软件学报 ISSN 1000-9825, CODEN RUXUEW
Journal of Software,2012,23(2):394−410 [doi: 10.3724/SP.J.1001.2012.03947]

E-mail: jos@iscas.ac.cn
http://www.jos.org.cn
Tel/Fax: +86-10-62562563

一种无随机预言机的无证书广义签密方案*

刘连东[1], 冀会芳[2+], 韩文报[2], 赵 龙[2]

[1](信息工程大学 电子技术学院,河南 郑州 450004)

[2](信息工程大学 信息工程学院,河南 郑州 450002)

Certificateless Generalized Signcryption Scheme without Random Oracles

LIU Lian-Dong[1], JI Hui-Fang[2+], HAN Wen-Bao[2], ZHAO Long[2]

[1](Institute of Electronic Technology, Information Engineering University, Zhengzhou 450004, China)

[2](Institute of Information Engineering, Information Engineering University, Zhengzhou 450002, China)

+ Corresponding author: E-mail: huifangji@126.com

Liu LD, Ji HF, Han WB, Zhao L. Certificateless generalized signcryption scheme without random oracles. *Journal of Software*, 2012,23(2):394−410. http://www.jos.org.cn/1000-9825/3947.htm

Abstract: This paper studies generalized signcryptions in the certificateless public key settings. The paper proposes the formal definition and security model of certificateless generalized signcryption. The Type II adversary in the security model is malicious, but a passive Type II attacker. Also an efficient construction of certificateless generalized signcryption scheme using bilinear maps is also implemented. The security of proposed scheme is based on the infeasibility of the Computational Diffie-Hellman problem and Decision Bilinear Diffie-Hellman problem. The scheme is formally proven without random oracles under the security model of certificateless generalized signcryption schemes. Due to its security, high efficiency and freedom from certificate management, it may have practical applications in electronic cash payment, firewall and key distribution, etc.

Key words: certificateless cryptography; generalized signcryption; bilinear maps; standard model; provable security

摘 要: 研究在无证书公钥密码系统下的广义签密问题,提出了无证书广义签密方案的形式化定义,并定义其较为完全的安全模型.该安全模型下的第 2 类攻击者是恶意但被动的攻击者.同时,利用双线性映射设计了一个高效的无证书广义签密方案.其安全性基于计算Diffie-Hellman问题和判定性Bilinear Diffie-Hellman问题的困难性,并在标准模型下给出正式的安全性证明.鉴于该方案具有安全高效和无证书的优点,它可以广泛地应用于电子商务、防火墙和密钥分配等领域.

关键词: 无证书密码;广义签密;双线性映射;标准模型;可证明安全

中图法分类号: TP309 **文献标识码**: A

广义签密(generalized signcryptions,简称 GSC)是韩益亮等人提出的密码学概念[1].它能够实现 3 种功能:如

* 基金项目: 国家高技术研究发展计划(863)(2009AA01Z417); 国家重点基础研究发展计划(973)(2007CB807902); 新世纪优秀人才支持计划(NCET-07-0384)

收稿时间: 2010-05-28; 定稿时间: 2010-09-29

果需要同时满足机密性和认证性,那么它能提供签密功能;当仅要求满足机密性或认证性时,无须附加其他步骤即可单独实现加密或签名功能.一个安全的广义签密方案需要满足以下要求:在加密模式下,方案满足机密性;在签名模式下,方案满足不可伪造性;在签密模式下,方案满足机密性和不可伪造性.广义签密适用于用户之间需要频繁传输不同秘密级别消息的场合.为适应不同的环境,有关学者研究了广义签密的其他形式,提出了基于身份广义签密的概念[2].众所周知,一个传统的公钥密码系统需要昂贵而又繁琐的证书管理系统,而一个基于身份的密码系统则存在私钥泄露问题.

为了弥补上述不足,Al-Riyami 和 Paterson 提出了无证书密码系统(certificateless public key cryptography,简称 CL-PKC)的概念[3].在一个无证书密码系统中,用户私钥由用户和 PKG(private key generator)共同生成,用户公钥由其私钥和系统参数运算生成.这样既避免了传统公钥密码中的证书管理问题,又解决了基于身份密码系统中的私钥泄露问题.无证书密码系统在传统公钥密码系统和基于身份密码系统之间建立了很好的平衡,从而引起有关学者的广泛关注,许多无证书的签名方案、加密方案[4]乃至签密方案已被提出.鉴于无证书密码的优点和广义签密方案灵活多变的特性,构造安全、有效的无证书广义签密方案(certificateless generalized signcryption,简称 CLGSC)成为一个值得研究的问题.Barbosa 和 Farshim 给出了第一个无证书签密方案[5],其他一些学者也给出了在随机预言模型下可证明安全的无证书签密方案[6,7].文献[8]指出,这些方案均存在不同程度的安全弱点.文献[9]设计了第一个在标准模型下可证明安全的无证书签密方案.文献[10]指出该方案对第 1 类攻击者不满足机密性;文献[11]对其加以改进,利用一个基于 Schnorr 的一次性强不可伪造签名方案生成用户公钥,从而弥补了该方案的不足.设计在标准模型下可证明安全的无证书广义签密,是本文研究的出发点.

本文首先给出了 CLGSC 方案的形式化定义,其次定义了 CLGSC 的安全模型.在安全模型中,我们考虑第 2 类攻击者为恶意但被动的 KGC(key generator center)的情形,假设攻击者在生成系统参数时已经选定一个攻击对象,即具有恶意[12].同时,我们构造了一个在标准模型下可证明安全的具体方案,并在此安全模型下给出具体安全性证明.方案的安全性基于 CDH 假设和 DBDH 假设是困难的.

本文第 1 节介绍文中涉及的一些背景知识.第 2 节给出 CLGSC 的形式化定义和安全模型.第 3 节给出一个具体的 CLGSC 方案.方案的效率分析和安全性证明在第 4 节给出.第 5 节总结全文.

1 背景知识

1.1 双线性映射和困难假设

设 G_1,G_2 是两个素数 p 阶的循环乘法群,g 是 G_1 的一个随机生成元,一个双线性映射 $e:G_1\times G_1\to G_2$ 满足以下性质:

1. 双线性性:对任意的 $a,b\in Z_p^*$ 和 $g,h\in G_1$,都有 $e(g^a,h^b)=e(g,h)^{ab}$ 成立;
2. 非退化性:如果 $g,h\neq 1_{G_1}$,则 $e(g,h)\neq 1_{G_2}$;
3. 可计算性:对任意的 $g,h\in G_1$,存在一个有效的算法计算 $e(g,h)$.

CDH 假设. 给定三元组$(g\in G_1,A=g^a,B=g^b)$,其中,$a,b\in Z_p^*$ 且未知,G_1 是 p 阶循环乘法群,g 是 G_1 的生成元,计算性 Diffie-Hellman(CDH)问题定义为计算 g^{ab}.算法$\mathcal{A}$解决 CDH 问题的优势定义为 $\Pr[\mathcal{A}(g,A,B)=g^{ab}]$.如果不存在 t 时间的算法以至少ε的优势解决 CDH 问题,则称 CDH 假设是(ε,t)安全的.

DBDH 假设. 给定五元组$(g\in G_1,A=g^a,B=g^b,C=g^c,Z\in G_2)$,其中,$a,b,c\in Z_p^*$ 且未知,G_1 是 p 阶循环乘法群,g 是 G_1 的生成元,e 是定义在(G_1,G_2)上的双线性映射.判定性双线性 Diffie-Hellman(DBDH)问题定义为判断 $Z=e(g,g)^{abc}$ 是否成立.算法$\mathcal{A}$解决 DBDH 问题的优势定义为$|\Pr[\mathcal{A}(A,B,C,e(g,g)^{abc})=1]-\Pr[\mathcal{A}(A,B,C,Z)=1]|$.如果不存在 t 时间的算法以至少ε的优势解决 DBDH 问题,则称 DBDH 假设是(ε,t)安全的.

1.2 CL-PKC的有关定义

定义 1. 一个无证书密码方案

$$CL\text{-}PKC=(Setup,Extract\text{-}Partial\text{-}Private\text{-}Key,Set\text{-}User\text{-}Key,*,*)$$

由 5 种概率多项式时间算法组成.其中,Setup 算法和 Extract-Partial-Private-Key 算法由 PKG 执行,其他算法由用户执行.如果是加密方案(CLE),两个“*”分别为加密算法 Enc 和解密算法 Dec;如果是签名方案(CLS),两个“*”分别为签名算法 Sign 和验证算法 Ver;如果是签密方案(CLSC),两个“*”分别为签密算法 SC 和解签密算法 USC.以下是各算法的具体描述:

- Setup(系统建立):给定一个安全参数 k,PKG 利用该算法生成系统公开参数 *Params* 和主密钥 s.PKG 公开 *Params* 并保留 s.
- Extract-Partial-Private-Key(部分私钥生成):给定一个用户身份 *ID*,PKG 利用该算法为用户生成部分私钥 D.
- Set-User-Key(用户生成):给定一个用户身份 *ID* 及其对应的部分私钥 D,用户运行该算法生成自己的秘密值 x 和公钥 PK,用户私钥为 $S=(x,D)$.

一个 CLE 方案还包含以下两种算法:

- Enc(加密):给定一个消息 m、接收者身份 B 及其公钥 PK_B,发送者运行该算法生成密文 $\sigma=Enc(m,PK_B)$.
- Dec(解密):给定一个密文 σ,接收者利用其私钥 S,运行该算法恢复明文消息 $m=Dec(\sigma,S)$.

一个 CLS 方案还包含以下两种算法:

- Sign(签名):给定一个消息 m,发送者利用其私钥 S 生成 m 的签名 $\sigma=Sig(m,S)$.
- Ver(验证):给定一个消息 m 和签名者的公钥 PK 及其对消息 m 的签名 σ,验证者运行该算法验证签名的有效性.若签名是合法的,则输出 1;反之,则输出 0.

一个 CLSC 方案还包含以下两种算法:

- GC(签密):给定一个消息 m、发送者身份 A 和接收者身份 B 及公钥 PK_B,A 利用其私钥 S_A 运行该算法生成对消息 m 的签密 $\sigma=SC(m,S_A,PK_B)$.
- USC(解签密):给定一个密文 σ 和发送者身份 A,接收者 B 利用其私钥 S_B 和发送者公钥 PK_A 恢复消息 $m=USC(\sigma,S_B,PK_A)$.

2 CLGSC 的形式化定义和安全模型

2.1 CLGSC的形式化定义

定义 2. 一个无证书广义签密方案

$$CLGSC=(Setup,Extract\text{-}Partial\text{-}Private\text{-}Key,Set\text{-}User\text{-}Key,GSC,UGSC)$$

由以下 5 种概率多项式时间算法组成:

- Setup(系统建立):该算法和定义 1 中的 Setup 算法相同.
- Extract-Partial-Private-Key(部分私钥生成):该算法和定义 1 中的 Extract-Partial-Private-Key 算法相同.
- Set-User-Key(用户生成):该算法和定义 1 中的 Set-User-Key 算法相同.
- GSC(广义签密):给定一个消息 m、发送者身份 A 和接收者身份 B,
  - 如果 $A\in\varnothing$(即 $ID_A=0$ 从而 $S_A=0$),则 $\sigma\leftarrow GSC(m,0,PK_B)=Enc(m,PK_B)$;
  - 如果 $B\in\varnothing$(即 $ID_B=0$ 从而 $PK_B=0$),则 $\sigma\leftarrow GSC(m,S_A,0)=Sig(m,S_A)$;
  - 如果 $A\notin\varnothing$ 且 $B\notin\varnothing$,则 $\sigma\leftarrow GSC(m,S_A,PK_B)=SC(m,S_A,PK_B)$.
- UGSC(解广义签密):给定一个密文 σ、发送者的身份 A 和接收者的身份 B,
  - 如果 $A\in\varnothing$(即 $ID_A=0$ 从而 $PK_A=0$),则 $m\leftarrow GSC(m,0,S_B)=Dec(m,S_B)$;
  - 如果 $B\in\varnothing$(即 $ID_B=0$ 从而 $S_B=0$),则 $(1,0)\leftarrow UGSC(m,PK_A,0)=Ver(m,PK_A)$;
  - 如果 $A\notin\varnothing$ 且 $B\notin\varnothing$,则 $m\leftarrow UGSC(m,S_A,PK_B)=USC(m,S_A,PK_B)$.

