无证书多接收者多消息签密机制

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 安全广播服务已经成为信息安全领域的一个研究热点,而多接收者签密技术被认为是实现安全广播的最有效方法之一,因此对多接收者签密机制的研究已成为信息安全领域的一个新分支.针对现有使用双线性映射的多接收者签密机制存在计算效率低的不足,同时为了满足广播通信环境下发送者的多消息发送需求,文中提出不使用双线性映射的无证书多接收者多消息签密机制,签密密文中不再包含接收者身份列表,实现对接收者身份等隐私信息的保护;并且具有密文解密的独立性,同时发送者可在一次签密操作中完成多消息发送任务.安全性证明及正确性分析表明文中机制是安全、有效的无证书多接收者多消息签密机制,由于未使用双线性映射等计算量较大的运算,文中方案的计算效率更高.与现有方案相比较而言,除具有保密性和不可伪造性之外,文中方案具有较强的匿名性及计算效率,满足广播通信环境中多消息的匿名发送需求.

关键词 无证书签密;多接收者;多消息;匿名性;无双线性映射

中图法分类号 TP309 **DOI 号** 10.11897/SP.J.1016.2017.01714

Multi-Receiver and Multi-Message of Certificateless 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 a cryptographic primitive that fulfills both the functions of digital signature and public key encryption simultaneously, at a cost significantly lower than that required by the traditional signature-then-encryption approach. Secure broadcasting service become more and more attractive and it has become a hot research topic in the field of information security. The multi-receiver signcryption technology is considered as one of the most efficient methods to implement secure broadcasting, and it has become a new branch of information security. In addition, the certificateless public key cryptography eliminates certificate management in traditional public key infrastructure and solves the key escrow problem in identity-based cryptography. Certificateless signcryption is one of the most important primitives in certificateless public key cryptography which achieves confidentiality and authentication simultaneously. In this paper, in order to satisfy the receivers' need of privacy protection, the multi-receiver and multi-message of certificateless signcryption scheme was proposed. The signcryption ciphertext no longer contains receivers'

收稿日期:2015-04-24;在线出版日期:2016-01-18.本课题得到国家自然科学基金(61272436,61572303)、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)、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,主要研究兴趣为密码学、匿名通信技术等. E-mail: zyw_snnu@foxmail.com; zhouyanwei1986@163.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. E-mail: byang@snnu.edu.cn. **张文政**,男,1966 年生,研究员,主要研究领域为信息安全等.

identity list to protect receivers' privacy. And, as well, the public information set guarantees the independency of decryption. The proofness of correctness and safety demonstrates this signcryption scheme is safe and effective. Apart from confidentiality and unforgery, this signcryption scheme is better in anonymity and has a higher computational efficiency, satisfy the needs of sending sensitive information in broadcast communication environment.

Keywords　certificateless signcryption; multi-receiver; multi-message; anonymity; without bilinear pairing

1　引　言

鉴于网络环境的复杂性，互联网用户往往希望通信消息能同时满足保密性和认证性，消息的保密性主要是通过加密来完成，而认证性则基于签名来实现. 然而传统采用先签名后加密的方式，虽能保证消息的保密性和认证性，但其计算量较大、效率较低，且传输代价大[1]. 文献[2]首先提出签密的概念，旨在让公钥加密和数字签名同时进行，使密文同时具有机密性和认证性，并且具有更小的计算和传输代价；随着广播通信技术的发展，发送者需向多人发送消息，并且希望仅有其授权的用户才能获悉其身份等隐私信息；广播通信环境下用户对隐私信息的保护需求，推进了对多接收者签密机制的研究，多接收者签密机制可通过一次签密操作完成向多个接收者发送消息的目的，比传统一对一方式更适用于广播和组播等通信业务.

近年来，国内外研究者相继提出了多个多接收者签密机制[3-17]（下文简称：机制），由于接收者的身份列表或密文标记列表是密文的一部分，导致多数机制[3-7,13-14,17]的密文信息易暴露接收者身份；部分机制[4-5,8-12,14-15,17]以基于身份的密码系统为基础，存在密钥托管的问题；同时，绝大多数机制[3-16]仅具有单消息发送能力，即发送者仅能发送单个相同的消息给多位接收者，无法满足用户的多消息的发送需求；并且部分机制[8-15]涉及双线线性映射或指数运算，导致相关机制的计算效率较低.

传统的公钥密码系统需要昂贵而又繁琐的证书管理系统，基于身份的密码系统却存在密钥托管的不足，为了弥补上述不足，Al-Riyami 和 Paterson 提出了无证书公钥密码系统（简称 CL-PKC）. 在 CL-PKC 中，用户私钥由用户和部分密钥生成中心（Private Key Generator，PKG）共同生成，公钥则由私钥和系统参数所决定. 鉴于 CL-PKC 避免了传统公钥密码中的证书管理问题，同时又解决了基于身份密码系统的密钥托管问题，因此基于 CL-PKC 进行无证书的多接收者签密机制的研究已成为当前签密领域的研究热点.

针对现有机制存在的不足，本文提出基于 CL-PKC 的多接收者多消息签密机制，该机制的签密密文不包含接收者的身份列表，实现了接收者隐私信息的安全隐藏，不仅使攻击者无法得到接收者的信息，而且所有的接收者彼此都无法获知除自己以外的其他接收者的相关信息，从而解决了接收者的隐私保护问题；并且仅有发送者授权的接收者才能正确解密；在解密密文时，接收者所需的相关参数均取自相同的数据集合，无需除自己之外的其他接收者的相关信息，满足解密的独立性；本文机制的签密和解签密阶段无需双线性映射和指数运算，并在一次签密操作中可向多个接收者发送多个消息，满足发送者的多消息发送需求；在随机谕言机模型下，基于相关困难性问题证明了本文无证书多接收者多消息签密机制的保密性和不可伪造性.

2　相关工作

文献[3]提出了第一个基于身份的多接收者签密机制，签密者对消息进行一次签密，每个接收者均可使用自己的私钥对消息的机密性和可靠性进行验证；Lal 等人①提出了更为高效的基于身份的多接收者签密算法，并在密文中补充了接收者身份列表；文献[4-5]分别提出了基于身份的多接收者签密机制，并在随机谕言机模型下基于相关困难性问题对机制的安全性进行了证明；遗憾的是 Selvi 等人②发现文

① Lal S, Kushwah P. Anonymous ID-based signcryption scheme for multiple receivers. http://eprint.iacr.org/2009/345.pdf

② Selvi S S D, Vivek S S, Gopalakrishnan R, et al. On the provable security of multi-receiver signcryption schemes. http://eprint.iacr.org/2008/238.pdf

献[4]中的机制无法满足其所声称的保密性和不可伪造性,并指出文献[5]中的机制无法满足其所声称的保密性.同时,对多接收者签密机制的安全性模型①进行了研究,该模型中定义了$\mathcal{A}_{\mathrm{I}}$和$\mathcal{A}_{\mathrm{II}}$两类敌手,并对文献[6]中的机制进行了安全性分析,指出该机制在$\mathcal{A}_{\mathrm{I}}$类敌手的攻击下无法满足其声称的保密性和不可伪造性;文献[7-8]分别提出相应的多接收者签密机制,并在随机谕言机模型下,基于相应的困难性问题证明了相关机制的安全性;文献[9-10]针对现有基于身份的多接收者签密机制存在的接收者身份易泄露和解签密不公平等问题,分别提出具有解签密公平性的基于身份的多接收者匿名签密机制;文献[11]在保持文献[4]高效性的基础上,针对其存在的安全缺陷,提出一种新的基于身份的多接收者签密机制.除此之外,还有一些相类似的多接收者签密机制[12-17]相继被提出.

分析现有的多接收者签密机制[3-17],发现存在下述不足:

(1)匿名性弱

机制[3-7,13-14,17]的密文中均包含接收者的身份列表或密文标记列表,导致接收者隐私信息的泄露,因此在上述机制中接收者不具备匿名性.

(2)无法满足多消息发送需求

机制[3-16]仅将同一消息进行签密操作后发送给所有的接收者,若在一次操作中需向多个接收者发送不同的多个消息时,传统机制将无法实现,即上述机制无法满足发送者的多消息发送需求,其中文献[8]在现有基础上,可在不增加额外计算的前提下扩展为多消息签密机制.

(3)存在密钥托管问题

机制[4-5,8-12,14-15,17]以基于身份的密码系统为基础构造,密钥生成中心具有伪造任意用户的合法密文或替代用户进行解密的能力.

(4)计算效率低

机制[3-17]中的签密或解签密算法中使用了双线性映射或指数运算,导致计算效率较低.

