软件学报 ISSN 1000-9825, CODEN RUXUEW
Journal of Software,2017,28(10):2757−2768 [doi: 10.13328/j.cnki.jos.005150]

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

安全的无双线性映射的无证书签密机制*

周彦伟[1,3], 杨 波[1,3], 王青龙[2]

[1](陕西师范大学 计算机科学学院,陕西 西安 710062)

[2](长安大学 信息工程学院,陕西 西安 710064)

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

通讯作者: 杨波, E-mail: byang@snnu.edu.cn

摘 要: 无证书签密是能够同时提供无证书加密和无证书签名的一种非常重要的密码学原语.近年来,多个无证书签密方案相继被提出,并声称他们的方案是可证明安全的.但是,通过给出具体的攻击方法,指出现有的一些无证书签密机制并不具备其所声称的安全性.针对上述问题,提出一种无双线性映射的高效无证书签密方案,并在随机谕言机模型下,基于计算性 Diffie-Hellman 问题和离散对数问题对所提方案的安全性进行了证明.同时,该方案还具有不可否认性和公开验证性等安全属性.与其他传统无证书签密方案相比,由于未使用双线性映射运算,在具有更高计算效率的同时,该方案的安全性更优.

关键词: 无证书签密;随机谕言机;无双线性映射;可证明安全性

中图法分类号: TP309

中文引用格式: 周彦伟,杨波,王青龙.安全的无双线性映射的无证书签密机制.软件学报,2017,28(10):2757−2768. http://www.jos.org.cn/1000-9825/5150.htm

英文引用格式: Zhou YW, Yang B, Wang QL. Secure certificateless signcryption scheme without bilinear pairing. Ruan Jian Xue Bao/Journal of Software, 2017,28(10):2757−2768 (in Chinese). http://www.jos.org.cn/1000-9825/5150.htm

Secure Certificateless Signcryption Scheme without Bilinear Pairing

ZHOU Yan-Wei[1,3], YANG Bo[1,3], WANG Qing-Long[2]

[1](School of Computer Science, Shaanxi Normal University, Xi'an 710062, China)

[2](School of Information Engineering, Chang'an University, Xi'an 710064, China)

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

Abstract: Certificateless signcryption is a useful cryptographic primitive which simultaneously provides the functionalities of certificateless encryption and certificateless signature. In the past few years, some certificateless signcryption schemes have been proposed, and claimed to be provably secure. Unfortunately, concrete attacks can be made that indicate that some existing certificateless signcryption schemes are not secure. To overcome these disadvantages, an efficient certificateless signcryption scheme without bilinear pairings is proposed. The proposal is provably secure in the random oracle model based on the computational Diffie-Hellman problem and discrete logarithm problem, and also has the security properties such as non-repudiation and public verifiability. Additionally, compared

* 基金项目: 国家自然科学基金(61572303, 61772326); 国家重点研发计划"网络空间安全"重点专项(2017YFB0802003, 2017YFB0802004); "十三五"国家密码发展基金 (MMJJ20170216); 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(2017-MS-03); 中央高校基本科研业务费项目(GK201702004)

Foundation item: National Natural Science Foundation of China (61572303, 61772326); National Key Research and Development Program of China (2017YFB0802003, 2017YFB0802004); National Cryptography Development Fund during the 13th Five-Year Plan Period (MMJJ20170216); Foundation of State Key Laboratory of Information Security (2017-MS-03); Fundamental Research Funds for the Central Universities (GK201702004)

收稿时间: 2015-12-24; 修改时间: 2016-04-27; 采用时间: 2016-10-09

with other existing certificateless signcryption schemes in the computational complexity, the proposed method is more efficient and secure due to the lack of bilinear pairings.

Key words: certificateless signcryption; random oracle; without bilinear pairing; provable security

保密性和认证性是消息通信服务的基本安全需求,通常,消息的保密性由加密来完成,而认证性则通过签名来实现,传统上采用“先签名后加密”的方式实现,但其代价往往是签名和加密的代价之和,因而效率较低.为了提高效率,1997 年,文献[1]首先提出了签密的概念,它能够在一个逻辑步骤内同时完成签名和加密,相较于传统策略,签密具有较低的计算和通信效率,是一种较为理想的数据信息安全传输方法.

Shamir 于 1984 年提出基于身份的公钥密码体制(ID-PKC)[2],改进了传统公钥密码体制中公钥证书的管理问题.在 ID-PKC 中,用户的身份信息(如电话号码、姓名、电子邮件等)直接被作为用户公钥,使得公钥无需与证书绑定,用户的私钥由可信第三方——密钥生成中心(key generation center,简称 KGC)提供.然而,由于 ID-PKC 中 KGC 生成了用户的完整私钥,因此恶意的 KGC 具备伪造任意用户的合法签密密文或替代任意用户进行解签密的能力,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.

2003 年,无证书公钥密码系统(CL-PKC)[3]由 Al-Riyami 和 Paterson 为了克服 ID-PKC 的密钥托管问题而提出.在 CL-PKC 中,依然存在可信的 KGC,它拥有系统的主密钥;并且根据用户的身份和系统主密钥为用户生成部分私钥;用户基于 KGC 为其计算的部分私钥和随机选取的秘密值生成用户完整的私钥;公钥由用户的秘密值、身份和系统参数计算得出,并对外安全公布.

由于 CL-PKC 很好地解决了 ID-PKC 中密钥托管的不足,因此,自 2008 年 Barbosa 等人[4]首次提出无证书签密概念以来,关于无证书签密方案的研究已成为当前签密领域的研究热点之一,国内外众多学者分别提出了新的签密方案[5−17].文献[5]和文献[6]分别利用双线性对构造了一种无证书签密方案;文献[7]提出一种签密和解签密计算均不需要进行双线性映射运算的无证书签密方案,但该方案的公钥生成阶段需要进行双线性映射运算;文献[8]指出文献[5]方案并不能保证不可否认性和保密性,同时指出文献[6]方案在保密性上存在问题,但文献[8]均未给出相应的改进方案;文献[9,10]基于双线性映射提出了可证明安全的无证书混合签密方案,并在随机谕言机模型下对其安全性进行了证明.由于双线性映射的运算负载较高,导致基于双线性映射构造的机制存在计算开销大的不足.针对上述不足,不使用双线性映射的无证书签密方案[11−17]相继被提出.文献[11,12]分别提出了无需双线性映射运算的无证书签密机制,并在随机谕言机模型下,基于计算性 Diffie-Hellman(computation Diffie-Hellman,简称 CDH)困难问题和离散对数(discrete logarithm,简称 DL)困难问题证明了各自机制的机密性和不可伪造性;然而,文献[13]指出文献[12]的方案不满足不可伪造性,并提出了改进方案;除此之外,多个不使用双线性映射的无证书签密机制在文献[8,14–16]中相继被提出,并在随机谕言机模型下基于相应的困难问题证明了各自方案的机密性和不可伪造性.近年来,鉴于无证书签密机制无密钥托管的优势,国内外研究者分别提出了适用于物联网[17−20]、无线传感器网[21]等网络环境的无证书签密机制.

本文分析发现,文献[8,14]和文献[16]中群上的点乘运算次数较多,导致计算效率依然较低;并且通过构造具体的攻击算法证明了文献[11–14]和文献[15]的方案在安全性方面均存在缺陷,要么无法满足对任意敌手所声称的机密性[11−13,15],要么对 A_I 类敌手不具有所声称的不可伪造性[11,12],要么不具有公开验证性[14];而文献[16]的密文长度较长,使得该方案的通信开销较大.此外,文献[17–21]中的方案是基于双线性映射构造的,导致相关方案的计算效率较低.虽然上述方案[11−21]在安全性、计算效率或通信效率方面存在一定的不足,但新颖的设计思路,确实为无证书签密方案的设计提供了参考,推进了无证书签密技术的发展.

本文提出不使用双线性映射的高效无证书签密方案,并基于 CDH 假设和 DL 困难问题,在随机谕言机模型中对本文方案的不可伪造性及机密性进行了证明.同时,本文方案还具有不可否认性和公开验证性等安全属性,相较于其他无证书签密方案[11−21],本文方案的效率更高,且安全性更佳.