这些算法满足一致性要求,即若 $\sigma=GSC(m,S_A,ID_B)$,则 $UGSC(S_B,\sigma,ID_A)$ 的输出包含消息 m(及其签名).据此,接收者 B 可以向第三方证明明文 m(及其签名)确实来自于发送者 A.

2.2 CLGSC的安全模型

本节我们定义 CLGSC 方案的安全模型.广义签密方案有 3 种工作模式,且每次只有 1 种发生.如文献[13]所述,攻击者可以得到更多的谕示服务.如考虑广义签密在加密模式下的机密性时,攻击者不但可以进行解密询问,还可以进行解签密询问,而解签密询问可能对攻击者解密挑战密文提供帮助.同样,考虑广义签密在签名模式下的不可伪造性时,攻击者可以进行签名询问和签密询问,而签密询问可能对攻击者的伪造提供帮助.考虑广义签密在签密模式下的机密性和不可伪造性时,解密询问可能对攻击者解签密挑战密文提供帮助,而签名询问则可能对攻击者的伪造提供帮助.另一方面,考虑加密方案安全性时,常强调解密询问而忽略加密询问.同样,考虑签名方案安全性时,常忽略验证询问.这是因为攻击者可以利用用户公钥实现加密和验证.这里,讨论方案安全性时考虑攻击者可以进行加密和解密询问、签名和验证询问、签密和解签密询问.

该模型是文献[9]定义的 CLSC 方案的安全模型的推广.考虑两类攻击者:第 1 类攻击者 A_{I} 和第 2 类攻击者 A_{II}.值得注意的是,在定义攻击游戏中,我们考虑第 2 类攻击者为恶意但被动 KGC 的情形,攻击者 A_{II} 可以自己生成系统参数和主密钥.

首先,我们给出攻击者可以进行的以下 10 种询问:

- Extract-Partial-Private-Key 询问:输入一个用户身份 *ID*,谕示返回与之对应的部分私钥 *D*.
- Extract-Private-Key 询问:输入一个用户身份 *ID*,谕示返回与之对应的私钥 *S*.
- Public-Key 询问:输入一个用户身份 *ID*,谕示返回与之对应的公钥 *PK*.
- Replace-Public-Key 询问:输入一个用户身份 *ID* 和一个合法的公钥 *PK′*,用 *PK′*替换用户 *ID* 的公钥 *PK*.
- Sign 询问:输入一个消息 *m* 和一个用户身份 *A*,谕示利用 *A* 的私钥 S_A 运行 Sign 算法,生成 *A* 对 *m* 的签名 σ并返回.如果用户 *A* 的公钥已被替换,则攻击者需要提供与新公钥对应的秘密值.
- Verify 询问:输入一个消息签名σ和签名者身份 *A*,谕示利用 *A* 的公钥 PK_A 运行 Ver 算法,并返回所得结果.
- Enc 询问:输入一个消息 *m* 和接收者身份 *B*,谕示利用 *B* 的公钥 PK_B 运行 Enc 算法对 *m* 进行加密,返回所得密文σ.
- Dec 询问:输入一个密文σ和接收者身份 *B*,谕示利用 *B* 的私钥 S_B 运行 Dec 算法对σ进行解密,并返回解密所得结果.如果用户 *B* 的公钥已被替换,则攻击者需要提供与新公钥对应的秘密值.
- SC 询问:输入一个消息 *m*、发送者身份 *A* 和接收者身份 *B*,谕示利用 *A* 的私钥 S_A 和 *B* 的公钥 PK_B 运行 SC 算法,对 *m* 进行签密,并返回签密结果σ.如果用户 *A* 的公钥已被替换,则攻击者需要提供与新公钥对应的秘密值.
- USC 询问:输入一个密文σ、发送者身份 *A* 和接收者身份 *B*,谕示利用 *B* 的私钥 S_B 和 *A* 的公钥 PK_A 运行 USC 算法,对σ进行解签密,并返回所得结果.如果用户 *B* 的公钥已被替换,则攻击者需要提供与新公钥对应的秘密值.

第 1 类攻击者可以访问以上所有询问,由于第 2 类攻击者拥有系统主密钥,因而无须进行 Extract-Partial-Private-Key 询问,但不能进行 Replace-Public-Key 询问.

无证书广义签密方案有 3 种工作模式:加密、签名和签密,分别记为 CLGSC-IN-EN,CLGSC-IN-SIGN 和 CLGSC-IN-SC.下面分别定义 CLGSC 在 3 种工作模式下的安全性.首先考虑 CLGSC-IN-EN 的机密性.该机密性通过以下定义的两个攻击游戏予以刻画:

游戏 1(挑战者 *C* 和攻击者 A_{I}):

系统建立:挑战者 *C* 运行 Setup 算法生成系统参数 *Params* 和系统主密钥 *s*,并把 *Params* 发送给 A_{I},保留 *s*.收到 *Params* 后,A_{I} 与 *C* 进行如下交互:

阶段 1:A_{I} 适用性地对以上定义的所有谕示进行最多多项式有界次的询问.

挑战阶段:A_{I} 输出一个身份 ID_{B^*}和两个挑战密文 m_0 和 m_1.*C* 选取一个随机比特$\gamma\in_R\{0,1\}$,利用 ID_{B^*}的公钥对 m_γ进行加密,返回所得挑战密文σ^*.

阶段 2:A_{I}继续进行同阶段 1 的询问.

猜测:A_{I}输出其对γ的猜测γ',如果$\gamma=\gamma'$,称 A_{I}赢得游戏.整个过程中,A_{I}满足以下限制:

(1) A_{I}不能对 ID_{B^*}进行 Extract-Private-Key 询问;

(2) A_{I}不能对公钥已被替换的用户进行 Extract-Private-Key 询问;

(3) 如果在挑战阶段之前 A_{I}已经替换了 ID_{B^*}的公钥,那么 A_{I}不能对 ID_{B^*}进行 Extract-Partial-Private-Key 询问;

(4) 在阶段 2,A_{I}不能对挑战密文σ^*在身份 ID_{B^*}下进行解密询问,除非对 m_γ进行加密的公钥 PK_{B^*}在挑战阶段之后被替换过.

定义 A_{I}的优势为

$$Adv_{A_{\mathrm{I}}}^{IND\text{-}(CLGSC\text{-}IN\text{-}EN)\text{-}CCA}=|2\Pr[\gamma'=\gamma]-1|.$$

游戏 2(挑战者 C 和攻击者 A_{II}):

系统建立:A_{II}运行 Setup 算法生成系统参数 *Params* 和系统主密钥 s,并把 *Params* 和 s 发送给挑战者 C.

阶段 1:A_{II}对以上定义的谕示进行最多多项式有界次的适用性询问,其中不能进行 Extract-Partial-Private-Key 询问和 Replace-Public-Key 询问.

挑战阶段:A_{II}输出一个身份 ID_{B^*}和两个挑战密文 m_0 和 m_1.C 选取一个随机比特$\gamma\in_R\{0,1\}$,利用 ID_{B^*}的公钥对 m_γ进行加密,返回所得挑战密文σ^*.

阶段 2:A_{II}继续进行同阶段 1 的询问.

猜测:A_{II}输出其对γ的猜测γ',如果$\gamma=\gamma'$,称 A_{II}赢得游戏.整个过程中,A_{II}满足以下限制:

(1) A_{II}不能对 ID_{B^*}进行 Extract-Private-Key 询问;

(2) 在阶段 2,A_{II}不能对挑战密文σ^*在身份 ID_{B^*}下进行解密询问.

定义 A_{II}的优势为

$$Adv_{A_{\mathrm{II}}}^{IND\text{-}(CLGSC\text{-}IN\text{-}EN)\text{-}CCA}=|2\Pr[\gamma'=\gamma]-1|.$$

定义 3(IND-(CLGSC-IN-EN)-CCA 安全). 一个 CLGSC 方案在加密模式下是 IND-CCA 安全的,如果不存在多项式时间有界的攻击者 A_{I}和 A_{II},以不可忽略的优势赢得上面定义的游戏 1 和游戏 2.

CLGSC-IN-SC 的机密性通过以下的游戏 1′和游戏 2′进行定义.

游戏 1′(挑战者 C 和攻击者 A_{I}'):

系统建立和阶段 1:挑战者 C 和攻击者 A_{I}'进行同游戏 1 中的操作.

挑战阶段: A_{I}'输出两个身份 ID_{A^*}和 ID_{B^*},两个挑战密文 m_0 和 m_1.C 选取一个随机比特$\gamma\in_R\{0,1\}$,利用 ID_{A^*}的私钥和 ID_{B^*}的公钥对 m_γ进行签密,返回所得挑战密文σ^*.

阶段 2: A_{I}'继续进行同阶段 1 的询问.

猜测: A_{I}'输出其对γ的猜测γ',如果$\gamma=\gamma'$,称 A_{I}'赢得游戏.整个过程中, A_{I}'满足游戏 1 中的限制(1)~限制(3),并且在阶段 2, A_{I}'不能对σ^*在身份 ID_{A^*}和 ID_{B^*}下进行解签密询问,除非对 m_γ进行签密的公钥 PK_{B^*}在挑战阶段之后被替换过.

定义 A_{I}'的优势为

$$Adv_{A_{\mathrm{I}}'}^{IND\text{-}(CLGSC\text{-}IN\text{-}SC)\text{-}CCA}=|2\Pr[\gamma'=\gamma]-1|.$$

游戏 2′(挑战者 C 和攻击者 A_{II}'):

系统建立和阶段 1:挑战者 C 和攻击者 A_{II}'进行同游戏 2 中的操作.

挑战阶段: A_{II}'输出两个身份 ID_{A^*}和 ID_{B^*},两个挑战密文 m_0 和 m_1.C 选取一个随机比特$\gamma\in_R\{0,1\}$,利用 ID_{A^*}的私钥和 ID_{B^*}的公钥对 m_γ进行签密,返回所得挑战密文σ^*.

阶段 2: A_{II}'继续进行同阶段 1 的询问.

猜测: A_{II}'输出其对γ的猜测γ',如果$\gamma=\gamma'$,称 A_{II}'赢得游戏.整个过程中, A_{II}'满足同游戏 2 中的限制(1),并且不能对挑战密文σ^*在身份 ID_{A^*}和 ID_{B^*}下进行解签密询问.

定义 A_{II}' 的优势为

$$Adv_{A_{\mathrm{II}}'}^{IND\text{-}(CLGSC\text{-}IN\text{-}SC)\text{-}CCA}=|2\Pr[\gamma'=\gamma]-1|.$$

定义 4(IND-(CLGSC-IN-SC)-CCA 安全). 一个 CLGSC 方案在签密模式下是 IND-CCA 安全的,如果不存在多项式时间有界的攻击者 A_{I}' 和 A_{II}',以不可忽略的优势赢得上面定义的攻击游戏 1′和游戏 2′.