综上所述,研究不使用双线性映射的无证书多接收者多消息签密机制已成为当前签密研究领域的热点问题.虽然基于CL-PKC机制[6-7,13]和多变量公钥密码体制[16]提出了相应的无证书多接收者签密机制,但是文献[6]的机制存在安全性缺陷,并且文献[7,13,16]中的机制无法满足发送者的多消息发送需求;此后,文献[17]首次提出一个多接收者多消息签密机制,但该机制存在密钥托管的不足,并且接收者不具有匿名性;鉴于传统机制所存在的上述不足,本文提出不使用双线性映射的无证书多接收者多消息签密机制,在增强用户匿名性,满足发送者多消息发送需求的同时,由于签密和解签密算法中未使用双线性映射和指数运算,本文机制具有更高的计算效率.

3 基础知识

3.1 相关困难性问题及假设

定义 1. 离散对数问题(DL).设群G是阶为素数q的循环群,P是群G的一个生成元;对于任意且未知的$a\in Z_q^*$,已知P,$aP\in G$,DL问题的目标是计算a.对于任意的概率多项式时间敌手$\mathcal{A}$成功解决DL问题的优势$Adv_{\mathcal{A}}^{\mathrm{DL}}(k)$是可忽略的.

$$Adv_{\mathcal{A}}^{\mathrm{DL}}(k)=\Pr[\mathcal{A}(P,aP)=a\,|\,a\in Z_q^*],$$

其中,概率来源于a在Z_q^*上的随机选取及算法$\mathcal{A}$的随机选择.

定义 2. 判定性Diffie-Hellman问题(DDH).设群G是阶为素数q的循环群,P是群G的一个生成元;对于任意且未知的$a,b\in Z_q^*$,已知元组$T_1=(P,aP,bP,abP)$和$T_2=(P,aP,bP,\tau\in G)$,DDH问题的目标为判断$\tau=abP$.对于任意的概率多项式时间敌手$\mathcal{A}$成功解决DL问题的优势$Adv_{\mathcal{A}}^{\mathrm{DL}}(k)$是可忽略的.

$$Adv_{\mathcal{A}}^{\mathrm{DDH}}(k)=|\Pr[1\leftarrow\mathcal{A}(T_1)]-\Pr[1\leftarrow\mathcal{A}(T_2)]|,$$

其中,概率来源于a,b在Z_q^*上的随机选取及算法$\mathcal{A}$的随机选择.

3.2 安全模型

参照文献[6-7,13]所定义的无证书多接收者签密的安全模型,本文无证书多接收者多消息签密机制将面临$\mathcal{A}_{\mathrm{I}}$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,但其具有替换合法用户公钥的能力.本文中$\mathcal{A}_{\mathrm{I}}^i(i=1,2)$为$\mathcal{A}_{\mathrm{I}}$类敌手,其中$\mathcal{A}_{\mathrm{I}}^1$是攻击保密性的敌手,$\mathcal{A}_{\mathrm{I}}^2$是攻击不可伪造性的敌手.

$\mathcal{A}_{\mathrm{II}}$:此类攻击者可掌握系统的主密钥,但其不具有替换合法用户公钥的能力.本文中$\mathcal{A}_{\mathrm{II}}^i(i=1,2)$为$\mathcal{A}_{\mathrm{II}}$类敌手,其中$\mathcal{A}_{\mathrm{II}}^1$是攻击保密性的敌手,$\mathcal{A}_{\mathrm{II}}^2$是攻击不可伪造性的敌手.

① Selvi S S D, Vivek S S, Rangan C P. A note on the certificateless multi-receiver signcryption scheme. http://eprint.iacr.org/2009/308.pdf

$\mathcal{A}_{\mathrm{I}}$和$\mathcal{A}_{\mathrm{II}}$两类敌手适应性选择密文攻击下的保密性和适应性选择消息攻击下的不可伪造性的具体定义及相关游戏详见文献[6-7,13]，篇幅所限，本文不再赘述.

4　本文机制

4.1　系统参数的建立(Setup)

PKG 执行下述操作：

(1) 加法循环群 G 的阶为素数 $q(q>2^k, k$ 为安全参数)，P 是群 G 的一个生成元；

(2) 分别定义抗碰撞的密码学单向哈希函数：

$H_1:\{0,1\}^{L_1}\times G\times G\rightarrow Z_q^*$,

$H_2:\{0,1\}^{L_1}\times\{0,1\}^{L_1}\times\{0,1\}^{L_2}\times G\rightarrow Z_q^*$,

$H_3:\{0,1\}^{L_1}\times G\rightarrow\{0,1\}^{L_2}\times G$,

其中 L_1 为用户身份标识的长度，L_2 为明文消息的长度；

(3) 定义单向索引函数 $f_{Index}:Z_q^*\times\{0,1\}^{L_1}\rightarrow Z_q^*$，在 $f_{Index}(n,ID)$ 中 $n(n\in Z_q^*)$ 为索引区间(即表示可输入的身份标识数量)，$ID\in\{ID_1,ID_2,\cdots,ID_n\}$ 为用户身份标识，则索引函数 $f_{Index}(n,ID)$ 的输出为 $\{1,2,\cdots,n\}$，即 $f_{Index}(n,ID)$ 的功能是将 n 个身份 $\{ID_1,ID_2,\cdots,ID_n\}$ 均匀映射到 $\{1,2,\cdots,n\}$ 上，即索引函数 f_{Index} 的作用仅仅是方便接收者从密文集合中准确定位自己的密文；

(4) 定义$\oplus$为字符串 $\{0,1\}^{L_2}$ 上的异或运算，且具有 $\forall M,N\in\{0,1\}^{L_2}$，满足 $M\oplus N\oplus M=N$；

(5) 选择系统主密钥 $S\in Z_q^*$，计算系统公钥为 $P_{Pub}=SP$，则系统公开参数为 $Params=\{G,q,P,P_{Pub},H_1,H_2,H_3,f_{Index}\}$，秘密保存主密钥 S.

4.2　用户密钥生成(KeyGen)

用户 ID_i 的密钥生成过程包含下述步骤：

(1) ID_i 随机选取秘密值 $x_{ID_i}\in Z_q^*$，计算公开参数 $X_{ID_i}=x_{ID_i}P$；

(2) 给定用户身份 ID_i 和公开参数 X_{ID_i}，PKG 随机选取秘密数 $r_{ID_i}\in Z_q^*$，计算 $Y_{ID_i}=r_{ID_i}P$ 和 $y_{ID_i}=r_{ID_i}+SH_1(ID_i,X_{ID_i},Y_{ID_i})$，通过安全信道将 y_{ID_i} 和 Y_{ID_i} 返回给用户 ID_i，y_{ID_i} 作为 ID_i 的部分私钥，Y_{ID_i} 作为 ID_i 的部分公钥；

(3) ID_i 通过 $y_{ID_i}P=Y_{ID_i}+P_{Pub}H_1(ID_i,X_{ID_i},Y_{ID_i})$ 验证 PKG 为其生成的部分私钥 y_{ID_i} 和部分公钥 Y_{ID_i} 的合法性；若验证通过，则 ID_i 的公私钥对为 $\langle PK_{ID_i}=(X_{ID_i},Y_{ID_i}),SK_{ID_i}=(x_{ID_i},y_{ID_i})\rangle$.

4.3　多消息签密(MSign)

多消息签密算法的输入为待签密消息集合 $M=\{m_1,m_2,\cdots,m_n\}$、发送者身份 ID_S 和接收者身份 $ID_R=\{ID_{R_1},ID_{R_2},\cdots,ID_{R_n}\}$. 发送者 ID_S 的具体操作步骤如下：

(1) 选取随机秘密数 $u_{ID_S}\in Z_q^*$，计算 $U_{ID_S}=u_{ID_S}P$，通过计算将 u_{ID_i} 安全擦除；

(2) 对每一位接收者 $R_i(i=\{1,2,\cdots,n\})$，发送者 ID_S 首先计算索引 $J_{R_i}=f_{Index}(n,ID_{R_i})$，则 $J_{R_i}\in[1,n]$；然后进行下述操作：

① 计算 $(K_{J_{R_i}}^1,K_{J_{R_i}}^2)=H_3(ID_{R_i},u_{ID_S}(X_{R_i}+Y_{R_i}+P_{Pub}h_{R_i}))$，其中 $K_{J_{R_i}}^1\in\{0,1\}^{L_2}$，$K_{J_{R_i}}^2\in G$ 和 $h_{R_i}=H_1(ID_{R_i},X_{R_i},Y_{R_i})$；

② 计算 $c_{J_{R_i}}^1=m_{J_{R_i}}\oplus K_{J_{R_i}}^1$；

③ 计算 $d_{J_{R_i}}=H_2(ID_S,ID_{R_i},c_{J_{R_i}}^1,U_{ID_S})$；

④ 计算 $T_{J_{R_i}}=H_2(ID_S,ID_{R_i},c_{J_{R_i}}^1,Q_{ID_S})$；

⑤ 计算 $V_{J_{R_i}}=d_{J_{R_i}}(x_{ID_S}+y_{ID_S})+u_{ID_S}T_{J_{R_i}}$，其中 $Q_{ID_S}=x_{ID_S}Y_{ID_S}$；

⑥ 计算 $c_{J_{R_i}}^2=V_{J_{R_i}}P+K_{J_{R_i}}^2$，则有 $C_{J_{R_i}}=(c_{J_{R_i}}^1,c_{J_{R_i}}^2)$.

