可证安全的高效无证书广义签密方案

周彦伟[1),2),3)] 杨 波[1),2),3)] 张文政[2)]

[1)](陕西师范大学计算机科学学院 西安 710119)

[2)](保密通信重点实验室 成都 610041)

[3)](中国科学院信息工程研究所信息安全国家重点实验室 北京 100093)

摘 要 广义签密方案的最显著特点是能够实现加密、签名和签密 3 种功能. Liu 等人构造了一个高效的无证书广义签密方案,并给出了正式的安全性证明;然而,文中通过构造具体的不可伪造性攻击算法,证明该方案对$\mathcal{A}_I$类敌手不具备其所声称的不可伪造性. 在不使用双线性映射的前提下,文中提出一个可证安全的高效无证书广义签密方案,并基于计算性 Diffie-Hellman 问题和离散对数问题的困难性,在随机预言机模型下对文中方案的机密性和不可伪造性进行了证明;由于文中方案具有安全、高效及无证书的优势,可广泛应用于秘密分发及安全通信等领域.

关键词 无证书广义签密;可证明安全;双线性映射;随机预言机模型

中图法分类号 TP309 **DOI 号** 10.11897/SP.J.1016.2016.00543

Provably Secure and Efficient Certificateless Generalized Signcryption Scheme

ZHOU Yan-Wei[1),2),3)] YANG Bo[1),2),3)] ZHANG Wen-Zheng[2)]

[1)](*School of Computer Science, Shaanxi Normal University, Xi'an* 710119)

[2)](*Science and Technology on Communication Security Laboratory, Chengdu* 610041)

[3)](*State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences, Beijing* 100093)

Abstract Signcryption is basically a cryptographic primitive which provides both signature and encryption functions simultaneously, but it is not useful when only one of the function is required. Generalized signcryption is a special cryptographic primitive which can provide signcryption function when security and authenticity are needed simultaneously, and can also provide encryption or signature function separately when any one of them is needed. It is very suitable for storage-constrained environments. Liu et al. proposed an effective certificateless generalized signcryption scheme with formal security proof. However, specific unforgeable attack algorithm proves that it does not have the claimed unforgeability. Thus, this paper proposed a security certificateless generalized signcryption scheme with no bilinear pairings, and whose security is based on the hardness of the classical Computational Diffie-Hellman (CDH) problem and Discrete Logarithm (DL) problem under the random oracle model. Furthermore, performance analysis shows the proposed scheme is efficient and practical. Due to the advantage of being secure, effective and certificateless, this scheme can be widely used in such fields as secret distribution and security communication.

Keywords certificateless generalized signcryption; provably security; bilinear pairings; random oracle model

收稿日期:2014-10-27;最终修改稿收到日期:2015-07-18. 本课题得到国家自然科学基金(61272436,61402275,61303092,61572303)、中国科学院信息工程研究所信息安全国家重点实验室开放课题(2015-MS-10)、保密通信重点实验室基金(9140C110206140C11050)、中央高校基本科研业务费专项资金(GK201504016)、陕西师范大学优秀博士论文项目(X2014YB01)资助.**周彦伟**,男,1986 年生,博士研究生,主要研究方向为密码学、匿名通信技术等. E-mail: zyw_snnu@foxmail.com. **杨 波**(通信作者),男,1963 年生,博士,教授,博士生导师,陕西省"百人计划"特聘教授,主要研究领域为信息安全、密码学等. **张文政**,男,1966 年生,研究员,主要研究领域为信息安全等.

1 引 言

公钥加密机制是信息安全领域的关键技术,但是在传统基于公钥证书的密码体制中,由于证书保证了持有人与公钥间的对应关系,涉及证书的管理、颁发和撤销等操作,因此,证书管理过程复杂且代价高.基于身份的公钥密码体制(Identity-Based Public Key Cryptography,ID-PKC)[1]中由于身份信息(如姓名、电子邮箱等)直接被作为公钥使用,使得公钥无需与证书绑定,改进了传统公钥证书的管理问题;ID-PKC 中由可信第三方私钥生成中心(Private Key Generator,PKG)负责生成用户的私钥. 则恶意的 PKG 具备伪造任意用户的合法密文或替代用户进行解密的能力,即 ID-PKC 存在密钥托管的不足,该不足制约了 ID-PKC 在实际中的应用. 为了克服 ID-PKC 密钥托管的不足,无证书公钥密码系统(Certificateless Public Key Cryptography,CL-PKC)[2]被提出;CL-PKC 增强了密钥生成过程中用户的自主性,即 PKG 仅为用户生成部分私钥;用户基于 PKG 为其计算的部分私钥和随机选取的秘密值生成完整的私钥;公钥由用户的秘密值、身份和系统参数计算得出,CL-PKC 中用户参与其私钥的生成,增强了私钥生成过程中用户的自主性,很好地解决了 ID-PKC 中的密钥托管问题.

广义签密(Generalized Signcryptions,GSC)[3]可根据应用环境的需求实现加密、签名和签密这 3 种功能,具有广泛的应用前景. 由于 CL-PKC 解决了证书管理、密钥托管等问题,因此无证书广义签密方案(Certificateless Generalized Signcryption,CLGSC)的构造及安全性证明已成为密码学领域当前的热点研究问题之一.

Wang 等人提出了无证书广义签密方案的安全模型①,并对文献[3]所提出的安全模型进行了修改;文献[4]指出上述安全模型并不完整,并对该模型进行了改进;文献[5]提出了一个使用双线性映射的广义签密方案,并且该方案具有较短的签名长度;Ji 等人提出了一种高效的无证书广义签密机制②,并在随机预言机模型下对该方案的安全性进行了证明;然而,Kushwah 等人发现该方案无法满足其所声称的对$\mathcal{A}_{\mathrm{I}}$类敌手的不可伪造性③;Lal 等人提出了第一个基于身份的广义签密方案④,并对相应的安全模型进行了定义,然而文献[6]指出该模型并不完整,同时提出了一个基于身份的广义签密方案,并证明了方案的安全性;文献[7]定义了不同 PKG 环境下基于身份的广义签密方案及其安全模型,同时提出了具体的多 PKG 环境下的广义签密方案,并在标准模型下基于相关困难性问题对方案的安全性进行了证明;文献[8]分析发现 Ji 等人的方案无法满足其所声称的安全性,并构造了具体的攻击算法,同时提出了一个可证安全的广义签密方案;文献[9]提出了一个无证书广义签密方案,基于相关困难性问题在标准模型下对方案的安全性进行了证明,然而,遗憾的是本文通过构造具体的攻击算法,证明了文献[9]中提出的方案无法满足其所声称的对$\mathcal{A}_{\mathrm{I}}$类敌手的不可伪造性,但需要特别指出的是,虽然 Liu 等人的方案没能满足对$\mathcal{A}_{\mathrm{I}}$类敌手的不可伪造性,但其对 CLGSC 安全模型的定义及详细介绍,确实为 CLGSC 的设计及安全性证明提出了新的研究思路.

针对文献[9]所存在的不足,本文在不使用双线性映射的前提下,提出可证安全的高效无证书广义签密方案,并基于离散对数问题的困难性在随机预言机模型下证明了本文方案的机密性和不可伪造性;相较于现有的无证书广义签密方案,由于未使用双线性映射和指数运算,本文方案具有较高的计算效率.

特别的,由于文献[9]中已详细介绍了 CL-PKC 的定义、CLGSC 的定义和安全模型及相关游戏的描述,篇幅所限本文不再对上述知识进行重复介绍,具体描述详见文献[9].