1 预备知识

1.1 困难性问题

离散对数(discrete logarithm,简称 DL)问题:令群 G 的阶为大素数 q,设 P 为群 G 的任意一个生成元,给定 $P,bP\in G$,对任意未知的 $b\in Z_q^*$,DL 问题的目标是计算 b.任意的概率多项式时间(probabilistic polynomial time,简称 PPT)算法 A 成功解决 DL 问题的概率 $Adv^{DL}(A)=\Pr[A(P,bP=b)]$是可忽略的,其中,概率来源于 b 在 Z_q^* 上的随机选取和算法 A 的随机选择.

计算性 Diffie-Hellman(CDH)问题:令群 G 的阶为大素数 q,设 P 为群 G 的任意一个生成元,给定 $P,aP,bP\in G$,对于任意未知的 $a,b\in Z_q^*$,CDH 问题的目标是计算 $abP\in G$.任意的 PPT 算法 A 成功解决 CDH 困难问题的概率 $Adv^{CDH}(A)\Pr[A(P,aP,bP)=abP]$是可忽略的,其中,概率来源于 a,b 在 Z_q^* 上的随机选取和算法 A 的随机选择.

1.2 无证书签密机制及安全模型

无证书签密机制的合法参与者有密钥生成中心 KGC、发送者 ID_S 和接收者 ID_R,具体算法的定义详见文献[11].无证书签密机制将面临 A_{I} 和 A_{II} 两类敌手的攻击,其中,A_{I} 类敌手无法掌握系统的主密钥,但其具有替换合法用户公钥的能力,则 A_{I} 类敌手为恶意的用户;本文中 $A_{\mathrm{I}}^i(i=1,2)$ 为 A_{I} 类敌手,其中, A_{I}^1 是攻击方案机密性的敌手, A_{I}^2 是攻击方案不可伪造性的敌手.A_{II} 类敌手可掌握系统的主密钥,但其不具有替换合法用户公钥的能力,则 A_{II} 类敌手为恶意的 KGC;本文中 $A_{\mathrm{II}}^i(i=1,2)$ 为 A_{II} 类敌手,其中, A_{II}^1 是攻击方案机密性的敌手, A_{II}^2 是攻击方案不可伪造性的敌手.文献[11,12,22]详细介绍了 A_{I} 和 A_{II} 两类敌手适应性选择消息攻击下不可伪造性和适应性选择密文攻击下机密性的定义及相应的游戏,篇幅所限,本文不再赘述,具体定义详见文献[11,12,22].

2 高效可证明安全的无证书签密机制

2.1 方案构造

本节提出的不使用双线性映射的无证书签密机制$\prod$=(*Setup*,*KeyGen*,*Sign*,*UnSign*)包含 4 种基本算法,具体描述如下.

2.1.1 初始化 *Setup*

系统初始化阶段,KGC 进行如下操作.

① 循环群 G 的阶为大素数 q,P 为 G 的一个生成元;选择抗碰撞哈希函数: $H_1:\{0,1\}^{l_1}\times G\times G\to Z_q^*$, $H_2:\{0,1\}^{l_1}\times\{0,1\}^{l_2}\times G\times G\to Z_q^*$, $H_3:\{0,1\}^{L_1}\times G\to\{0,1\}^{l_2}$,其中,$l_1$ 为用户身份标识 ID 的长度,l_2 为明文消息的长度.

② 随机选取需秘密保存的主密钥 $S_{msk}\in Z_q^*$,计算系统主公钥 $P_{Pub}=S_{msk}P$;公开系统参数 $Params=\langle q,G,P,P_{Pub},H_1,H_2,H_3,ID,M\rangle$,其中,$ID$ 是用户的身份空间,M 是消息空间.

2.1.2 用户密钥生成 *KeyGen*

用户 ID_i 的密钥生成过程如下所述.

① 随机选取秘密值 $x_i\in Z_q^*$,计算 $X_i=x_iP$,发送身份标识 ID_i 和公开参数 X_i 给 KGC;

② 给定用户身份标识 ID_i 及公开参数 X_i,KGC 随机选取秘密数 $r_i\in Z_q^*$,分别计算 $Y_i=r_iP$ 和 $y_i=r_i+S_{msk}H_1(ID_i,X_i,Y_i)$,通过安全信道将 y_i 和 Y_i 返回给 ID_i,则 ID_i 的公钥为 $PK_i=(X_i,Y_i)$,私钥为 $SK_i=(x_i,y_i)$.用户 ID_i 通过等式 $y_iP=Y_i+P_{Pub}H_1(ID_i,X_i,Y_i)$是否成立来验证 KGC 分配密钥的合法性.

2.1.3 签密 *Sign*

若要发送消息 m 给接收者 *Bob*(身份标识为 ID_{Bob})、发送者 *Alice*(身份标识为 ID_{Alice}),则进行下述操作.

① 选取随机秘密数 $u\in Z_q^*$,计算 $W=u(X_{Bob}+Y_{Bob}+P_{Pub}h_{Bob})$和 $Q=uP$,其中,$h_{Bob}=H_1(ID_{Bob},X_{Bob},Y_{Bob})$;然后生成密文 $C=m\oplus H_3(ID_{Bob},W)$;

② 计算 $n=H_2(ID_{Alice},C,X_{Alice},Q)$和 $k=H_2(ID_{Alice},C,Y_{Alice},Q)$,生成签名 $U=u(x_{Alice}+y_{Alice})^{-1}$ 和 $V=n(x_{Alice}+y_{Alice})+uk$;

③ 发送签密密文$\sigma=(U,V,C)$给接收者 *Bob*.

2.1.4 解签密 *UnSingn*

收到发送者 *Alice* 的密文$\sigma=(U,V,C)$后,接收者 *Bob* 进行下述操作.

① (解密过程)计算 $Q'=U(X_{Alice}+Y_{Alice}+P_{Pub}h_{Alice})$和 $W'=(x_{Bob}+y_{Bob})Q'$,其中,$h_{Alice}=H_1(ID_{Alice},X_{Alice},Y_{Alice})$;恢复明文消息 $m=C\oplus H_3(ID_{Bob},W')$;

② (验证过程)验证等式 $VP=n(X_{Alice}+Y_{Alice}+P_{Pub}h_{Alice})+KQ'$是否成立,其中,$h_{Alice}=H_1(ID_{Alice},X_{Alice},Y_{Alice})$,$n=H_2(ID_{Alice},C,X_{Alice},Q')$和 $k=H_2(ID_{Alice},C,Y_{Alice},Q')$,若成立,则接收消息 m;否则,输出⊥,表示输入的密文无效.

2.2 正确性分析

2.2.1 解密的正确性

由等式(1)和等式(2)成立,可知 $m=m\oplus H_3(ID_{Bob},W)\oplus H_3(ID_{Bob},W')$,则 *Bob* 能够还原出 *Alice* 的原始通信消息,即解密过程是正确的.

$$Q'=U(x_{Alice}+y_{Alice})P=u(x_{Alice}+y_{Alice})^{-1}(x_{Alice}+y_{Alice})P=uP=Q \tag{1}$$

$$W'=(x_{Bob}+y_{Bob})Q'=(x_{Bob}+r_{Bob}+sh_{Bob})Q'=u(x_{Bob}+r_{Bob}+sh_{Bob})P=u(X_{Bob}+Y_{Bob}+P_{Pub}h_{Bob})=W \tag{2}$$

其中,$X_{Alice}+Y_{Alice}+P_{Pub}h_{Alice}=(x_{Alice}+y_{Alice})P$ 和 $y_{Bob}=r_{Bob}+S_{msk}h_{Bob}$.

2.2.2 验证的正确性.