值得注意的是,定义 3 和定义 4 之间的区别体现在以下两个方面:首先,在游戏 1 和游戏 2 中,攻击者不能对挑战密文σ^*进行解密询问,但是可以把σ^*变换为另一个有效的密文$\sigma^{*\prime}$,然后对$\sigma^{*\prime}$进行解签密询问;其次,在游戏 1′和游戏 2′中,攻击者不能对挑战密文σ^*进行解签密询问,但是可以把σ^*变换为另一个有效的密文$\sigma^{*\prime}$,然后对$\sigma^{*\prime}$进行解密询问.

下面通过两个攻击游戏来定义 CLGSC-IN-SIGN 的不可伪造性.

游戏 3(挑战者 C 和攻击者 F_{I}):

系统建立和阶段 1:挑战者 C 和攻击者 F_{I} 进行同游戏 1 中的操作.

伪造:F_{I}输出一个身份 ID_A和一个消息 m 的签名σ^*,如果 $Verify(m,\sigma^*,PK_A)$=1,并且σ^*不是任意一个在身份 ID_A 下的签名询问的输出,则称 F_{I} 赢得游戏.以上过程中,F_{I}需要满足以下限制:

(1) F_{I}不能对 ID_{A^*}进行 Extract-Private-Key 询问和 Extract-Partial-Private-Key 询问;

(2) F_{I}不能对公钥已被替换的用户进行 Extract-Private-Key 询问.

定义 F_{I}的成功概率为

$$Succ_{F_{\mathrm{I}}}^{EUF\text{-}(CLGSC\text{-}IN\text{-}SIGN)\text{-}ACM}=\Pr[F_{\mathrm{I}}\ wins].$$

游戏 4(挑战者 C 和攻击者 F_{II}):

系统建立和阶段 1:挑战者 C 和攻击者 F_{II}进行同游戏 2 中的操作.

伪造:F_{II} 输出一个身份 ID_A 和一个消息 m 的签名σ^*,如果 $Verify(m,\sigma^*,PK_A)$=1,并且σ^*不是任意一个在身份 ID_A 下的签名询问的输出,则称 F_{II} 赢得游戏.以上过程中,F_{II} 不能对 ID_{A^*}进行 Extract-Private-Key 询问.

定义 F_{II}的成功概率为

$$Succ_{F_{\mathrm{II}}}^{EUF\text{-}(CLGSC\text{-}IN\text{-}SIGN)\text{-}ACM}=\Pr[F_{\mathrm{II}}\ wins].$$

定义 5(EUF-(CLGSC-IN-SIGN)-ACM 安全). 一个 CLGSC 方案在签名模式下是 EUF-ACM 安全的,如果不存在多项式时间有界的攻击者 F_{I}和 F_{II},以不可忽略的优势赢得上面定义的攻击游戏 3 和游戏 4.

CLGSC-IN-SC 的不可伪造性通过下面的游戏 3′和游戏 4′刻画.

游戏 3′(挑战者 C 和攻击者 F_{I}'):

系统建立和阶段 1:挑战者 C 和攻击者 F_{I}' 进行同游戏 1 中的操作.

伪造: F_{I}' 输出两个身份 ID_A 和 ID_B、一个密文σ^*.用 ID_B 的私钥对σ^*进行解签密,所得结果记为(m^*,X^*,V^*).如果 $ID_A\neq 0, ID_A\neq ID_B, Verify(m^*,X^*,V^*)=1$,并且$(\sigma^*,ID_A,ID_B)$不是任意一个签密询问的输出,则称 F_{I}' 赢得游戏.以上过程中, F_{I}' 需要满足以下限制:

(1) F_{I}' 不能对 ID_{A^*}进行 Extract-Private-Key 询问和 Extract-Partial-Private-Key 询问;

(2) F_{I}' 不能对公钥已被替换的用户进行 Extract-Private-Key 询问.

定义 F_{I}' 的成功概率为

$$Succ_{F_{\mathrm{I}}'}^{EUF\text{-}(CLGSC\text{-}IN\text{-}SC)\text{-}ACM}=\Pr[F_{\mathrm{I}}'\ wins].$$

游戏 4′(挑战者 C 和攻击者 F_{II}'):

系统建立和阶段 1:挑战者 C 和攻击者 F_{II}' 进行同游戏 2 中的操作.

伪造: F_{II}' 输出两个身份 ID_A 和 ID_B、一个密文σ^*.用 ID_B 的私钥对σ^*进行解签密,所得结果记为(m^*,X^*,V^*).如果 $ID_A\neq 0, ID_A\neq ID_B, Verify(m^*,X^*,V^*)=1$,并且$(\sigma^*,ID_A,ID_B)$不是任意一个签密询问的输出,则称 F_{II}' 赢得游戏.以上过程中, F_{II}' 不能对 ID_{A^*}进行 Extract-Private-Key 询问.

定义 F_{II}' 的成功概率为

$$Succ_{F_{II}'}^{EUF\text{-}(CLGSC\text{-}IN\text{-}SC)\text{-}ACM} = \Pr[F_{II}' \ wins].$$

定义 6(EUF-(CLGSC-IN-SC)-ACM 安全). 一个 CLGSC 方案在签密模式下是 EUF-ACM 安全的,如果不存在多项式时间有界的攻击者 F_I' 和 F_{II}',以不可忽略的优势赢得上面定义的攻击游戏 3′和游戏 4′.

值得注意的是,定义 5 和定义 6 之间的区别体现在以下两个方面:首先,在游戏 3 和游戏 4 中,攻击者伪造的签名不是任意一个签名询问的输出,但可能是由某个签密询问的输出经变换得到的;同样,在游戏 3′和游戏 4′中,攻击者伪造的签密不是任意一个签密询问的输出,但可能是由某个签名询问的输出经变换得到的.

3 具体方案

本节给出一个在标准模型下可以抵抗恶意但被动的 KGC 攻击的无证书广义签密方案,这里假设所有的用户身份都是 n 长的比特串.该方案还可以推广到所有用户身份是任意长比特串的情形,只需要利用一个抗碰撞的 Hash 函数把所有用户身份都映射为 n 长的比特串.该方案是在文献[14]及其变体的基础上给出的.

设 G_1,G_2 和 $e:G_1\times G_1\to G_2$ 如第 1 节中定义,g 是 G_1 的随机生成元.记 $a\in_R B$ 为从集合 B 中随机选择元素 a. 方案的具体描述如下:

Setup:PKG 随机选择 $\alpha\in Z_p^*$,计算 $g_1=g^\alpha$,选择 $g_2\in_R G_1$.选择元素 $u',v'\in_R G_1$,选择向量 $U=(u_i)_{1\leqslant i\leqslant n}$,$V=(v_i)_{1\leqslant i\leqslant m}$,其中,$u_i,v_j\in_R G_1$,$1\leqslant i\leqslant n$,$1\leqslant j\leqslant m$.定义两个函数:

$$F_u(ID)=u'\prod_{j=1}^{n}u_j^{i_j},\ F_v(w)=v'\prod_{j=1}^{m}v_j^{w_j},$$

其中,$ID=i_1i_2\ldots i_n$ 和 $w=w_1w_2\ldots w_m$ 分别为 n 长和 m 长比特串.定义两个抗碰撞的 Hash 函数 $H_1:\{0,1\}^*\to Z_p^*$ 和 $H_2:\{0,1\}^*\to\{0,1\}^m$.系统参数定义为 $mpk=(g,g_1,g_2,u',U,v',V,H_1,H_2)$,主密钥为 $msk=g_2^\alpha$.

Extract-Partial-Private-Key:给定一个用户身份 ID,PKG 随机选取 $r\in_R Z_p^*$,计算 ID 的部分私钥:

$$d_{ID}=(d_1,d_2)=(g_2^\alpha\cdot F_u(ID)^r,g^r).$$

Set-User-Key:用户 ID 随机选取 x_{ID} 为其秘密值,用户公钥及其签名为

$$PK_{ID}=(K,h,pk_{ID},Y,z)=(ID,e(g_1,g_2),e(g_1,g_2)^{x_{ID}},e(g_1,g_2)^{y_{ID}},y_{ID}+cx_{ID}\ \bmod p),$$

其中,$c=H_1(ID,Y\|mpk)$,用户随机选取 $r'\in_R Z_p^*$,其私钥定义为

$$sk_{ID}=(s_{ID,1},s_{ID,2})=(d_1^{x_{ID}}\cdot F_u(ID)^{r'},d_2^{x_{ID}}\cdot g^{r'})=(g_2^{\alpha x_{ID}}\cdot F_u(ID)^t,g^t),$$

其中,$t=t'+rx_{ID}$.

GSC:分以下 3 种情况讨论:

(1) SC:给定一个消息 $M\in G_2$ 和一个接收者身份 B,发送者 A 首先通过等式 $h^z=Y\cdot pk_B^c$ 是否成立来验证 B 的公钥是否有效.如果无效,则停止;否则,A 随机选取 $s\in_R Z_p^*$,生成密文 σ 为

$$\sigma=(\sigma_0,\sigma_1,\sigma_2,\sigma_3,\sigma_4)=(M\cdot pk_B^s,g^s,F_u(B)^s,sk_{A,2},sk_{A,1}\cdot F_v(w)^s),$$

其中,$w=H_2(\sigma_0,\sigma_1,\sigma_2,\sigma_3,B,pk_B)$.

(2) Sign:给定一个消息 $M\in G_2$,签名者 A 随机选取 $s\in_R Z_p^*$,生成其对 M 的签名 σ 为

$$\sigma=(\sigma_0,\sigma_1,\sigma_2,\sigma_3,\sigma_4)=(M,g^s,1,sk_{A,2},sk_{A,1}\cdot F_v(w)^s),$$

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

(3) Enc:给定一个消息 $M\in G_2$,加密者首先通过等式 $h^z=Y\cdot pk_B^c$ 是否成立来验证 B 的公钥是否有效.如果无效,则停止;否则,A 随机选取 $s\in_R Z_p^*$,生成密文 σ 为

$$\sigma=(\sigma_0,\sigma_1,\sigma_2,\sigma_3,\sigma_4)=(M\cdot pk_B^s,g^s,F_u(B)^s,1,F_v(w)^s),$$

其中,$w=H_2(\sigma_0,\sigma_1,\sigma_2,\sigma_3,B,pk_B)$.

UGSC:给定一个密文 σ 和一个接收者身份 B,接收者执行如下步骤:

(1) 计算

$$\begin{cases} w = H_2(\sigma_0,\sigma_1,\sigma_2,\sigma_3,0,1), & \sigma_2 = 1 \\ w = H_2(\sigma_0,\sigma_1,\sigma_2,\sigma_3,B,pk_B), & \text{else} \end{cases}.$$

(2) 验证

$$\begin{cases} e(g,\sigma_2\cdot\sigma_4) = e(\sigma_1,F_u(B)\cdot F_v(w)), & \sigma_3 = 1 \\ e(g,\sigma_4) = pk_A\cdot e(F_u(A),\sigma_3)\cdot e(F_v(w),\sigma_1), & \text{else} \end{cases}$$

是否成立.如果不成立,则返回 0;否则继续.

如果σ_2=1,则返回 1 表示σ是 M 的一个合法签名;否则,返回 $M = \sigma_0\cdot\dfrac{e(\sigma_2,sk_{B,2})}{e(\sigma_1,sk_{B,1})}$.