2 Liu 等人方案的安全性分析

方案的具体介绍详见文献[9],本文不再赘述.在进行安全性分析之前,对敌手的攻击类型进行简要介绍:根据文献[9]中的安全模型,无证书广义签密方案将面临$\mathcal{A}_{\mathrm{I}}$和$\mathcal{A}_{\mathrm{II}}$两类敌手的攻击.

$\mathcal{A}_{\mathrm{I}}$:此类攻击者无法掌握系统的主密钥,但可利用合法用户的公钥完成对方案安全性的攻击,即具有替换合法用户公钥的能力.本文中$\mathcal{A}_{\mathrm{I}\text{-}i}(i=1,2)$为$\mathcal{A}_{\mathrm{I}}$类敌手,其中$\mathcal{A}_{\mathrm{I}\text{-}1}$是攻击方案机密性的敌手,$\mathcal{A}_{\mathrm{I}\text{-}2}$是攻击方案不可伪造性的敌手.

$\mathcal{A}_{\mathrm{II}}$:此类攻击者可掌握系统的主密钥,但其不具

① Wang X, Yang Y, Han Y. Provable secure generalized signcryption. https://eprint. iacr. org/2007/173. pdf

② Ji H, Han W, Zhao L. Certificateless generalized signcryption. http://eprint. iacr. org/2010/204. pdf, 2010

③ Kushwah P, Lal S. Efficient Generalized Signcryption Schemes. http://eprint. iacr. org/2010/346. pdf, 2010

④ Lal S, Kushwah P. ID based generalized signcryption. http://eprint. iacr. org/2008/84. pdf, 2008

有替换合法用户公钥的能力. 本文中$\mathcal{A}_{\mathrm{II}\text{-}i}(i=1,2)$为$\mathcal{A}_{\mathrm{II}}$类敌手，其中$\mathcal{A}_{\mathrm{II}\text{-}1}$是攻击方案机密性的敌手，$\mathcal{A}_{\mathrm{II}\text{-}2}$是攻击方案不可伪造性的敌手.

本节针对 Liu 等人所提出的方案构造具体的不可伪造性攻击算法，证明该方案[9]不具备其所声称的对$\mathcal{A}_{\mathrm{I}}$类敌手的不可伪造性.

令用户 Alice(其身份标识为 ID_A)和 Bob(其身份标识为 ID_B)分别为文献[9]中无证书广义签密方案的参与者，则 Alice 的公私钥对为$\langle PK_A, SK_A\rangle$，Bob 的公私钥对为$\langle PK_B, SK_B\rangle$.

$\mathcal{A}_{\mathrm{I}}$类敌手$\mathcal{A}_{\mathrm{I}\text{-}2}$具有替换合法用户公钥的能力，但其不掌握系统主密钥 msk. 敌手$\mathcal{A}_{\mathrm{I}\text{-}2}$与接收者 Bob 间的具体交互过程如下所示：

(1) 敌手$\mathcal{A}_{\mathrm{I}\text{-}2}$获悉 Alice 的公钥 PK_A、身份标识 ID_A及 mpk 等公开信息后，随机选取秘密值 $x, y\in Z_p^*$，计算 Alice 的伪造公钥及其公钥签名：

$$\begin{aligned}PK'_A&=(K'_A,h'_A,pk'_A,Y'_A,z'_A)\\&=(ID_A,e(g_1,g_2),e(g_1,g_2)^x,e(g_1,g_2)^y,\\&\quad y+c'_A x \bmod p),\end{aligned}$$

其中，$c'_A=H_1(ID_A, Y'_A\,\|\,mpk)$.

(2) 敌手$\mathcal{A}_{\mathrm{I}\text{-}2}$使用 PK'_A代替参与者 Alice 的原始公钥 PK_A，则参与者 Bob 认为 Alice 的公钥就是 PK'_A；PK'_A能够通过 Bob 对其的合法性验证，即有等式 $h_A'^{z'_A}=Y'_A\cdot pk_A'^{c'_A}$ 成立.

$$\begin{aligned}h_A'^{z'_A}&=e(g_1,g_2)^{y+c'_A x}=e(g_1,g_2)^y\cdot e(g_1,g_2)^{c'_A x}\\&=Y'_A\cdot pk_A'^{c'_A}.\end{aligned}$$

给定一个消息 $M\in G_2$，敌手$\mathcal{A}_{\mathrm{I}\text{-}2}$按下述步骤伪装成 Alice 与参与者 Bob 进行通信，交互过程分以下 3 种情况讨论：

① SC(签密)：敌手$\mathcal{A}_{\mathrm{I}\text{-}2}$通过验证等式 $h_B^{z_B}=Y_B\cdot pk_B^{c_B}$(其中 $c_B=H_1(ID_B, Y_B\,\|\,mpk)$)是否成立来验证 Bob 的公钥是否有效(合法用户 Bob 的公钥能够通过此验证). $\mathcal{A}_{\mathrm{I}\text{-}2}$随机选取秘密数 $b\in Z_p^*$ 生成签密密文 σ 为

$$\begin{aligned}\sigma&=(\sigma_0,\sigma_1,\sigma_2,\sigma_3,\sigma_4)\\&=(M\cdot pk_B^x, g^x, F_u(ID_B)^x, g^b,\\&\quad g^x\cdot F_u(ID_A)^b\cdot F_v(W)^x),\end{aligned}$$

其中，$W=H_2(\sigma_0,\sigma_1,\sigma_2,\sigma_3,ID_B,pk_B)$.

② $Sign$(签名)：敌手$\mathcal{A}_{\mathrm{I}\text{-}2}$随机选取秘密数 $b\in Z_p^*$，生成其对消息 M 的签名 σ 为

$$\begin{aligned}\sigma&=(\sigma_0,\sigma_1,\sigma_2,\sigma_3,\sigma_4)\\&=(M, g^x, 1, g^b, g^x\cdot F_u(ID_A)^b\cdot F_v(W)^x),\end{aligned}$$

其中，$W=H_2(\sigma_0,\sigma_1,\sigma_2,\sigma_3,0,1)$.

③ Enc(加密)：敌手$\mathcal{A}_{\mathrm{I}\text{-}2}$通过验证等式 $h_B^{z_B}=Y_B\cdot pk_B^{c_B}$是否成立来验证 Bob 的公钥是否有效. $\mathcal{A}_{\mathrm{I}\text{-}2}$生成其对消息 M 的加密密文 σ 为

$$\begin{aligned}\sigma&=(\sigma_0,\sigma_1,\sigma_2,\sigma_3,\sigma_4)\\&=(M\cdot pk_B^x, g^x, F_u(ID_B)^x, 1, F_v(W)^x),\end{aligned}$$

其中，$W=H_2(\sigma_0,\sigma_1,\sigma_2,\sigma_3,ID_B,pk_B)$.

(3) Bob 收到敌手$\mathcal{A}_{\mathrm{I}\text{-}2}$所发送的密文(或签名)信息 $\sigma=(\sigma_0,\sigma_1,\sigma_2,\sigma_3,\sigma_4)$后，验证其合法性. 若 σ 合法，则 Bob 通过了对敌手$\mathcal{A}_{\mathrm{I}\text{-}2}$的身份合法性验证，则敌手$\mathcal{A}_{\mathrm{I}\text{-}2}$生成了 Alice 的合法密文(或签名)信息 σ，因此，敌手$\mathcal{A}_{\mathrm{I}\text{-}2}$伪装 Alice 成功.

定理 1.　$\mathcal{A}_{\mathrm{I}}$类敌手$\mathcal{A}_{\mathrm{I}\text{-}2}$伪造了 Alice 的合法密文(或签名)信息 $\sigma=(\sigma_0,\sigma_1,\sigma_2,\sigma_3,\sigma_4)$.