由等式(3)成立可知,*Bob* 能够验证 *Alice* 签名的正确性,即验证过程是正确的.

$$VP=(n(x_{Alice}+y_{Alice})+uk)P=n(x_{Alice}+y_{Alice})P+ukP=n'(X_{Alice}+Y_{Alice}+P_{Pub}h_{Alice})+k'Q' \tag{3}$$

其中,$(x_{Alice}+y_{Alice})P=X_{Alice}+Y_{Alice}+P_{Pub}h_{Alice}$,$n'=H_2(ID_{Alice},C,X_{Alice},Q')$,$n=H_2(ID_{Alice},C,X_{Alice},Q)$,$k'=H_2(ID_{Alice},C,Y_{Alice},Q')$,$k=H_2(ID_{Alice},C,Y_{Alice},Q)$和 $Q'=Q=uP$.

3 安全性证明

3.1 机密性

定理 1(A_I类敌手攻击下的机密性). 在随机谕言机模型中,若存在敌手 A_{I}^1 可在多项式时间内,以不可忽略的概率 $\varepsilon_{\mathrm{I}}^1$ 赢得相关游戏(游戏中 A_{I}^1 最多进行 q_S次签密询问和 q_{SK}次私钥提取询问),则存在算法 B 可在多项式时间内至少以不可忽略的概率 $\frac{1}{q}\left(1-\frac{q_{SK}}{2^k}\right)\frac{\varepsilon_{\mathrm{I}}^1}{\mathrm{e}(q_S+q_{SK})}$ (其中,e 是自然对数底数,k 是安全参数,q 是大素数)解决 CDH 困难问题.

证明:算法 B 是一个 CDH 困难问题的解决者,其输入为元组$\langle P,aP,bP\rangle$,其中, $a,b\in Z_q^*$ 且未知,目标为计算 abP. 算法 B 以敌手 A_{I}^1 为子程序并充当游戏的挑战者.游戏开始后,B 运行 *Setup* 算法,并发送系统公开参数 *Params* 给 A_{I}^1,令 $P_{Pub}=bP$(意味着主密钥为 b);维护列表 L_1,L_2,L_3,L_{SK} 和 L_{PK} 分别用于跟踪敌手 A_{I}^1 对谕言机 H_1,H_2,H_3 的询问以及对私钥和公钥的提取询问,初始时各列表均为空.

询问:敌手 A_{I}^1 进行下述询问.

H_2 询问:当 B 收到敌手 A_{I}^1 对 H_2 的询问$\langle ID_i,C_i,X_i(Y_i),Q_i\rangle$时,若存在$\langle ID_i,C_i,X_i(Y_i),Q_i,h_2\rangle\in L_2$,则返回 h_2 给 A_{I}^1;否则,B 随机选取 $h_2\in Z_q^*$ 满足$\langle *,*,*,*,h_2\rangle\notin L_2$(避免哈希函数碰撞的发生),添加元组$\langle ID_i,C_i,X_i(Y_i),Q_i,h_2\rangle$到 L_2 中,并返回 h_2 给 A_{I}^1.

H_3 询问:当 B 收到敌手 A_{I}^1 对 H_3 的询问$\langle ID_i,W_i\rangle$时,若存在$\langle ID_i,W_i,h_3\rangle\in L_3$,则返回 h_3 给 A_{I}^1;否则,B 随机选取 $h_3\in\{0,1\}^{l_2}$ 满足$\langle *,*,h_3\rangle\notin L_3$,添加$\langle ID_i,W_i,h_3\rangle$到 L_3 中,并返回 h_3 给 A_{I}^1.

公钥提取询问:当 B 收到敌手 A_{I}^1 对身份 ID_i 的公钥生成询问时,B 进行下述操作.

① 若存在$\langle ID_i,X_i,Y_i,c_i\rangle\in L_{PK}$,则返回相应的公钥值$PK_i=\langle X_i,Y_i\rangle$给$A_1^1$;

② 否则,B选取随机数$c_i\leftarrow\{0,1\}$,且$\Pr[c_i=1]=\delta=\dfrac{1}{q_S+q_{Sk}+1}$(游戏中,$A_1^1$选取了$q_{SK}$个身份进行私钥提取询问,选取了$q_S$个身份进行签密询问,选取1个身份作为挑战身份).若c_i=0,B随机选取$x_i,y_i,h_1\in Z_q^*$,计算$X_i=x_iP$和$Y_i=y_iP-P_{Pub}h_1$满足$\langle *,X_i,Y_i,*\rangle\notin L_{PK}$,否则,需重新选取相应的随机数;添加相应的元组$\langle ID_i,X_i,Y_i,c_i\rangle$到$L_{PK}$中,返回$PK_i=\langle X_i,Y_i\rangle$给$A_1^1$;同时,添加$\langle ID_i,x_i,y_i\rangle$到$L_{SK}$中;添加$\langle ID_i,X_i,Y_i,h_1\rangle$到$L_1$中.若$c_i$=1,令$X_i=r_{know}^1P$和$Y_i=r_{know}^2P$(其中,$r_{Know}^1,r_{Know}^2\in Z_q^*$是$B$已知的随机参数)满足$\langle *,X_i,Y_i,*\rangle\notin L_{PK}$,否则,需重新选取$r_{Know}^1$和$r_{Know}^2$,添加元组$\langle ID_i,X_i,Y_i,c_i\rangle$到$L_{PK}$中,添加$\langle ID_i,X_i,Y_i,h_1\rangle$到$L_1$中,$B$返回$PK_i=\langle X_i,Y_i\rangle$给$A_1^1$.

H_1询问:当B收到敌手A_1^1对H_1的询问$\langle ID_i,X_i,Y_i\rangle$时,若存在$\langle ID_i,X_i,Y_i,h_1\rangle\in L_1$,则返回$h_1$给$A_1^1$;否则,$B$对$ID_i$进行公钥生成询问后(在该询问中将添加相应的元组$\langle ID_i,X_i,Y_i,h_1\rangle$到$L_1$中),返回相应元组$\langle ID_i,X_i,Y_i,h_1\rangle$中的$h_1$给$A_1^1$.

私钥提取询问:当B收到A_1^1对ID_i的私钥生成询问时,

① 若存在$\langle ID_i.x_i,y_i\rangle\in L_{SK}$,则返回相应的私钥$SK_i=\langle x_i,y_i\rangle$给$A_1^1$;

② 否则,B对ID_i进行公钥生成询问并获得相应的应答$\langle ID_i,X_i,Y_i,c_i\rangle$;若$c_i$=0,则在$ID_i$的公钥生成询问中已向$L_{SK}$添加了相应的元组$\langle ID_i,x_i,y_i\rangle$,$B$在返回$L_{SK}$中相应的私钥$SK_i=\langle x_i,y_i\rangle$给$A_1^1$;若$c_i$=1,则$B$结束,并终止模拟.

公钥替换:敌手A_1^1可选择任意一个新公钥$PK_i'=\langle X_i',Y_i'\rangle$替换合法用户$ID_i$的原始公钥$PK_i$.

签密询问:当B收到A_1^1对元组$\langle ID_S,ID_R,m\rangle$(假设$A_1^1$对$ID_R$已进行了公钥生成询问)的签密询问时,$B$在$L_{PK}$中查询$ID_R$对应的元组$\langle ID_R,X_R,Y_R,c_R\rangle$,并进行下述操作.

① 若c_R=1,则B结束,并终止模拟;

② 否则,B在L_{SK}与L_{PK}中分别查询ID_S及ID_R对应的元组$\langle ID_S,x_S,y_S\rangle\in L_{SK}$和$\langle ID_R,X_R,Y_R\rangle\in L_{PK}$,运行算法$Sign(Params,ID_S,SK_S,ID_R,PK_R,m)$生成相应的密文$\sigma=(U,V,C)$,并将$\sigma$返回给$A_1^1$.

解签密询问:当B收到A_1^1对元组$\langle ID_S,ID_R,\sigma=(U,V,C)\rangle$(假设$A_1^1$对$ID_R$已进行了公钥生成询问)的解签密询问时,$B$在$L_{PK}$中查询$ID_R$所对应的元组$\langle ID_R,X_R,Y_R,c_R\rangle$,并进行下述操作.