(3) 计算 $\pi_{ID_S}=u_{ID_S}(x_{ID_S}+y_{ID_S})^{-1}$，将密文 $\sigma=\{\pi_{ID_S},Q_{ID_S},C\}$(其中 $C=C_1,C_2,\cdots,C_n$)发给每一位接收者 $R_i(i=\{1,2,\cdots,n\})$.

4.4　解签密(UnSign)

接收者 $R_i(1\leq i\leq n)$ 收到密文 $\sigma=\{U_{ID_S},Q_{ID_S},C\}$ 后，计算 $J_{R_i}=f_{Index}(n,ID_{R_i})$，则 $J_{R_i}\in[1,n]$，根据索引 J_{R_i} 从集合 C 中准确定位相应的密文 $C_{J_{R_i}}$. 具体的解密及签名合法性验证过程如下：

① 计算 $U'_{ID_S}=\pi_{ID_S}(X_{ID_S}+Y_{ID_S}+P_{Pub}h_{ID_S})$；

② 计算 $(K'^1_{J_{R_i}},K'^2_{J_{R_i}})=H_3(ID_{R_i},(x_{R_i}+y_{R_i})U'_{ID_S})$；

③ 计算 $d'_{J_{R_i}}=H_2(ID_S,ID_{R_i},c_{J_{R_i}}^1,U'_{ID_S})$；

④ 计算 $T'_{J_{R_i}}=H_2(ID_S,ID_{R_i},c_{J_{R_i}}^1,Q_{ID_S})$；

验证等式(1)是否成立，若成立，则计算并输出 $m_{J_{R_i}}=c_{J_{R_i}}^1\oplus K'^1_{J_{R_i}}$，否则返回$\perp$.

$$c_{J_{R_i}}^2-K'^2_{J_{R_i}}=d'_{J_{R_i}}(X_{ID_S}+Y_{ID_S}+P_{Pub}h_{ID_S})+T'_{J_{R_i}}U'_{ID_S}\tag{1}$$

4.5　正确性

定理 1.　接收者 $R_i(1\leq i\leq n)$ 收到的消息 $m_{J_{R_i}}$ 是合法的通信消息.

证明.　(1) 解密的正确性

因为 $U'_{ID_S}=\pi_{ID_S}(X_{ID_S}+Y_{ID_S}+P_{Pub}h_{ID_S})$
$=u_{ID_S}(x_{ID_S}+y_{ID_S})^{-1}(x_{ID_S}+r_{ID_S}+Sh_{ID_S})P$
$=U_{ID_S}$,

其中 $h_{ID_S}=H_1(ID_S,X_{ID_S},Y_{ID_S})$.

$(K'^1_{J_{R_i}},K'^2_{J_{R_i}})=H_3(ID_{R_i},(x_{R_i}+y_{R_i})u_{ID_S}P)$
$=H_3(ID_{R_i},u_{ID_S}(X_{R_i}+Y_{R_i}+P_{Pub}h_{R_i}))$
$=(K^1_{J_{R_i}},K^2_{J_{R_i}})$,

其中 $h_{R_i}=H_1(ID_{R_i},X_{R_i},Y_{R_i})$. 则有

$$m_{J_{R_i}}=c^1_{J_{R_i}}\oplus K'^1_{J_{R_i}}=m_{J_{R_i}}\oplus K^1_{J_{R_i}}\oplus K'^1_{J_{R_i}}.$$

(2) 签名验证的正确性

因为 $T'_{J_{R_i}}=H_2(ID_S,ID_{R_i},c^1_{J_{R_i}},Q_{ID_S})=T_{J_{R_i}}$ 和 $d'_{J_{R_i}}=H_2(ID_S,ID_{R_i},c^1_{J_{R_i}},U'_{ID_S})=d_{J_{R_i}}$; 则有等式 $c^2_{J_{R_i}}-K'^2_{J_{R_i}}=V_{J_{R_i}}P+K^2_{J_{R_i}}-K'^2_{J_{R_i}}=(d_{J_{R_i}}(x_{ID_S}+y_{ID_S})+u_{ID_S}T_{J_{R_i}})P=d'_{J_{R_i}}(X_{ID_S}+Y_{ID_S}+P_{Pub}h_{ID_S})+T'_{J_{R_i}}U'_{ID_S}$ 成立.

综上所述,若等式(1)成立,则 $R_i(1\le i\le n)$ 收到的消息 $m_{J_{R_i}}$ 是发送者 ID_S 的合法通信消息. 证毕

5 安全性证明

5.1 保密性

定理 2($\mathcal{A}_\mathrm{I}$类敌手的保密性). 在随机谕言机模型下,若存在$\mathcal{A}_\mathrm{I}$类敌手$\mathcal{A}^1_\mathrm{I}$能以不可忽略的优势 ε 赢得相关游戏($\mathcal{A}^1_\mathrm{I}$最多进行 q_{SK} 次私钥生成询问,q_S 次签密询问和 q_U 次解签密询问),则存在区分者$\mathcal{B}$能以优势 $Adv^{\mathrm{DDH}}_{\mathcal{B},\mathcal{A}^1_\mathrm{I}}(k)>\left(1-\frac{q_{SK}}{2^k}\right)\left(\varepsilon-\frac{q_U}{2^k}\right)\frac{1}{\mathrm{e}(q_S+1)}$ 解决 DDH 困难性问题(其中 e 为自然对数底数).

证明. 对于输入元组 $T_1=(P,aP,bP,abP)$ 和 $T_2=(P,aP,bP,\tau)$,区分者$\mathcal{B}$的目标为判断 $\tau=abP$ 是否成立. $\mathcal{B}$运行 *Setup* 算法生成相应的参数 *Params*,并发送 *Params* 给$\mathcal{A}^1_\mathrm{I}$;同时维护列表 L_1,L_2,L_{SK},L_{PK},L_S和 L_U分别用于跟踪对谕言机 H_1和 H_2的询问及记录私钥提取、公钥提取、签密和解签密询问,开始时各列表均为空.

H_2询问. 当收到询问 $H_2(ID_i,ID_j,c_i,U_i(Q_i))$,若存在$\langle ID_i,ID_j,c_i,U_i(Q_i),h_2\rangle\in L_2$,则$\mathcal{B}$返回相应的 h_2给$\mathcal{A}^1_\mathrm{I}$;否则,$\mathcal{B}$选取满足条件$\langle *,*,*,*,h_2\rangle\notin L_2$(避免哈希函数碰撞的产生)的随机数 $h_2\in Z^*_q$,存储$\langle ID_i,ID_j,c_i,U_i(Q_i),h_2\rangle$到$L_2$中,并返回$h_2$给$\mathcal{A}^1_\mathrm{I}$.

公钥生成询问. 当收到$\mathcal{A}^1_\mathrm{I}$关于 ID_i的公钥生成询问时,$\mathcal{B}$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 $PK_i=\langle X_i,Y_i\rangle$给$\mathcal{A}^1_\mathrm{I}$;

(2) 否则,$\mathcal{B}$选取随机数$c_i\leftarrow\{0,1\}$,且$\Pr[c_i=1]=\delta=\frac{1}{q_S+1}$;若 $c_i=0$,$\mathcal{B}$随机选取$x_i,y_i,h_1\in Z^*_q$,计算 $X_i=x_iP$ 和 $Y_i=y_iP-P_{Pub}h_1$,$\mathcal{B}$添加$\langle ID_i,X_i,Y_i,c_i\rangle$到 L_{PK}中,添加$\langle ID_i,x_i,y_i\rangle$到 L_{SK}中,添加$\langle ID_i,X_i,Y_i,h_1\rangle$到 L_1中,并返回相应的 $PK_i=\langle X_i,Y_i\rangle$给$\mathcal{A}^1_\mathrm{I}$;若 $c_i=1$,令 $X_i=aP$ 和 $Y_i=bP$,添加$\langle ID_i,X_i,Y_i,c_i\rangle$到 L_{PK} 中,并返回相应的 $PK_i=\langle X_i,Y_i\rangle$给$\mathcal{A}^1_\mathrm{I}$,随机选取$h_1\in Z^*_q$,添加$\langle ID_i,X_i,Y_i,h_1\rangle$到 L_1中.

H_1询问. 当收到询问 $H_1(ID_i,X_i,Y_i)$时,$\mathcal{B}$以 ID_i为索引检索 L_1获得元组$\langle ID_i,X_i,Y_i,h_1\rangle$,并返回 h_1给$\mathcal{A}^1_\mathrm{I}$. 特别的,对 ID_i进行 H_1询问之前,已完成公钥生成询问,获知相应的公钥 $PK_i=\langle X_i,Y_i\rangle$.

公钥替换询问. 敌手$\mathcal{A}^1_\mathrm{I}$能够随机产生 $PK'_i=\langle X'_i,Y'_i\rangle$ 替换任意用户 ID_i 的合法公钥 $PK_i=\langle X_i,Y_i\rangle$.