证明.　若敌手$\mathcal{A}_{\mathrm{I}\text{-}2}$的伪造信息 σ 能通过 Bob 的合法性验证，则敌手$\mathcal{A}_{\mathrm{I}\text{-}2}$伪装 Alice 成功.

Bob 收到信息 σ 后，σ 的合法性验证过程如下所示：

(1) 计算

$$\begin{cases}W=H_2(\sigma_0,\sigma_1,\sigma_2,\sigma_3,0,1), & \sigma_2=1\\ W=H_2(\sigma_0,\sigma_1,\sigma_2,\sigma_3,ID_B,pk_B), & \text{其他}\end{cases}.$$

(2) 验证

$$\begin{cases}e(g,\sigma_2\cdot\sigma_4)=e(\sigma_1,F_u(ID_B)\cdot F_v(w)), & \sigma_3=1\\ e(g,\sigma_4)=pk'_A\cdot e(F_u(ID_A),\sigma_3)\cdot e(F_v(W),\sigma_1), & \text{其他}\end{cases}.$$

若 $\sigma_3=1$，即有

$$\begin{aligned}e(g,\sigma_2\cdot\sigma_4)&=e(g,F_u(ID_B)^x\cdot F_v(W)^x)\\&=e(g^x,F_u(ID_B))\cdot e(g^x,F_v(W))\\&=e(\sigma_1,F_u(ID_B)\cdot F_v(w));\end{aligned}$$

否则，$\sigma_3\neq 1$，即有

$$\begin{aligned}e(g,\sigma_4)&=e(g,g^x\cdot F_u(ID_A)^b\cdot F_v(W)^x)\\&=e(g,g)^x\cdot e(g^b,F_u(ID_A))\cdot e(g^x,F_v(W))\\&=pk'_A\cdot e(F_u(ID_A),\sigma_3)\cdot e(F_v(W),\sigma_1).\end{aligned}$$

(3) 若 $\sigma_2=1$，则返回 1，表示 σ 是 M 的合法签名；否则，返回 $M=\sigma_0\cdot\dfrac{e(\sigma_2,sk_{B,2})}{e(\sigma_1,sk_{B,1})}$，表示 M 是发送者 Alice 的原始明文(Bob 认为是 Alice 与其进行通信).

$$\begin{aligned}M&=\sigma_0\cdot\frac{e(\sigma_2,sk_{B,2})}{e(\sigma_1,sk_{B,1})}\\&=M\cdot e(g_1,g_2)^{xx_{ID_B}}\cdot\frac{e(F_u(ID_B)^x,g^t)}{e(g^x,g_2^{ax_{ID_B}}\cdot F_u(ID_B)^t)}\\&=M\cdot e(g_1,g_2)^{xx_{ID_B}}\cdot\frac{e(F_u(ID_B),g)^{tx}}{e(g^a,g_2)^{xx_{ID_B}}e(g,F_u(ID_B))^{tx}}\\&=M,\end{aligned}$$

其中，$g_1=g^a$.

因此伪造的密文(或签名)信息 σ 通过了接收者 Bob 的合法性验证，即$\mathcal{A}_{\mathrm{I}}$类敌手$\mathcal{A}_{\mathrm{I}\text{-}2}$具有伪装 Alice

的能力.综上所述,$\mathcal{A}_{\mathrm{I}}$类敌手$\mathcal{A}_{\mathrm{I}\text{-}2}$伪造了合法用户的合法密文(或签名)信息,伪造攻击成功. 证毕.

由上述定理 1 的证明过程可知,敌手$\mathcal{A}_{\mathrm{I}\text{-}2}$的伪造密文(或签名)信息 σ 通过了 Bob 的合法性验证,则敌手$\mathcal{A}_{\mathrm{I}\text{-}2}$伪装 Alice 成功,因此,$\mathcal{A}_{\mathrm{I}}$类敌手获得任意用户的相关公开信息后,能够伪装成该用户,并生成其合法的密文(或签名)信息,即伪造的密文(或签名)信息能够通过接收者对其的合法性验证.所以,文献[9]中的方案无法满足其所声称的对$\mathcal{A}_{\mathrm{I}}$类敌手的不可伪造性.

3 本文方案的构造

由于双线性映射的计算复杂度较高,因此本文提出可证安全的无需双线性映射的无证书广义签密方案,具体细节如下所述:

(1)系统建立阶段($Setup$)

①设群 G 是阶为素数 p($p>2^k$,k 为安全参数)的循环群,P 是群 G 的一个生成元.

②PKG 随机选取主密钥 $s\in Z_p^*$,计算 $P_{Pub}=sP$;选择抗碰撞的密码学哈希函数:$H_0:\{0,1\}^L\times G\times G\rightarrow Z_p^*$,$H_1:\{0,1\}^L\times G\times G\rightarrow\{0,1\}^m$;$H_2:\{0,1\}^L\times\{0,1\}^m\times G\times G\rightarrow Z_p^*$,其中,$L$ 为身份标识 ID 的长度,m 为明文消息 M 的长度.

③PKG 定义函数 $Fun(A,\mathrm{ID})$,其输入 A 为非 0 的任意值,即输入 A 不能为 0;输入 ID 为身份标识且 $ID\in\{0,1\}^L$,其输出为 $Fun(A,ID)=\begin{cases}0, & ID=\varnothing\\ A, & \text{其他}\end{cases}$.

④PKG 公开系统参数 $Params=\langle p,G,P,P_{Pub},Fun(),\boldsymbol{H}_0,\boldsymbol{H}_1,\boldsymbol{H}_2\rangle$,秘密保存主密钥 s.

(2)用户密钥生成($Set\text{-}User\text{-}Key$)

用户的密钥生成过程包含下述步骤:

①用户 ID 选取随机数 $x_{ID}\in Z_p^*$ 作为其秘密值,并计算相应的公开参数 $X_{ID}=x_{ID}P$;同时,将身份标识 ID 和公开参数 X_{ID} 发给 PKG;

②给定用户的身份标识 ID 和公开参数 X_{ID},PKG 计算 ID 的部分私钥 y_{ID} 和部分公钥 Y_{ID}:

随机选取 $f_{ID}\in Z_p^*$;计算 $Y_{ID}=f_{ID}P$ 和 $y_{ID}=s+f_{ID}H_0(ID,X_{ID},Y_{ID})$,PKG 通过安全信道将 Y_{ID} 和 y_{ID} 传送给用户 ID;

③通过等式 $y_{ID}P=P_{Pub}+Y_{ID}H_0(ID,X_{ID},Y_{ID})$可验证 PKG 生成的部分私钥 y_{ID} 和部分公钥 Y_{ID} 的合法性;若合法性验证通过,则用户 ID 的公私钥对为$\langle PK_{ID}=(X_{ID},Y_{ID}),SK_{ID}=(x_{ID},y_{ID})\rangle$.

(3)广义签密算法(GSC)

给定一个消息 $M\in\{0,1\}^m$ 和接收者 Bob(身份标识为 ID_B),则发送者 Alice(身份标识为 ID_A)选取随机秘密数 $r\in Z_p^*$ 进行下述计算生成消息 M 所对应的密文(或签名)信息 σ.

①计算 $U=rP$;

②计算 $h=Fun(H_1(ID_B,U,Q_{ID_B}),ID_B)$,其中 $Q_{ID_B}=r(X_{ID_B}+Y_{ID_B}H_0(ID_B,X_{ID_B},Y_{ID_B})+P_{Pub})$;

③计算 $C=M\oplus h$;

④计算 $u=H_2(ID_A,C,U,X_{ID_A})$和 $w=H_2(ID_A,C,U,Y_{ID_A})$;

⑤计算 $V=Fun(y_{ID_A}+ux_{ID_A}+wr,ID_A)$;

⑥生成密文(或签名)信息 $\sigma=(U,V,C)$.