① 若存在且c_R=0,则B分别在L_{SK}与L_{PK}中查询ID_R及ID_S相对应的元组$\langle ID_R,x_R,y_R\rangle\in L_{SK}$和$\langle ID_S,X_S,Y_S\rangle\in L_{PK}$,对密文$\sigma=(U,V,C)$运行解签密算法$UnSign(Params,ID_S,PK_S,ID_R,SK_R,\sigma)$,并返回$m$给$A_1^1$,若输入的密文无效,则$B$输出特殊符号$\perp$;

② 若存在且c_R=1,B在列表L_1,L_2和L_3中查询元组$\langle ID_S,X_S,Y_S,h_1\rangle\in L_1$,$\langle ID_S,C,X_S,Q,h_2^X\rangle\in L_2$,$\langle ID_S,C,Y_S,Q,h_2^Y\rangle\in L_2$和$\langle ID_R,W,h_3\rangle\in L_3$,计算$m=C\oplus h_3$,若等式$VP=h_2^X(X_S+Y_S+P_{Pub}h_1)+h_2^YQ$成立,则返回$m$给$A_1^1$,否则,$B$输出特殊符号$\perp$;

③ 若列表L_{PK}中不存在元组$\langle ID_S,X_S,Y_S\rangle$(即公钥被替换),$B$在列表$L_1$,$L_2$和$L_3$中查询元组$\langle ID_S,X_S',Y_S',h_1'\rangle\in L_1$,$\langle ID_S,C,X_S',Q,h_2'^X\rangle\in L_2$,$\langle ID_S,C,Y_S',Q,h_2'^Y\rangle\in L_2$,$\langle ID_R,W,h_3\rangle\in L_3$,计算$m=C\oplus h_3$,若等式$VP=h_2'^X(X_S'+Y_S'+P_{Pub}h_1)+h_2'^YQ$成立,则返回$m$给$A_1^1$,否则,$B$输出特殊符号$\perp$.

挑战:敌手A_1^1输出两个身份$ID_S,ID_R\in ID$(ID_R是挑战身份)和两个等长的挑战消息$m_0,m_1\in M$.

算法B对ID_R进行公钥生成询问,获得其对应的元组$\langle ID_R,X_R,Y_R,c_R\rangle$,并进行下述操作.

① 若c_R=0,则B结束,并终止模拟;

② 否则,令$Q=aP$,B随机选取$W\in G$,计算$C=m_d\oplus H_3(ID_R,W)$(其中,$d\leftarrow\{0,1\}$);选取满足条件$VP=n(X_S+Y_S+P_{Pub}h_S)+kQ$(其中,$n=H_2(ID_S,C,X_S,Q)$,$k=H_2(ID_S,C,Y_S,Q)$)和$Q=U(X_S+Y_S+P_{Pub}h_S)$的随机数$U,V\in Z_q^*$,发送挑战密文$\sigma=(U,V,C)$给$A_1^1$.

敌手 A_{I}^{1} 经过概率多项式时间次数的上述询问后输出对 d 的猜测 $d'\leftarrow\{0,1\}$,若 $d'=d$,则 B 输出 $abP=\frac{1}{h_R}[W-(r_{know}^{1}+r_{know}^{2})Q]$(其中,$W=a(X_R+Y_R+P_{Pub}h_R)=(r_{Know}^{1}+r_{Know}^{2}+bh_R)Q$, $Q=aP$,$h_R=H_1(ID_R,X_R,Y_R)$)作为 CDH 困难问题的有效解;否则,B 没有解决 CDH 困难问题.

B 为 A_{I}^{1} 模拟了真实的攻击环境,若 B 在模拟过程中未终止,并且敌手 A_{I}^{1} 以不可忽略的概率 $\varepsilon_{\mathrm{I}}^{1}$ 攻破了本文机制的机密性,则 B 输出 CDH 困难问题的有效解.令事件 ε 表示在挑战阶段算法 B 输出了有效挑战密文,即 B 选择了正确的参数 W,则 $\Pr[\varepsilon]=\frac{1}{q}$;事件 ε_1 表示敌手对挑战身份 ID_R 未进行私钥生成询问,则 $\Pr[\varepsilon_1]=1-\frac{q_{SK}}{2^k}$;事件 ε_2 表示询问阶段算法 B 未终止,则 $\Pr[\varepsilon_2]=(1-\delta)^{q_S+q_{SK}}$;事件 ε_3 表示挑战阶段算法 B 未终止,则 $\Pr[\varepsilon_3]=\delta$.

整个模拟过程中算法 B 不终止的概率为 $Pr[\varepsilon\wedge\varepsilon_1\wedge\varepsilon_2\wedge\varepsilon_3]=\frac{1}{q}\left(1-\frac{q_{SK}}{2^k}\right)(1-\delta)^{q_S+q_{SK}}\delta$. 由于 $\delta=\frac{1}{q_S+q_{SK}+1}$,当 q_S+q_{SK} 足够大时,$\left(1-\frac{1}{q_S+q_{SK}+1}\right)^{q_S+q_{SK}+1}$ 趋向于 e^{-1}(e 是自然对数底数),因此,模拟过程中算法 B 不终止的概率至少为 $\frac{1}{q}\left(1-\frac{q_{SK}}{2^k}\right)\frac{1}{\mathrm{e}(q_S+q_{SK})}$.

综上所述,若算法 B 在模拟过程中未终止,且敌手 A_{I}^{1} 以不可忽略的概率 $\varepsilon_{\mathrm{I}}^{1}$ 攻破了本文方案的机密性,则 B 至少以不可忽略的概率 $\frac{1}{q}\left(1-\frac{q_{SK}}{2^k}\right)\frac{\varepsilon_{\mathrm{I}}^{1}}{\mathrm{e}(q_S+q_{SK})}$ 输出 CDH 困难问题的有效解. □

定理 2(A_{II} 类敌手攻击下的机密性). 在随机谕言机模型中,若存在敌手 A_{II}^{1} 可在多项式时间内,以不可忽略的概率 $\varepsilon_{\mathrm{II}}^{1}$ 赢得相关游戏(游戏中 A_{II}^{1} 最多进行 q_S 次签密询问和 q_{SK} 次私钥生成询问),则存在算法 B 可在多项式时间内至少以不可忽略的概率 $\frac{1}{q}\left(1-\frac{q_{SK}}{2^k}\right)\frac{\varepsilon_{\mathrm{II}}^{1}}{\mathrm{e}(q_S+q_{SK})}$ 解决 CDH 困难问题.

证明:算法 B 是一个 CDH 困难问题的解决者,输入为元组$\langle P,aP,bP\rangle$,其中,$a,b\in Z_q^*$ 且未知,目标是计算 abP. 算法 B 以敌手 A_{II}^{1} 为子程序并充当游戏的挑战者.游戏开始后,B 运行 *Setup* 算法,并发送 *Params* 和主密钥 S_{msk} 给 A_{II}^{1} (A_{II}类敌手掌握主密钥),维护列表 L_1,L_2,L_3,L_{SK} 和 L_{PK} 分别用于跟踪 A_{II}^{1} 对谕言机 H_1,H_2,H_3 的询问以及对私钥和公钥的提取询问,初始时各列表均为空.

询问:敌手 A_{II}^{1} 执行定理 1 中对谕言机 H_1、H_2、H_3 的询问、私钥生成询问和签密询问.

公钥生成询问:当 B 收到 A_{II}^{1} 对 ID_i 的公钥提取询问时,B 进行下述操作.

