID_A 和公钥 PK_A 的询问，则返回解密的明文 m。

· 不可伪造性

CLSC 方案的选择消息攻击的存在不可伪造性(EUF-CMA)是通过下列与类型 1 敌手和类型 2 敌手的两个游戏来定义的。

游戏 1 挑战者 $\mathcal{C}$ 与类型 1 敌手 $\mathcal{A}_1$ 完成如下的游戏：

初始化：挑战者 $\mathcal{C}$ 运行 Setup 算法，然后将返回的系统参数 *params* 交给 $\mathcal{A}_1$，秘密保存系统主密钥 *mk*。

询问：$\mathcal{A}_1$ 适应性地向挑战者 $\mathcal{C}$ 提交多项式绑定数量的 *Public-Key-Request*，*Partial-Pirvate-Key-Extract*，*Secret-Value-Extract*，*Public-Key-Replace*，*Signcrypt* 和 *Unsigncrypt* 询问。

输出：游戏结束，$\mathcal{A}_1$ 输出一个新的三元组 (ID_A^*, ID_B^*, σ)，这个三元组不是由 *Signcrypt* 询问得到的，其中 ID_A^* 和 ID_B^* 分别是发送者 A^* 和接收者 B^* 的身份信息。如果下列条件满足，则 $\mathcal{A}_1$ 赢得游戏：

(1)解签密的结果不是 $\perp$。

(2)$\mathcal{A}_1$ 不能提取 A^* 的部分私钥 D_A^*。

我们定义 $\mathcal{A}_1$ 在游戏 1 中成功的概率为

$Succ_{\mathcal{A}_1}^{EUF\text{-}CLSC\text{-}CMA}=\Pr[\mathcal{A}_1\ wins]$。

游戏 2 挑战者 $\mathcal{C}$ 与类型 2 敌手 $\mathcal{A}_2$ 完成如下的游戏：

初始化 挑战者运行 *Setup* 算法，然后将返回的系统参数 *params* 和系统主密钥 *mk* 交给 $\mathcal{A}_2$。

询问：$\mathcal{A}_2$ 适应性地向挑战者 $\mathcal{C}$ 提交多项式绑定数量的 Public-Key-Request，Partial-Pirvate-Key-Extract，Secret-Value-Extract，Signcrypt 和 Unsigncrypt 询问。

输出：游戏结束，$\mathcal{A}_2$ 输出一个新的三元组 (ID_A^*, ID_B^*, σ)，这个三元组不是由 *Signcrypt* 询问得到的，其中 ID_A^* 和 ID_B^* 分别是发送者 A^* 和接收者 B^* 的身份信息。如果下列条件满足，则 $\mathcal{A}_1$ 赢得游戏：

(3)解签密的结果不是 $\perp$。

(4)$\mathcal{A}_2$ 不能提取 A^* 的秘密值 sk_A^*。

我们定义 $\mathcal{A}_2$ 在游戏 2 中成功的概率为

$Succ_{\mathcal{A}_2}^{EUF\text{-}CLSC\text{-}CMA}=\Pr[\mathcal{A}_2\ wins]$

定义 3 如果不存在多项式时间绑定的敌手 $\mathcal{A}\mathcal{A}\in\{\mathcal{A}_1,\mathcal{A}_2\}$能以不可忽略的概率赢得上述两个游戏(游戏 1,游戏 2),则称一个 CLSC 方案满足 EUF-CMA 安全性。

· 机密性

无证书签密需满足的机密性(适应性选择密文攻击的不可区分性(IND-CCA2))是通过下列与类型 1 敌手和类型 2 敌手的两个游戏来定义的。

游戏 3 挑战者 $\mathcal{C}$ 与类型 1 敌手 $\mathcal{A}_1$ 完成如下的游戏:

初始化:挑战者 $\mathcal{C}$ 运行 *Setup* 算法,然后将返回的系统参数 *params* 交给 $\mathcal{A}_1$,秘密保存系统主密钥 *mk*。

阶段 1:$\mathcal{A}_1$ 适应性地向挑战者 $\mathcal{C}$ 提交多项式绑定数量的 *Public-Key-Request*, *Partial-Pirvate-Key-Extract*, *Secret-Value-Extract*, *Public-Key-Replace*, *Signcrypt* 和 *Unsigncrypt* 询问。

挑战:一旦敌手 $\mathcal{A}_1$ 决定结束游戏的第一阶段,他提交两个不同的身份 ID_{A^*} 和 ID_{B^*},和两条等长的不同消息 M_0 和 M_1,ID_{A^*} 和 ID_{B^*} 分别是发送者 A^* 和接收者 B^* 的身份信息。挑战者选取一个随机比特 β 并用 A^* 的私钥和 B^* 的公钥签密 M_β,产生密文 σ^*。挑战者 $\mathcal{C}$ 将 σ^* 发送给敌手 A_1。

阶段 2:敌手 $\mathcal{A}_1$ 如阶段 1 一样继续向挑战者发起相同类型的询问。

应答:$\mathcal{A}_1$ 输出一个比特 β' 作为对 β 的猜测。我们称敌手 $\mathcal{A}_1$ 赢得游戏,如果 $\beta'=\beta$,且满足下列限制条件:

(1)$\mathcal{A}_1$ 不能提取 B^* 的部分私钥;

(2)在阶段 2,$\mathcal{A}_1$ 不能对挑战密文 σ^* 做 *Unsigncrypt* 询问,除非用于签密 M_b 的发送者的公钥 PK_{A^*} 或者接收者的公钥 PK_{B^*} 在挑战提交之后已经被替换了。

我们定义 $\mathcal{A}_1$ 成功的优势为

$$Succ_{\mathcal{A}_1}^{IND\text{-}CLSC\text{-}CCA2}=|2\Pr[\beta'=\beta]-1|$$

其中,$\Pr[\beta'=\beta]$表示 $\beta'=\beta$ 的概率。

游戏 4 挑战者 $\mathcal{C}$ 与类型 2 敌手 $\mathcal{A}_2$ 完成如下的游戏:

初始化:挑战者运行 *Setup* 算法,然后将返回的系统参数 *params* 和系统主密钥 *mk* 交给 $\mathcal{A}_2$。

阶段 1:$\mathcal{A}_2$ 适应性地向挑战者 $\mathcal{C}$ 提交多项式绑定数量的 *Public-Key-Request*, *Partial-Pirvate-Key-Extract*, *Secret-Value-Extract*, *Signcrypt* 和 *Unsigncrypt* 询问。

挑战:一旦敌手 $\mathcal{A}_2$ 决定结束游戏的第一阶段,他提交两个不同的身份 ID_{A^*} 和 ID_{B^*},和两条等长的不同消息 M_0 和 M_1,ID_{A^*} 和 ID_{B^*} 分别是发送者 A^* 和接收者 B^* 的身份信息。挑战者选取一个随机比特 β 并用 A^* 的私钥和 B^* 的公钥签密 M_β,产生密文 σ^*。挑战者 $\mathcal{C}$ 将 σ^* 发送给敌手 $\mathcal{A}_2$。

阶段 2:敌手 $\mathcal{A}_2$ 如阶段 1 一样继续向挑战者发起相同类型的询问。

应答:$\mathcal{A}_2$ 输出一个比特 β' 作为对 β 的猜测。我们称敌手 $\mathcal{A}_2$ 赢得游戏,如果 $\beta'=\beta$,且满足下列限制条件:

(1)$\mathcal{A}_2$ 不能提取 B^* 的部分私钥;

(2)在阶段 2,$\mathcal{A}_2$ 不能对挑战密文 σ^* 做 *Unsigncrypt* 询问。

我们定义 $\mathcal{A}_2$ 成功的优势为

$$Succ_{\mathcal{A}_2}^{IND\text{-}CLSC\text{-}CCA2}=|2\Pr[\beta'=\beta]-1|$$

其中,$\Pr[\beta'=\beta]$ 表示 $\beta'=\beta$ 的概率。

定义 4 如果不存在多项式时间绑定敌手 $\mathcal{A}\in\{\mathcal{A}_1,\mathcal{A}_2\}$ 能以不可忽略的优势赢得上述游戏(游戏 3,游戏 4),则称一个 CLSC 方案满足 IND-CCA2 安全性。

3 Jing 等人的无证书签密方案及其安全性分析

在这一节,我们回顾和分析 Jing 等人的无证书签密方案[21]。通过具体的攻击,我们得出 Jing 等人的方案既不满足不可伪造性也不满足机密性。而且这种攻击方法同样可成功攻击 Zhu 等人的方案[19]和 Liu 等人的方案[20]。由于篇幅限制,我们不详细介绍对这两个方案的攻击。

3.1 Jing 等人的无证书签密方案

Jing 等人的方案由下列 7 个算法构成:*Setup*, *SetSecretValue*, *PartialPirvateKeyExtract*, *SetPrivateKey*, *SetPublicKey*, *Signcrypt* 和 *Unsigncrypt*。

Setup:输入安全参数 k,KGC 按照下列步骤产生主密钥 *mk* 和系统公开参数 *param*。

1)产生两个大素数 p 和 q,满足 $p=2q+1$,选择一个 q 阶生成元 g,q 的长度为 k;

2)随机均匀地选取 $x\in Z_q^*$,并计算 $y=g^x \bmod p$;

3)选择 hash 函数 $H_1:\{0,1\}^*\times Z_p^*\rightarrow Z_q^*$,$H_2:\{0,1\}^*\times\{0,1\}^*\times Z_p^*\times Z_p^*\times\{0,1\}^n\times\{0,1\}^n\rightarrow\{0,1\}^*$ 和 $H_3:Z_p^*\times Z_p^*\rightarrow\{0,1\}^n$,其中 n 是待签密消息的长度;

4)输出系统参数 $param=(p,q,g,y,H_1,H_2,H_3)$ 和主密钥 $mk=x$。

SetSecretValue:输入系统参数 *param*,用户 U 按下列步骤产生秘密值 *sk* 和公钥 *pk*:

1)随机选取 $z_U\in Z_q^*$,计算 $u_U=g^{z_U}$;

2)返回$(sk_U,pk_U)=(z_U,u_U)$。

PartialPirvateKeyExtract:输入 *param*,*mk* 和用户的身份信息 ID_U,KGC 按下列步骤产生用户的部分私钥 D_U 和部分公钥 P_U:

1)随机选取 $s_U\in Z_q^*$,计算 $w_U=g^{s_U} \bmod p$ 和 $t_U=(s_U+xH_1(ID_U,w_U)) \bmod q$;

2)输出$(D_U,P_U)=(t_U,w_U)$。

SetPrivateKey:输入 *param*,D_U 和 sk_U,用户设置其私钥为 $SK_U=(sk_U,D_U)=(z_U,t_U)$。

SetPublicKey:输入 *param*,P_U 和 pk_U,用户设置其公钥为 $PK_U=(pk_U,P_U)=(u_U,w_U)$。

Signcrypt:输入明文 M,系统参数 *param*,发送者的身份信息 ID_A 和私钥 SK_A,接收者的身份信息 ID_B 和公钥 PK_B,发送者 A 运行下列步骤计算签密密文 C:

1)随机选取 $r_A\in Z_q^*$ 并计算 $c_1=g^{r_A} \bmod p$;

2)计算 $c_2=H_3(c_1,(u_Bw_By^{H_1(ID_B,w_B)})^{z_A+t_A+r_A} \bmod p)\oplus M$ 和 $c_3=H_2(ID_A,ID_B,c_1,(u_Bw_By^{H_1(ID_B,w_B)})^{z_A+t_A+r_A} \bmod p,M,c_2)$;

3)输出密文 $C=(c_1,c_2,c_3)$。

Unsigncrypt:输入密文 C,系统参数 *param*,发送者的身份信息 ID_A 和公钥 PK_A,接收者的身份信息 ID_B 和私钥 SK_B,接收者运行以下步骤解密,结果是明文信息或者一条"拒绝"信息:

1)计算 $M=H_3(c_1,(c_1u_Aw_Ay^{H_1(ID_A,w_A)})^{z_B+t_B} \bmod p)\oplus$

c_2；

2)若 $c_3 = H_2(ID_A, ID_B, c_1, (c_1 u_A w_A y^{H_1(ID_A, w_A)})^{z_B + t_B} \bmod p, M, c_2)$，则返回 M；否则返回一条“拒绝”信息。

3.2 Jing 等人方案的安全性分析

·不可伪造性

Jing 等人声称他们的方案对于 CLPKC 下的两类敌手都满足不可伪造性。本节我们通过一个具体攻击表明类型 1 敌手 $\mathcal{A}_1$ 能伪造合法密文。$\mathcal{A}_1$ 能按照下列步骤伪造合法密文：

1)$\mathcal{A}_1$ 随机选择 $a \in Z_q^*$，并计算 $u_A' = \frac{g^a}{w_A y^{H_1(ID_A, w_A)}} \bmod p$；

2)$\mathcal{A}_1$ 用 u_A' 替换 u_A；

3)$\mathcal{A}_1$ 随机选择 $r_A \in Z_q^*$ 并计算 $c_1 = g^{r_A} \bmod p$；

4)$\mathcal{A}_1$ 计算 $c_2 = H_3(c_1, (u_B w_B y^{H_1(ID_B, w_B)})^{a + r_A} \bmod p) \oplus M$ 和 $c_3 = H_2(ID_A, ID_B, c_1, (u_B w_B y^{H_1(ID_B, w_B)})^{a + r_A} \bmod p, M, c_2)$；

5)$\mathcal{A}_1$ 输出伪造密文 $C = (c_1, c_2, c_3)$。

由于 $u_B = g^{z_B}$，$w_B = g^{s_B} \bmod p$，$t_B = (s_B + x H_1(ID_B, w_B)) \bmod q$，因此可得

$$\begin{aligned}
&(c_1 u_A' w_A y^{H_1(ID_A, w_A)})^{z_B + t_B} \bmod p \\
&= (c_1 \frac{g^a}{w_A y^{H_1(ID_A, w_A)}} w_A y^{H_1(ID_A, w_A)})^{z_B + t_B} \bmod p \\
&= (g^{r_A} g^a)^{z_B + t_B} \bmod p = (g^{a + r_A})^{z_B + t_B} \bmod p \\
&= (g^{z_B + t_B})^{a + r_A} \bmod p = (u_B w_B y^{H_1(ID_B, w_B)})^{a + r_A} \bmod p
\end{aligned} \tag{1}$$