特别的,仅对消息 M 进行签名时,不存在具体的接收者,即 $ID_B=\varnothing$,则有 $C=M$,即签名信息为 $\sigma=(U,V,M)$;仅对消息 M 进行加密时,不存在具体的发送者,即 $ID_A=\varnothing$,则有 $V=0$,即密文信息为 $\sigma=(U,0,C)$.

(4)解广义签密算法($UnGSC$)

给定一个密文(或签名)信息 $\sigma=(U,V,C)$和接收者 Bob 的身份 ID_B,接收者 Bob 执行如下步骤:

①密文解密

(i)计算 $h'=Fun(H_1(ID_B,U,Q'_{ID_B}),ID_B)$,其中 $Q'_{ID_B}=U(x_{ID_B}+y_{ID_B})$;

(ii)计算 $M=C\oplus h'$.

②合法性验证

(i)若 $V=0$,则消息 σ 是 M 的加密密文,返回解密后的明文消息 M;

(ii)否则,计算 $u'=H_2(ID_A,C,U,X_{ID_A})$和 $w'=H_2(ID_A,C,U,Y_{ID_A})$,验证等式 $VP=P_{Pub}+Y_{ID_A}H_0(ID_A,X_{ID_A},Y_{ID_A})+u'X_{ID_A}+w'U$ 是否成立,若等式成立,则返回相应的消息 M;否则,返回 $\perp$,表示输入的密文(或签名)σ 无效.

(5)正确性

①部分私钥及公钥的验证

由于 $y_{ID}P=(s+f_{ID}H_0(ID,X_{ID},Y_{ID}))P=P_{Pub}+Y_{ID}H_0(ID,X_{ID},Y_{ID})$;

则当等式 $y_{ID}P=P_{Pub}+Y_{ID}H_0(ID,X_{ID},Y_{ID})$成立时,PKG 生成了合法的部分私钥 y_{ID} 和部分公

钥 Y_{ID}.

② 密文解密

已知 $h'=Fun(H_1(ID_B,U,Q'_{ID_B}),ID_B)$ 和 $h=Fun(H_1(ID_B,U,Q_{ID_B}),ID_B)$；

(i) 若 $ID_B=\varnothing$，有 $h'=h=0$；

(ii) 否则 $ID_B\neq\varnothing$，有 $h'=H_1(ID_B,U,Q'_{ID_B})$ 和 $h=H_1(ID_B,U,Q_{ID_B})$.

$$\begin{aligned}Q'_{ID_B}&=U(x_{ID_B}+y_{ID_B})\\&=rP(x_{ID_B}+s+f_{ID_B}H_0(ID_B,X_{ID_B},Y_{ID_B}))\\&=r(X_{ID_B}+Y_{ID_B}H_0(ID_B,X_{ID_B},Y_{ID_B})+P_{Pub})\\&=Q_{ID_B},\end{aligned}$$

则 $h'=H_1(ID_B,U,Q'_{ID_B})=H_1(ID_B,U,Q_{ID_B})=h$.

由上述等式可知接收者解密后的明文消息即为发送者的原始消息，即有等式 $M=C\oplus h'=M\oplus h\oplus h'$ 成立.

③ 签名的合法性验证

(i) 若 $V=0$，则有 $ID_A=\varnothing$，因此消息 σ 是 M 的加密密文，返回明文消息 M；

(ii) 否则，有 $V\neq0$，则 $ID_A\neq\varnothing$，即消息签名为 $V=y_{ID_A}+ux_{ID_A}+wr$. 因此消息 σ 是明文消息 M 的签密密文(或签名)，需验证等式 $VP=P_{Pub}+Y_{ID_A}H_0(ID_A,X_{ID_A},Y_{ID_A})+u'X_{ID_A}+w'U$ 是否成立.

$$\begin{aligned}VP&=(y_{ID_A}+ux_{ID_A}+wr)P\\&=(s+f_{ID_A}H_0(ID_A,X_{ID_A},Y_{ID_A})+ux_{ID_A}+wr)P\\&=P_{Pub}+Y_{ID_A}H_0(ID_A,X_{ID_A},Y_{ID_A})+u'X_{ID_A}+w'U,\end{aligned}$$

其中，$u=u'=H_2(ID_A,C,U,X_{ID_A})$ 和 $w=w'=H_2(ID_A,C,U,Y_{ID_A})$.

等式 $VP=P_{Pub}+Y_{ID_A}H_0(ID_A,X_{ID_A},Y_{ID_A})+u'X_{ID_A}+w'U$ 成立，则返回明文消息 M；否则，返回表示输入的密文无效.

4　安全性分析

本节在随机预言机模型下证明本文方案的机密性和不可伪造性. 在进行相关证明之前首先简要介绍证明过程中所涉及的相关困难性问题.

离散对数(DL)问题：群 G 是阶为素数 $p(p>2^k$，k 为安全参数)的循环群，P 是群 G 的一个生成元；给定元组 (P,aP)，其中 $a\in Z_p^*$ 且未知，DL 问题的目标是计算 a.

算法 $\mathcal{B}$ 在概率多项式时间内成功解决 DL 问题的优势为 $Adv^{DL}(\mathcal{B})=Pr[\mathcal{B}(P,aP)=a]$.

其中，概率来源于算法 $\mathcal{B}$ 的随机选择和 a 在 Z_p^* 上的随机选取.

定义 1(DL 假设). 对于任意的概率多项式时间算法 $\mathcal{B}$，优势 $Adv^{DL}(\mathcal{B})$ 是可忽略的.

计算性 Diffie-Hellman(CDH)问题：群 G 是阶为素数 $p(p>2^k$，k 为安全参数)的循环群，P 是群 G 的一个生成元；给定元组 (P,aP,bP)，其中 $a,b\in Z_p^*$ 且未知，CDH 困难问题的目标是计算 abP.

算法 $\mathcal{B}$ 在概率多项式时间内成功解决 CDH 问题的优势为 $Adv^{CDH}(\mathcal{B})=Pr[\mathcal{B}(P,aP,bP)=abP]$.

其中，概率来源于算法 $\mathcal{B}$ 的随机选择和 a,b 在 Z_p^* 上的随机选取.

定义 2(CDH 假设). 对于任意的概率多项式时间算法 $\mathcal{B}$，优势 $Adv^{CDH}(\mathcal{B})$ 是可忽略的.

4.1　机密性

定理 2($\mathcal{A}_I$ 类攻击下的机密性). 在随机预言机模型中，若 $\mathcal{A}_I$ 类敌手 $\mathcal{A}_{I\text{-}1}$ 能以不可忽略的优势 ε 在多项式时间内赢得相关游戏(游戏的具体定义见文献[9])，$\mathcal{A}_{I\text{-}1}$ 最多进行 q_S 次广义签密询问和 q_{SK} 次私钥生成询问)，则算法 $\mathcal{B}$ 能以不可忽略的优势 $Adv(\mathcal{B})\geq\left(1-\frac{q_{SK}}{2^k}\right)^2\frac{\varepsilon}{e(q_S+1)}$(e 是自然对数底数)在多项式时间内解决 CDH 困难问题.