4 方案分析

4.1 正确性分析

方案的正确性很容易通过以下等式得到:

当σ_3=1 时,

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

否则,

$$\begin{aligned} e(g,\sigma_4) &= e(g,sk_{A,1}\cdot F_v(w)^s) \\ &= e(g,g_2^{\alpha x_A}\cdot F_u(A)^t\cdot F_v(w)^s) \\ &= e(g,g_2^{\alpha x_A})e(g,F_u(A)^t)e(g,F_v(w)^s) \\ &= e(g_1,g_2)^{x_A}\cdot e(g^t,F_u(A))\cdot e(g^s,F_v(w)) \\ &= pk_A\cdot e(\sigma_3,F_u(A))\cdot e(\sigma_1,F_v(w)), \end{aligned}$$

且

$$\begin{aligned} \sigma_0\cdot\frac{e(\sigma_2,sk_{B,2})}{e(\sigma_1,sk_{B,1})} &= M\cdot pk_B^s\cdot\frac{e(F_u(B)^s,g^{t_B})}{e(g^s,g_2^{\alpha x_B}\cdot F_u(B)^{t_B})} \\ &= M\cdot pk_B^s\cdot\frac{e(F_u(B)^s,g^{t_B})}{e(g^s,g_2^{\alpha x_B})e(g^s\cdot F_u(B)^{t_B})} \\ &= M\cdot e(g_1,g_2)^{x_B\cdot s}\cdot\frac{e(F_u(B)^{t_B},g^s)}{e(g^s,g_2^{\alpha x_B})e(g^s\cdot F_u(B)^{t_B})} \\ &= M. \end{aligned}$$

4.2 效率分析

广义签密的主要目的是降低操作复杂度,即方案在实现签密、签名和加密功能时,与普通的签密、签名和加密方案相比,计算复杂度不能有明显的增加.表 1 给出了我们的方案和文献[9,15,16]中方案的效率比较.M 表示数乘运算,E 表示指数运算,P 表示对运算.

在计算效率方面,本文方案在签名模式下效率高于文献[15]中签名方案,在签密模式下与文献[9]的签密方案效率相当,在加密模式下与文献[16]中的加密方案效率相当.文献[15]中加密方案还需要一个 MAC 方案和密钥封装机制来实现加密,因而效率并不高.本文方案弥补了以上方案中不满足机密性或不能抵抗恶意但被动 KGC 攻击的弱点,利用一个强不可伪造的一次签名方案生成用户公钥,并且考虑第 2 类攻击者为恶意但被动攻击者的情况,因此是在标准模型下可证明安全的.

Table 1 Efficiency comparison between certificateless schemes

表 1 无证书密码方案效率比较

方案	签密	解签密	签名	验证	加密	解密
文献[15]的签名方案	—	—	$(m+4)M+4E$	$(m+3)M+3P$	—	—
文献[15]的加密方案	—	—	—	—	$2M+5E$	$2M+1E+3P$
文献[16]的加密方案	—	—	—	—	$(m+2)M+4E$	$(m+6)M+4P$
文献[9]的签密方案	$(m+3)M+4E$	$(m+6)M+4P$	—	—	—	—
本文的方案	$(m+3)M+4E$	$(m+6)M+4P$	$(m+2)M+2E$	$(m+2)M+2P$	$(m+2)M+4E$	$(m+6)M+4P$

4.3 安全性分析

本节给出我们提出的方案在第 2.2 节定义的安全模型下的安全结论.我们的结果都是在标准模型下得到的.在以下结果中,假设攻击者可进行 $q_{pp}/q_p/q_{pk}/q_r/q_{enc}/q_{dec}/q_{sign}/q_{ver}/q_{sc}/q_{usc}$ 次 Extract-Partial-Private-Key/Extract-Private-Key/Public-Key/Replace-Public-Key/Enc/Dec/Sign/Ver/SC/USC 询问,当攻击者为第 2 类攻击者时,

$$q_{pp}=q_r=0.$$

定理 1. 在 DBDH 假设下,文中给出的 CLGSC 方案在加密模式下是语义安全的,即 IND-(CLGSC-IN-EN)-CCA 安全的.

定理 1 的证明可由以下的引理 1 和引理 2 得到.

引理 1. 假设存在一个 IND-CCA 的 t 时间的第 1 类攻击者 A_1 可以 ε 的优势赢得第 2.2 节定义的游戏 1,则存在一个区分者 $\mathcal{C}$ 可在时间 t' 内以 ε' 的优势解决 DBDH 问题.其中,

$$\varepsilon' \geqslant \varepsilon/16(n+1)(m+1)(q_{pp}+q_p+q_{sign}+q_{sc}+q_{dec}+q_{usc})(q_{dec}+q_{usc}),$$

$$t' = t + O(t_m(n(q_{pp}+q_p+q_{sign}+q_{ver}+q_{enc}+q_{dec}+q_{sc}+q_{usc})+m(q_{sign}+q_{ver}+q_{enc}+q_{dec}+q_{sc}+q_{usc})+q_{pk})+ t_e(q_{pp}+q_p+q_{pk}+q_{sign}+q_{enc}+q_{dec}+q_{sc}+q_{usc})+t_p(q_{ver}+q_{dec}+q_{usc})).$$

证明:假设一个区分者 $\mathcal{C}$ 收到一个随机的 DBDH 问题实例 $(g,A=g^a,B=g^b,C=g^c,Z\in G_2)$,他需要判定 $Z=e(g,g)^{abc}$ 是否成立.$\mathcal{C}$ 运行游戏 1 中的攻击者 A_1,并且扮演其中的挑战者.为了避免发生碰撞,$\mathcal{C}$ 维护一个初始为空的列表

$$\mathcal{DB}=\{(ID,d_{ID},x_{ID},PK_{ID},sk_{ID},sta=0)\}.$$

Setup:令 $\tau_u=2(q_{pp}+q_p+q_{sign}+q_{sc}+q_{dec}+q_{usc})$, $\tau_v=2(q_{dec}+q_{usc})$,$\mathcal{C}$ 随机选择以下参数:

两个整数 $k_u\in_R\{0,1,\ldots,n\}$ 和 $k_v\in_R\{0,1,\ldots,m\}$,假设 $\tau_u(n+1)<p$, $\tau_v(m+1)<p$;

选择 $x'_u\in_R Z_{\tau_u}, x_{u,i}\in_R Z_{\tau_u}, i=1,...,n$;选择 $x'_v\in_R Z_{\tau_v}, x_{v,j}\in_R Z_{\tau_v}, j=1,...,m$;

选择 $y'_u,y'_v\in_R Z_p, y_{u,i},y_{v,j}\in_R Z_p, i=1,...,n, j=1,...,m$;

为便于分析,定义函数

$$J_u(ID)=x'_u+\sum_{j=1}^{n}i_jx_{u,j}-k_u\tau_u, K_u(ID)=y'_u+\sum_{j=1}^{n}i_jy_{u,j},$$

$$J_v(w)=x'_v+\sum_{j=1}^{m}w_jx_{v,j}-k_v\tau_v, K_v(w)=y'_v+\sum_{j=1}^{m}w_jy_{v,j},$$

其中,$ID=i_1\ldots i_n$ 和 $w=w_1\ldots w_m$ 分别为 n 长和 m 长比特串.

$\mathcal{C}$ 设定系统参数为

$$g_1=g^a, g_2=g^b; u'=g_2^{x'_u-k_u\tau_u}g^{y'_u}, u_i=g_2^{x_{u,i}}g^{y_{u,i}}, i=1,...,n; v'=g_2^{x'_v-k_v\tau_v}g^{y'_v}, v_j=g_2^{x_{v,j}}g^{y_{v,j}}, j=1,...,m.$$

这些参数和游戏 1 中的参数具有相同的分布,系统公开参数 $mpk=(g_1,g_2,u',u_i,i=1,\ldots,n,v',v_j,j=1,\ldots,m,H_1,H_2)$,系统主密钥为 $g_2^{\alpha}=g_2^a=g^{ab}$. 对任意的身份 ID 和 $w\in\{0,1\}^m$,有

$$F_u(ID)=u'\prod_{j=1}^{n}u_j^{i_j}=g_2^{J_u(ID)}\cdot g^{K_u(ID)}, F_v(w)=v'\prod_{j=1}^{m}v_j^{w_j}=g_2^{J_v(w)}\cdot g^{K_v(w)}.$$

Phase 1. $\mathcal{C}$ 按照如下方式回答 A_1 的所有询问:

- Extract-Partial-Private-Key:输入一个身份 ID,$\mathcal{C}$ 首先查询 $\mathcal{DB}$ 中是否存在相应的值,如果存在,则返回 d_{ID};

否则,$\mathcal{C}$按照如下方式生成 d_{ID}:

如果 $J_u(ID)\neq 0 \bmod p$,$\mathcal{C}$选取 $r\in_R Z_p^*$,计算 $d_{ID}=(d_1,d_2)=\left(g_1^{-K_u(ID)/J_u(ID)}\cdot F_u(ID)^r, g_1^{-1/J_u(ID)}\cdot g^r\right)=(g_2^a\cdot F_u(ID)^{\tilde{r}}, g^{\tilde{r}})$,

其中,$\tilde{r}=r-\dfrac{a}{J_u(ID)}$;否则,如果 $J_u(ID)=0 \bmod p$,则模拟终止,$\mathcal{C}$返回一个随机比特.

为简便起见,如果 $J_u(ID)=0 \mod \tau_u$,则模拟终止.事实上,根据 $\tau_u(n+1)<p$,有 $0\leqslant \tau_u k_u<p$ 和 $0\leqslant x'_u+\sum_{j=1}^{n} i_j x_{u,j}<p$ 成立,有 $-p<J_u(ID)<p$,从而得到:$J_u(ID)=0 \bmod p \Rightarrow J_u(ID)=0 \bmod \tau_u$,因此有 $J_u(ID)\neq 0 \bmod \tau_u \Rightarrow J_u(ID)\neq 0 \bmod p$.

• Extract-Private-Key:输入一个身份 ID,$\mathcal{C}$首先查询$\mathcal{DB}$中是否存在相应的值,如果存在,则返回 sk_{ID};否则,$\mathcal{C}$按照如下方式生成 sk_{ID}:

如果 $J_u(ID)\neq 0 \mod \tau_u$,$\mathcal{C}$随机选取 $t\in Z_p^*$,如果需要,则$\mathcal{C}$先运行 Set-User-Key 算法生成(x_{ID},PK_{ID}),计算 $sk_{ID}=(sk_{ID,1},sk_{ID,2})=(g_1^{x_{ID}})^{-K_u(ID)/J_u(ID)}\cdot F_u(ID)^t, (g_1^{x_{ID}})^{-1/J_u(ID)}\cdot g^t)=(g_2^{ax_{ID}}\cdot F_u(ID)^{\tilde{t}}, g^{\tilde{t}})$, 其中,$\tilde{t}=t-\dfrac{ax_{ID}}{J_u(ID)}$; 否则,如果 $J_u(ID)=0 \mod \tau_u$,则模拟终止,$\mathcal{C}$返回一个随机比特.如果$\mathcal{C}$的公钥已被替换,则$\mathcal{C}$询问 A_1 相应的 x'_{ID},然后进行同样的操作.

• Public-Key-Query:$\mathcal{C}$查询$\mathcal{DB}$中是否存在相应的值,如果存在,则返回 PK_{ID};否则,运行 Set-User-Key 算法生成(x_{ID},PK_{ID}), $PK_{ID}=(K,h,pk_{ID},Y,z)=(ID,e(g_1,g_2),e(g_1,g_2)^{x_{ID}},e(g_1,g_2)^{y_{ID}},y_{ID}+cx_{ID} \bmod p)$,其中,$c=H_1(K,Y||mpk)$,然后返回 PK_{ID}.

• Replace-Public-Key:输入一个身份 ID 和一个合法的公钥 PK',如果 ID 的公钥 PK_{ID} 存在,则用 PK'替换 PK_{ID};否则,$\mathcal{C}$运行 Set-User-Key 算法生成(x_{ID},PK_{ID}),然后用 PK'替换 PK_{ID},并置 sta=1.