私钥生成询问. 当收到$\mathcal{A}^1_\mathrm{I}$关于 ID_i的私钥生成询问时,区分者$\mathcal{B}$进行下述操作:

(1) 若存在$\langle ID_i,x_i,y_i\rangle\in L_{SK}$,则返回相应的 $SK_i=\langle x_i,y_i\rangle$给$\mathcal{A}^1_\mathrm{I}$;

(2) 否则,$\mathcal{B}$对 ID_i进行公钥生成询问,获得相应的元组$\langle ID_i,X_i,Y_i,c_i\rangle$,若 $c_i=0$,则在公钥生成询问中已生成了相应的私钥,$\mathcal{B}$查询 L_{SK}并返回相应的 $SK_i=\langle x_i,y_i\rangle$给$\mathcal{A}^1_\mathrm{I}$;否则,无能力回答 ID_i所对应的私钥,$\mathcal{B}$停止模拟,并退出.

签密询问. 当收到敌手$\mathcal{A}^1_\mathrm{I}$关于 ID_S和 $ID_R=\{ID_{R_1},ID_{R_2},\cdots,ID_{R_n}\}$及 $M=\{m_1,m_2,\cdots,m_n\}$的多消息签密询问时,首先,$\mathcal{B}$查询列表 L_{PK}获得身份 ID_S相对应的元组$\langle ID_S,X_{ID_S},Y_{ID_S},c_{ID_S}\rangle$;然后,$\mathcal{B}$进行下述操作:

(1) 如果 $c_{ID_S}=0$,$\mathcal{B}$对 ID_S进行私钥生成询问,对 $ID_{R_j}(j=1,\cdots,n)$进行公钥生成询问;运行算法 $MSign(M,ID_{ID_S},SK_{ID_S},ID_R,PK=\{PK_{R_1},\cdots,PK_{R_n}\})$,并返回密文$\sigma$给$\mathcal{A}^1_\mathrm{I}$;

(2) 如果 $c_{ID_S}=1$,$\mathcal{B}$停止模拟,并退出.

解签密询问. 当收到$\mathcal{A}^1_\mathrm{I}$关于ID_S,ID_{R_j}及 $C_{J_{R_j}}=(c^1_{J_{R_i}},c^2_{J_{R_i}})$的解签密询问时,首先,$\mathcal{B}$针对身份 ID_S查询列表 L_{PK};然后$\mathcal{B}$进行下述操作:

(1) 若$\langle ID_S,X_{ID_S},Y_{ID_S},c_{ID_S}\rangle\in L_{PK}$且 $c_{ID_S}=0$,则$\mathcal{B}$运行 $UnSign(ID_{ID_S},PK_{ID_S},ID_{R_j},SK_{ID_{R_j}},C_{J_{R_j}})$,

并返回相应的结果给$\mathcal{A}_{\mathrm{I}}^1$；

(2) 若$\langle ID_S, X_{ID_S}, Y_{ID_S}, c_{ID_S}\rangle \in L_{PK}$且$c_{ID_S}=1$，则$\mathcal{B}$按下述步骤进行解签密：

以ID_{R_j}和ID_S为索引检索L_{SK}，L_1和L_2获得相应的元组$\langle ID_{R_j}, x_{R_j}, y_{R_j}\rangle$，$\langle ID_S, X_{ID_S}, Y_{ID_S}, h_1\rangle$，$\langle ID_S, ID_{R_j}, c_{J_{R_j}}, U_{ID_S}, h_2^U\rangle$和$\langle ID_S, ID_{R_j}, c_{J_{R_j}}, Q_{ID_S}, h_2^Q\rangle$，计算$(K'^1_{J_{R_i}}, K'^2_{J_{R_i}}) = H_3(ID_{R_i}, (x_{R_i}+y_{R_i})U_{ID_S})$，若等式$c^2_{J_{R_i}} - K'^2_{J_{R_i}} = h_2^U(X_{ID_S}+Y_{ID_S}+P_{Pub}h_1) + h_2^Q U_{ID_S}$成立，则$\mathcal{B}$返回$m_{J_{R_j}} = c^1_{J_{R_i}} \oplus K'^1_{J_{R_i}}$给$\mathcal{A}_{\mathrm{I}}^1$；否则，$\mathcal{B}$停止模拟，拒绝密文；

(3) 若L_{PK}中不存在相应的元组，即公钥被替换，$\mathcal{B}$按下述步骤进行解签密：

以ID_{R_j}和ID_S为索引检索L_{SK}，L_1和L_2获得相应的元组$\langle ID_{R_j}, x_{R_j}, y_{R_j}\rangle$，$\langle ID_S, X'_{ID_S}, Y'_{ID_S}, h_1\rangle$，$\langle ID_S, ID_{R_j}, c_{J_{R_j}}, U_{ID_S}, h_2^U\rangle$和$\langle ID_S, ID_{R_j}, c_{J_{R_j}}, Q_{ID_S}, h_2^Q\rangle$，计算$(K'^1_{J_{R_i}}, K'^2_{J_{R_i}}) = H_3(ID_{R_i}, (x_{R_i}+y_{R_i})U_{ID_S})$，若等式$c^2_{J_{R_i}} - K'^2_{J_{R_i}} = h_2^U(X'_{ID_S}+Y'_{ID_S}+P_{Pub}h_1) + h_2^Q U_{ID_S}$成立，则$\mathcal{B}$返回$m_{J_{R_j}} = c^1_{J_{R_i}} \oplus K'^1_{J_{R_i}}$给$\mathcal{A}_{\mathrm{I}}^1$；否则，$\mathcal{B}$停止模拟，拒绝密文.

挑战. 在第一阶段的结尾，$\mathcal{A}_{\mathrm{I}}^1$生成两组挑战明文$M_0=\{m_0^1, m_0^2, \cdots, m_0^n\}$和$M_1=\{m_1^1, m_1^2, \cdots, m_1^n\}$(其中$|m_0^i| = |m_1^i|(i=1,\cdots,n)$)及挑战身份$ID_S$和$ID_R=\{ID_{R_1}, ID_{R_2}, \cdots, ID_{R_u}\}$，$\mathcal{B}$以$ID_S$为索引检索$L_{PK}$获得相应的元组$\langle ID_S, X_{ID_S}, Y_{ID_S}, c_{ID_S}\rangle$，然后，$\mathcal{B}$进行下述操作：

(1) 若$c_{ID_S}=0$，$\mathcal{B}$失败，并停止模拟；

(2) 若$c_{ID_S}=1$，$\mathcal{B}$随机选取$b \leftarrow \{0,1\}$，并按下述步骤生成$M_b=\{m_b^1, m_b^2, \cdots, m_b^n\}$的签密密文：

① 随机选取秘密数$u_{ID_S} \in Z_q^*$，计算$U_{ID_S}=u_{ID_S}P$；

② 对每一位接收者$R_i(i=\{1,2,\cdots,n\})$，首先计算索引$J_{R_i}=f_{Index}(n, ID_{R_i})$，则$J_{R_i}\in[1,n]$；然后计算$(K^1_{J_{R_i}}, K^2_{J_{R_i}}) = H_3(ID_{R_i}, u_{ID_S}(X_{R_i}+Y_{R_i}+P_{Pub}h_{R_i}))$(其中$h_{R_i}=H_1(ID_{R_i}, X_{R_i}, Y_{R_i})$)，$c^1_{J_{R_i},b} = m_b^{J_{R_i}} \oplus K^1_{J_{R_i}}$和$c^{2*}_{J_{R_i},b} = d_{J_{R_i}}(X_{ID_S}+Y_{ID_S}+P_{Pub}h_{ID_S}) + T_{J_{R_i}}U_{ID_S} + K^2_{J_{R_i}}$(其中$d_{J_{R_i}} = H_2(ID_S, ID_{R_i}, c^1_{J_{R_i},b}, U_{ID_S})$，$T_{J_{R_i}} = H_2(ID_S, ID_{R_i}, c^1_{J_{R_i},b}, \tau)$)；

③ 选取满足$U_{ID_S}=\pi_{ID_S}(X_{ID_S}+Y_{ID_S}+P_{Pub}h_{ID_S})$的随机数$\pi_{ID_S}\in Z_q^*$，并返回$\sigma=\{\pi_{ID_S}, \tau, C\}$给$\mathcal{A}_{\mathrm{I}}^1$.

在模拟的最后，敌手$\mathcal{A}_{\mathrm{I}}^1$输出猜测$b'$，如果$b=b'$，那么$\mathcal{B}$返回1作为相应的结果，即$\sigma$是关于$M_b=\{m_b^1, m_b^2, \cdots, m_b^n\}$的有效签密密文；否则，若$b\neq b'$，那么$\mathcal{B}$返回0.

区分者$\mathcal{B}$为$\mathcal{A}_{\mathrm{I}}^1$模拟了真实的攻击环境，若$\mathcal{B}$在模拟过程中未终止，同时$\mathcal{A}_{\mathrm{I}}^1$以不可忽略的优势$\varepsilon$攻破本文无证书多接收者多消息签密机制，并且$\mathcal{B}$的输出为1，则$\mathcal{B}$成功解决DDH困难性问题.