和

$$\begin{aligned}
c_3 &= H_2(ID_A, ID_B, c_1, (u_B w_B y^{H_1(ID_B, w_B)})^{a + r_A} \bmod p, M, c_2) \\
&= H_2(ID_A, ID_B, c_1, (c_1 u_A' w_A y^{H_1(ID_A, w_A)})^{z_B + t_B} \bmod p, M, c_2)
\end{aligned} \tag{2}$$

因此，伪造的签密密文能通过接收者 B 的验证。

从以上攻击看出，类型 1 敌手 $\mathcal{A}_1$ 能伪造合法的密文，所以，Jing 等人的方案不满足不可伪造性。

·机密性

Jing 等人声称他们的方案对于 CLPKC 的两类敌手都满足机密性。在本节我们通过具体的攻击表明类型 1 敌手 $\mathcal{A}_1$ 能解密有效密文。$\mathcal{A}_1$ 能按照下列步骤解密密文：

1)$\mathcal{A}_1$ 随机选择 $b \in Z_q^*$，计算 $u'_B = \frac{g^b}{w_B y^{H_1(ID_B, w_B)}} \bmod p$；

2)$\mathcal{A}_1$ 用 u'_B 替换 u_B；

3)发送者 A 随机选择 $r_A \in Z_q^*$，计算 $c_1 = g^{r_A} \bmod p$；

4)A 计算 $c_2 = H_3(c_1, (u_B' w_B y^{H_1(ID_B, w_B)})^{z_A + t_A + r_A} \bmod p) \oplus M$ 和 $c_3 = H_2(ID_A, ID_B, c_1, (u_B' w_B y^{H_1(ID_B, w_B)})^{z_A + t_A + r_A} \bmod p, M, c_2)$；

5)A 输出密文 $C = (c_1, c_2, c_3)$；

6)$\mathcal{A}_1$ 计算 $M = H_3(c_1, (c_1 u_A w_A y^{H_1(ID_A, w_A)})^b \bmod p) \oplus c_2$。

由于 $u_A = g^{z_A}$，$w_A = g^{s_A} \bmod p$，$t_A = (s_A + x H_1(ID_A, w_A)) \bmod q$，$u_B' = \frac{g^b}{w_B y^{H_1(ID_B, w_B)}} \bmod p$，因此可得

$$\begin{aligned}
&(u_B' w_B y^{H_1(ID_B, w_B)})^{z_A + t_A + r_A} \bmod p \\
&= (\frac{g^b}{w_B y^{H_1(ID_B, w_B)}} w_B y^{H_1(ID_B, w_B)})^{z_A + t_A + r_A} \bmod p \\
&= (g^b)^{z_A + t_A + r_A} \bmod p = (g^{z_A + t_A + r_A})^b \bmod p \\
&= (c_1 u_A w_A y^{H_1(ID_A, w_A)})^b \bmod p
\end{aligned} \tag{3}$$

和

$$\begin{aligned}
&H_3(c_1, (c_1 u_A w_A y^{H_1(ID_A, w_A)})^b \bmod p) \\
&= H_3(c_1, (u_B' w_B y^{H_1(ID_B, w_B)})^{z_A + t_A + r_A} \bmod p)
\end{aligned} \tag{4}$$

从上面的攻击看出，类型 1 敌手 $\mathcal{A}_1$ 能得到明文信息，因此 Jing 等人的方案不满足机密性。

4 我们的无证书签密方案

我们的无证书签密方案由以下 7 个概率多项式时间算法构成：

Setup：输入安全参数 k，KGC 根据下列步骤产生主密钥 mk 和系统参数 $param$：

1)产生两个大素数 p 和 q，满足 $p = 2q + 1$，选择一个 q 阶生成元 g，其中 q 的长度为 k；

2)随机均匀选择 $x \in Z_q^*$，并计算 $y = g^x \bmod p$；

3)选择 Hash 函数 $H_1: \{0,1\}^* \times Z_p^* \to Z_q^*$，$H_2: \{0,1\}^* \times Z_p^* \times Z_p^* \times Z_p^* \to Z_q^*$，$H_3: Z_p^* \times Z_p^* \to \{0,1\}^n$ 和 $H_4: \{0,1\}^* \times Z_p^* \times Z_p^* \times \{0,1\}^n \times Z_p^* \to Z_q^*$，其中 n 是待签密消息的长度；

4)返回系统参数 $param = (p, q, g, y, H_1, H_2, H_3)$ 和主密钥 $mk = (p, q, g, x, H_1, H_2, H_3)$。

SetSecretValue：输入系统参数 $param$，用户 U 按下列步骤产生秘密值 sk 和公钥 pk：

1) 随机选择 $z_U \in Z_q^*$，计算 $u_U = g^{z_U}$；

2) 返回 $(sk_U, pk_U) = (z_U, u_U)$。

PartialPrivateKeyExtract：输入 $param$，mk，用户的身份信息 ID_U，KGC 按以下步骤产生用户的部分私钥 D_U 和部分公钥 P_U：

1)随机选择 $s_U \in Z_q^*$，计算 $w_U = g^{s_U} \bmod p$ 和 $t_U = (s_U + x H_1(ID_U, w_U)) \bmod q$；

2)返回 $(D_U, P_U) = (t_U, w_U)$。

SetPrivateKey：输入 $param$，D_U 和 sk_U，用户产生完整私钥 $SK_U = (sk_U, D_U) = (z_U, t_U)$。

SetPublicKey：输入 $param$，P_U 和 pk_U，用户产生完整公钥 $PK_U = (pk_U, P_U) = (u_U, w_U)$。

Signcrypt：输入明文信息 M，系统参数 $param$，发送者的身份信息 ID_A 和私钥 SK_A，接收者的身份信息 ID_B 和公钥 PK_B，发送者 A 运行下列步骤计算签密密文 C：

1)随机选择 $r_A \in Z_q^*$，计算 $c_1 = g^{r_A} \bmod p$；

2)计算 $k_A = H_2(ID_A, u_A, w_A, y)$，$k_B = H_2(ID_B, u_B, w_B, y)$ 和 $h_B = H_1(ID_B, w_B)$；

3)计算 $\xi = (u_B^{k_B} w_B y^{h_B})^{r_A} \bmod p$，$c_2 = H_3(\xi) \oplus M$ 和 $c_3 = \frac{k_A z_A + t_A}{r_A + h} \bmod q$，其中 $h = H_4(ID_A, u_A, w_A, c_1, c_2, \xi, M)$；

4)返回 $C = (c_1, c_2, c_3)$。

Unsigncrypt：输入密文 C，系统参数 $param$，发送者的身份信息 ID_A 和公钥 PK_A，接收者的身份信息 ID_B 和私钥 SK_B，接收者运行以下步骤解密，结果是明文信息或者一条

"拒绝"信息：

1)计算 $h_A=H_1(ID_A,w_A)$，$h_B=H_1(ID_B,w_B)$，$k_A=H_2(ID_A,u_A,w_A,y)$，$k_B=H_2(ID_B,u_B,w_B,y)$，$\xi=(c_1)^{k_B z_B+t_B} \bmod p$ 和 $M=c_2\oplus H_3(\xi)$；