证明. 令算法 $\mathcal{B}$ 是 CDH 困难问题解决者，其输入为元组 (P,aP,bP)，其中 $a,b\in Z_p^*$ 且未知，目标是计算 abP. $\mathcal{B}$ 以敌手 $\mathcal{A}_{I\text{-}1}$ 为子程序并充当游戏的挑战者. 游戏开始后，$\mathcal{B}$ 运行 $Setup$ 算法并发送系统参数 $Params=\langle p,G,P,P_{Pub},Fun(),\boldsymbol{H}_0,\boldsymbol{H}_1,\boldsymbol{H}_2\rangle$ 给 $\mathcal{A}_{I\text{-}1}$，其中 $P_{Pub}=aP$(则系统公钥为 a，但 $\mathcal{B}$ 并不掌握 a)；$\mathcal{B}$ 维持列表 $\boldsymbol{L}_0,\boldsymbol{L}_1,\boldsymbol{L}_D,\boldsymbol{L}_{SK}$ 和 $\boldsymbol{L}_{PK}$ 分别用于跟踪敌手 $\mathcal{A}_{I\text{-}1}$ 对预言机 $\boldsymbol{H}_0,\boldsymbol{H}_1$ 的询问及对部分密钥生成、私钥生成和公钥生成询问，初始时各列表均为空. $\mathcal{B}$ 猜测 $ID_J(J\in[1,q_S+1]$，询问阶段对 q_S 个身份进行广义签密询问，挑战阶段生成 1 个身份的广义签密密文)是 $\mathcal{A}_{I\text{-}1}$ 选取的挑战身份.

询问：敌手 $\mathcal{A}_{I\text{-}1}$ 进行下述询问：

H_1 询问：当收到 $\mathcal{A}_{I\text{-}1}$ 的询问 $H_1(ID_i,U_i,Q_{ID_i})$ 时，若有 $\langle ID_i,U_i,Q_{ID_i},h_1\rangle\in L_1$，则 $\mathcal{B}$ 返回 h_1 给 $\mathcal{A}_{I\text{-}1}$；否则，$\mathcal{B}$ 选取满足条件 $\langle *,*,*,h_1\rangle\notin L_1$(避免哈希函数碰撞的产生)的随机数 $h_1\in\{0,1\}^m$，添加 $\langle ID_i,U_i,Q_{ID_i},h_1\rangle$ 到 $\boldsymbol{L}_1$ 中，并返回 h_1 给 $\mathcal{A}_{I\text{-}1}$.

部分密钥生成询问：当 $\mathcal{B}$ 收到 $\mathcal{A}_{I\text{-}1}$ 关于 ID_i 和 X_{ID_i} 的部分密钥生成询问时，$\mathcal{B}$ 进行下述操作：

① 若有$\langle ID_i, X_{ID_i}, (y_{ID_i}, Y_{ID_i})\rangle \in L_D$，则返回相应元组中的$(y_{ID_i}, Y_{ID_i})$给$\mathcal{A}_{I\text{-}1}$；

② 否则，若$ID_i \neq ID_J$，则$\mathcal{B}$随机选取$y_{ID_i}, h_0^{ID_i} \in Z_p^*$，计算$Y_{ID_i} = y_{ID_i}P - h_0^{ID_i}P_{Pub}$；若$ID_i = ID_J$，则令$Y_{ID_i} = mP$(其中$m \in Z_p^*$是$\mathcal{B}$已知的参数)，选取满足等式$y_{ID_i}P = Y_{ID_i} + h_0^{ID_i}P_{Pub}$的随机数$y_{ID_i}, h_0^{ID_i} \in Z_p^*$；添加$\langle ID_i, X_{ID_i}, (y_{ID_i}, Y_{ID_i})\rangle$到$\boldsymbol{L}_D$中，添加$\langle ID_i, X_{ID_i}, Y_{ID_i}, h_0^{ID_i}\rangle$到$\boldsymbol{L}_0$中，并返回$(y_{ID_i}, Y_{ID_i})$给$\mathcal{A}_{I\text{-}1}$.

公钥生成询问：当$\mathcal{A}_{I\text{-}1}$对ID_i进行公钥生成询问时，$\mathcal{B}$进行下述操作：

① 若有$\langle ID_i, X_{ID_i}, Y_{ID_i}\rangle \in L_{PK}$，则$\mathcal{B}$返回相应的公钥$PK_i = \langle X_{ID_i}, Y_{ID_i}\rangle$给$\mathcal{A}_{I\text{-}1}$；

② 否则，若$ID_i \neq ID_J$，则$\mathcal{B}$选取$x_{ID_i} \in Z_p^*$，并计算$X_{ID_i} = x_{ID_i}P$；若$ID_i = ID_J$，则$\mathcal{B}$令$x_{ID_i} = n$，并计算$X_{ID_i} = nP$(其中$n \in Z_p^*$是$\mathcal{B}$已知的参数)；$\mathcal{B}$对ID_i和X_{ID_i}进行部分密钥生成询问，并获得相应的应答(y_{ID_i}, Y_{ID_i})，添加$\langle ID_i, X_{ID_i}, Y_{ID_i}\rangle$到$\boldsymbol{L}_{PK}$中，添加$\langle ID_i, x_{ID_i}, y_{ID_i}\rangle$到$\boldsymbol{L}_{SK}$中，并返回相应的公钥$PK_{ID_i} = \langle X_{ID_i}, Y_{ID_i}\rangle$给$\mathcal{A}_{I\text{-}1}$.

$\boldsymbol{H}_0$询问：当收到$\mathcal{A}_{I\text{-}1}$的询问$H_0(ID_i, X_i, Y_i)$时，若有$\langle ID_i, X_i, Y_i, h_0^{ID_i}\rangle \in L_0$成立.则$\mathcal{B}$返回$h_0^{ID_i}$给$\mathcal{A}_{I\text{-}1}$；否则，$\mathcal{B}$对$ID_i$进行公钥生成询问后，检索$\boldsymbol{L}_0$并返回相应的$h_0^{ID_i}$给$\mathcal{A}_{I\text{-}1}$.

私钥生成询问：当$\mathcal{A}_{I\text{-}1}$对ID_i进行私钥生成询问时，$\mathcal{B}$进行下述操作：

① 若有$\langle ID_i, x_{ID_i}, y_{ID_i}\rangle \in L_{SK}$，则$\mathcal{B}$返回相应的私钥$SK_i = \langle x_{ID_i}, y_{ID_i}\rangle$给$\mathcal{A}_{I\text{-}1}$；

② 否则，$\mathcal{B}$对ID_i进行公钥生成询问，则公钥生成询问中添加了相应的元组$\langle ID_i, x_{ID_i}, y_{ID_i}\rangle$到$\boldsymbol{L}_{SK}$中；$\mathcal{B}$在$\boldsymbol{L}_{SK}$中查找身份$ID_i$所对应的元组，并返回相应的私钥$SK_{ID_i} = \langle x_{ID_i}, y_{ID_i}\rangle$给$\mathcal{A}_{I\text{-}1}$.

公钥替换：$\mathcal{A}_{I\text{-}1}$能以任意的新公钥PK'_{ID_i}替换用户ID_i的原始公钥PK_{ID_i}.

广义签密询问：当收到$\mathcal{A}_{I\text{-}1}$关于ID_S、ID_R和M的广义签密询问时，算法$\mathcal{B}$进行下述操作：

① 若$ID_R \neq ID_J$，$\mathcal{B}$对ID_S进行私钥生成询问获得$SK_{ID_S} = \langle x_{ID_S}, y_{ID_S}\rangle$，对$ID_R$进行公钥生成询问获得$PK_{ID_R} = \langle X_{ID_R}, Y_{ID_R}\rangle$，$\mathcal{B}$运行广义签密算法$GSC(M, ID_S, SK_{ID_S}, ID_R, PK_{ID_R})$生成相应的密文(或签名)$\sigma = \langle U, V, C\rangle$，并返回$\sigma$给$\mathcal{A}_{I\text{-}1}$.

② 若$ID_R = ID_J$，则$\mathcal{B}$停止模拟，并退出.