• Sign:输入(M,ID_A),如果 $J_u(ID_A)\neq 0 \mod \tau_u$,则$\mathcal{C}$首先运行 Extract-Partial-Private-Key 算法生成 d_A,若 x_A 不存在,则运行 Set-User-Key 算法生成(x_A,PK_A,sk_A),然后运行 Sign 算法生成 ID_A 关于 M 的签名;如果 $J_u(ID_A)=0 \mod \tau_u$,则模拟终止,$\mathcal{C}$返回一个随机比特.

• Ver:输入(σ,ID_A),首先计算 $w=H_2(\sigma_0,\sigma_1,1,\sigma_3,0,1)$,如果 $e(g,\sigma_4)=pk_A\cdot e(F_u(ID_A),\sigma_3)\cdot e(F_v(w),\sigma_1)$,则返回 1;否则,返回 0.

• Enc:输入(M,ID_B),$\mathcal{C}$查询$\mathcal{DB}$中 PK_B 是否存在,如果存在,则通过 $h_B^{z_B}=Y_B\cdot pk_B^c$ 是否成立验证公钥合法性.若合法,则运行 Enc 算法生成密文 $\sigma=(M\cdot pk_B^s, g^s, F_u(ID_B)^s, 1, F_v(w)^s)$,其中,$w=H_2(\sigma_0,\sigma_1,\sigma_2,1,B,pk_B)$.

• Dec:输入(σ,ID_B),$\mathcal{C}$首先查询$\mathcal{DB}$得到 PK_B,计算 $w=H_2(\sigma_0,\sigma_1,\sigma_2,1,B,pk_B)$,判定 $e(g,\sigma_2\cdot\sigma_4)=e(\sigma_1,F_u(ID_B)\cdot F_v(w))$是否成立.如果不成立,则输出 0;否则,分以下两种情况讨论:

(1) 若 sta_B=0 且 $J_u(ID_B)\neq 0 \mod \tau_u$,$\mathcal{C}$可以得到 sk_B,进而利用 Dec 算法对σ进行解密并返回所得结果.如果必要,则首先运行 Extract-Partial-Private-Key 和 Extract-Private-Key 算法生成 d_B 和 sk_B,然后进行解密.

(2) 若 sta_B=1 或 $J_u(ID_B)=0 \mod \tau_u$,如果 $J_v(w)=0 \mod \tau_v$,则终止模拟,$\mathcal{C}$返回一个随机比特;否则,$\mathcal{C}$查询$\mathcal{DB}$得到(x_B,PK_B)(若 sta_B=1,$\mathcal{C}$询问 A_1 获得与新公钥相应的秘密值 x'_B),计算 $M=\sigma_0/e(g_1^{x_B},g_2^s)$, 其中, $g_2^s=\left(\dfrac{\sigma_4}{\sigma_1^{K_v(w)}}\right)^{1/J_v(w)}$.

• SC:输入(M,ID_A,ID_B),如果 $J_u(ID_A)\neq 0 \mod \tau_u$,$\mathcal{C}$查询$\mathcal{DB}$得到$(x_A,PK_A,sk_A)$和 PK_B,运行 SC 算法生成密文σ并返回.如果必要,则首先运行 Extract-Partial-Private-Key 算法,生成 d_A,运行 Set-User-Key 算法生成(x_A,PK_A,sk_A)和(x_B,PK_B),然后生成密文;否则,如果 $J_u(ID_A)=0 \mod \tau_u$,则模拟终止,$\mathcal{C}$返回一个随机比特.

• USC:输入(σ,ID_A,ID_B),$\mathcal{C}$首先查询$\mathcal{DB}$得到 PK_B,计算 $w=H_2(\sigma_0,\sigma_1,\sigma_2,\sigma_3,B,pk_B)$,判定 $e(g,\sigma_4)=pk_A\cdot e(F_u(ID_A),\sigma_3)\cdot e(F_v(w),\sigma_1)$是否成立,如果不成立,则输出 0;否则,分以下两种情况讨论:

(1) 若 sta_B=0 且 $J_u(ID_B)\neq 0 \mod \tau_u$,$\mathcal{C}$可以得到 sk_B,进而利用 USC 算法对σ进行解签密并返回所得结果.如果必要,则首先运行 Extract-Partial-Private-Key 和 Extract-Private-Key 算法生成 d_B 和 sk_B,然后进行解签密.

(2) 若 sta_B=1 或 $J_u(ID_B)$=0 mod τ_u,如果 $J_v(w)$=0 mod τ_v,则终止模拟,$\mathcal{C}$返回一个随机比特;否则,$\mathcal{C}$查询$\mathcal{DB}$得到(x_A,PK_A)和(x_B,PK_B)(若 sta_B=1,则$\mathcal{C}$询问 A_1获得与新公钥相应的秘密值 x'_B),计算 $M=\sigma_0 \Big/ e(g_1^{x_B}, g_2^s)$,其中,

$$g_2^s=\left(\frac{\sigma_4}{sk_{A,1}\cdot\sigma_1^{K_v(w)}}\right)^{1/J_v(w)}.$$

Challenge:经过多项式有界次询问后,A_1输出两个密文 M_0,M_1 和一个挑战身份 ID^*,在 Phase 1,A_1没有对 ID^*进行过 Extract-Private-Key 询问.如果 $J_u(ID^*)\neq 0 \bmod p$,则$\mathcal{C}$终止模拟并返回随机比特;否则,$\mathcal{C}$随机选取$\gamma\in\{0,1\}$,计算 $\sigma_0^*=M_\gamma\cdot Z^{x^*}$,$\sigma_1^*=C$,$\sigma_2^*=C^{K_u(ID^*)}$,$\sigma_3^*=1$,计算 $w^*=H_2(\sigma_0^*,\sigma_1^*,\sigma_2^*,1,ID^*,pk_{ID^*})$,如果 $J_v(w^*)\neq 0 \bmod p$,则$\mathcal{C}$终止模拟并返回随机比特;否则,计算 $\sigma_4^*=C^{K_v(w^*)}$,返回 $\sigma^*=(\sigma_0^*,\sigma_1^*,\sigma_2^*,\sigma_3^*,\sigma_4^*)$ 给 A_1.

Phase 2:A_1继续进行同 Phase 1 的询问,但不能在身份 ID^*下对σ^*进行解密询问,除非 ID^*的公钥在挑战阶段之后被替换过.

Guess:A_1输出其对γ的猜测γ',如果$\gamma=\gamma'$,则$\mathcal{C}$输出 1 作为对 DBDH 的回答,此时,$Z=e(g,g)^{abc}$;否则,$\mathcal{C}$输出 0.

以上是整个游戏的模拟过程.下面分析$\mathcal{C}$成功的概率.如果模拟过程不终止,则需要满足以下条件:

(1) 在所有 Extract-Partial-Private-Key 和 Extract-Private-Key 询问中,身份 ID 满足 $J_u(ID)\neq 0 \bmod \tau_u$;

(2) 在所有 Sign 和 SC 询问中,身份 ID_A 满足 $J_u(ID_A)\neq 0 \bmod \tau_u$;

(3) 在所有 Dec 和 USC 询问中,身份 ID_B 和 w 满足 $J_u(ID_B)\neq 0 \bmod \tau_u$ 或 $J_v(w)\neq 0 \bmod \tau_v$;

(4) $J_u(ID^*)=0 \bmod p$ 且 $J_v(w^*)=0 \bmod p$.

设 $ID_1,...,ID_{q_1}$ 为在所有询问中出现的不含挑战身份的身份,$w_1,...,w_{q_{II}}$ 是在Dec和USC询问中出现的不含挑战 w^*的 Hash 值,则有 $q_I\leqslant q_{pp}+q_p+q_{sign}+q_{sc}+q_{dec}+q_{usc}$,$q_{II}\leqslant q_{dec}+q_{usc}$.定义以下概率事件:

$$A^*: J_u(ID^*)=0 \bmod p,\quad A_i: J_u(ID_i)\neq 0 \bmod \tau_u,\ i=1,\ldots,q_I.$$

$$B^*: J_v(w^*)=0 \bmod p,\quad B_j: J_v(w_j)\neq 0 \bmod \tau_v,\ j=1,\ldots,q_{II}.$$

$\mathcal{C}$模拟过程不终止的概率为

$$\Pr[\overline{abort}]\geqslant \Pr\left[\bigcap_{i=1}^{q_I} A_i\cap A^*\bigcap_{j=1}^{q_{II}} B_j\cap B^*\right].$$

由于函数 $J_u(ID)$和 $J_v(w)$是独立选取的,故事件 $\bigcap_{i=1}^{q_I} A_i\cap A^*$ 和 $\bigcap_{j=1}^{q_{II}} B_j\cap B^*$ 相互独立.据 $\tau_u(n+1)<p$ 可知,

$$J_u(ID)=0 \bmod p \Rightarrow J_u(ID)=0 \bmod \tau_u.$$

如果 $J_u(ID)=0 \bmod \tau_u$,则存在唯一的 $0\leqslant k_u\leqslant n$,使得 $J_u(ID)=0 \bmod p$.根据 k_u,u',u_i,$i=1,\ldots,n$ 的随机性,有

$$\begin{aligned}\Pr[A^*]&=\Pr[J_u(ID^*)=0 \bmod p]\\&=\Pr[J_u(ID^*)=0 \bmod p\cap J_u(ID^*)=0 \bmod \tau_u]\\&=\Pr[J_u(ID^*)=0 \bmod \tau_u]\Pr[J_u(ID^*)=0 \bmod p\mid J_u(ID^*)=0 \bmod \tau_u]\\&=\frac{1}{\tau_u}\frac{1}{n+1}.\end{aligned}$$

另外,对任意的 i,j,$J_u(ID_i)$和 $J_u(ID_j)$相互独立,且 $J_u(ID_i)$和 $J_u(ID^*)$相互独立.因此有

$$\begin{aligned}\Pr\left[\bigcap_{i=1}^{q_I} A_i\cap A^*\right]&=\Pr[A^*]\Pr\left[\bigcap_{i=1}^{q_I} A_i\mid A^*\right]=\Pr[A^*]\left(1-\Pr\left[\bigcup_{i=1}^{q_I}\overline{A_i}\,\middle|\,A^*\right]\right)\\&\geqslant \Pr[A^*]\left(1-\sum_{i=1}^{q_I}\Pr[\overline{A_i}\mid A^*]\right)=\frac{1}{\tau_u}\frac{1}{n+1}\left(1-\frac{q_I}{\tau_u}\right)\\&\geqslant \frac{1}{\tau_u}\frac{1}{n+1}\left(1-\frac{q_{pp}+q_p+q_{sign}+q_{sc}+q_{dec}+q_{usc}}{\tau_u}\right)\geqslant \frac{1}{2}\frac{1}{\tau_u}\frac{1}{n+1}.\end{aligned}$$

同理,有

$$\Pr\left[\bigcap_{j=1}^{q_{\mathrm{II}}} B_j \cap B^*\right] \geqslant \frac{1}{2}\frac{1}{\tau_v}\frac{1}{m+1}.$$

从而有

$$\Pr[\overline{abort}] \geqslant \Pr\left[\bigcap_{i=1}^{q_{\mathrm{I}}} A_i \cap A^* \bigcap_{j=1}^{q_{\mathrm{II}}} B_j \cap B^*\right]$$
$$\geqslant 1/16(n+1)(m+1)(q_{dec}+q_{usc})(q_{pp}+q_p+q_{sign}+q_{sc}+q_{dec}+q_{usc}).$$