2)计算 $h=H_4(ID_A,u_A,w_A,c_1,c_2,\xi,M)$；

3)若 $(c_1 g^h)^{c_3}=u_A^{k_A} w_A y^{h_A} \bmod p$，返回 M；否则返回"拒绝"信息。

5 安全性分析

本节我们将证明我们的无证书签密方案在随机预言机模型下是可证明安全的，在证明时将 hash 函数 H_1、H_2、H_3 和 H_4 都模拟为随机预言机。我们将通过证明以下定理来证明方案的安全性。

定理 1 我们的 CLSC 方案是在随机预言机模型下是 EUF-CMA 安全的当且仅当离散对数假设成立。

此定理将由引理 1 和引理 2 得出。由于两个引理证明是类似的，为节省篇幅，我们仅给出引理 1 的详细证明。

引理 1 如果类型 1 敌手 $\mathcal{A}_1$ 能以不可忽略的概率 $\varepsilon=Succ_{\mathcal{A}_1}^{EUF\text{-}CLSC\text{-}CMA}$ 赢得游戏 1，则我们能构造一个算法 $\mathcal{C}$ 以不可忽略的概率 $\varepsilon'\geqslant\frac{1}{q_{H_1}}(1-\frac{1}{q_{H_1}})^{q_{PPK}} Succ_{\mathcal{A}_1}^{EUF\text{-}CLSC\text{-}CMA}$ 解离散对数问题(DLP)，其中 q_{H_1} 和 q_{PPK} 分别表示 H_1 询问和 *Partial-Private-Key-Extract* 询问的次数。

证明：假设类型 1 敌手 $\mathcal{A}_1$ 能以不可忽略的概率 ε 赢得游戏 1。我们将构造算法 $\mathcal{C}$ 利用 $\mathcal{A}_1$ 解 DLP 问题。$\mathcal{C}$ 收到一个 DLP 实例 (p,q,g,g^a)，其中 $a\in Z_q^*$ 是随机数，其目标是计算 a。$\mathcal{C}$ 随机选择一个用户身份为 ID^*，并按以下方式回答 A_1 的询问：

Setup：$\mathcal{C}$ 设置 $y=g^a \bmod p$，$param=(p,q,g,y,H_1,H_2,H_3,H_4)$，$mk=\perp$。$\mathcal{C}$ 将 *param* 给 $\mathcal{A}_1$；

H_1-query：当 $\mathcal{A}_1$ 对 (ID,w) 做 H_1 询问时，若 *H_1-List* 中包含 $\langle ID,w,h_1\rangle$ 条目，$\mathcal{C}$ 直接返回 h_1 给 $\mathcal{A}_1$；否则 $\mathcal{C}$ 随机选择 $h_1\in Z_q^*$，返回 h_1 给 $\mathcal{A}_1$，并将新条目 $\langle ID,w,h_1\rangle$ 添加到 *H_1-List* 中；

H_2-query：当 $\mathcal{A}_1$ 对 (ID_U,u_U,w_U,y) 做 H_2 询问时，若 *H_2-List* 中包含 $\langle ID_U,u_U,w_U,y,h_2\rangle$ 条目，$\mathcal{C}$ 直接返回 h_2 给 $\mathcal{A}_1$；否则 $\mathcal{C}$ 随机选择 $h_2\in Z_q^*$，返回 h_2 给 $\mathcal{A}_1$，并将新条目 $\langle ID_U,u_U,w_U,y,h_2\rangle$ 添加到 *H_2-List* 中；

H_3-query：当 $\mathcal{A}_1$ 对 $(\tilde{\omega})$ 做 H_3 询问时，若 *H_3-List* 中包含 $\langle\tilde{\omega},h_3\rangle$ 条目，$\mathcal{C}$ 直接返回 h_3 给 $\mathcal{A}_1$；否则，$\mathcal{C}$ 随机选择 $h_3\in\{0,1\}^n$，返回 h_3 给 $\mathcal{A}_1$，并将新条目 $\langle\tilde{\omega},h_3\rangle$ 添加到 *H_3-List* 中；

H_4-query：当 $\mathcal{A}_1$ 对 $(ID_U,u_U,w_U,c_1,c_2,\xi,m)$ 做 H_4 询问时，若 *H_4-List* 中包含 $(ID_U,u_U,w_U,c_1,c_2,\xi,m,h_4)$ 条目，$\mathcal{C}$ 直接返回 h_4 给 A_1；否则，$\mathcal{C}$ 随机选择 $h_4\in Z_q^*$，返回 h_4 给 $\mathcal{A}_1$，并将新条目 $\langle ID_U,u_U,w_U,c_1,c_2,\xi,m,h_4\rangle$ 添加到 *H_4-List* 中；

Public-Key-Request：当 $\mathcal{A}_1$ 对 ID_U 做此询问时，$\mathcal{C}$ 做如下反应：

• 若 $\langle ID_U,u_U,w_U\rangle$ 在 *PublicKey-List* 中，$\mathcal{C}$ 直接返回 $PK_U=(u_U,w_U)$；

• 若 $ID_U\neq ID^*$，$\mathcal{C}$ 随机选择 $z_U,t,h\in Z_q^*$，计算 $u_U=g^{z_U} \bmod p$ 和 $w_U=g^t y^{-h} \bmod p$。然后 $\mathcal{C}$ 将 $\langle ID_U,w_U,-h\rangle$，$\langle ID_U,z_U,t_U\rangle$ 和 $\langle ID_U,u_U,w_U\rangle$ 分别加入到 *H_1-List*，*PrivateKey-List* 和 *PublicKey-List* 中。最后，$\mathcal{C}$ 返回 $PK_U=(u_U,w_U)$。注意到根据部分私钥生成算法，$(w_U,t_U,H_1(ID_U,w_U))$ 满足等式 $g^{t_U}=w_U y^{H_1(ID_U,w_U)}$；

• 否则，若 $ID_U=ID^*$，$\mathcal{C}$ 随机选择 $z_U,s_U\in Z_q^*$，计算 $u_U=g^{z_U} \bmod p$，$w_U=g^{s_U} \bmod p$，并将 $\langle ID,(z_U,*),s_U\rangle$（$*$ 代表任意值）加入到 *PrivateKey-List* 中，将 $\langle ID_U,u_U,w_U\rangle$ 加入到 *PublicKey-List* 中。最后 $\mathcal{C}$ 返回 $PK_U=(u_U,w_U)$；

Secret-Value-Extract：当 $\mathcal{A}_1$ 对 ID_U 做此询问时，$\mathcal{C}$ 做如下反应：

• $\mathcal{C}$ 对 ID_U 运行 *Public-Key-Request*，从 *Public Key-List* 中得到一个条目 $\langle ID_U,u_U,w_U\rangle$；

• $\mathcal{C}$ 从 *PrivateKey-List* 中搜索 $\langle ID_U,z_U,t_U\rangle$，并返回对应的 z_U；

Partial-Pirvate-Key-Extract：当 $\mathcal{A}_1$ 对 ID_U 做此询问时，$\mathcal{C}$ 做如下反应：

• $\mathcal{C}$ 对 ID_U 运行 *Public-Key-Request*，从 *Public Key-List* 中得到一个条目 $\langle ID_U,u_U,w_U\rangle$；

• 若 $ID_U\neq ID^*$，$\mathcal{C}$ 从 *PrivateKey-List* 中搜索 $\langle ID_U,z_U,t_U\rangle$，并返回对应的 t_U；