解广义签密询问：当收到$\mathcal{A}_{I\text{-}1}$关于ID_S和ID_R及密文$\sigma = \langle U, V, C\rangle$的解广义签密询问时，$\mathcal{B}$针对$ID_S$查询列表$\boldsymbol{L}_{PK}$($\mathcal{A}_{I\text{-}1}$对$ID_S$已进行了公钥生成询问)，并进行下述操作：

① 若$\langle ID_S, X_{ID_S}, Y_{ID_S}\rangle \in L_{PK}$且$ID_R \neq ID_J$.$\mathcal{B}$对$ID_R$进行私钥生成询问，对$ID_S$进行公钥生成询问后，运行解广义签密算法$UnGSC(\sigma, ID_S, PK_{ID_S}, ID_R, SK_{ID_R})$对$\sigma = \langle U, V, C\rangle$进行解密，并返回相应的结果给$\mathcal{A}_{I\text{-}1}$.

② 若$\langle ID_S, X_{ID_S}, Y_{ID_S}\rangle \in L_{PK}$且$ID_R = ID_J$.当$\langle ID_S, X_{ID_S}, Y_{ID_S}, h_0^{ID_S}\rangle \in \boldsymbol{L}_0$和$\langle ID_R, U_{ID_R}, Q_{ID_R}, h_1\rangle \in L_1$，并且等式$VP = P_{Pub} + Y_{ID_S}h_0^{ID_S} + h_2^u X_{ID_S} + h_2^w U$(其中$h_2^u = H_2(ID_S, C, U, X_{ID_S})$和$h_2^w = H_2(ID_S, C, U, Y_{ID_S})$)成立，则$\mathcal{B}$返回$M = C \oplus h_1$给$\mathcal{A}_{I\text{-}1}$；否则，$\mathcal{B}$拒绝密文.

③ 若$\boldsymbol{L}_{PK}$中不存在相应的元组(公钥被替换).当$\langle ID_S, X'_{ID_S}, Y'_{ID_S}, h_0^{ID_S}\rangle \in \boldsymbol{L}_0$和$\langle ID_R, U_{ID_R}, Q_{ID_R}, h_1\rangle \in L_1$，并且等式$VP = P_{Pub} + Y'_{ID_S}h_0^{ID_S} + h_2'^u X'_{ID_S} + h_2'^w U$(其中$h_2'^u = H_2(ID_S, C, U, X'_{ID_S})$和$h_2'^w = H_2(ID_S, C, U, Y'_{ID_S})$)成立，则$\mathcal{B}$返回$M = C \oplus h_1$给$\mathcal{A}_{I\text{-}1}$；否则，$\mathcal{B}$拒绝密文.

挑战：第1阶段结束时，$\mathcal{A}_{I\text{-}1}$生成两个等长的挑战消息M_0和M_1及希望挑战的身份ID_S和ID_R，$\mathcal{B}$收到$\mathcal{A}_{I\text{-}1}$的挑战信息后进行下述操作：

① 若$ID_R \neq ID_J$，$\mathcal{B}$失败，并停止模拟.

② 若$ID_R = ID_J$，令$U = bP$，$\mathcal{B}$计算$Q_{ID_R} = U(x_{ID_R} + y_{ID_R})$，$h = H_1(ID_R, U, Q_{ID_R})$和$C = M_d \oplus h$(其中$d \leftarrow \{0, 1\}$)；选取满足等式$VP = P_{Pub} + Y_{ID_S}H_0(ID_S, X_{ID_S}, Y_{ID_S}) + u'X_{ID_S} + w'U$(其中$u' = H_2(ID_S, C, U, X_{ID_S})$和$w' = H_2(ID_S, C, U, Y_{ID_S})$)的随机数$V \in Z_p^*$，将密文$\sigma = \langle U, V, C\rangle$返回给$\mathcal{A}_{I\text{-}1}$.

模拟的最后，$\mathcal{A}_{I\text{-}1}$输出对d的猜测d'，若$d' = d$，$\mathcal{B}$输出$abP = (h_0^{ID_R})^{-1}(Q_{ID_R} - (n+m)U)$(其中$h_0^{ID_R} = H_0(ID_R, X_{ID_R}, Y_{ID_R})$)作为CDH问题的有效解；否则，$\mathcal{B}$终止并退出，即$\mathcal{B}$未解决CDH问题.

$\mathcal{B}$为$\mathcal{A}_{I\text{-}1}$模拟了真实的攻击环境，若$\mathcal{B}$在模拟过程中未终止，且$\mathcal{A}_{I\text{-}1}$以不可忽略的优势ε攻破本文广义签密机制的机密性，则$\mathcal{B}$同样能以不可忽略的优势解决CDH困难问题.

设δ为游戏中$\mathcal{A}_{I\text{-}1}$的挑战身份等于$\mathcal{B}$猜测身份的概率，则有$\delta = Pr[ID_R = ID_J] = \frac{1}{q_S + 1}$(下文中$\delta$

的含义与此相同，不再赘述）.

定义事件$\mathcal{E}$表示$\mathcal{A}_{\text{I-1}}$对挑战身份ID_S和ID_R未进行私钥生成询问；事件$\mathcal{E}_1$表示在询问阶段$\mathcal{B}$未终止，即广义签密询问过程中$\mathcal{B}$未终止；事件$\mathcal{E}_2$表示挑战阶段$\mathcal{B}$未终止，即挑战阶段$\mathcal{A}_{\text{I-1}}$选取的挑战身份ID_R就是$\mathcal{B}$的猜测身份ID_J. 则有$Pr[\mathcal{E}]=\left(1-\frac{q_{SK}}{2^k}\right)^2$，$Pr[\mathcal{E}_1]=(1-\delta)^{q_S}$和$Pr[\mathcal{E}_2]=\delta$. 因此，在模拟过程中$\mathcal{B}$不终止的概率为$\left(1-\frac{q_{SK}}{2^k}\right)^2(1-\delta)^{q_S}\delta$. 由于$\delta=\frac{1}{q_S+1}$，当$q_S$足够大时，有$(1-\delta)^{q_S}=\left(1-\frac{1}{q_S+1}\right)^{q_S}$趋向于$\mathrm{e}^{-1}$，因此，$\mathcal{B}$不终止的概率至少为$\left(1-\frac{q_{SK}}{2^k}\right)^2\frac{1}{\mathrm{e}(q_S+1)}$.

综上所述，若算法$\mathcal{B}$在模拟过程中未终止，并且敌手$\mathcal{A}_{\text{I-1}}$以不可忽略的优势ε攻破了本文广义签密机制的机密性，则算法$\mathcal{B}$输出CDH困难问题有效解的优势为$Adv(\mathcal{B})\geq\left(1-\frac{q_{SK}}{2^k}\right)^2\frac{\varepsilon}{\mathrm{e}(q_S+1)}$.　　证毕.

定理 3（$\mathcal{A}_{\text{II}}$类攻击下的机密性）.　在随机预言机模型中，若$\mathcal{A}_{\text{II}}$类敌手$\mathcal{A}_{\text{II-1}}$能以不可忽略的优势$\varepsilon$在多项式时间内赢得相关游戏（游戏的具体定义见文献[9]），$\mathcal{A}_{\text{II-1}}$最多进行$q_S$次广义签密询问和$q_{SK}$次私钥生成询问），则算法$\mathcal{B}$能以不可忽略的优势$Adv(\mathcal{B})\geq\left(1-\frac{q_{SK}}{2^k}\right)^2\frac{\varepsilon}{\mathrm{e}(q_S+1)}$（e是自然对数底数）在多项式时间内解决CDH困难问题.

证明思路与定理3类似，不再赘述.