① 若存在$\langle ID_i,X_i,Y_i,c_i\rangle\in L_{PK}$,则返回相应的公钥值 $PK_i=\langle X_i,Y_i\rangle$给 A_{II}^{1};

② 否则,B 选取随机数 $c_i\leftarrow\{0,1\}$,且 $\Pr[c_i=1]=\delta=\frac{1}{q_S+q_{SK}+1}$.若 $c_i=0$,B 随机选取 $x_i,y_i,h_1\in Z_q^*$,计算 $X_i=x_iP$ 和 $Y_i=y_iP-P_{Pub}h_1$ 满足$\langle *,X_i,Y_i,*\rangle\notin L_{PK}$,否则,需重新选取相应的随机数;添加$\langle ID_i,X_i,Y_i,c_i\rangle$到 L_{PK} 中,返回 $PK_i=\langle X_i,Y_i\rangle$给 A_{II}^{1};同时,添加$\langle ID_i,x_i,y_i\rangle$到 L_{SK} 中;添加$\langle ID_i,X_i,Y_i,h_1\rangle$到 L_1 中.若 $c_i=1$,则令 $X_i=r_{Know}P$ 和 $Y_i=bP$(r_{Know} 为 B 已知的参数)满足$\langle *,X_i,*,*\rangle\notin L_{PK}$,否则,需重新选取参数 r_{Know},添加$\langle ID_i,X_i,Y_i,c_i\rangle$到 L_{PK} 中,添加$\langle ID_i,X_i,Y_i,h_1\rangle$到 L_1 中,并返回 $PK_i=\langle X_i,Y_i\rangle$给 A_{II}^{1}.

解签密询问:当 B 收到敌手 A_{II}^{1} 对元组$\langle ID_S,ID_R,\sigma=(U,V,C)\rangle$(假设敌手 A_{II}^{1} 对 ID_R 已进行了公钥生成询问)的解签密询问时,B 在 L_{PK} 中查询 ID_R 所对应的元组$\langle ID_R,X_R,Y_R,c_R\rangle$,并进行下述操作.

① 若存在且 $c_R=0$,则 B 分别在 L_{SK} 与 L_{PK} 查询 ID_R 及 ID_S 对应的元组$\langle ID_R,x_R,y_R\rangle$和$\langle ID_S,X_S,Y_S\rangle$,对密文 $\sigma=(U,S,C)$运行解签密算法 $UnSign(Params,ID_S,PK_S,ID_R,SK_R,\sigma)$,并返回 m 给 A_{II}^{1},若输入的密文无效,则 B 输出特殊符号$\perp$;

② 若存在且 c_R=0,B 在列表 L_1,L_2 和 L_3 中查询元组$\langle ID_S,X_S,Y_S,h_1\rangle\in L_1$,$\langle ID_S,C,X_S,Q,h_2^X\rangle\in L_2$,$\langle ID_S,C,Y_S,Q,h_2^Y\rangle\in L_2$ 和$\langle ID_R,W,h_3\rangle\in L_3$,计算 $m=C\oplus h_3$,若等式 $VP=h_2^X(X_S+Y_S+P_{Pub}h_1)+h_2^YQ$ 成立,则返回 m 给 A_{II}^1,否则,B 输出特殊符号$\perp$.

挑战:敌手 A_{II}^1 输出两个身份 ID_S,$ID_R\in ID$ 和两个等长的挑战消息 m_0,$m_1\in M$,其中,ID_R 是挑战身份.

算法 B 对 ID_R 进行公钥生成询问,获得其对应的元组$\langle ID_R,X_R,Y_R,c_R\rangle$,并进行下述操作.

① 若 c_R=0,则 B 放弃,并终止模拟;

② 否则,令 $Q=aP$,B 随机选取 $W\in G$,计算 $C=m_d\oplus H_3(ID_R,W)$(其中,$d\leftarrow\{0,1\}$);选取满足条件 $VP=n(X_S+Y_S+P_{Pub}h_S)+kQ$(其中,$n=H_2(ID_S,C,X_S,Q)$,$k=H_2(ID_S,C,Y_S,Q)$)和 $Q=U(X_S+Y_S+P_{Pub}+h_S)$的随机数 $U,V\in Z_q^*$,发送挑战密文 $\sigma=(U,V,C)$给 A_{II}^1.

敌手 A_{II}^1 经过概率多项式时间次数的上述询问后输出对 d 的猜测 $d'\leftarrow\{0,1\}$,若 $d'=d$,B 输出 $abP=W-(r_{Know}+sh_R)Q$(其中,$Q=aP$,$h_R=H_1(ID_R,X_R,Y_R)$,$W=(r_{Know}+b+sh_R)Q$)作为 CDH 困难问题的解;否则,B 没有解决 CDH 困难问题.

由定理 1 证明可知,若敌手 A_{II}^1 以不可忽略的概率 $\varepsilon_{\text{II}}^1$ 攻破了本文机制的机密性,则 B 至少以不可忽略的概率 $\frac{1}{q}\left(1-\frac{q_{SK}}{2^k}\right)\frac{\varepsilon_{\text{II}}^1}{\mathrm{e}(q_S+q_{SK})}$ 输出 CDH 困难问题的有效解. □

3.2 不可伪造性

定理 3(A_{I}类敌手攻击下的不可伪造性). 在随机谕言机模型中,若存在一个敌手 A_{I}^2 可在多项式时间内,以不可忽略的概率 ε_{I}^2 赢得相关游戏(游戏中 A_{I}^2 最多进行 q_S 次签密询问和 q_{SK} 次私钥生成询问),则存在算法 B 可在多项式时间内至少以不可忽略的概率 $\left(1-\frac{q_{SK}}{2^k}\right)\frac{\varepsilon_{\text{I}}^2}{\mathrm{e}(q_S+q_{SK})}$ 解决 DL 困难问题.

证明:算法 B 是一个 DL 困难问题的解决者,输入为元组$\langle P,bP\rangle$,其中,$b\in Z_q^*$ 且未知,目标是计算 $b\in Z_q^*$. 算法 B 以敌手 A_{I}^2 为子程序并充当游戏的挑战者.游戏开始后,B 运行 *Setup* 算法,并发送公开参数 *Params* 给 A_{I}^2,令 $P_{Pub}=bP$(意味着主密钥为 b),维护列表 L_1,L_2,L_3,L_4,L_{SK} 和 L_{PK} 分别用于跟踪 A_{I}^2 对谕言机 H_1,H_2 的询问及对私钥和公钥的提取询问,初始时各列表均为空.

询问:敌手 A_{I}^2 执行定理 1 中对谕言机 H_1,H_2 的询问及公钥提取、私钥提取和公钥替换询问.

签名询问:当算法 B 收到敌手 A_{I}^2 关于(m,ID_S)(假设 A_{I}^2 对 ID_S 已进行了公钥生成询问)的签名询问时,B 首先在列表 L_{PK} 中查询 ID_S 所对应的元组$\langle ID_S,X_S,Y_S,c_S\rangle$.

① 若 c_S=1,则 B 放弃,并终止模拟;

② 否则,B 在 L_{SK} 中查询 ID_S 对应的元组$\langle ID_S,x_S,y_S\rangle$,运行算法 *Sign*(*Params*,$ID_S$,$SK_S$,$m$),生成相应的签名 $\sigma=(U,V,m)$,并将其发送给 A_{I}^2.

签名验证询问:当 B 收到敌手 A_{I}^2 对$\langle ID_S,\sigma=(U,V,m)\rangle$(假设 A_{I}^2 对 ID_S 已进行了公钥生成询问)的签名验证询问时,B 在 L_{PK} 中查询 ID_S 对应的元组$\langle ID_S,X_S,Y_S,c_S\rangle$.

① 若存在且 c_S=0,则 B 对签名 $\sigma=(U,V,m)$运行 *UnSign*(*Params*,ID_S,PK_S,σ),并返回 m 给 A_{I}^2,若输入的签名无效,则 B 输出特殊符号$\perp$;

② 若存在且 c_S=1,则 B 在 L_1 和 L_2 中查询元组$\langle ID_S,X_S,Y_S,h_1\rangle\in L_1$,$\langle ID_S,m,X_S,Q,h_2^X\rangle\in L_2$ 和$\langle ID_S,m,Y_S,Q,h_2^Y\rangle\in L_2$,若等式 $VP=h_2^X(X_S+Y_S+P_{Pub}h_1)+h_2^YQ$ 成立,则返回 m 给 A_{I}^2,否则,B 输出特殊符号$\perp$;

③ 若列表 L_{PK} 中不存在元组$\langle ID_S,X_S,Y_S\rangle$(即公钥被替换),$B$ 在 L_1 和 L_2 中查询元组$\langle ID_S,X_S',Y_S',h_1\rangle\in L_1$,$\langle ID_S,m,X_S',Q,h_2'^X\rangle\in L_2$ 和$\langle ID_S,m,Y_S',Q,h_2'^Y\rangle\in L_2$,若等式 $VP=h_2'^X(X_S'+Y_S'+P_{Pub}h_1)+h_2'^YQ$ 成立,则返回 m 给 A_{I}^2,否则,B 输出特殊符号$\perp$.