现在评估区分者$\mathcal{B}$成功的概率，询问阶段当敌手$\mathcal{A}_{\mathrm{I}}^1$对$ID_S$进行了私钥生成询问，则$\mathcal{B}$会终止. 令事件$\mathcal{E}_1$表示$\mathcal{A}_{\mathrm{I}}^1$对$ID_S$未进行私钥生成询问；事件$\mathcal{E}_2$表示签密询问中$\mathcal{B}$未终止；则$\Pr[\mathcal{E}_1]=1-\frac{q_{SK}}{2^k}$，$\Pr[\mathcal{E}_2]=(1-\delta)^{q_S}$，即询问阶段$\mathcal{B}$不终止的概率为$\left(1-\frac{q_{SK}}{2^k}\right)(1-\delta)^{q_S}$；挑战阶段$\mathcal{B}$不终止的概率为$\delta$.

在整个模拟过程中区分者$\mathcal{B}$不终止的概率为$\left(1-\frac{q_{SK}}{2^k}\right)(1-\delta)^{q_S}\delta$. 由于$\delta=\frac{1}{q_S+1}$，则当$q_S$足够大时，$(1-\delta)^{q_S}=\left(\frac{q_S}{q_S+1}\right)^{q_S}$趋向于$\mathrm{e}^{-1}$. 因此，在模拟过程中$\mathcal{B}$不终止的概率至少为$\left(1-\frac{q_{SK}}{2^k}\right)\frac{1}{\mathrm{e}(q_S+1)}$；同时$\mathcal{B}$拒绝一个有效密文的概率不超过$\frac{q_U}{2^k}$.

因为$P_1=\Pr[b=b'|(T_1,\sigma)]=\frac{1}{2}+\varepsilon-\frac{q_U}{2^k}$，其中$\sigma=MSign(M_b, ID_S, SK_{ID_S}, ID_R, PK_R)$；

$P_0=\Pr[b'=i|(T_2,\sigma^*)]=\frac{1}{2}$，其中，$i=0,1$.

则区分者$\mathcal{B}$成功区分元组$T_1=(P, aP, bP, abP)$和$T_2=(P, aP, bP, \tau)$(其中$a,b\in Z_q^*, \tau\in G$)的优势为

$$\begin{aligned} Adv(\mathcal{B}) &= |\Pr[\mathcal{B}(T_1)=1]-\Pr[\mathcal{B}(T_2)=1]| \\ &> \left(1-\frac{q_{SK}}{2^k}\right)\frac{1}{\mathrm{e}(q_S+1)}|P_1-P_0| \\ &= \left(1-\frac{q_{SK}}{2^k}\right)\left(\varepsilon-\frac{q_U}{2^k}\right)\frac{1}{\mathrm{e}(q_S+1)}. \end{aligned}$$

若$\mathcal{A}_{\mathrm{I}}^1$以不可忽略的优势$\varepsilon$攻破本文机制的保密性，且模拟过程中区分者$\mathcal{B}$未终止，则$\mathcal{B}$以优势$Adv^{\mathrm{DDH}}_{\mathcal{B},\mathcal{A}_{\mathrm{I}}^1}(k) > \left(1-\frac{q_{SK}}{2^k}\right)\left(\varepsilon-\frac{q_U}{2^k}\right)\frac{1}{\mathrm{e}(q_S+1)}$成功解决DDH困难性问题.　　证毕.

定理3($\mathcal{A}_{\mathrm{II}}$类敌手的保密性).　在随机谕言机模型下，若存在$\mathcal{A}_{\mathrm{II}}$类敌手$\mathcal{A}_{\mathrm{II}}^1$以不可忽略的优势$\varepsilon$赢得相关游戏($\mathcal{A}_{\mathrm{II}}^1$最多进行$q_{SK}$次私钥生成询问，$q_S$次签密询问，$q_U$次解签密询问)，则存在区分者$\mathcal{B}$能以

优势 $Adv^{\mathrm{DDH}}_{\mathcal{B},\mathcal{A}^1_{\mathrm{II}}}(k)>\left(1-\frac{q_{SK}}{2^k}\right)\left(\varepsilon-\frac{q_U}{2^k}\right)\frac{1}{\mathrm{e}(q_S+1)}$ 成功解决 DDH 困难性问题(其中 e 为自然对数底数).

证明过程与定理 2 相类似,本文不再赘述.

5.2 不可伪造性证明

定理 4($\mathcal{A}_{\mathrm{I}}$类敌手的不可伪造性). 在随机谕言机模型下,若存在$\mathcal{A}_{\mathrm{I}}$类敌手$\mathcal{A}^2_{\mathrm{I}}$以不可忽略的优势 ε 赢得相关游戏($\mathcal{A}^2_{\mathrm{I}}$最多进行 q_S次签名询问),则存在算法 $\mathcal{B}$以优势 $Adv^{\mathrm{DL}}_{\mathcal{B},\mathcal{A}^2_{\mathrm{I}}}(k)\geq\frac{\varepsilon}{\mathrm{e}(q_S+1)}$ 成功解决 DL 困难性问题(其中 e 为自然对数底数).

证明. 对于输入元组(P,aP),算法 $\mathcal{B}$的目标为计算 a. $\mathcal{B}$运行 *Setup* 算法生成相应的系统参数 *Params*,并发送 *Params* 给$\mathcal{A}^2_{\mathrm{I}}$,令 $P_{Pub}=aP$;同时维护列表 L_1,L_2,L_{SK},L_{PK},L_S,L_U分别用于跟踪对谕言机 H_1和 H_2的询问及记录私钥提取、公钥提取、签名和签名验证询问,开始时各列表均为空.

询问. 敌手$\mathcal{A}^2_{\mathrm{I}}$执行定理 2 中对谕言机 H_1和 H_2的询问和公钥替换询问.

公钥生成询问. 当收到$\mathcal{A}^2_{\mathrm{I}}$关于 ID_i的公钥生成询问时,算法$\mathcal{B}$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 $PK_i=\langle X_i,Y_i\rangle$给$\mathcal{A}^2_{\mathrm{I}}$;

(2) 否则,$\mathcal{B}$首先随机选取数 $c_i\leftarrow\{0,1\}$,且 $\Pr[c_i=1]=\delta=\frac{1}{q_S+1}$;如果 $c_i=0$,$\mathcal{B}$随机选取 x_i,y_i,$h_1\in Z_q^*$,计算 $X_i=x_iP$ 和 $Y_i=y_iP-P_{Pub}h_1$,$\mathcal{B}$添加$\langle ID_i,X_i,Y_i,c_i\rangle$到 L_{PK}中,添加$\langle ID_i,x_i,y_i\rangle$到 L_{SK}中,添加$\langle ID_i,X_i,Y_i,h_1\rangle$到 L_1中,并返回相应的 $PK_i=\langle X_i,Y_i\rangle$给$\mathcal{A}^2_{\mathrm{I}}$;如果 $c_i=1$,令 $X_i=d_1P$和 $Y_i=d_2P$(d_1和 d_2为$\mathcal{B}$已知的参数),选取满足条件 $Y_i=y_iP-P_{Pub}h_1$,$\langle *,*,y_i\rangle\notin L_{SK}$和$\langle *,*,*,h_1\rangle\notin L_1$的随机数 $y_i,h_1\in Z_q^*$,添加$\langle ID_i,X_i,Y_i,c_i\rangle$到 L_{PK}中,添加$\langle ID_i,d_1,y_i\rangle$到 L_{SK}中,添加$\langle ID_i,X_i,Y_i,h_1\rangle$到 L_1中,并返回相应的 $PK_i=\langle X_i,Y_i\rangle$给$\mathcal{A}^2_{\mathrm{I}}$.

私钥生成询问. 当收到$\mathcal{A}^2_{\mathrm{I}}$关于 ID_i的私钥生成询问时,算法$\mathcal{B}$进行下述操作:

(1) 若存在$\langle ID_i,x_i,y_i\rangle\in L_{SK}$,则返回相应的 $SK_i=\langle x_i,y_i\rangle$给$\mathcal{A}^2_{\mathrm{I}}$;

(2) 否则,$\mathcal{B}$对 ID_i进行公钥生成询问,在公钥生成询问中已生成了相应的私钥,$\mathcal{B}$查询 L_{SK}并返回相应的 $SK_i=\langle x_i,y_i\rangle$给$\mathcal{A}^2_{\mathrm{I}}$.