A_{I}成功的概率为ε,故$\mathcal{C}$的成功概率为

$$\varepsilon' \geqslant \varepsilon/16(n+1)(m+1)(q_{dec}+q_{usc})(q_{pp}+q_p+q_{sign}+q_{sc}+q_{dec}+q_{usc}).$$

$\mathcal{C}$的时间复杂度主要取决于各个询问中的指数运算时间(t_e)、乘法运算时间(t_m)和对运算时间(t_p).每个 Extract-Partial-Private-Key 和 Extract-Private-Key 询问需要 $O(n)$个乘法运算和 $O(1)$个指数运算,每个 Sign 询问、Enc 询问和 SC 询问需要 $O(n)$+$O(m)$个乘法运算和 $O(1)$个指数运算,每个 Dec 询问和 USC 询问需要 $O(n)$+$O(m)$个乘法运算、$O(1)$个指数运算和 $O(1)$个对运算,每个 Ver 询问需要 $O(n)$+$O(m)$个乘法运算和 $O(1)$个对运算,每个 Public-key 询问需要 $O(1)$个指数运算和 $O(1)$个乘法运算.故$\mathcal{C}$的时间复杂度为

$$t' = t + O(t_m(n(q_{pp}+q_p+q_{sign}+q_{ver}+q_{enc}+q_{dec}+q_{sc}+q_{usc})+m(q_{sign}+q_{ver}+q_{enc}+q_{dec}+q_{sc}+q_{usc})+q_{pk})+$$
$$t_e(q_{pp}+q_p+q_{pk}+q_{sign}+q_{enc}+q_{dec}+q_{sc}+q_{usc})+t_p(q_{ver}+q_{dec}+q_{usc})).$$

□

引理 2. 假设存在一个 IND-CCA 的 t 时间的第 2 类攻击者 A_{II}可以ε的优势赢得第 2.2 节定义的游戏 2,则存在一个区分者$\mathcal{C}$可在时间 t'内以ε'的优势解决 DBDH 问题.其中,

$$\varepsilon' \geqslant \varepsilon/16(n+1)(m+1)(q_p+q_{sign}+q_{sc}+q_{dec}+q_{usc})(q_{dec}+q_{usc}),$$
$$t' = t + O(t_m(n(q_p+q_{sign}+q_{ver}+q_{enc}+q_{dec}+q_{sc}+q_{usc})+m(q_{sign}+q_{ver}+q_{enc}+q_{dec}+q_{sc}+q_{usc})+q_{pk})+$$
$$t_e(q_p+q_{pk}+q_{sign}+q_{enc}+q_{dec}+q_{sc}+q_{usc})+t_p(q_{ver}+q_{dec}+q_{usc})).$$

证明:假设一个区分者$\mathcal{C}$收到一个随机的 DBDH 问题实例(g,$A=g^a$,$B=g^b$,$C=g^c$,$Z\in G_2$),他需要判定 $Z=e(g,g)^{abc}$是否成立.$\mathcal{C}$运行游戏 2 中的攻击者 A_{II},并且扮演其中的挑战者.为了避免发生碰撞,$\mathcal{C}$维护一个初始为空的列表$\mathcal{DB}$={(ID,d_{ID},x_{ID},PK_{ID},sk_{ID})}.

Setup:令τ_u=2(q_p+q_{sign}+q_{sc}+q_{dec}+q_{usc}),τ_v=2(q_{dec}+q_{usc}),攻击者 A_{II} 随机选取α作为系统主密钥,令 $g_1=g^{\alpha}$,其他参数同引理 1 中设置.A_{II}发送系统参数和主密钥α给$\mathcal{C}$.

Phase 1:A_{II}进行除 Extract-Partial-Private-Key 和 Replace-Public-Key 之外的所有询问,$\mathcal{C}$按照如下方式回答A_{II}的询问:

• Extract-Private-Key:输入一个身份 ID,$\mathcal{C}$首先查询$\mathcal{DB}$中是否存在相应的值.如果存在,则返回 sk_{ID};否则,$\mathcal{C}$按照如下方式生成 sk_{ID}:

如果 $J_u(ID)\neq 0 \bmod \tau_u$,$\mathcal{C}$随机选取 $t\in Z_p^*$,如果需要,则$\mathcal{C}$先运行 Set-User-Key 算法生成(x_{ID},PK_{ID}),计算 $sk_{ID}=(sk_{ID,1},sk_{ID,2})=(A^{\alpha\cdot x_{ID}})^{-K_u(ID)/J_u(ID)}\cdot F_u(ID)^t,(A^{\alpha\cdot x_{ID}})^{-1/J_u(ID)}\cdot g^t)=(g_2^{a\alpha x_{ID}}\cdot F_u(ID)^{\tilde{t}},g^{\tilde{t}})$, 其中, $\tilde{t}=t-\frac{a\alpha x_{ID}}{J_u(ID)}$; 否则,如果 $J_u(ID)=0 \bmod \tau_u$,则模拟终止,$\mathcal{C}$返回一个随机比特.

• Public-Key-Query:$\mathcal{C}$查询$\mathcal{DB}$中是否存在相应的值,如果存在,则返回 PK_{ID};否则,运行 Set-User-Key 算法生成 $PK_{ID}=(K,h,pk_{ID},Y,z)=(ID,e(B,A^{\alpha}),e(B,A^{\alpha})^{x_{ID}},e(B,A^{\alpha})^{y_{ID}},y_{ID}+cx_{ID} \bmod p)$, 其中,$c=H_1(K,Y||mpk)$,然后返回 PK_{ID}.

• Sign/Ver/Enc/SC 询问:不考虑用户公钥被替换的情况之外,$\mathcal{C}$按照同引理 1 中的方式回答.

• Dec:输入(σ,ID_B),$\mathcal{C}$首先查询$\mathcal{DB}$得到 PK_B,计算 $w=H_2(\sigma_0,\sigma_1,\sigma_2,1,B,pk_B)$,判定 $e(g,\sigma_2\cdot\sigma_4)=e(\sigma_1,F_u(ID_B)\cdot F_v(w))$是否成立.如果不成立,则输出 0;否则,分以下两种情况讨论:

(1) 若 $J_u(ID_B)\neq 0 \bmod \tau_u$,则$\mathcal{C}$可以得到 sk_B,进而利用 Dec 算法对σ进行解密并返回所得结果.如果必要,则首

先运行 Extract-Partial-Private-Key 和 Extract-Private-Key 算法生成 d_B 和 sk_B,然后进行解密.

(2) 若 $J_u(ID_B)=0 \bmod \tau_u$,如果 $J_v(w)=0 \bmod \tau_v$,则终止模拟,$\mathcal{C}$返回一个随机比特;否则,$\mathcal{C}$查询$\mathcal{DB}$得到(x_B,PK_B),计算 $M=\sigma_0 \Big/ e(A^{\alpha x_B},g_2^s)$, 其中, $g_2^s=\left(\frac{\sigma_4}{\sigma_1^{K_v(w)}}\right)^{1/J_v(w)}$.

• USC:输入(σ,ID_A,ID_B),$\mathcal{C}$首先查询$\mathcal{DB}$得到 PK_B,计算 $w=H_2(\sigma_0,\sigma_1,\sigma_2,\sigma_3,B,pk_B)$,判定 $e(g,\sigma_4)=pk_A\cdot e(F_u(ID_A),\sigma_3)\cdot e(F_v(w),\sigma_1)$是否成立.如果不成立,则输出 0;否则,分以下两种情况讨论:

(1) 若 $J_u(ID_B)\neq 0 \bmod \tau_u$,则$\mathcal{C}$可以得到 sk_B,进而利用 USC 算法对σ进行解签密并返回所得结果.如果必要,则首先运行 Extract-Partial-Private-Key 和 Extract-Private-Key 算法生成 d_B 和 sk_B,然后进行解签密.

(2) 若 $J_u(ID_B)=0 \bmod \tau_u$,如果 $J_v(w)=0 \bmod \tau_v$,则终止模拟,$\mathcal{C}$返回一个随机比特;否则,$\mathcal{C}$查询$\mathcal{DB}$得到(x_A,sk_A)和(x_B,PK_B),计算 $M=\sigma_0 \Big/ e(A^{\alpha x_B},g_2^s)$, 其中, $g_2^s=\left(\frac{\sigma_4}{sk_{A,1}\cdot\sigma_1^{K_v(w)}}\right)^{1/J_v(w)}$.

Challenge:经过多项式有界次询问后,A_{II}输出两个密文 M_0,M_1和一个挑战身份 ID^*,在 Phase 1,A_{II}没有对 ID^*进行过 Extract-Private-Key 询问.如果 $J_u(ID^*)\neq 0 \bmod p$,则$\mathcal{C}$终止模拟并返回随机比特;否则,$\mathcal{C}$随机选取$\gamma\in\{0,1\}$,计算 $\sigma_0^*=M_\gamma\cdot Z^{\alpha x^*},\sigma_1^*=C,\sigma_2^*=C^{K_u(ID^*)},\sigma_3^*=1$, 计算 $w^*=H_2(\sigma_0^*,\sigma_1^*,\sigma_2^*,1,ID^*,pk_{ID^*})$, 如果 $J_v(w^*)\neq 0 \bmod p$,则$\mathcal{C}$终止模拟并返回随机比特;否则,计算 $\sigma_4^*=C^{K_v(w^*)}$, 返回 $\sigma^*=(\sigma_0^*,\sigma_1^*,\sigma_2^*,\sigma_3^*,\sigma_4^*)$ 给 A_{II}.

Phase 2:A_{II}继续进行同 Phase 1 的询问,但不能在身份 ID^*下对σ^*进行解密询问.

Guess:A_{II}输出其对γ的猜测γ',如果$\gamma=\gamma'$,则$\mathcal{C}$输出 1 作为对 DBDH 的回答,此时,$Z=e(g,g)^{abc}$;否则,$\mathcal{C}$输出 0.

以上是整个游戏的模拟过程.除了 $q_{pp}=0$ 之外,$\mathcal{C}$的成功概率和时间复杂度分析与引理 1 类似.故$\mathcal{C}$的成功概率为

$$\varepsilon' \geqslant \varepsilon/16(n+1)(m+1)(q_{dec}+q_{usc})(q_p+q_{sign}+q_{sc}+q_{dec}+q_{usc}),$$

时间复杂度为

$$t'=t+O(t_m(n(q_p+q_{sign}+q_{ver}+q_{enc}+q_{dec}+q_{sc}+q_{usc})+m(q_{sign}+q_{ver}+q_{enc}+q_{dec}+q_{sc}+q_{usc})+q_{pk})+ t_e(q_p+q_{pk}+q_{sign}+q_{enc}+q_{dec}+q_{sc}+q_{usc})+t_p(q_{ver}+q_{dec}+q_{usc})).$$ □

定理 2. 在 CDH 假设下,文中给出的 CLGSC 方案在签名模式下是存在性不可伪造的,即 EUF-(CLGSC-IN-SIGN)-ACM 安全的.

定理 2 的证明可由引理 3 和引理 4 得到.