伪造:经过多项式有界次上述询问后,敌手 A_{I}^2 输出对 ID_S 和 m 的伪造签名$\sigma=(U,V,m)$(伪造前 A_{I}^2 对 ID_S 已进行了公钥生成询问),同时 B 知道被替换的公钥;若 A_{I}^2 伪造签名成功,并且 ID_S 在 L_{PK} 中对应元组$\langle ID_S,X_S,Y_S,c_S\rangle$中的 $c_S=1$,则 B 输出 $b=\dfrac{1}{Uh_S}[u-U(r_{Know}^1+r_{Know}^2)]$ (其中,$h_S=H_1(ID_S,X_S,Y_S)$, $U=u(r_{Know}^1+r_{Know}^2+bh_S)^{-1}$)作为 DL 困难问题的有效解;否则,$B$ 没有解决 DL 问题.

令事件 ε'表示敌手对挑战身份 ID_S 未进行私钥提取询问,则 $\Pr[\varepsilon]=1-\dfrac{q_{SK}}{2^k}$; 事件 ε''表示询问阶段算法 B 未终止,则 $\Pr[\varepsilon]=(1-\delta)^{q_S+q_{SK}}$; 事件 ε''' 表示伪造阶段敌手 A_{I}^2 伪造合法签名后算法 B 未终止,则 $\Pr[\varepsilon''']=\delta$; 则模拟过程中 B 不终止的概率为 $\Pr[\varepsilon'\wedge\varepsilon''\wedge\varepsilon''']=\left(1-\dfrac{q_{SK}}{2^k}\right)(1-\delta)^{q_S+q_{SK}}\delta$, 由于 $\delta=\dfrac{1}{q_S+q_{SK}+1}$, 当 q_S+q_{SK} 足够大时, $\left(1-\dfrac{1}{q_S+q_{SK}+1}\right)^{q_S+q_{SK}+1}$ 趋向于 e^{-1},因此,模拟过程中算法 B 不终止的概率至少为 $\left(1-\dfrac{q_{SK}}{2^k}\right)\dfrac{1}{\mathrm{e}(q_S+q_{SK})}$.

综上所述,若算法 B 在模拟过程中未终止,并且敌手 A_{I}^2 以不可忽略的概率 $\varepsilon_{\mathrm{I}}^2$ 攻破本文方案的不可伪造性,则 B 能以不可忽略的概率 $\left(1-\dfrac{q_{SK}}{2^k}\right)\dfrac{\varepsilon_{\mathrm{I}}^2}{\mathrm{e}(q_S+q_{SK})}$ 输出 DL 困难问题的有效解. □

定理 4(A_{II} 类敌手攻击下的不可伪造性). 在随机谕言机模型中,若存在一个敌手 A_{II}^2 可在多项式时间内,以不可忽略的概率 $\varepsilon_{\mathrm{II}}^2$ 赢得相关游戏(游戏中, A_{II}^2 最多进行 q_S 次签密询问和 q_{SK} 次私钥生成询问),则有算法 B 可在多项式时间内至少以不可忽略的概率 $\left(1-\dfrac{q_{SK}}{2^k}\right)\dfrac{\varepsilon_{\mathrm{II}}^2}{\mathrm{e}(q_S+q_{SK})}$ 解决 DL 困难问题.

证明:算法 B 是一个 DL 困难问题的解决者,输入为元组$\langle P,bP\rangle$,其中, $b\in Z_q^*$ 且未知,目标是计算 $b\in Z_q^*$.算法 b 以敌手 A_{II}^2 为子程序并充当游戏的挑战者.B 运行 *Setup* 算法,发送 *Params* 和主密钥 s 给 A_{II}^2 (A_{II}类敌手掌握主密钥),B 维护列表 L_1,L_2,L_{SK} 和 L_{PK} 分别用于跟踪 A_{II}^2 对谕言机 H_1,H_2 的询问以及对私钥和公钥的提取询问,初始时各列表均为空.

询问:敌手 A_{II}^2 执行定理 2 中对谕言机 H_1,H_2 的询问、私钥提取和公钥提取询问;执行定理 3 中的签名询问.

签名验证询问:当 B 收到敌手 A_{II}^2 对元组$\langle ID_S,\sigma=(Q,S,m)\rangle$(假设 A_{II}^2 对 ID_S 已进行了公钥生成询问)的解签密询问时,B 在 L_{PK} 中查询获得 ID_S 对应的元组$\langle ID_S,X_S,Y_S,c_S\rangle$,并进行下述操作.

① 若 $c_S=0$,则 B 对签名$\sigma=(Q,V,m)$运行 *UnSign*(*Params*,ID_S,PK_S,σ),并返回 m 给 A_{II}^2, 若输入的签名无效,则 B 输出特殊符号$\perp$;

② 若 $c_S=1$,B 在 L_1 和 L_2 中查询$\langle ID_S,X_S,Y_S,h_1\rangle\in L_1$, $\langle ID_S,m,X_S,Q,h_2^X\rangle\in L_2$ 和 $\langle ID_S,m,Y_S,Q,h_2^Y\rangle\in L_2$,若等式 $VP=h_2^X(X_S+Y_S+P_{Pub}h_1)+h_2^YQ$ 成立,则返回 m 给 A_{II}^2, 否则,B 输出特殊符号$\perp$.

伪造:经过多项式有界次上述询问后,敌手 A_{II}^2 输出对 ID_S 及 m 的伪造签名$\sigma=(Q,V,m)$(伪造过程中 A_{II}^2 对 ID_S 已进行了公钥生成询问);若签名伪造成功,且 L_{PK} 中 ID_S 对应元组$\langle ID_S,X_S,Y_S,c_S\rangle$中的 $c_S=1$,则算法 B 输出 $b=\dfrac{1}{U}[u-U(r_{Know}+sh_S)]$ (其中,$h_S=H_1(ID_S,X_S,Y_S)$, $U=u(r_{Know}+b+sh_S)^{-1}$)作为 DL 困难问题的有效解;否则,$B$ 没有解决 DL 困难问题.

由定理 3 可知,若算法 B 在模拟过程中未终止,且敌手 A_{II}^2 以不可忽略的概率 $\varepsilon_{\mathrm{II}}^2$ 攻破本文方案的不可伪造性,则 B 能以不可忽略的概率 $\left(1-\dfrac{q_{SK}}{2^k}\right)\dfrac{\varepsilon_{\mathrm{II}}^2}{\mathrm{e}(q_S+q_{SK})}$ 输出 DL 困难问题的有效解. □

4 机制分析

4.1 效率分析

本节将从计算效率和通信开销两个方面对本文方案的执行效率进行分析,表 1 给出了本文方案与其他相关方案[8,11−18]的效率比较结果.与现有方案[8,11−18]进行比较时,计算开销主要取决于签密和签密验证算法的计算量,且计算量主要统计群上点乘运算、指数运算和双线性映射的执行次数,对异或和 Z_q^* 上的相关运算并不进行统计;同时也未统计可提前计算的相关运算.通信开销主要通过密文的长度来衡量.令 E_e 表示双线性映射操作,E_M 表示群上的点乘运算,E_Q 表示群上的指数运算,其中,$E_e>E_M$ 和 $E_e>E_Q$;l_m 表示明文消息的长度;$|G|$表示群上相应元素的长度;$|Z_q^*|$表示 Z_q^* 中元素的长度.