4.2　不可伪造性

定理 4（$\mathcal{A}_{\text{I}}$类攻击下的不可伪造性）.　在随机预言机模型中，若$\mathcal{A}_{\text{I}}$类敌手$\mathcal{A}_{\text{I-2}}$能以不可忽略的优势ε在多项式时间内赢得相关游戏（游戏的具体定义见文献[9]），$\mathcal{A}_{\text{I-2}}$最多进行q_S次签名询问和q_{SK}次私钥生成询问），则算法$\mathcal{B}$能以不可忽略的优势$Adv(\mathcal{B})\geq\left(1-\frac{q_{SK}}{2^k}\right)\frac{\varepsilon}{\mathrm{e}(q_S+1)}$（e是自然对数底数）在多项式时间内解决DL困难问题.

证明.　令算法$\mathcal{B}$是DL困难问题解决者，其输入为元组(P,aP)，其中$a\in Z_p^*$且未知，目标是计算a. $\mathcal{B}$以敌手$\mathcal{A}_{\text{I-2}}$为子程序并充当游戏的挑战者. 游戏开始后，$\mathcal{B}$运行$Setup$算法并发送参数$Params=\langle p,G,P,P_{Pub},Fun(),\boldsymbol{H}_0,\boldsymbol{H}_1,\boldsymbol{H}_2\rangle$给$\mathcal{A}_{\text{I-2}}$，其中$P_{Pub}=aP$. $\mathcal{B}$维持列表$\boldsymbol{L}_0$，$\boldsymbol{L}_D$，$\boldsymbol{L}_{SK}$和$\boldsymbol{L}_{PK}$分别用于跟踪敌手$\mathcal{A}_{\text{I-2}}$对预言机$\boldsymbol{H}_0$的询问及对部分密钥生成、私钥生成和公钥生成询问，初始时各列表均为空. $\mathcal{B}$猜测ID_J（$J\in[1,q_S+1]$）是$\mathcal{A}_{\text{I-2}}$选取的挑战身份.

询问：敌手$\mathcal{A}_{\text{I-2}}$执行定理2中对预言机$\boldsymbol{H}_0$的询问、部分密钥生成、公钥生成、公钥替换和私钥生成询问.

签名询问：当收到$\mathcal{A}_{\text{I-2}}$关于ID_S及M的签名询问时，$\mathcal{B}$进行下述操作：

① 若$ID_S\neq ID_J$，$\mathcal{B}$对ID_S进行私钥生成询问获得$SK_{ID_S}=\langle x_{ID_S},y_{ID_S}\rangle$，$\mathcal{B}$运行签名算法$Sig(M,ID_S,SK_{ID_S})$生成签名$\sigma=\langle U,V,M\rangle$，并返回$\sigma$给$\mathcal{A}_{\text{I-2}}$.

② 若$ID_S=ID_J$，则$\mathcal{B}$停止模拟，并退出.

签名验证询问：当收到$\mathcal{A}_{\text{I-2}}$关于ID_S及$\sigma=\langle U,V,M\rangle$的签名验证询问时，算法$\mathcal{B}$针对$ID_S$查询列表$\boldsymbol{L}_{PK}$（$\mathcal{A}_{\text{I-2}}$对$ID_S$已进行了公钥生成询问），并进行下述操作：

① 若$\langle ID_S,X_{ID_S},Y_{ID_S}\rangle\in L_{PK}$且$ID_S\neq ID_J$. $\mathcal{B}$对ID_S进行公钥生成询问后，运行签名验证算法$UnSig(\sigma,ID_S,PK_{ID_S})$对$\sigma=\langle U,V,M\rangle$进行验证，并返回结果给$\mathcal{A}_{\text{I-2}}$.

② 若$\langle ID_S,X_{ID_S},Y_{ID_S}\rangle\in L_{PK}$且$ID_S=ID_J$. 当$\langle ID_S,X_{ID_S},Y_{ID_S},h_0^{ID_S}\rangle\in L_0$，且等式$VP=P_{Pub}+Y_{ID_S}h_0^{ID_S}+h_2^uX_{ID_S}+h_2^wU$（其中$h_2^u=H_2(ID_S,M,U,X_{ID_S})$和$h_2^w=H_2(ID_S,M,U,Y_{ID_S})$）成立，则$\mathcal{B}$返回$M$给$\mathcal{A}_{\text{I-2}}$；否则，$\mathcal{B}$拒绝密文.

③ 若$\boldsymbol{L}_{PK}$中不存在相应的元组（公钥被替换）. 当$\langle ID_S,X'_{ID_S},Y'_{ID_S},h_0^{ID_S}\rangle\in L_0$，且等式$VP=P_{Pub}+Y'_{ID_S}h_0^{ID_S}+h_2'^uX'_{ID_S}+h_2'^wU$（其中$h_2'^u=H_2(ID_S,M,U,X'_{ID_S})$和$h_2'^w=H_2(ID_S,M,U,Y'_{ID_S})$）成立，则$\mathcal{B}$返回$M$给$\mathcal{A}_{\text{I-2}}$；否则，$\mathcal{B}$拒绝密文.

伪造：经过多项式有界次上述询问后，敌手$\mathcal{A}_{\text{I-2}}$随机选取$r\in Z_p^*$，计算$U=rP$，选取满足等式$VP=P_{Pub}+Y_{ID_S}H_0(ID_S,X_{ID_S},Y_{ID_S})+u'X_{ID_S}+w'U$（其中$u'=H_2(ID_S,M,U,X_{ID_S})$和$w'=H_2(ID_S,M,U,Y_{ID_S})$）的随机数$V\in Z_p^*$，生成签名$\sigma=(U,V,M)$；则$\sigma$即为$\mathcal{A}_{\text{I-2}}$伪造的用户$ID_S$对消息$M$的签名.

$\mathcal{B}$知道被替换的公钥；若$\mathcal{A}_{\text{I-2}}$伪造了ID_S关于M的合法签名σ且$ID_S=ID_J$，则输出$a=(h_0^{ID_S})^{-1}(V-m-h_2^un-h_2^wr)$作为DL问题的有效解；否则，$\mathcal{B}$终止

并退出,即$\mathcal{B}$未解决 DL 问题.

定义事件$\mathcal{E}$表示$\mathcal{A}_{\text{I-2}}$对挑战身份 ID_S未进行私钥生成询问;事件$\mathcal{E}'$表示在询问阶段$\mathcal{B}$未终止;事件$\mathcal{E}''$表示挑战阶段$\mathcal{B}$未终止. 则有 $Pr[\mathcal{E}]=1-\frac{q_{SK}}{2^k}$, $Pr[\mathcal{E}']=(1-\delta)^{q_S}$和 $Pr[\mathcal{E}'']=\delta$. 则由定理 2 证明可知,整个模拟过程中$\mathcal{B}$不终止的概率至少为 $\left(1-\frac{q_{SK}}{2^k}\right)\frac{1}{\mathrm{e}(q_S+1)}$.

综上所述,若算法$\mathcal{B}$在模拟过程中未终止,且敌手$\mathcal{A}_{\text{I-2}}$以不可忽略的优势 ε 攻破本文广义签密机制的不可伪造性,则算法$\mathcal{B}$输出 DL 困难问题解的优势为 $Adv(\mathcal{B})\geq\left(1-\frac{q_{SK}}{2^k}\right)\frac{\varepsilon}{\mathrm{e}(q_S+1)}$. 证毕.

定理 5($\mathcal{A}_{\text{II}}$类攻击下的不可伪造性). 在随机预言机模型中,若$\mathcal{A}_{\text{II}}$类敌手$\mathcal{A}_{\text{II-2}}$能以不可忽略的优势 ε 在多项式时间内赢得相关游戏(游戏的具体定义见文献[9],$\mathcal{A}_{\text{II-2}}$最多进行 q_S次签名询问和 q_{SK} 次私钥生成询问),则算法$\mathcal{B}$能以不可忽略的优势 $Adv(\mathcal{B})\geq\left(1-\frac{q_{SK}}{2^k}\right)\frac{\varepsilon}{\mathrm{e}(q_S+1)}$(e 是自然对数底数)在多项式时间内解决 DL 困难问题.