• 否则，$\mathcal{C}$ 返回"中止"信息并停止游戏；

Public-Key-Replace：当 $\mathcal{A}_1$ 对 (ID_U,u_U,w_U,u_U',w_U') 做此询问时，$\mathcal{C}$ 做如下反应：

• $\mathcal{C}$ 对 ID_U 运行 *Public-Key-Request*，从 *Public Key-List* 中得到一个条目 $\langle ID_U,u_U,w_U\rangle$；

• $\mathcal{C}$ 用 (u_U',w_U') 替换 (u_U,w_U)；

Signcrypt：当 $\mathcal{A}_1$ 对 (ID_A,PK_A,ID_B,PK_B,M) 做此询问时，$\mathcal{C}$ 做如下反应：

• 若 $ID_A\neq ID^*$，由于 $\mathcal{C}$ 知道私钥 $SK_A=(z_A,t_A)$，$\mathcal{C}$ 按照第 4 节 *Signcrypt* 算法的规范做回复。$\mathcal{C}$ 将 $(ID_A,PK_A,ID_B,PK_B,M,C)$ 加入到 *Signcrypt-List* 中，并返回密文 $C=(c_1,c_2,c_3)$；

• 否则，若 $ID_A=ID^*$ 且 $ID_B\neq ID^*$，$\mathcal{C}$ 产生两个随机数 $c_3,h\in Z_q^*$，设置 $c_1\leftarrow\frac{(u_A^{k_A} w_A y^{h_A})^{c_3^{-1}}}{g^h} \bmod p$ 和 $c_2\leftarrow M\oplus H_3((c_1)^{k_B z_B+t_B} \bmod p)$。$\mathcal{C}$ 将 $(ID_A,PK_A,ID_B,PK_B,M,C)$ 和 (ID_A,u_A,w_A,M,c_1,h) 分别加入到 *Signcrypt-List* 和 *H_1-List* 中，并返回密文 $C=(c_1,c_2,c_3)$；

Unsigncrypt：当 $\mathcal{A}_1$ 对 (ID_A,PK_A,ID_B,PK_B,C) 做此询问时，$\mathcal{C}$ 做如下反应：

• 若 $ID_B\neq ID^*$，由于 $\mathcal{C}$ 知道私钥 $SK_A=(z_A,t_A)$，$\mathcal{C}$ 根据第 4 节的 *Unsigncrypt* 算法运行结果给出回复；

• 否则，若 $ID_B=ID^*$ 且 $ID_A\neq ID^*$，$\mathcal{C}$ 检查 $(ID_A,PK_A,ID_B,PK_B,*,C)$ 是否在 *Signcrypt-List* 中，若在 *Signcrypt-List* 中存在一个条目 $(ID_A,PK_A,ID_B,PK_B,M,C)$，$\mathcal{C}$ 返回 M 作为回复；否则，$\mathcal{C}$ 返回"拒绝"信息。

最后，$\mathcal{A}_1$ 输出一条 ID_A 给 ID_B 的签密密文 $C=(c_1,c_2,c_3)$，其中 ID_A 和 ID_B 分别是发送者和接收者的身份信息。若 $ID_A\neq ID^*$，$\mathcal{C}$ 返回"中止"信息并结束游戏；否则，若 $ID_A=ID^*$ 且 $ID_B\neq ID^*$，$\mathcal{C}$ 分别从列表 *PrivateKey-List* 和 *PublicKey-List* 搜索 $\langle ID_B,z_B,t_B\rangle$ 和 $\langle ID_A,u_A,w_A\rangle$。注意到 ID_A

公钥 $PK_A=(u_A,w_A)$ 可能是被 $\mathscr{A}_1$ 替换的公钥。$\mathscr{C}$ 通过计算 $M=c_2\oplus H_3((c_1)^{k_B x_B+t_B} \bmod p)$ 恢复出明文。很容易看出 $\sigma=(c_1,c_3)$ 是消息 M 的签名。令 $\sigma^{(1)}=(c_1^{(1)},c_3^{(1)})$ 表示第一个签名。由分叉引理[22]，若对于相同的输入随机预言机 H_1，H_2 和 H_4 的输入，有不同的输出值，$\mathscr{A}_1$ 将输出其他 3 个签名 $\sigma^{(i)}=(c_1,c_3^{(i)})$，$(i=2,3,4)$。因为它们是有效的签名，所以下列等式成立

$$(c_1 g^{h^{(i)}})^{c_3^{(i)}}=u_A^{k_A^{(i)}} w_A y^{h_A^{(i)}} \bmod p \tag{5}$$

我们用 r_A,z_A,s_A 和 a，分别表示 c_1,u_A,w_A 和 y 的离散对数结果，即，$c_1=g^{r_A} \bmod p$，$u_A=g^{z_A} \bmod p$，$w_A=g^{s_A} \bmod p$ 和 $y=g^a \bmod p$。从式(5)我们可得以下等式

$$c_3^{(i)} r_A+c_3^{(i)} h^{(i)}=k_A^{(i)} z_A+s_A+h_A^{(i)} a \bmod q,\ i=1,2,3,4 \tag{6}$$

在上面的等式中，对于 $\mathscr{C}$，只有 r_A,z_A,s_A 和 a 是未知的。$\mathscr{C}$ 可以通过解上述方程组，计算出 a。a 就是离散对数问题的解。

分析：通过分析下列事件来分析 $\mathscr{C}$ 成功解离散对数问题的概率。

E_1：$\mathscr{C}$ 在所有的 *Partial-Pirvate-Key-Extract* 询问中不“中止”游戏。

E_2：$\mathscr{A}_1$ 输出一条 ID_A 给 ID_B 的签密密文 $C=(c_1,c_2,c_3)$，其中 ID_A 和 ID_B 分别是发送者和接收者的身份信息。

E_3：$\mathscr{A}_1$ 输出一条 ID_A 给 ID_B 的签密密文 $C=(c_1,c_2,c_3)$ 且满足 $ID_A=ID^*$；

从以上的模拟游戏可知，$\Pr[E_1]\geqslant(1-\frac{1}{q_{H_1}})^{q_{PPK}}$，$\Pr[E_2|E_1]\geqslant Succ_{\mathscr{A}_1}^{EUF\text{-}CLSC\text{-}CMA}$，$\Pr[E_3|E_1\wedge E_2]\geqslant\frac{1}{q_{H_1}}$，其中 q_{H_1} 和 q_{PPK} 分别表示 H_1 询问和 *Partial-Private-Key* 询问的次数。$\mathscr{C}$ 解离散对数问题的成功概率为

$$\begin{aligned}\varepsilon'&=\Pr[E_1\wedge E_2\wedge E_3]\\&=\Pr[E_1]\Pr[E_2|E_1]\Pr[E_3|E_1\wedge E_2]\\&\geqslant\frac{1}{q_{H_1}}(1-\frac{1}{q_{H_1}})^{q_{PPK}} Succ_{\mathscr{A}_1}^{EUF\text{-}CLSC\text{-}CMA}\end{aligned} \tag{7}$$

因此 $\mathscr{C}$ 能以不可忽略的优势解离散对数问题。这与离散对数假设矛盾。所以我们的无证书签密方案，在离散对数假设成立的条件下，对于类型 1 敌手在随机预言机模型下满足存在不可伪造性。