引理 3. 假设存在一个 EUF-ACM 的 t 时间的第 1 类攻击者 F_{I}可以ε的优势赢得第 2.2 节定义的游戏 3,则存在一个区分者$\mathcal{C}$可在时间 t'内以ε'的优势解决 CDH 问题.其中,

$$\varepsilon' \geqslant \varepsilon/16(n+1)(m+1)(q_{pp}+q_p+q_{sign}+q_{sc}+q_{dec}+q_{usc})(q_{dec}+q_{usc}),$$

$$t'=t+O(t_m(n(q_{pp}+q_p+q_{sign}+q_{ver}+q_{enc}+q_{dec}+q_{sc}+q_{usc})+m(q_{sign}+q_{ver}+q_{enc}+q_{dec}+q_{sc}+q_{usc})+q_{pk})+ t_e(q_{pp}+q_p+q_{pk}+q_{sign}+q_{enc}+q_{dec}+q_{sc}+q_{usc})+t_p(q_{ver}+q_{dec}+q_{usc})).$$

证明:假设一个区分者$\mathcal{C}$收到一个随机的 CDH 问题实例$(g,A=g^a,B=g^b)$,他需要计算 g^{ab}.$\mathcal{C}$运行游戏 3 中的攻击者 F_{I},并且扮演其中的挑战者.

Setup 和 Phase 1:$\mathcal{C}$按照同引理 1 的方式生成系统参数,并且回答 F_{I}在 Phase 1 的所有询问.

Forgery:经过最多多项式有界次的询问之后,如果不终止模拟过程,则$\mathcal{C}$输出一个身份 ID^*关于消息 M 的签名σ^*,其中,F_{I}没有对 M 进行过签名询问,并且 ID^*目前的公钥为 $pk_{ID^*}=e(g^a,g^b)^x$.

如果 $J_u(ID^*)\neq 0 \bmod p$ 或 $J_v(w^*)\neq 0 \bmod p$,则$\mathcal{C}$终止模拟并输出一个随机比特,其中, $w^*=H_2(\sigma_0^*,\sigma_1^*,1,\sigma_3^*,0,1)$; 否则,如果 $J_u(ID^*)=0 \bmod p$ 且 $J_v(w^*)=0 \bmod p$,则$\mathcal{C}$计算

$$\frac{\sigma_4^*}{(\sigma_3^*)^{K_u(ID^*)}(\sigma_1^*)^{K_v(w^*)}}=\frac{g_2^{\alpha x}F_u(ID^*)^{t^*}F_v(w^*)^s}{g^{K_u(ID^*)t^*}g^{K_v(w^*)s}}=g_2^{\alpha x}=g^{abx}.$$

$\mathcal{C}$查询$\mathcal{DB}$得到 x,从而恢复 g^{ab}.

$\mathcal{C}$成功的概率和时间复杂度分析与引理 1 相同. □

引理 4. 假设存在一个 EUF-ACM 的 t 时间的第 2 类攻击者 F_{II} 可以ε的优势赢得第 2.2 节定义的游戏 4,则存在一个区分者$\mathcal{C}$可在时间 t'内以ε'的优势解决 CDH 问题.其中,

$$\varepsilon' \geqslant \varepsilon/16(n+1)(m+1)(q_p+q_{sign}+q_{sc}+q_{dec}+q_{usc})(q_{dec}+q_{usc}),$$

$$t' = t + O(t_m(n(q_p+q_{sign}+q_{ver}+q_{enc}+q_{dec}+q_{sc}+q_{usc})+m(q_{sign}+q_{ver}+q_{enc}+q_{dec}+q_{sc}+q_{usc})+q_{pk})+ t_e(q_p+q_{pk}+q_{sign}+q_{enc}+q_{dec}+q_{sc}+q_{usc})+t_p(q_{ver}+q_{dec}+q_{usc})).$$

证明:假设一个区分者$\mathcal{C}$收到一个随机的 CDH 问题实例$(g,A=g^a,B=g^b)$,他需要计算 g^{ab}.$\mathcal{C}$运行游戏 4 中的攻击者 F_{II},并且扮演其中的挑战者.

Setup 和 Phase 1:F_{II} 按照同引理 2 的方式生成系统参数,$\mathcal{C}$按照同引理 2 的方式回答 F_{II} 在 Phase 1 的所有询问.

Forgery:经过最多多项式有界次的询问之后,如果不终止模拟过程,则$\mathcal{C}$输出一个身份 ID^*关于消息 M 的签名σ^*,其中,F_{II} 没有对 M 进行过签名询问,并且 ID^*的公钥为 $pk_{ID^*}=e(B,A^{\alpha})^x$.如果 $J_u(ID^*)\neq 0 \bmod p$ 或 $J_v(w^*)\neq 0 \bmod p$,$\mathcal{C}$终止模拟并输出一个随机比特,其中, $w^* = H_2(\sigma_0^*,\sigma_1^*,1,\sigma_3^*,0,1)$;否则,如果 $J_u(ID^*)=0 \bmod p$ 且 $J_v(w^*)=0 \bmod p$,则$\mathcal{C}$计算

$$\frac{\sigma_4^*}{(\sigma_3^*)^{K_u(ID^*)}(\sigma_1^*)^{K_v(w^*)}} = \frac{g_2^{a\alpha x}F_u(ID^*)^{t^*}F_v(w^*)^s}{g^{K_u(ID^*)t^*}g^{K_v(w^*)s}} = (g_2^{ax})^{\alpha} = (g^{ab})^{\alpha x}.$$

$\mathcal{C}$已知α,查询$\mathcal{DB}$得到 x,从而恢复 g^{ab}.

$\mathcal{C}$成功的概率和时间复杂度分析和引理 2 相同. □

定理 3. 在 DBDH 假设下,文中给出的 CLGSC 方案在签密模式下是语义安全的,即 IND-(CLGSC-IN-SC)-CCA 安全的.

定理 3 的证明可由引理 5 和引理 6 得到.

引理 5. 假设存在一个 IND-CCA 的 t 时间的第 1 类攻击者 A_{I}' 可以ε的优势赢得第 2.2 节定义的游戏 1′,则存在一个区分者$\mathcal{C}$可在时间 t'内以ε'的优势解决 DBDH 问题.其中,

$$\varepsilon' \geqslant \varepsilon/16(n+1)(m+1)(q_{pp}+q_p+q_{sign}+q_{sc}+q_{dec}+q_{usc})(q_{dec}+q_{usc}),$$

$$t' = t + O(t_m(n(q_{pp}+q_p+q_{sign}+q_{ver}+q_{enc}+q_{dec}+q_{sc}+q_{usc})+m(q_{sign}+q_{ver}+q_{enc}+q_{dec}+q_{sc}+q_{usc})+q_{pk})+ t_e(q_{pp}+q_p+q_{pk}+q_{sign}+q_{enc}+q_{dec}+q_{sc}+q_{usc})+t_p(q_{ver}+q_{dec}+q_{usc})).$$

证明:假设一个区分者$\mathcal{C}$收到一个随机的 DBDH 问题实例$(g,A=g^a,B=g^b,C=g^c,Z\in G_2)$,他需要判定 $Z=e(g,g)^{abc}$ 是否成立.$\mathcal{C}$运行游戏 1′中的攻击者 A_{I}',并且扮演其中的挑战者.

Setup 和 Phase 1:$\mathcal{C}$按照引理 1 中的方法生成系统参数和回答 A_{I}' 的所有询问.

Challenge:经过多项式有界次询问后, A_{I}' 输出两个密文 M_0,M_1 和两个挑战身份 ID_{A^*}和 ID_{B^*}.在 Phase 1, A_{I}' 没有对 ID_{B^*}进行过 Extract-Private-Key 询问.

如果 $J_u(ID_{A^*})=0 \bmod p$ 或 $J_u(ID_{B^*})\neq 0 \bmod p$,则$\mathcal{C}$终止模拟并返回随机比特;否则,$\mathcal{C}$随机选取$\gamma\in\{0,1\}$,计算 $\sigma_0^* = M_\gamma \cdot Z^{x_{B^*}}, \sigma_1^* = C, \sigma_2^* = C^{K_u(ID_{B^*})}, \sigma_3^* = (g_1^{x_{A^*}})^{-1/J_u(ID_{A^*})}g^{t_{A^*}}$, 计算 $w^* = H_2(\sigma_0^*,\sigma_1^*,\sigma_2^*,\sigma_3^*,ID_{B^*},pk_{ID_{B^*}})$.

如果 $J_v(w^*)\neq 0 \bmod p$,则$\mathcal{C}$终止模拟并返回随机比特;否则,计算 $\sigma_4^* = (g_1^{x_{A^*}})^{-K_u(ID_{A^*})/J_u(ID_{A^*})}\cdot F_u(ID_{A^*})^{t_{A^*}}\cdot C^{K_v(w^*)}$. 返回 $\sigma^* = (\sigma_0^*,\sigma_1^*,\sigma_2^*,\sigma_3^*,\sigma_4^*)$ 给 A_{I}'.

Phase 2:A_{I}' 继续进行最多多项式有界次的询问,但不能在身份 ID_{A^*}和 ID_{B^*}下对σ^*进行解签密询问.

Guess:A_{I}' 输出其对γ的猜测γ',如果$\gamma=\gamma'$,则$\mathcal{C}$输出 1 作为对 DBDH 的回答,此时,$Z=e(g,g)^{abc}$;否则,$\mathcal{C}$输出 0.

以上是整个游戏的模拟过程.$\mathcal{C}$的成功概率和时间复杂度分析和引理 1 相同. □

引理 6. 假设存在一个 IND-CCA 的 t 时间的第 2 类攻击者 A_{II}' 可以ε的优势赢得第 2.2 节定义的游戏 2′,则

存在一个区分者$\mathcal{C}$可以在时间 t'内以ε'的优势解决 DBDH 问题.其中,

$$\varepsilon' \geqslant \varepsilon/16(n+1)(m+1)(q_p+q_{sign}+q_{sc}+q_{dec}+q_{usc})(q_{dec}+q_{usc}),$$

$$t' = t + O(t_m(n(q_p+q_{sign}+q_{ver}+q_{enc}+q_{dec}+q_{sc}+q_{usc})+m(q_{sign}+q_{ver}+q_{enc}+q_{dec}+q_{sc}+q_{usc})+q_{pk})+$$
$$t_e(q_p+q_{pk}+q_{sign}+q_{enc}+q_{dec}+q_{sc}+q_{usc})+t_p(q_{ver}+q_{dec}+q_{usc})).$$

证明:假设一个区分者$\mathcal{C}$收到一个随机的 DBDH 问题实例$(g,A=g^a,B=g^b,C=g^c,Z\in G_2)$,他需要判定 $Z=e(g,g)^{abc}$是否成立.$\mathcal{C}$运行游戏 2′中的攻击者 A'_{II},并且扮演其中的挑战者.

Setup 和 Phase 1: A'_{II}按照引理 2 的方式生成系统参数,$\mathcal{C}$按照引理 2 的方式回答 A'_{II}在 Phase 1 的所有询问.

Challenge:经过多项式有界次询问后, A'_{II}输出两个密文 M_0,M_1和两个挑战身份 ID_{A^*}和 ID_{B^*},在 Phase 1, A'_{II}没有对 ID_{B^*}进行过 Extract-Private-Key 询问.

如果 $J_u(ID_{A^*})=0 \bmod p$ 或 $J_u(ID_{B^*})\neq 0 \bmod p$,则$\mathcal{C}$终止模拟并返回随机值;否则,$\mathcal{C}$随机选取$\gamma\in\{0,1\}$,计算 $\sigma_0^*=M_\gamma\cdot Z^{\alpha x_{B^*}},\sigma_1^*=C,\sigma_2^*=C^{K_u(ID_{B^*})},\sigma_3^*=(A^{\alpha x_{A^*}})^{-1/J_u(ID_{A^*})}g^{t_{A^*}}$, 计算 $w^*=H_2(\sigma_0^*,\sigma_1^*,\sigma_2^*,\sigma_3^*,ID_{B^*},pk_{ID_{B^*}})$.