签名询问. 当收到敌手$\mathcal{A}^2_{\mathrm{I}}$关于 ID_S和 $ID_R=\{ID_{R_1},ID_{R_2},\cdots,ID_{R_n}\}$及 $M=\{m_1,m_2,\cdots,m_n\}$的签名询问时,$\mathcal{B}$查询 L_{PK}获得身份 ID_S相对应的元组$\langle ID_S,X_{ID_S},Y_{ID_S},c_{ID_S}\rangle$后进行下述操作:

(1) 如果 $c_{ID_S}=0$,$\mathcal{B}$对 ID_S进行私钥生成询问,对 $ID_{R_j}(j=1,\cdots,n)$进行公钥生成询问;运行算法 $MSign(M,ID_{ID_S},SK_{ID_S},ID_R,PK=\{PK_{R_1},\cdots,PK_{R_n}\})$,并返回签名 σ给$\mathcal{A}^2_{\mathrm{I}}$.

(2) 如果 $c_{ID_S}=1$,$\mathcal{B}$停止模拟,并退出.

签名验证询问. 当收到$\mathcal{A}^2_{\mathrm{I}}$关于 ID_S,ID_{R_j}及 $C_{J_{R_i}}=\langle U_{ID_S},Q_{ID_S},c^1_{J_{R_i}}=m_{J_{R_i}},c^2_{J_{R_i}}\rangle$的签名验证询问,$\mathcal{B}$针对 ID_S查询列表 L_{PK}后进行下述操作:

(1) 若$\langle ID_S,X_{ID_S},Y_{ID_S},c_{ID_S}\rangle\in L_{PK}$且 $c_{ID_S}=0$,则$\mathcal{B}$运行$UnSign(ID_{ID_S},PK_{ID_S},ID_{R_j},SK_{ID_{R_j}},C_{J_{R_j}})$(其中 $C_{J_{R_j}}=\langle c^1_{J_{R_i}},c^2_{J_{R_i}}\rangle$),并返回相应的结果给$\mathcal{A}^2_{\mathrm{I}}$.

(2) 若$\langle ID_S,X_{ID_S},Y_{ID_S},c_{ID_S}\rangle\in L_{PK}$且 $c_{ID_S}=1$,则$\mathcal{B}$按下述步骤进行解签密:

以 ID_{R_j}和 ID_S为索引检索 L_{SK},L_1和 L_2获得相应的元组$\langle ID_{R_j},x_{R_j},y_{R_j}\rangle$,$\langle ID_S,X_{ID_S},Y_{ID_S},h_1\rangle$,$\langle ID_S,ID_{R_j},c_{J_{R_j}},U_{ID_S},h_2^U\rangle$和$\langle ID_S,ID_{R_j},c_{J_{R_j}},Q_{ID_S},h_2^Q\rangle$,计算$(K'^1_{J_{R_i}},K'^2_{J_{R_i}})=H_3(ID_{R_i},(x_{R_i}+y_{R_i})U_{ID_S})$,若等式 $c^2_{J_{R_i}}-K'^2_{J_{R_i}}=h_2^U(X_{ID_S}+Y_{ID_S}+P_{Pub}h_1)+h_2^QU_{ID_S}$成立,则$\mathcal{B}$返回 $m_{J_{R_j}}$给$\mathcal{A}^2_{\mathrm{I}}$;否则,$\mathcal{B}$停止模拟.

(3) 若 L_{PK}中不存在相应的元组,即公钥被替换,$\mathcal{B}$按下述步骤进行解签密:

以 ID_{R_j}和 ID_S为索引检索 L_{SK},L_1和 L_2获得相应的元组$\langle ID_{R_j},x_{R_j},y_{R_j}\rangle$,$\langle ID_S,X'_{ID_S},Y'_{ID_S},h_1\rangle$,$\langle ID_S,ID_{R_j},c_{J_{R_j}},U_{ID_S},h_2^U\rangle$和$\langle ID_S,ID_{R_j},c_{J_{R_j}},Q_{ID_S},h_2^Q\rangle$,计算$(K'^1_{J_{R_i}},K'^2_{J_{R_i}})=H_3(ID_{R_i},(x_{R_i}+y_{R_i})U_{ID_S})$,若等式 $c^2_{J_{R_i}}-K'^2_{J_{R_i}}=h_2^U(X'_{ID_S}+Y'_{ID_S}+P_{Pub}h_1)+h_2^QU_{ID_S}$成立,则$\mathcal{B}$返回 $m_{J_{R_j}}$给$\mathcal{A}^2_{\mathrm{I}}$;否则,$\mathcal{B}$停止模拟.

伪造. 经过多项式有界次上述询问后,敌手$\mathcal{A}^2_{\mathrm{I}}$伪造 ID_S关于消息 $M=\{m_1,m_2,\cdots,m_n\}$和接收者 $ID_R=\{ID_{R_1},ID_{R_2},\cdots,ID_{R_n}\}$的伪造签名:

随机选取秘密数 $u_{ID_S}\in Z_q^*$,计算 $U^*_{ID_S}=u_{ID_S}P$;令 $c^{1*}_{J_{R_i},b}=m_{J_{R_i}}$,随机选取 $Q^*\in G$;对每一位接收者 $R_i(i=\{1,2,\cdots,n\})$,首先计算 $J_{R_i}=f_{Index}(n,ID_{R_i})$,则 $J_{R_i}\in[1,n]$;然后计算 $d_{J_{R_i}}=H_2(ID_S,ID_{R_i},c^{1*}_{J_{R_i},b},U^*_{ID_S})$、$T_{J_{R_i}}=H_2(ID_S,ID_{R_i},c^{1*}_{J_{R_i},b},Q^*)$;计算$(K^1_{J_{R_i}},K^2_{J_{R_i}})=H_3(ID_{R_i},U^*(x_{R_i}+y_{R_i}))$和 $c^{2*}_{J_{R_i},b}=d_{J_{R_i}}(X_{ID_S}+Y_{ID_S}+P_{Pub}h_1^{ID_S})+T_{J_{R_i}}U^*_{ID_S}+$

$K^2_{J_{R_i}}$；计算 $\pi^*_{ID_S}=u_{ID_S}(x_{ID_S}+y_{ID_S})^{-1}$，输出伪造签名 $\sigma^*=\{\pi^*_{ID_S},Q^*,C^*\}$.

若 $\mathcal{A}_{\mathrm{I}}^2$ 伪造签名成功，则 $\mathcal{B}$ 以 ID_S 为索引查询 L_{PK} 获得相应的元组 $\langle ID_S,X_S,Y_S,c_S\rangle$，若 $c_S=1$，$\mathcal{B}$ 输出 $a=(h_1^{ID_S}\pi^*_{ID_S})^{-1}(u_{ID_S}-\pi^*_{ID_S}(d_1+d_2))$ 作为 DL 困难性问题的解；否则，$c_S=0$，$\mathcal{B}$ 失败，并终止模拟，即 $\mathcal{B}$ 未解决 DL 困难性问题.

令事件 $\mathcal{E}_1$ 表示签名询问过程中 $\mathcal{B}$ 未终止，即 $\Pr[\mathcal{E}_1]=(1-\delta)^{q_S}$，则询问阶段 $\mathcal{B}$ 不终止的概率为 $(1-\delta)^{q_S}$，伪造阶段 $\mathcal{B}$ 不终止的概率为 δ.

模拟中 $\mathcal{B}$ 不终止的概率为 $(1-\delta)^{q_S}\delta$. 由于 $\delta=\frac{1}{q_S+1}$，则当 q_S 足够大时，$(1-\delta)^{q_S}=\left(\frac{q_S}{q_S+1}\right)^{q_S}$ 趋向于 e^{-1}. 因此，在模拟过程中 $\mathcal{B}$ 不终止的概率至少为 $\frac{1}{\mathrm{e}(q_S+1)}$.

若 $\mathcal{A}_{\mathrm{I}}^2$ 能以不可忽略的优势 ε 攻破本文机制的不可伪造性，且模拟过程中算法 $\mathcal{B}$ 未终止，则 $\mathcal{B}$ 以优势 $Adv^{\mathrm{CDH}}_{\mathcal{B},\mathcal{A}_{\mathrm{I}}^2}(k)\geq\frac{\varepsilon}{\mathrm{e}(q_S+1)}$ 解决 DL 困难问题. 证毕.

定理 5（$\mathcal{A}_{\mathrm{II}}$ 类敌手的不可伪造性）. 在随机谕言机模型下，若存在 $\mathcal{A}_{\mathrm{II}}$ 类敌手 $\mathcal{A}_{\mathrm{II}}^2$ 能以不可忽略的优势 ε 赢得相关游戏（$\mathcal{A}_{\mathrm{II}}^2$ 最多进行 q_S 次签名询问），则存在算法 $\mathcal{B}$ 能以优势 $Adv^{\mathrm{DL}}_{\mathcal{B},\mathcal{A}_{\mathrm{II}}^2}(k)\geq\frac{\varepsilon}{\mathrm{e}(q_S+1)}$ 成功解决 DL 困难问题（其中 e 为自然对数底数）.

证明过程与定理 4 相类似，本文不再赘述.