引理 2 假设存在类型 2 敌手 $\mathscr{A}_2$ 能以不可忽略的优势 $Succ_{\mathscr{A}_2}^{EUF\text{-}CLSC\text{-}CMA}$ 赢得游戏 2。我们可以构造算法 $\mathscr{C}$ 以不可忽略的优势 $\varepsilon'\geqslant\frac{1}{q_{H_1}}(1-\frac{1}{q_{H_1}})^{q_{SV}} Succ_{\mathscr{A}_2}^{EUF\text{-}CLSC\text{-}CMA}$ 解离散对数问题，其中 q_{H_1} 和 q_{SV} 分别表示 H_1 询问和 *Secret-Value -Extract* 询问的次数。

定理 2 在 CDHP 困难问题假设成立的条件下，我们的无证书签密方案满足随机预言机模型下的 IND-CCA2 安全性。

此定理将由引理 3 和引理 4 得出。由于两个引理证明是类似的，为节省篇幅，我们仅给出引理 4 的详细证明。

引理 3 如果类型 1 敌手 $\mathscr{A}_1$ 能以不可忽略的概率 $Succ_{\mathscr{A}_1}^{IND\text{-}CLSC\text{-}CCA2}$ 赢得游戏 3，则我们能构造一个算法 $\mathscr{C}$ 以不可忽略的概率 $\varepsilon'\geqslant\frac{1}{q_{H_1}}(1-\frac{1}{q_{H_1}})^{q_{PPK}} Succ_{\mathscr{A}_1}^{IND\text{-}CLSC\text{-}CCA2}$ 解计算 Diffie-Hellman 问题(CDHP)，其中 q_{H_1} 和 q_{PPK} 分别表示 H_1 询问和 *Partial-Pirvate-Key-Extract* 询问的次数。

引理 4 如果类型 2 敌手 $\mathscr{A}_2$ 能以不可忽略的概率 $\varepsilon=Succ_{\mathscr{A}_2}^{IND\text{-}CLSC\text{-}CCA2}$ 赢得游戏 4，则我们能构造一个算法 $\mathscr{C}$ 以不可忽略的概率 $\varepsilon'\geqslant\frac{1}{q_{H_1}}(1-\frac{1}{q_{H_1}})^{q_{SV}} Succ_{\mathscr{A}_2}^{IND\text{-}CLSC\text{-}CCA2}$ 解计算 Diffie-Hellman 问题(CDHP)，其中 q_{H_1} 和 q_{SV} 分别表示 H_1 询问和 *Secret-Value-Extract* 询问的次数。

证明：假设类型 2 敌手 $\mathscr{A}_2$ 能以不可忽略的概率 ε 赢得游戏 4。假设 H_1,H_2,H_3 和 H_4 为随机预言机[22]。我们将构造算法 $\mathscr{C}$ 利用 $\mathscr{A}_2$ 解 CDHP 问题。$\mathscr{C}$ 收到一个 CDHP 实例 (p,q,g,g^a,g^b)，其中 $a,b\in Z_q^*$ 是随机数，其目标是计算 $g^{ab} \bmod p$。

第一阶段

$\mathscr{C}$ 如引理 1 中一样回答 H_1,H_2,H_3 和 H_4 询问，并按下列方式回复 $\mathscr{A}_2$ 的其他询问：

Setup：$\mathscr{C}$ 随机选择 $x\in Z_q^*$ 并计算 $y=g^x \bmod p$，设置系统参数为 $param=(p,q,g,y,H_1,H_2,H_3,H_4)$，主密钥为 $mk=x$。然后 $\mathscr{C}$ 将 *param* 和 *mk* 发送给 $\mathscr{A}_2$；

Public-Key-Request：当 $\mathscr{A}_2$ 对 ID_U 做此询问时，$\mathscr{C}$ 做如下反应：

- 若 $\langle ID_U,u_U,w_U\rangle$ 在 *PublicKey-List* 中，$\mathscr{C}$ 直接返回 $PK_U=(u_U,w_U)$；
- 若 $ID_U\neq ID^*$，$\mathscr{C}$ 随机选择 $s_U,z_U,h_1\in Z_q^*$，计算 $u_U=g^{z_U} \bmod p$，$w_U=g^{s_U} \bmod p$ 和 $t_U=(s_U+xH_1(ID_U,w_U)) \bmod q$。然后 $\mathscr{C}$ 将 $\langle ID_U,w_U,h_1\rangle$，$\langle ID_U,z_U,t_U\rangle$ 和 $\langle ID_U,u_U,w_U\rangle$ 分别加入到 H_1-*List*，*PrivateKey-List* 和 *PublicKey-List* 中。最后，$\mathscr{C}$ 返回 $PK_U=(u_U,w_U)$；
- 否则，$\mathscr{C}$ 随机选择 $s_U,z_U,h_1\in Z_q^*$，计算 $w_U=g^{s_U} \bmod p$，$t_U=(s_U+xH_1(ID_U,w_U)) \bmod q$，设置 $u_U\leftarrow g^a$，并将 $\langle ID_U,w_U,h_1\rangle$，$\langle ID_U,*,t_U\rangle$（$*$ 代表任意值），$\langle ID_U,u_U,w_U\rangle$ 分别加入到 H_1-*List*，*PrivateKey-List* 和 *PublicKey-List* 中。最后，$\mathscr{C}$ 返回 $PK_U=(u_U,w_U)$；

Secret-Value-Extract：当 $\mathscr{A}_2$ 对 ID_U 做此询问时，$\mathscr{C}$ 做如下反应：

- $\mathscr{C}$ 对 ID_U 运行 *Public-Key-Request*，从 *Public Key-List* 中得到一个条目 $\langle ID_U,u_U,w_U\rangle$；
- 若 $ID_U\neq ID^*$，$\mathscr{C}$ 从 *PrivateKey-List* 中搜索 $\langle ID_U,z_U,t_U\rangle$，并返回对应的 z_U；
- 否则，$\mathscr{C}$ 返回“中止”信息，并停止游戏；

Partial-Pirvate-Key-Extract：当 $\mathscr{A}_2$ 对 ID_U 做此询问时，$\mathscr{C}$ 做如下反应：

- $\mathscr{C}$ 对 ID_U 运行 *Public-Key-Request*，从 *Public Key-List* 中得到一个条目 $\langle ID_U,u_U,w_U\rangle$；
- $\mathscr{C}$ 从 *PrivateKey-List* 中搜索 $\langle ID_U,z_U,t_U\rangle$，并返回对应的 t_U；

Signcrypt：当 $\mathscr{A}_2$ 对 (ID_A,PK_A,ID_B,PK_B,M) 做此询问时，$\mathscr{C}$ 做如下反应：

- 若 $ID_A\neq ID^*$，由于 $\mathscr{C}$ 知道私钥 $SK_A=(z_A,t_A)$，$\mathscr{C}$ 按照第 4 节 *Signcrypt* 算法的规范做回复。$\mathscr{C}$ 将 $(ID_A,PK_A,ID_B,PK_B,M,C)$ 加入到 *Signcrypt-List* 中，并返回密文 $C=$

(c_1, c_2, c_3)；

• 否则，若 $ID_A = ID^*$ 且 $ID_B \neq ID^*$，$\mathscr{C}$ 产生两个随机数 $c_3, h \in Z_q^*$，设置 $c_1 \leftarrow \frac{(u_A^{k_A} w_A y^{h_A})^{c_3^{-1}}}{g^h} \bmod p$ 和 $c_2 \leftarrow M \oplus H_3((c_1)^{k_B z_B + t_B} \bmod p)$。$\mathscr{C}$ 将 $(ID_A, PK_A, ID_B, PK_B, M, C)$ 和 $(ID_A, u_A, w_A, M, c_1, h)$ 分别加入到 *Signcrypt-List* 和 H_1-*List* 中，并返回密文 $C=(c_1, c_2, c_3)$；