如表 1 所示,在计算效率方面,由于文献[17–21]涉及双线性映射操作,而文献[8,14,16]的运算量较大,导致上述方案[8,14,16–21]的计算效率较低.在通信开销方面,由于文献[16–18]的密文较长(文献[16]的密文长度并未统计密文中的代理授权部分),导致传输代价较大,其他方案[11−13,15]和本文方案具有较高的计算效率和传输效率.由表 1 可知,与现有的无证书签密方案[11−21]相比,本文机制的计算效率和通信开销更优.

Table 1 Comparison of efficiency with the previous works

表 1 效率比较结果

签密方案	计算效率		通信开销	安全属性				
	签密阶段	解签密阶段	密文长度	不可伪造性	机密性	公开验证性	不可否认性	无密钥托管
文献[8]	$5E_Q$	$7E_Q$	$l_m+2\|G\|$	√	√	√	√	√
文献[11]	$3E_Q$	$5E_Q$	$l_m+2\|Z_q^*\|$	×	×	×	×	√
文献[12]	$3E_M$	$3E_M$	$l_m+2\|Z_q^*\|$	×	×	×	×	√
文献[13]	$3E_M$	$3E_M$	$l_m+2\|Z_q^*\|$	√	×	√	√	√
文献[14]	$4E_Q$	$8E_Q$	$l_m+\|Z_q^*\|+\|G\|$	√	√	×	√	√
文献[15]	$3E_Q$	$3E_Q$	$l_m+\|Z_q^*\|+\|G\|$	√	×	×	√	√
文献[16]	$5E_M$	$6E_M$	$l_m+\|Z_q^*\|+2\|G\|$	√	√	√	√	√
文献[17]	$1E_M+2E_Q$	$1E_M+E_Q+2E_e$	$l_m+\|Z_q^*\|+2\|G\|$	√	√	×	√	√
文献[18]	$3E_M+1E_e$	$3E_M+3E_e$	$l_m+2\|Z_q^*\|+2\|G\|$	×	×	√	×	√
本文方案	$2E_M$	$4E_M$	$l_m+2\|Z_q^*\|$	√	√	√	√	√

注:√表示方案具有该属性,×表示方案不具有该属性

4.2 安全性分析

本节针对相关方案构造具体的保密性或不可伪造性攻击算法.

4.2.1 保密性攻击

以文献[12]中方案为例构造具体的保密性攻击算法.设敌手 A 是 A_{I} 或 A_{II} 类敌手.在文献[12]的定义 1 和定义 2 游戏中,敌手 A 向谕言机发送的挑战信息包括:两个等长的消息 $m_0,m_1\in M$ 和两个挑战身份标识 $ID_S,ID_R\in ID$,其中,不能对 ID_R 是挑战身份且不能对其执行私钥提出询问,在挑战阶段,敌手 A 可获知 ID_S 的公钥 $PK_S=(X_S,R_S)$.

签密谕言机收到敌手 A 的签密询问后,随机选取 $b\leftarrow\{0,1\}$,并计算对消息 m_b 的挑战密文 $\sigma'=(h',S',C')$;当敌手 A 收到谕言机的挑战密文 σ' 后,A 对 b 做出猜测,首先令 $b=0$,A 验证等式 $h'=H_2(S'(X_S+R_S+h_1'y+h'P)\|ID_S\|m_0)$ 是否成立,若成立,则说明消息 m_0 是挑战密文 σ' 的对应明文,否则 m_1 是 σ' 的对应明文.同理,对文献[9,11,13,15]中的方案,可使用同样的方法对其进行保密性攻击.因此,文献[9,11–13,15]中的方案对 A_{I} 和 A_{II} 类敌手均不具有密文的保密性.由于密文的合法性验证过程中的相关参数均为发送者的公开信息,即明文 m 与部分密文 h 之间形成了

对应关系,因此,敌手可通过尝试验证的策略完成机密性攻击.

4.2.2 不可伪造性攻击

文献[13]指出文献[12]中的方案对 A_1 类敌手不具备其所声称的不可伪造性,并构造了具体的不可伪造性攻击算法.由该攻击算法可知,文献[11]的方案也无法满足其所声称的对 A_1 类敌手的不可伪造性.本文以文献[12]为例,构造了新的不可伪造性的攻击算法,具体过程如下所示.

A_1 类敌手 A^1 获悉发送者 *Alice* 的公钥 $PK_A=(R_A,X_A)$后,使用伪造公钥替代 *Alice* 的公钥生成合法的伪造签密密文.敌手 A^1 与接收者 *Bob* 间的具体消息交互过程如下所示.

① A^1 获悉 *Alice* 的公钥 $PK_A=(R_A,X_A)$和身份标识 ID_A 后,计算 $X'_A=-H_1(ID_A,R_A)y-R_A$(其中,y 是系统公钥);

② A^1 使用 $PK'_A=(R_A,X'_A)$ 代替 *Alice* 的原始公钥 $PK_A=(R_A,X_A)$,则此时密文接收者 *Bob* 认为 *Alice* 的公钥就是 $PK'_A=(R_A,X'_A)$;

③ 敌手 A^1 生成 *Alice* 的伪造签密密文:随机选取 $r\in Z_q^*$,首先计算 $R=rP$;然后计算 $h_1=H_1(ID_B,R_B)$,$h'=H_2(R\|ID_A\|m)$;得到 $S'=\frac{r}{h'}$,$C'=H_3(r(R_B+X_B+yh_1))\oplus m$,发送密文消息 $\sigma'=(h',S',C')$给 *Bob*.

Bob 收到密文 $\sigma'=(h',S',C')$后,合法性验证过程如下.

① 计算 $h'_1=H_1(ID_A,R_A)$;

② 计算 $V_B=S'(X'_A+R_A+yh'_1+h'P)(x_B+D_B)$, 恢复消息 $m'=H_3(V_B)\oplus C'$. 由下述等式可知 $m'=m$;

$$V_B=S'(X'_A+R_A+yh'_1+h'P)(x_B+D_B)=S'(h'P)(x_B+D_B)=rP(x_B+D_B)=r(R_B+X_B+yh_1) \tag{4}$$

③ 验证 $h'=H_2(S'(X'_A+R_A+yh'_1+h'P)\|ID_A\|m')$ 是否成立,若成立,则 *Bob* 认为 $\sigma'=(h',S',C')$是由 *Alice* 生成的合法签密密文,由等式(5)可知,上述验证成立.

$$S'(X'_A+R_A+yh'_1+h'P)=S'(h'P)=rP=R \tag{5}$$

由等式(4)和等式(5)可知,伪造密文 $\sigma'=(h',S',C')$通过了密文接收者 *Bob* 的合法性验证,即敌手 A^1 具有伪造 *Alice* 合法密文的能力.

综上所述:在安全性方面,文献[11−15]中的方案均存在安全性缺陷,其中,本文通过构造具体的攻击算法证明了文献[11−13,15]的方案均不满足其所声称的机密性;文献[14,17]的方案不具有公开验证性.同时,文献[11,12]中的方案对 A_1 类敌手不具备其所声称的不可伪造性.文献[19]指出,若获得文献[18]的完整签密密文,即使是一般敌手(既不替换用户的公钥也不用获知系统主密钥)也能掌握发送者的完整私钥,导致该机制不具有其所声称的机密性、不可伪造性和不可否认性等安全属性.因此,相较于现有的无证书签密方案[8,11−18],本文机制的安全性更优.

5 改进机制

由于求逆运算在签密算法中的使用在一定程度上会降低本文机制∏的执行效率,因此,本节在∏的基础上提出一种改进的无证书签密机制∏′=(*Setup′*,*KeyGen′*,*Sign′*,*UnSign′*),其中,算法 *Setup′*和 *KeyGen′*与机制∏的算法 *Setup* 和 *KeyGen* 一致;签密 *Sign′*和解签密 *UnSign′*算法分别描述如下.

5.1 签 密

若要发送消息 m 给接收者 *Bob*,发送者 *Alice* 进行下述操作.