6　机制分析

（1）公开验证性

在本文机制中，需公开验证发送者身份时，发送者 R_i 发送 $C^*_{J_{R_i}}=\langle\pi_{ID_S},Q_{ID_S},\{c^1_{J_{R_i}},c^2_{J_{R_i}}-k^2_{J_{R_i}}\}\rangle$ 及身份 ID_S 和 ID_{R_i} 给任何的可信第三方；无需参与者的私有信息，只需计算 $d'_{J_{R_j}}=H_2(ID_S,ID_{R_j},c^1_{J_{R_i}},U_{ID_S})$ 和 $T'_{J_{R_j}}=H_3(ID_S,ID_{R_j},c^1_{J_{R_i}},Q_{ID_S})$；并验证等式 $c^2_{J_{R_i}}-k^2_{J_{R_i}}=d'_{J_{R_j}}(X_{ID_S}+Y_{ID_S}+P_{Pub}h_{ID_S})+T'_{J_{R_j}}U_{ID_S}$ 是否成立即可. 由于密文是不可伪造的，则当上述等式成立时，表示密文是由 ID_S 为 ID_{R_i} 生成的合法密文.

（2）不可否认性

由定理 4 和定理 5 可知，本文机制具有不可伪造性，即密文消息是不可伪造的；由公开验证性可知，任何第三方均可公开验证密文发送者的身份；若用户确实生成了签密密文，就不能进行否认.

（3）索引函数 f_{Index} 的安全性

由于攻击者无法获知接收者的具体身份，使得无法完成索引函数 f_{Index} 的计算；即使攻击者获知了接收者的身份，从密文集合中准确定位了该接收者的具体密文，由于无法获知接收者的具体私钥等隐私信息，无法完成对密文的解密.

（4）发送者身份验证

接收者通过计算 $U'_{ID_S}=\pi_{ID_S}(X_{ID_S}+Y_{ID_S}+P_{Pub}h_{ID_S})$ 可确认发送者是否是其议定的密文发送者，因为正确的 U_{ID_S} 仅能通过发送者的公钥及身份信息恢复.

7　性能及效率分析

7.1　性能分析

本节就匿名性、安全性等性质将本文机制与现有的相关机制[4-17]进行比较，并给出具体如表 1 所示的比较结果. 表 1 中相关符号的定义为：*UnAnon* 表示相应的参与者不具有匿名性；*Anon* 表示相应的参与者具有匿名性；*UnSec* 表示机制不具有相应的安全属性；*Sec* 表示机制具有相应的安全属性.

表 1　本文机制与现有机制的性能比较结果

机制	匿名性		安全性		通信模式	不足
	接收者	发送者	保密性	不可伪造性		
文献[4]	*UnAnon*	*Anon*	*UnSec*	*UnSec*(*KGC*)	单消息	存在密钥托管问题，接收者不具有匿名性
文献[5]	*UnAnon*	*Anon*	*UnSec*	*Sec*	单消息	接收者不具有匿名性
文献[7-8]	*UnAnon*	*Anon*	*Sec*	*Sec*	单消息	接收者不具有匿名性
文献[6]	*UnAnon*	*Anon*	*UnSec*	*UnSec*	单消息	接收者不具有匿名性
文献[9,15]	*Anon*	*Anon*	*Sec*	*UnSec*(*KGC*)	单消息	存在密钥托管问题，不具有公开验证性
文献[10-12]	*Anon*	*Anon*	*Sec*	*Sec*	单消息	存在密钥托管问题
文献[13]	*UnAnon*	*Anon*	*Sec*	*Sec*	单消息	接收者不具有匿名性
文献[14]	*UnAnon*	*Anon*	*Sec*	*UnSec*(*KGC*)	单消息	存在密钥托管问题，接收者不具有匿名性
文献[16]	*UnAnon*	*Anon*	*Sec*	*Sec*	单消息	所有接收者都能获知接收者身份列表
文献[17]	*UnAnon*	*Anon*	*Sec*	*UnSec*(*KGC*)	多消息	存在密钥托管问题，接收者不具有匿名性
本文机制	*Anon*	*Anon*	*Sec*	*Sec*	多消息	与现有机制[5-21]比较尚无

注：其中 *UnSec*(*PKG*) 表示由密钥托管问题引起的伪造性攻击.

(1)接收者匿名性

接收者匿名性是指每一个接收者对于攻击者以及其他接收者来说都是匿名的.文献[4,6,7,13-14]中的相应机制必须包含接收者身份列表或相应的密文标记列表;文献[3,5,8,17]中的机制虽然密文中未包含接收者身份列表,但机制正确运行的前提是每个接收者都能准确定位密文集合中属于自己的密文,文献[9]经分析得知是由于作者笔误导致未将接收者身份列表加入到密文中;文献[16]中所有的接收者可从密文信息中还原接收者身份列表,即每一个接收者对于其他接收者而言不具有匿名性,仅对攻击者具有匿名性;而本文和文献[9-12,15]的密文中无需包含接收者身份列表,确保了接收者的匿名性.

(2)发送者匿名性

发送者匿名性是指发送者对于攻击者而言是匿名的.文献[9,15]中将发送者隐藏于发送者伪装列表中,使得发送者具有强匿名性,即发送者对于攻击者和所有接收者来说都是匿名的.由于接收者无法确认具体的发送者,因此上述机制[9,15]不具有公开验证性和不可否认性;然而在实际应用中,若发送者否认签密行为,将导致收发双发纠纷的产生;文献[4-8,11-14,16-17]中对于发送者的匿名性未进行介绍,但分析解签密算法可知,所有的接收者必须掌握发送者的身份信息;本文和文献[10]中的机制采用发送者弱匿名性,每一位接收者可从密文中恢复出发送者的身份信息,即发送者对于攻击者而言是匿名的,因此本文和文献[10]中的机制具有公开验证性,但是相较与文献[9,15]中的机制而言,本文和文献[10]机制中发送者的匿名性较弱.因此,有必要研究发送者的匿名可控性.

(3)通信模式

通信模式根据发送消息数量的不同可分为单消息和多消息两种,若一次操作中发送者仅发送一个消息给不同的接收者称为单消息通信模式;一次操作中发送多个消息给不同的接收者称为多消息通信模式.文献[3-16]中的机制仅适用于发送者发送同一个消息给不同的接收者,当发送者需要发送不同的消息给不同的接收者时,上述机制无法满足发送者的多消息发送需求,只能采用传统一对一的模式,将导致通信效率的降低;其中文献[8]可在不增加额外计算的基础上将现有机制的单消息模式扩展为多消息模式;而本文和文献[17]中的机制可在一次操作中发送不同的消息给不同的接收者,为发送者提供了多消息安全发送策略,通信效率较高.

(4)密钥托管

密钥托管是指 PKG 完全掌握用户的私钥.由于文献[4-5,9-12,14-15,17]中的机制是以基于身份的密码系统为基础,因此存在密钥托管的问题;而本文和文献[6-7,13]基于 CL-PKC 构建,避免了传统公钥密码中的证书管理问题,同时又解决了基于身份密码系统的密钥托管问题;文献[16]基于多变量公钥体制构建了无证书多接收者签密机制,同样解决了基于身份密码系统的密钥托管问题.

(5)解密独立性

解密独立性是指每一个接收者可单独解密密文信息,不受其他接收者的限制.文献[5]中接收者在解密时需其他接收者的相关公开参数,若恶意接收者提供虚假的公开参数,这将导致其他接收者解密失败;而本文和文献[4,6-17]中接收者在解密时无需其他接收者的参数信息,可独自完成解密操作.

(6)安全性

文献[4]的机制无法满足其所声称的机密性和不可伪造性,文献[5]中的机制无法满足其所声称的机密性;文献[6]的机制在 $\mathcal{A}_1$ 类敌手攻击下不具有保密性和不可伪造性;由密钥托管问题导致文献[9-12,14-15,17]中恶意 PKG 可伪造任意用户的密文或替任意用户进行解密;本文和文献[8,13,16]中的多接收者签密机制具有较高的安全性.

7.2 效率分析

本节将从计算效率和通信开销两个方面将本文机制与相关多接收者签密机制进行比较,并给出具体如表 2 所示的比较结果,其中计算效率以签密和解签密阶段的运算量大小来衡量,而通信效率以密文的长短来衡量.表 2 中相关符号的定义为:B_e 表示双线性映射运算;B_M 表示群上的乘法运算;B_E 表示指数运算.$|Z_q^*|$ 表示 Z_q^* 中元素的长度;$|G|$ 表示群 G 中元素的长度;$|M|$ 表示明文的长度;$|ID|$ 表示用户身份标识 ID 的长度;$|Params|$ 表示相应机制中的相关参数的长度.m 表示发送者伪装列表的成员数;n 表示接收者列表的成员数.