Unsigncrypt：当 A_2 对 $(ID_A, PK_A, ID_B, PK_B, C)$ 做此询问时，$\mathscr{C}$ 做如下反应：

• 若 $ID_B \neq ID^*$，由于 C 知道私钥 $SK_A = (z_A, t_A)$，$\mathscr{C}$ 根据第 4 节的 *Unsigncrypt* 算法运行结果给出回复；

• 否则，若 $ID_B = ID^*$ 且 $ID_A \neq ID^*$，$\mathscr{C}$ 检查 $(ID_A, PK_A, ID_B, PK_B, *, C)$ 是否在 *Signcrypt-List* 中，若在 *Signcrypt-List* 中存在一个条目 $(ID_A, PK_A, ID_B, PK_B, M, C)$，$\mathscr{C}$ 返回 M 作为回复；否则，$\mathscr{C}$ 返回“拒绝”信息。

挑战：最后，$\mathscr{A}_2$ 输出两条挑战消息 (M_0, M_1) 和两个挑战身份 ID_A 和 ID_B，ID_A 和 ID_B 分别是发送者和接收者的身份信息。若 $ID_B \neq ID^*$，$\mathscr{C}$ 返回“中止”信息并结束游戏；否则，$\mathscr{C}$ 随机选择一个比特 $\beta \in \{0,1\}$，设置 $c_1 \leftarrow g^b$，$c_2 = H_3(\tilde{\omega}) \oplus M_\beta$，选取随机数 $c_3 \in Z_q^*$。$\mathscr{C}$ 返回 $C=(c_1, c_2, c_3)$ 给 $\mathscr{A}_2$。如果此模拟与真正的攻击是不可区分的，$\mathscr{A}_2$ 若成功，他以极大的概率对 $\tilde{\omega} = (g^b)^{k_B z_B + t_B} = (g^{bz_B})^{k_B} (g^b)^{t_B}$ 做了 H_3 询问。

第二阶段　在挑战结束后，$\mathscr{C}$ 像第一阶段一样回答 $\mathscr{A}_2$ 的各种询问。

猜测　最后，$\mathscr{A}_2$ 输出一个对 β 的猜测 β'。$\mathscr{C}$ 从 *PrivateKey-List* 中搜索 $\langle ID_B, *, t_B \rangle$，从 H_3-*List* 中选择一个 $\langle \tilde{\omega}, h_3 \rangle$，输出 $\left(\frac{h_3}{(g^b)^{t_B}}\right)^{\frac{1}{k_B}}$ 作为 CDHP 问题的答案。

分析：我们分析 $\mathscr{C}$ 成功解给定实例的 CDHP 问题的概率 ε'。我们分析导致 $\mathscr{C}$ 成功的 3 个事件。

E_1：$\mathscr{C}$ 在所有的 *Secret-Value-Extract* 询问中不中止游戏；

E_2：$\mathscr{A}_2$ 输出正确的猜测 $\beta' = \beta$；

E_3：$\mathscr{A}_2$ 挑战的两个身份 ID_A 和 ID_B，满足 $ID_B = ID^*$；

从上述的模拟得到 $\Pr[E_1] \geqslant (1-\frac{1}{q_{H_1}})^{q_{SV}}$，$\Pr[E_2 | E_1] \geqslant Succ_{\mathscr{A}_2}^{IND\text{-}CLSC\text{-}CCA2}$，$\Pr[E_3 | E_1 \wedge E_2] \geqslant \frac{1}{q_{H_1}}$，其中 q_{H_1} 和 q_{PPK} 分别表示 H_1 询问和 *Partial-Private-Key* 询问的次数。$\mathscr{C}$ 解 CDHP 问题的概率为

$$\begin{aligned}\varepsilon' &= \Pr[E_1 \wedge E_2 \wedge E_3] \\ &= \Pr[E_1]\Pr[E_2 | E_1]\Pr[E_3 | E_1 \wedge E_2] \\ &\geqslant \frac{1}{q_{H_1}}(1-\frac{1}{q_{H_1}})^{q_{SV}} Succ_{\mathscr{A}_2}^{IND\text{-}CLSC\text{-}CCA2} \end{aligned} \tag{8}$$

由于 $\varepsilon = Succ_{\mathscr{A}_2}^{IND\text{-}CLSC\text{-}CCA2}$ 是不可忽略的，则 $\mathscr{C}$ 能以不可忽略的概率解 CDHP 问题。因此，若 CDHP 假设成立，我们的无证书签密方案在随机预言机模型下，对于类型 2 敌手，满足 IND-CCA2 安全性。

6　方案比较

本节我们从安全性和计算开销方面，将新方案与 Xie 等人的方案[18]、Zhu 等人的方案[19]、Liu 等人的方案[20]、Jing 等人的方案[21]做了比较。由于 Hash 运算与模指数运算比较来看 Hash 运算量很小，所以忽略方案中的 Hash 运算。因此在计算开销方面，我们只考虑模指数运算和标量乘运算。用 *Exp* 表示模指数运算。表 1 给出了我们的方案与其他 4 个方案的性能比较。表 1 说明，Zhu 等人的方案[19]、Liu 等人的方案[20]和 Jing 等人的方案[21]在性能上优于 Xie 等人的方案[18]和我们的方案。然而，这 3 个方案[19-21]都不能抵抗 CLPKC 的类型 1 敌手的攻击。所以他们的方案不适用于实际应用。只有我们的方案和 Xie 等人的方案能同时抵抗类型 1 敌手和类型 2 敌手的攻击，但我们的方案比 Xie 等人的方案具有更好的性能；而且我们的方案是一个标准的无证书签密方案。由此我们的方案更适用于实际应用。

表 1　不同无证书签密方案的比较

	Xie 等人的方案	Zhu 等人的方案	Liu 等人的方案	Jing 等人的方案	我们的方案
标准 CLSC	否	是	是	是	是
对 $\mathscr{A}_1$ 安全	是	否	否	否	是
对 $\mathscr{A}_2$ 安全	是	是	是	是	是
Signcrypt	6Exp	3Exp	3Exp	3Exp	3Exp
Unsigncrypt	8Exp	4Exp	4Exp	2Exp	5Exp

结束语　构造对于 CLPKC 的两类敌手都安全且高效的无证书签密方案是一个重要的研究课题。本文提出了一个不含双线性对的无证书签密方案。通过安全性分析和性能分析表明，该方案与其他无证书签密方案比较，更适合于实际的应用。我们的方案的安全性能在无证书签密的最强的安全模型下得到证明，对于类型 1 和类型 2 敌手都满足适应性选择消息和身份攻击的不可伪造性，以及 IND-CCA2 安全性。

参 考 文 献

[1] Shamir A. Identity based cryptosystems and signature scheme [C]// Crypto 1984, in: LNCS. Springer-Verlag, 1984, 196: 47-53

[2] Al-Riyami S, Paterson K. Certificateless public key cryptography [C]// Asiacrypt 2003. 2003: 452-473