① 选取随机秘密数 $u\in Z_q^*$,计算 $Q=uP$;

② 计算 $W=u(X_{Bob}+Y_{Bob}+P_{Pub}h_{Bob})$,其中,$h_{Bob}=H_1(ID_{Bob},X_{Bob},Y_{Bob})$;

③ 生成密文 $C=m\oplus H_3(ID_{Bob},W)$和签名 $V=n(x_{Alice}+y_{Alice})+u_k$,其中,$n=H_2(ID_{Alice},C,X_{Alice},Q)$,$k=H_2(ID_{Alice},C,Y_{Alice},Q)$;

④ 发送密文 $\sigma=(Q,V,C)$给接收者 *Bob*.

5.2 解签密

收到发送者 *Alice* 的密文 $\sigma=(Q,V,C)$后,接收者 *Bob* 进行下述操作.

若等式(6)成立,则计算 $W'=(x_{Bob}+y_{Bob})Q$,恢复明文消息 $m=C\oplus H_3(ID_{Bob},W')$;否则,输出⊥表示输入的密文无效.

$$VP=n(X_{Alice}+Y_{Alice}+P_{Pub}h_{Alice})+kQ \tag{6}$$

其中,$h_{Alice}=H_1(ID_{Alice},X_{Alice},Y_{Alice})$,$n=H_2(ID_{Alice},C,X_{Alice},Q)$,$k=H_2(ID_{Alice},C,Y_{Alice},Q)$.

改进机制$\prod'$与原始机制$\prod$具有相同的安全性.受篇幅所限,本文不再赘述机制$\prod'$的安全性证明过程,其证明过程与机制$\prod$相类似.

6 结束语

签密作为一种较为理想的数据信息安全传输方法,其安全性和计算开销对其实际应用起着至关重要的作用.本文提出了不使用双线性映射的高效、安全无证书签密方案,在随机谕言机模型下,基于 CDH 假设和 DL 困难问题证明了本文方案的安全性.分析可知,本文方案还具有公开验证和不可否认等安全属性.相较于现有的无证书签密方案,本文方案的计算和通信效率及安全性更优.由于具有更优的性能,本文方案在实际环境中具有更广的应用前景.

References:

[1] Zheng YL. Digital signcryption or how to achieve cost (signature and encryption)≤cost (signature)+cost (encryption). In: Proc. of the 17th Annual Int'l Cryptology Conf. on Advances in Cryptology (CRYPTO'97). Santa Barbara, 1997,(8):17–21. [doi: 10.1007/BFb0052234]

[2] Al-Riyami SS, Paterson KG. Certificateless public key cryptography. In: Proc. of the 9th Int'l Conf. on the Theory and Application of Cryptology and Information Security, Advances in Cryptology (ASIACRYPT 2003). 2003. [doi: 10.1007/978-3-540-40061-5_29]

[3] Shamir A. Identity-Based cryptosystems and signature schemes. In: Advances in Cryptology (CRYPTO'84). Santa Barbara, 1984,(8):19–22. [doi: 10.1007/3-540-39568-7_5]

[4] Barbosa M, Farshim P. Certificateless signcryption. In: Proc. of the ACM Symp. on Information, Computer and Communications Security. Tokyo, 2008,(3):18–20. [doi: 10.1145/1368310.1368364]

[5] Yu G, Yang HZ, Fan SQ, Shen Y, Han W. Efficient certificateless signcryption scheme. In: Proc. of the 3rd Int'l Symp. on Electronic Commerce and Security Workshops. Guangzhou, 2010. 55–59. http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.403.7629

[6] Wu CH, Chen ZX. A new efficient certificateless signcryption scheme. In: Proc. of the Int'l Symp. on Information Science and Engineering. Washington, 2008,(12):20–22. [doi: 10.1109/ISISE.2008.206]

[7] Barreto PSLM, Deusajute AM, De E, Cruz S, Pereira GCCF, Da Silva RR. Toward efficient certificateless signcryption from (and without) bilinear pairings. 2008. http://ceseg.inf.ufpr.br//anais/2008/data/pdf/st03_03_artigo.pdf

[8] Sharmila DS, Vivek SS, Pandu RC. Cryptanalysis of certificateless signcryption schemes and an efficient construction without pairing. In: Proc. of the 5th Int'l Conf. on Information Security and Cryptology. Beijing, 2009. 75–92. [doi: 10.1007/978-3-642-16342-5_6]

[9] Yu HF, Yang B. Provably secure certificateless hybrid signcryption. Chinese Journal of Computers, 2015,38(4):804–813 (in Chinese with English abstract).

[10] Li FG, Masaaki S, Tsuyoshi T. Certificateless hybrid signcryption. Mathematical and Computer Modelling, 2013,57(3-4):324–343. [doi: 10.1016/j.mcm.2012.06.011]

[11] Zhu H, Li H, Wang YM. Certificateless signcryption scheme without pairing. Journal of Computer Research and Development, 2010,47(9):1587–1594 (in Chinese with English abstract).

[12] Liu WH, Xu CX. Certificateless signcryption scheme without bilinear pairing. Ruan Jian Xue Bao/Journal of Software, 2011,22(8):1918–1926 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/3891.htm [doi: 10.3724/SP.J.1001.2011.03891]

[13] He DB. Security analysis of a certificateless signcryption scheme. Ruan Jian Xue Bao/Journal of Software, 2013,24(3):618–622 (in Chinese with English abtract). http://www.jos.org.cn/1000-9825/4245.htm [doi: 10.3724/SP.J.1001.2013.04245]

[14] Xie WJ, Zhang Z. Certificateless signcryption without pairing. 2010. http://eprint.iacr.org/2010/187.pdf

[15] Jing XF. Provably secure certificateless signcryption scheme without pairing. In: Proc. of the Int'l Conf. on Electronic and Mechanical Engineering and Information Technology. Harbin, 2011. 4753–4756. [doi: 10.1109/EMEIT.2011.6024098]

[16] Qi YF, Tang CM, Lou Y, Xu MZ, Guo BA. Certificateless proxy identity-based signcryption scheme without bilinear pairings. China Communications, 2013,22(11):37–41. [doi: 10.1109/CC.2013.6674208]

[17] Li F, Han Y, Jin C. Certificateless online/offline signcryption for the Internet of Things. Wireless Networks, 2015,1–14. [doi: 10.1007/s11276-015-1145-3]

[18] Luo M, Tu M, Xu J. A security communication model based on certificateless online/offline signcryption for Internet of Things. Security & Communication Networks, 2013,7(10):1560–1569. [doi: 10.1002/sec.836]

[19] Shi W, Kumar N, Gong P, Chilamkurti N, Chang H. On the security of a certificateless online/offline signcryption for Internet of Things. Peer-to-Peer Networking and Applications, 2015,37(1):1–5. [doi: 10.1007/s12083-014-0249-3]

[20] Yin A, Liang H. Certificateless hybrid signcryption scheme for secure communication of wireless sensor networks. Wireless Personal Communications, 2015,80(3):1049–1062. [doi: 10.1007/s11277-014-2070-y]

[21] Huang Q, Wong DS. Generic certificateless encryption in the standard model. In: Proc. of the Advances in Information and Computer Security, the 2nd Int'l Workshop on Security. Nara, 2007. 278–291. [doi: 10.1007/978-3-540-75651-4_19]

附中文参考文献:

[9] 俞惠芳,杨波.可证安全的无证书混合签密.计算机学报,2015,38(4):804–813.

[11] 朱辉,李晖,王育民.不使用双线性对的无证书签密方案.计算机研究与发展,2010,47(9):1587–1594.

[12] 刘文浩,许春香.无双线性配对的无证书签密方案.软件学报,2011,22(8):1918–1926. http://www.jos.org.cn/1000-9825/3891.htm [doi: 10.3724/SP.J.1001.2011.03891]

[13] 何德彪.无证书签密机制的安全性分析.软件学报,2013,24(3):618–622. http://www.jos.org.cn/1000-9825/4245.htm [doi: 10.3724/SP.J.1001.2013.04245]

周彦伟(1986－),男,甘肃通渭人,工程师,主要研究领域为密码学,匿名通信技术,可信计算.

王青龙(1970－),男,博士,副教授,主要研究领域为密码学及其应用.

杨波(1963－),男,博士,教授,博士生导师,主要研究领域为密码学,信息安全.