如果 $J_v(w^*)\neq 0 \bmod p$,则$\mathcal{C}$终止模拟并返回随机比特;否则,计算 $\sigma_4^*=(A^{\alpha x_{A^*}})^{-K_u(ID_{A^*})/J_u(ID_{A^*})}\cdot F_u(ID_{A^*})^{t_{A^*}}C^{K_v(w^*)}$. 返回 $\sigma^*=(\sigma_0^*,\sigma_1^*,\sigma_2^*,\sigma_3^*,\sigma_4^*)$给 A'_{II}.

Phase 2: A'_{II}继续进行同阶段 1 的询问,但不能在身份 ID_{A^*}和 ID_{B^*}下对σ^*进行解签密询问.

Guess: A'_{II}输出其对γ的猜测γ',如果$\gamma=\gamma'$,则$\mathcal{C}$输出 1 作为对 DBDH 的回答,此时,$Z=e(g,g)^{abc}$;否则,$\mathcal{C}$输出 0.

以上是整个游戏的模拟过程.$\mathcal{C}$的成功概率和复杂度分析和引理 2 相同. □

定理 4. 在 CDH 假设下,文中给出的 CLGSC 方案在签密模式下是存在性不可伪造的,即 EUF-(CLGSC-IN-SC)-ACM 安全的.

定理 4 的证明可由引理 7 和引理 8 得到.

引理 7. 假设存在一个 EUF-ACM 的 t 时间的第 1 类攻击者 F'_{I} 可以ε的优势赢得第 2.2 节定义的游戏 3′,则存在一个区分者$\mathcal{C}$可在时间 t'内以ε'的优势解决 CDH 问题.其中,

$$\varepsilon' \geqslant \varepsilon/16(n+1)(m+1)(q_{pp}+q_p+q_{sign}+q_{sc}+q_{dec}+q_{usc})(q_{dec}+q_{usc}),$$

$$t' = t + O(t_m(n(q_{pp}+q_p+q_{sign}+q_{ver}+q_{enc}+q_{dec}+q_{sc}+q_{usc})+m(q_{sign}+q_{ver}+q_{enc}+q_{dec}+q_{sc}+q_{usc})+q_{pk})+$$
$$t_e(q_{pp}+q_p+q_{pk}+q_{sign}+q_{enc}+q_{dec}+q_{sc}+q_{usc})+t_p(q_{ver}+q_{dec}+q_{usc})).$$

证明:假设一个区分者$\mathcal{C}$收到一个随机的 CDH 问题实例$(g,A=g^a,B=g^b)$,他需要计算 g^{ab}.$\mathcal{C}$运行游戏 3′中的攻击者 F'_{I},并且扮演其中的挑战者.

Setup 和 Phase 1:$\mathcal{C}$按照同引理 1 的方式生成系统参数,并且回答 F'_{I} 在 Phase 1 的所有询问.

Forgery:经过最多多项式有界次的询问之后,如果不终止模拟过程,$\mathcal{C}$输出一个身份 ID_{A^*}和 ID_{B^*}关于消息 M 的签密σ^*,其中, F'_{I} 没有对 M 进行过签密询问,并且 ID_{A^*}目前的公钥为 $pk_{ID_{A^*}}=e(g^a,g^b)^{x_{A^*}}$. 如果 $J_u(ID_{A^*})\neq 0 \bmod p$ 或$J_v(w^*)\neq 0 \bmod p$,则$\mathcal{C}$终止模拟并输出一个随机比特,其中, $w^*=H_2(\sigma_0^*,\sigma_1^*,\sigma_2^*,\sigma_3^*,ID_{B^*},pk_{B^*})$; 否则,如果$J_u(ID_{A^*})=0 \bmod p$ 且 $J_v(w^*)=0 \bmod p$,$\mathcal{C}$计算

$$\frac{\sigma_4^*}{(\sigma_3^*)^{K_u(ID^*)}(\sigma_1^*)^{K_v(w^*)}}=\frac{g_2^{\alpha x}F_u(ID^*)^{t^*}F_v(w^*)^s}{g^{K_u(ID^*)t^*}g^{K_v(w^*)s}}=g_2^{\alpha x}=g^{abx}.$$

$\mathcal{C}$查询$\mathcal{DB}$得到 x,从而恢复 g^{ab}.

$\mathcal{C}$成功的概率和时间复杂度分析和引理 1 相同. □

引理 8. 假设存在一个 EUF-ACM 的 t 时间的第 2 类攻击者 F'_{II} 可以ε的优势赢得第 2.2 节定义的游戏 4′,则存在一个区分者$\mathcal{C}$可在时间 t'内以ε'的优势解决 CDH 问题.其中,

$$\varepsilon' \geqslant \varepsilon/16(n+1)(m+1)(q_p+q_{sign}+q_{sc}+q_{dec}+q_{usc})(q_{dec}+q_{usc}),$$

$$t' = t + O(t_m(n(q_p+q_{sign}+q_{ver}+q_{enc}+q_{dec}+q_{sc}+q_{usc})+m(q_{sign}+q_{ver}+q_{enc}+q_{dec}+q_{sc}+q_{usc})+q_{pk})+ t_e(q_p+q_{pk}+q_{sign}+q_{enc}+q_{dec}+q_{sc}+q_{usc})+t_p(q_{ver}+q_{dec}+q_{usc})).$$

证明:假设一个区分者$\mathcal{C}$收到一个随机的 CDH 问题实例$(g,A=g^a,B=g^b)$,他需要计算 g^{ab}.$\mathcal{C}$运行游戏 4′中的攻击者 F_{II}',并且扮演其中的挑战者.

Setup 和 Phase 1:F_{II}' 按照引理 2 的方式生成系统参数,$\mathcal{C}$按照引理 2 的方式回答 F_{II}' 在 Phase 1 的所有询问.

Forgery:经过最多多项式有界次的询问之后,如果不终止模拟过程,则$\mathcal{C}$输出一个身份 ID_{A^*}和 ID_{B^*}关于消息 M 的签密σ^*,其中,F_{II}' 没有对 M 进行过签密询问,并且 ID_{A^*}目前的公钥为 $pk_{ID_{A^*}}=e(B,A^{\alpha})^{x_{A^*}}$. 如果 $J_u(ID_{A^*})\neq 0 \bmod p$ 或 $J_v(w^*)\neq 0 \bmod p$,则$\mathcal{C}$终止模拟并输出一个随机比特,其中,$w^*=H_2(\sigma_0^*,\sigma_1^*,\sigma_2^*,\sigma_3^*,ID_{B^*},pk_{B^*})$; 否则,如果 $J_u(ID_{A^*})=0 \bmod p$ 且 $J_v(w^*)=0 \bmod p$,则$\mathcal{C}$计算

$$\frac{\sigma_4^*}{(\sigma_3^*)^{K_u(ID^*)}(\sigma_1^*)^{K_v(w^*)}}=\frac{g_2^{a\alpha x}F_u(ID^*)^{t^*}F_v(w^*)^s}{g^{K_u(ID^*)t^*}g^{K_v(w^*)s}}=(g_2^{ax})^{\alpha}=(g^{ab})^{\alpha x}.$$

$\mathcal{C}$已知α,查询$\mathcal{DB}$得到 x,从而恢复 g^{ab}.

$\mathcal{C}$成功的概率和时间复杂度分析和引理 2 相同. □

5 结 论

本文首次提出了 CLGSC 的形式化定义和安全模型.该安全模型讨论了系统在不同工作模式下的安全性,赋予了第 2 类攻击者较强的攻击能力,在攻击游戏中自己生成系统参数.在此基础上,给出一个具体的 CLGSC 方案.该方案在标准模型下可证明是安全的.效率分析表明,该方案是有效的.广义签密体制在一般签密体制能够同时提供机密性和认证性的基础上,可以只实现机密性和认证性一种功能,在节约时间和成本的基础上满足不同的需求环境,因而具有广泛的应用前景.

致谢 对审稿专家提出的宝贵修改意见,我们在此表示衷心的感谢.

References:

[1] Han YL, Yang XY. New ECDSA—Verifiable generalized signcryption. Chinese Journal of Computers, 2006,29(11):2003−2012 (in Chinese with English abstract).

[2] Lal S, Kushwah P. ID-Based generalized signcryption. 2008. http://eprint.iacr.org/2008/084.pdf

[3] Al-Riyami SS, Paterson KG. Certificateless public-key cryptography. In: Proc. of the Asiacrypt 2003. LNCS 2894, Berlin: Spring-Verlag, 2003. 452−473. [doi: 10.1007/978-3-540-40061-5_29]

[4] Dent AW. A survey of certificateless encryption schemes and security models. Int'l Journal of Information Security, 2008,7(5): 349−377. [doi: 10.1007/s10207-008-0055-0]

[5] Barbosa M, Farshim P. Certificateless signcryption. In: Proc. of the 2008 ACM Symp. on Information, Computer and Communications Security. 2008. 369−372. [doi: 10.1145/1368310.1368364]

[6] Aranha D, Castro R, López J, Dahab R. Efficient certificateless signcryption. 2008. http://sbseg2008.inf.ufrgs.br/proceedings/data/pdf/st03_01_resumo.pdf

[7] Wu CH, Chen ZX. A new efficient certificateless signcryption scheme. In: Proc. of the ISISE 2008. 2008. 661−664. [doi: 10.1109/ISISE.2008.206]

[8] Selvi SSD, Vivek SS, Rangan CP. Cryptanalysis of certificateless signcryption schemes and an efficient construction without pairing. 2009. http://eprint.iacr.org/2009/298.pdf

[9] Liu ZH, Hu YP, Zhang XS, Ma H. Certificateless signcryption scheme in the standard model. Information Science, 2010,180(3): 452−464. [doi:10.1016/j.ins.2009.10.011]

[10] Selvi SS, Vivek SS, Rangan CP. Security weaknesses in two certificateless signcryption schemes. 2010. http://eprint.iacr.org/2010/092

[11] Jin ZP, Wen QY, Zhang H. A supplement to Liu *et al.*'s certificateless signcryption scheme in the standard model. 2010. http://eprint.iacr.org/2010/252

[12] Au HM, Mu Y, Chen J, Wong DS, Liu JK, Yang GM. Malicious KGC attacks in certificateless cryptography. In: Deng R, Samarati P, eds. Proc. of the ASIACCS 2007. New York: ACM, 2007. 302−311. [doi: 10.1145/1229285.1266997]

[13] Wang XA, Yang XY, Han YL. Provable secure generalized signcryption. 2007. http://eprint.iacr.org/2007/173.pdf

[14] Waters B. Efficient identity based encryption without random oracles. In: Cramer P, ed. Proc. of the Eurocrypt 2005. LNCS 3494, Berlin: Springer-Verlag, 2005. 114−127. [doi: 10.1007/11426639_7]

[15] Liu JK, Au MH, Susilo W. Self-Generated-Certificate public key cryptography and certificateless signature/encryption scheme in the standard model. In: Deng R, Samarati P, eds. Proc. of the ASIACCS 2007. New York: ACM, 2007. 273−283. [doi: 10.1145/1229285.1266994]

[16] Dent AW, Libert B, Paterson KG. Certificateless encryption schemes strongly secure in the standard model. In: Cramer ed. Proc. of the 11th Int'l Workshop on Practice and Theory in Public Key Cryptography 2008. LNCS 4939, Berlin: Springer-Verlag, 2008. 344−359. [doi:10.1016/j.ins.2009.10.011]

附中文参考文献:

[1] 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.

刘连东(1979－),男,河南周口人,博士生,讲师,主要研究领域为信息安全.

韩文报(1963－),男,博士,教授,博士生导师,主要研究领域为信息安全,网络密码.

冀会芳(1982－),女,博士,主要研究领域为公钥密码体制设计与分析.

赵龙(1983－),男,博士,主要研究领域为椭圆曲线.