[3] Zheng Y. Digital signcryption or how to achieve cost (signature and encryption) 6 cost (signature) + cost (encryption) [C]// Cryptology-Crypto 1997. 1997: 291-312

[4] An J H, Dodis Y, Rabin T. On the security of joint signature and encryption [C]// Advances in Cryptology-Eurocrypt 2002. 2002: 83-107

[5] Malone-Lee J. Identity based signcryption [OL]. Cryptology ePrint Archive, Report 2002/098. http://eprint.iacr.org/2002/098

[6] Barbosa M, Farshim P. Certificateless signcryption [C]// Proc. ACM Symposium on Information, Computer and Communications Security (ASIACCS 2008). 2008: 369-372

[7] Wu C, Chen Z. A new efficient certificateless signcryption scheme [C]// International Symposium on Information Science and Engieering, 2008. ISISE'08. 2008: 661-664

[8] Selvi S S D, Vivek S S, Ragan C P. On the security of certificateless signcryption schemes [OL]. Cryptology ePrint Archive: Report 2009/298, Available from: http://eprint.iacr.org/2009/298

[9] Xie W, Zhang Z. Efficient and provably secure certificateless signcryption from bilinear maps [OL]. Cryptology ePrint Archive: Report 2009/578, Available from: http://eprmt.iacr.org/2009/578.pdf

（下转第 223 页）

冗余信息，因而一般能获得较好的容量-失真性能。在此类RDH算法中，算法性能在很大程度上决定于预测算子的预测精度。图像的基本理论告诉我们，距离目标像素越近的近邻与目标像素相关度越高，文中提出的FCGAP，基于12最近邻进行像素值预测处理，有利于充分挖掘目标像素的相关信息，获得比现有仅基于部分最近邻像素的预测算子更好的预测精度。实验结果表明，文中基于FCGAP的图像RDH较现有可逆数据隐藏算法具有更理想的容量-失真性能，FCGAP适用于RDH算法，基于完整上下文的预测算子用于RDH是可行的。

参 考 文 献

[1] Cox I J, Miller M L, Bloom J A, et al. Digital watermarking and steganography (2nd ed) [M]. Burlington: Morgan Kauffman, 2008: 385-395

[2] 罗剑高，韩国强，沃焱，等. 篡改定位精度可动态调整的无损图像认证算法[J]. 华南理工大学学报：自然科学版，2011，39(7)：121-126

[3] 罗剑高，韩国强，沃焱，等. 基于自适应图像块组合的无损图像认证算法[J]. 通信学报，2012，33(6)：64-72

[4] Yu Y H, Chang C C. A high capacity reversible data hiding scheme for annotation [A] // Second International Symposium on Intelligent Information Technology Application [C]. Shanghai, China, 2008: 940-944

[5] Celik M U, Sharma G, Tekalp A M, et al. Lossless generalized-LSB data embedding [J]. IEEE Transactions on Image Processing, 2005, 14(2): 253-266

[6] Tian J. Reversible data embedding using a difference expansion [J]. IEEE Transactions on Circuits and Systems for Video Technology, 2003, 13(8): 890-896

[7] Alattar A M. Reversible watermark using the difference expansion of a generalized integer transform [J]. IEEE Transactions on Image Processing, 2004, 13(8): 1147-1156

[8] 曾宪庭，李卓，平玲娣. 基于块参照像素的无损信息隐藏算法[J]. 计算机科学，2012，39(2)：47-51

[9] Thodi D M, Rodriguez J J. Expansion embedding techniques for reversible watermarking [J]. IEEE Transactions on Image Processing, 2007, 16(3): 721-730

[10] Li X L, Yang B, Zeng T Y. Efficient reversible watermarking based on adaptive prediction-error expansion and pixel selection [J]. IEEE Transactions on Image Processing, 2011, 20(12): 3524-3533

[11] 曾骁，陈真勇，陈明，等. 基于全方向预测与误差扩展的可逆数据隐藏 [J]. 计算机研究与发展，2010，47(9)：1595-1603

[12] Chen M, Chen Z Y, Zeng X, et al. Model order selection in reversible image watermarking [J]. IEEE Journal of Selected Topics in Signal Processing, 2010, 4(3): 592-604

[13] Yang W J, Chung K L, Liao H Y M, et al. Efficient reversible data hiding algorithm based on gradient-based edge direction prediction [J]. The Journal of Systems and Software, 2013, 86(2): 567-580

[14] Wu X L, Memon N. Context-based, adaptive, lossless image coding [J]. IEEE Transactions on Communication, 1997, 45(4): 437-444

[15] Signal and Image Processing Institute, University Southern California, Los Angeles. Image Database [EB/OL]. http://sipi.usc.edu/database/, 2012-3-26

[16] Luo L X, Chen Z Y, Chen M, et al. Reversible image watermarking using interpolation technique [J]. IEEE Transactions on Information Forensics and Security, 2010, 5(1): 187-193

(上接第209页)

[10] Selvi S S D, Vivek S S, Ragan C P. Security weaknesses in two certificateless signcryption schemes[OL]. Cryptology ePrint Archive: Report 2010/092, Available from: http://eprint.iacr.org/2010/092

[11] Liu Z, Hu Y, Zhang X, et al. Certificateless signcryption scheme in the standard model[J]. Information Sciences, 2010, 180(3): 452-464

[12] Weng J, Yao G, Deng R H, et al. Cryptanalysis of a certificateless signcryption scheme in the standard model[J]. Information Sciences, 2011, 181(3): 661-667

[13] Chen L, Cheng Z, Smart N. Identity-based key agreement protocols from pairings[J]. International Journal of Information Security, 2007, 6(2): 213-241

[14] Cao X, Kou W. A Pairing-free Identity-based Authenticated Key Agreement Scheme with Minimal Message Exchanges[J]. Information Sciences, 2010, 180(6): 2895-2903

[15] He D, Chen J, Hu J. An ID-based proxy signature schemes without bilinear pairings[J]. Annals of Telecommunications, 2011, 66(11/12): 657-662

[16] Barreto P, Deusajute A, Cruz E, et al. Toward efficient certificateless signcryption from (and without) bilinear pairings[OL]. http://sbseg2008.inf.ufrgs.br/proceedings/data/pdf/st03_03_artigo.pdf

[17] Selvi S S D, Vivek S S, Ragan C P. Cryptanalysis of Certificateless Signcryption Schemes and an Efficient Construction Without Pairing[C] // Inscrypt 2009. 2010: 75-92

[18] Xie W, Zhang Z. Certificateless Signcryption without Pairing", Cryptology ePrint Archive: Report 2010/187 [OL]. Available from: http://eprint.iacr.org/2010/187

[19] Zhu H, Li H, Wang Y. Certificateless Signcryption Scheme Without Pairing[J]. Journal of Computer Research and Development, 2010, 47(9): 1587-1594

[20] Liu W, Xu C. Certificateless Signcryption Scheme Without Bilinear Pairing[J]. Journal of Software, 2011, 22(8): 1918-1926

[21] Jing X. Provably Secure Certificateless Signcryption Scheme without Pairing[C] // 2011 International Conference on Electronic & Mechanical Engineering and Information Technology. 2011: 4753-4756

[22] David P, Jacque S. Security Arguments for Digital Signatures and Blind Signatures[J]. Journal of Cryptology, 2000, 13(3): 361-396