证明思路与定理 4 类似,不再赘述.

5 效率分析

广义签密可根据实际应用环境的需求实现加密、签名和签密的功能,与相应的传统方案[10-12]相比,在实现相关功能时不能明显增加广义签密的计算复杂度.本节将综合分析本文方案与现有的广义签密方案[6-9]在实现加密、签名和签密等功能时的计算效率,具体的性能比较结果如表 1 所示. 表 1 中 E_E表示指数运算;E_B表示双线性映射运算.

表 1 相关方案的性能比较结果

相关方案	签密	解签密	签名	签名验证	加密	解密
方案[6]	$1E_E+1E_B$	$3E_E+4E_B$	$1E_E+1E_B$	$2E_E+3E_B$	$1E_E+1E_B$	$1E_E+3E_B$
方案[8]	$2E_E$	$1E_E+2E_B$	$2E_E$	$1E_E+1E_B$	$2E_E$	$1E_B$
方案[9]	$4E_E$	$4E_B$	$2E_E$	$2E_B$	$4E_E$	$4E_B$
方案[10]	—	—	$4E_E$	$3E_B$	—	—
方案[11]	—	—	—	—	$4E_E$	$4E_B$
方案[12]	$1E_E$	$3E_B$	—	—	—	—
本文方案	0	0	0	0	0	0

在计算效率方面,由于双线性映射和指数运算的计算复杂度高于点乘运算的计算时复杂度,因此指数运算和双线性映射的计算量是影响方案性能的主要因素,所以本文在表 1 中仅对各方案中的双线性映射和指数运算的次数进行了统计.

如表 1 所示,由于本文方案在密文(或签名)生成阶段和验证阶段均无需进行双线性映射和指数运算,与现有的广义签密方案[6-9]相比,本文方案具有较高的计算效率;相较与传统的加密[11]、签名[10]和签密[12]方案而言,本文方案实现加密功能时效率优于文献[11];实现签名功能时效率优于文献[10];实现签密功能时效率优于文献[12].

6 结束语

本文针对文献[9]中所提出的无证书广义签密方案,通过构造具体的攻击算法,证明了该方案无法满足其所声称的对$\mathcal{A}_{\text{I}}$类敌手的不可伪造性. 同时,本文提出了可证安全的不使用双线映射的无证书广义签密方案,并基于离散对数问题的困难性在随机预言机模型下对本文方案的机密性和不可伪造性进行了证明;与现有的相关方案相比,在未增加计算复杂度的前提下,本文方案高效地实现了加密、签名和签密的功能.

下一步我们将在本文方案的基础上继续进行标准模型下可证安全的高效无证书广义签密方案的相关研究.

致 谢 感谢审稿专家和编辑老师的细致审阅!

参 考 文 献

[1] Shamir A. Identity-based cryptosystems and signature schemes//Advances in Cryptology-Crypto 84. Berlin: Springer-Verlag, 1984: 47-53

[2] Al-Riyami S S, Paterson K G. Certificateless public key cryptography//Proceedings of the 9th International Conference on the Theory and Application of Cryptology and Information Security. Taipei, China, 2003: 452-473

[3] Han Yi-Liang, Yang Xiao-Yuan. New ECDSA-verifiable generalized signcryption. Chinese Journal of Computers, 2006, 29(11): 2003-2012(in Chinese)
(韩益亮，杨晓元. ECDSA 可公开验证广义签密. 计算机学报，2006，29(11)：2003-2012)

[4] Han Yi-Liang, Yang Xiao-Yuan, Wei Ping, et al. ECGSC: Elliptic curve based generalized signcryption//Proceedings of the 3rd International Conference Ubiquitous Intelligence and Computing. Wuhan, China, 2006: 956-965

[5] Han Yi-Liang, Gui Xiao-Lin. Adaptive secure multicast in wireless networks. International Journal of Communication System, 2009, 22(9): 1213-1239

[6] Yu Gang, Ma Xiao-Xiao, Shen Yong, et al. Provable secure identity based generalized signcryption scheme. Theoretical Computer Science, 2010, 411(40): 3614-3624

[7] Ji Hui-Fang, Han Wen-Bao, Liu Lian-Dong. Identity based generalized signcryption scheme for multiple PKGs in standard model. Journal of Electronics & Information Technology, 2011, 33(5): 1204-1210(in Chinese)
(冀会芳，韩文报，刘连东. 标准模型下多个 PKG 的基于身份广义签密. 电子与信息学报，2011，33(5)：1204-1210)

[8] Kushwah P, Lal S. Provable secure certificateless generalized signcryption scheme. International Journal of Computer Technology & Applications, 2012, 3(3): 925-939

[9] Liu Lian-Dong, Ji Hui-Fang, Han Wen-Bao, et al. Certificateless generalized signcryption scheme without random oracles. Journal of Software, 2012, 23(2): 394-410 (in Chinese)
(刘连东，冀会芳，韩文报等. 一种无随机预言机的无证书广义签密方案. 软件学报，2012，23(2)：394-410)

[10] Liu J K, Au M H, Susilo W. Self-generated-certificate public key cryptography and certificateless signature/encryption scheme in the standard model//Proceedings of the 2nd ACM Symposium on Information, Computer and Communications Security. New York, USA, 2007: 273-283

[11] Dent A W, Libert B, Paterson K G. Certificateless encryption schemes strongly secure in the standard model//Proceedings of the 11th International Workshop on Practice and Theory in Public-Key Cryptography. Barcelona, Spain, 2008: 344-359

[12] Li Peng-Cheng, He Ming-Xing, Li Xiao, et al. Efficient and provably secure certificateless signcryption from bilinear pairings. Journal of Computational Information Systems, 2010, 6(11): 3643-3650

ZHOU Yan-Wei, born in 1986, Ph. D. candidate. His research interests include cryptography and anonymous communication.

YANG Bo, born in 1963, Ph. D., professor, Ph. D. supervisor. His research interests include information security and cryptography.

ZHANG Wen-Zheng, born in 1966, professor. His research interest is information security.

Background

Public key cryptography is an important technique to realize network and information security. Traditional public key cryptography requires a trusted certification authority to issue a certificate binding the identity and the public key of an entity. Shamir defined a new public key cryptography called identity-based public key cryptography (ID-PKC). However, ID-PKC needs a trusted key generation center to generate the private key for every entity according to his identity. So we are confronted with the key escrow problem. Fortunately, the problems in traditional public key infrastructure and ID-PKC can be prohibited by certificateless public key cryptography.

A certificateless generalized signcryption scheme from bilinear maps was proposed by Liu et al. However, by giving a concrete algorithm for attacking the unforgeability, we find that Liu's certificateless generalized signcryption scheme is not secure. We propose a safely and efficient certificateless generalized signcryption scheme without bilinear pairings, whose security is based on Discrete Logarithm problem, and formal security proof is presented under the random oracle model, and compared with other certificateless generalized signcryption scheme in the computational complexity, our scheme is more efficient.

This research is supported by the National Natural Science Foundation of China under Grant Nos. 61272436, 61402275, 61303092 and 61572303. Foundation of Science and Technology on Communication Security Laboratory under Grant No. 9140C110206140C11050, Foundation of State Key Laboratory of Information Security under Grant No. 2015-MS-10, and Fundamental Research Funds for the Central Universities under Grant No. GK201504016. The team has published several research articles about anonymous communication, trusted computing, internet of things and cryptography, submitted three industry specifications for trusted digital home, and registered five computer software copyrights.