在计算效率方面,由于运行双线性映射和指数运算的计算时间远高于点乘运算,因此双线性映射和指数运算的计算量较大,是影响机制性能的主要因素,因此表 2 主要对各机制的双线性映射、指数运算和群上乘法运算的次数进行了统计,对计算量较少的哈希、异或等运算并未统计;并且对提前进行的相关运算也未统计.由表 2 可知,传统多接收者签密机制[8-15]的签密或解签密阶段均进行了双线性映射

表 2　本文机制与现有机制的效率比较结果

机制	签密效率	解签密效率	密文长度
文献[8]	$nB_e+nB_E+1B_M$	$3B_e+1B_E$	$2\|G\|+n\|M\|$
文献[9]	$1B_E+(3+m+n)B_M$	$4B_e+(4+m)B_M$	$2\|G\|+(n+1)\|Z_q^*\|+\|M\|+m\|ID\|$
文献[10]	$1B_e+(4+n)B_M$	$5B_e+1B_M$	$2\|G\|+n\|Z_q^*\|+\|M\|+\|ID\|$
文献[11]	$2B_e+(4+n)B_M$	$1B_e+4B_M$	$2\|G\|+(n+1)\|Z_q^*\|+2\|M\|$
文献[12]	$2B_e+3B_E+3nB_M$	$(n+4)B_e$	$(n+2)\|G\|+\|M\|$
文献[13]	$2nB_E+(1+n)B_M$	$2B_E+3B_E+1B_M$	$(2n+1)\|G\|+\|M\|+n\|ID\|$
文献[14]	$1B_E+(1+n)B_M$	$2B_e+1B_E$	$(n+1)\|G\|+\|M\|+n\|ID\|$
文献[15]	$1B_e+(2+m+n)B_E$	$(n+3)B_e$	$(m+n+2)\|G\|+2n\|M\|+m\|ID\|$
本文机制	$(3n+1)B_M$	$5B_M$	$(n+1)\|G\|+\|Z_q^*\|+n\|M\|$

或指数运算，其计算效率较低；而本文机制无需双线性映射或指数运算，计算效率较高.

在通信效率方面，由于本文机制是多消息签密机制，签密者需对不同的消息产生不同的签名，导致本文机制中的密文长度较长；若使用本文机制进行单消息签密，则其密文长度降低为 $2|G|+|Z_q^*|+n|M|$；在同等条件下(单消息模式)，本文机制的密文长度远低于文献[9,13-15]中的密文长度，与文献[8,10-12]一样具有较高的通信效率.

综上所述，与现有机制相比较而言，本文无证书多接收者多消息签密机制在完成多消息签密的同时，具有较高的通信和计算效率，并且本文机制的性能更优.

8　结束语

多接收者签密机制可满足广播服务对保密性及不可伪造性的需求，以安全且认证的方式对多个授权用户广播消息，然而伴随网络通信环境的日益复杂，用户更加关注自身隐私的安全性. 本文为满足接收者的匿名性和发送者的多消息发送需求，提出无证书的多接收者多消息签密机制，签密密文中不再包含接收者的身份列表，实现对接收者隐私信息的保护；同时公用的信息集合确保密文解密的独立性. 相关分析表明除具有保密性和不可伪造性之外，本文机制中密文的接收者也具有较强的匿名性，并且功能更加完善；同时本文机制未使用双线性映射和指数运算等计算量较大的运算，具有较高的计算和通信效率；因此本文机制是安全有效的无证书多接收者多消息签密机制.

本文机制中发送者的匿名性较弱，仅对攻击者具有匿名性；但是当发送者具有强匿名性时，多接收者签密机制又不具有公开验证性和不可否认性，会导致签密密文收发双方纠纷的产生. 因此，下一步本文将在现有工作的基础上，研究发送者具有可控匿名性的无证书多接收者多消息签密机制.

致　谢　感谢审稿专家和编辑老师的细致审阅！

参　考　文　献

[1] Zhao Xiu-Feng, Xu Qiu-Liang. An efficient multi-PKG ID-based signcryption scheme. Chinese Journal of Computers, 2012, 35(4): 673-681(in Chinese)
(赵秀凤，徐秋亮. 一个有效的多 PKG 环境下基于身份的签密方案. 计算机学报，2012，35(4)：673-681)

[2] Zheng Y L. Digital signcryption or how to achieve cost (signature&encryption) ≪ cost(signature) + cost(encryption)//Proceedings of the 17th Annual International Cryptology Conference. California, USA, 1997: 165-179

[3] Duan S, Cao Z. Efficient and provably secure multi receiver identity based signcryption//Proceedings of the Information Security and Privacy 11th Australasian Conference. Melbourne, Australia, 2006: 195-206

[4] Yu Y, Yang B, Huang X, Zhang M. Efficient identity based signcryption scheme for multiple receivers//Proceedings of the Autonomic and Trusted Computing 4th International Conference. Hong Kong, China, 2007: 13-21

[5] Li Fa-Gen, Hu Yu-Pu, Liu Shuang-Gen. Efficient and provably secure multi-recipient signcryption from bilinear pairings. Wuhan University Journal of Natural Sciences, 2007, 12(1): 17-20

[6] Selvi S S D, Vivek S S, Shukla D, et al. Efficient and provably secure certicateless multi-receiver signcryption//Baek J, Bao F, Chen K, Lai X eds. Provable Security. Springer Berlin Heidelberg, 2008: 52-67

[7] Selvi S S D, Vivek S S, Srinivasan R, et al. An efficient identity-based signcryption scheme for multiple receivers//Proceedings of the 4th International of Workshop on Security. Toyama, Japan, 2009: 71-88

[8] Wu Lei. An ID-based multi-receiver signcryption scheme. Journal of Theoretical and Applied Information Technology, 2012, 46(1): 120-124

[9] Pang Liao-Jun, Cui Jing-Jing, LI Hui-Xian, et al. A new multi-receiver ID-based anonymous signcryption. Chinese Journal of Computers, 2011, 34(11): 2104-2113(in Chinese)
(庞辽军，崔静静，李慧贤等. 新的基于身份的多接收者匿名签密方案. 计算机学报，2011，34(11)：2104-2113)

[10] Pang Liao-Jun, Gao Lu, Pei Qing-Qi, et al. Fair and anonymous ID-based multi-receiver signcryption. Journal on Communications, 2013, 34(8): 161-168(in Chinese)
(庞辽军，高璐，裴庆祺等. 基于身份公平的匿名多接收者签密方案. 通信学报，2013，34(8)：161-168)

[11] Li Hui-Xian, Chen Xu-Bao, Ju Long-Fei, et al. Improve mulit-receiver signcryption scheme. Journal of Computer Research and Development, 2013, 50(7): 1418-1425(in Chinese)
(李慧贤，陈绪宝，巨龙飞等. 改进的多接收者签密方案. 计算机研究与发展. 2013，50(7)：1418-1425)

[12] Zhang Bo, Xu Qiu-Liang. Identity-based multi-signcryption scheme without random oracles. Chinese Journal of Computers, 2010, 33(1): 103-110(in Chinese)
(张波，徐秋亮，无随机预言机的基于身份多签密方案. 计算机学报，2010，33(1)：103-110)

[13] Miao S, Zhang F, Zhang L. Cryptanalysis of a certificateless multi-receiver signcryption scheme//Proceedings of the 2010 International Conference on Multimedia Information Networking and Security. Nanjing, China, 2010: 593-597

[14] Li Fagen, Xiong Hu, Nie Xuyun. A new multi-receiver ID-based signcryption scheme for group communications//Proceedings of the International Conference on Communications, Circuits and Systems. Milpitas, USA, 2009: 296-300

[15] Zhang B, Xu Q. An ID-based anonymous signcryption scheme for multiple receivers secure in the standard model. Advances in Computer Science and Information Technology. Berlin Heidelberg, Germany: Springer, 2010: 15-27

[16] Li Hui-Xian, Chen Xu-Bao, Pang Liao-Jun, et al. Certificateless Multi-receiver Signcryption Scheme Based on Multivariate Public Key Cryptography. Chinese Journal of Computers, 2012, 35(9): 1881-1889(in Chinese)
(李慧贤，陈绪宝，庞辽军等. 基于多变量公钥密码体制的无证书多接收者签密体制. 计算机学报，2012，35(9)：1881-1889)

[17] Qiu Jing, Bai Jun, Song Xin-chuan, et al. Secure and efficient multi-message and multi-receiver ID-based signcryption for rekeying in ad hoc networks. Journal of Chongqing University (English Edition), 2013, 12(2): 91-96

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

Secure multicast holds great promise in reducing the network band width required for the transmission of multimedia information such as video and audio data. It has become a hotspot in information security field. The multi-receiver signcryption scheme is considered as one of the most efficient approaches to implement secure multicast, and it has become a new branch of information security. In the recent years, some multi-receiver signcryption schemes based on bilinear pairings operations have been proposed, but most of them cannot satisfy the receivers' need of privacy protection.

In this paper, the multi-receiver and multi-message of certificateless signcryption scheme was proposed. The signcryption no longer contains receivers' identity list to protect receivers' privacy. The proofness of correctness and safety demonstrates this signcryption scheme is safe and effective. Apart from confidentiality and unforgery, this signcryption scheme is better in anonymity and has a higher computational efficiency.

This research was supported by the National Natural Science Foundation of China under Grant Nos. 61272436 and 61572303, the Foundation of State Key Laboratory of Information Security under Grant No. 2015-MS-10, and the 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.