新的基于身份的多接收者匿名签密方案

庞辽军[1),2)] 崔静静[2)] 李慧贤[3)] 裴庆祺[2)] 姜正涛[4)] 王育民[2)]

[1)](西安电子科技大学生命科学技术学院 西安 710071)

[2)](西安电子科技大学计算机网络与信息安全教育部重点实验室 西安 710071)

[3)](西北工业大学计算机学院 西安 710072)

[4)](中国传媒大学计算机学院 北京 100024)

摘 要 针对现有基于身份的多接收者签密方案存在的接收者身份泄露和解签密不公平等问题,文中提出一种具有公平性的基于身份的多接收者匿名签密方案.该方案运用拉格朗日插值多项式实现匿名性,不仅能解决现有方案不能保护接收者隐私的问题,而且具有解签密公平性,可防止发送者的欺骗行为.最后,对方案的正确性以及安全性进行了证明,并与其它方案进行了性能比较.分析发现,该方案是一个安全有效的多接收者签密方案,可以用于不安全和开放网络环境中的敏感消息广播.

关键词 匿名性;公平性;多接收者签密;基于身份的签密;拉格朗日插值

中图法分类号 TP309 **DOI 号**: 10.3724/SP.J.1016.2011.02104

A New Multi-Receiver ID-Based Anonymous Signcryption

PANG Liao-Jun[1),2)] CUI Jing-Jing[2)] LI Hui-Xian[3)] PEI Qing-Qi[2)] JIANG Zheng-Tao[4)] WANG Yu-Min[2)]

[1)](*School of Life Sciences and Technology, Xidian University, Xi'an* 710071)

[2)](*Key Laboratory of Computer Networks and Information Security of Ministry of Education, Xidian University, Xi'an* 710071)

[3)](*School of Computer Science and Engineering, Northwestern Polytechnical University, Xi'an* 710072)

[4)](*School of Computer Science, Communication University of China, Beijing* 100024)

Abstract Aiming at the receiver privacy exposure and de-signcryption unfairness problems that exist in the existing multi-receiver ID-based signcryption schemes, a fair multi-receiver ID-based anonymous signcryption scheme is proposed. The Lagrange interpolating polynomial is adopted to achieve the anonymity, which can not only solve the problem that the existing schemes cannot protect the privacy of receivers, but also meet the fairness of de-signcryption so that it can prevent the possible cheating behavior of the sender effectively. Finally, the proof of correctness and security is provided in details, and the performance comparison between the proposed scheme and other correlative schemes are given in succession. Analysis results show that this scheme is a secure and effective signcryption scheme and it can be used to broadcast sensitive information in unsafe and open network environment.

Keywords anonymity; fairness; multi-receiver signcryption; identity-based signcryption; Lagrange interpolating

---

收稿日期:2011-08-29;最终修改稿收到日期:2011-09-09.本课题得到国家自然科学基金(60803151,60803150,61103178,61103199)、国家自然科学基金委员会-广东联合基金重点项目(U0835004)、高等学校博士学科点专项科研基金新教师基金(20096102120045)、教育部计算机网络与信息安全重点实验室(西安电子科技大学)开放基金课题(2008CNIS-07)、西北工业大学"翱翔之星"项目(2008)、北京市自然科学基金(4112052)资助.**庞辽军**,男,1978 年生,博士,副教授,中国计算机学会(CCF)高级会员,主要研究方向为密码学、安全协议设计与分析.E-mail: ljpang@mail.xidian.edu.cn. **崔静静**,女,1986 年生,硕士,主要研究方向为网络与信息安全. **李慧贤**,女,1977 年生,博士,副教授,主要研究方向为多接收者签密及其应用. **裴庆祺**,男,1975 年生,博士,副教授,主要研究方向为网络与信息安全. **姜正涛**,男,1976 年生,博士,副教授,主要研究方向为密码学. **王育民**,男,1936 年生,教授,博士生导师,主要研究领域为信息论、密码、编码.

1 引　言

在网络广播服务中，消息发送者通常需要对外发布一些敏感消息，并希望只有其授权的用户才可以得到该消息，因此，需要对广播信息进行加密. 另外，用户为了避免收到某些无聊的信息，他也希望可以对接收到的广播消息来源进行认证. 由于以上需求，多接收者签密思想[1]被提出. 随着网络广播技术的发展，在一些特殊情况下，发送者希望其授权用户只验证消息来自某个可靠群体中的一员，无需确切得到发送者真实身份，以保护自身隐私. 基于这一需要，匿名的多接收者签密方案[2]被提出. 在一个多接收者匿名签密方案中，签密者，即消息发送者，将自己的身份隐藏在一个身份集合中，并利用自己的私钥对一组信息进行签密，而每一个授权的解签密者，即消息接收者，可以利用自己的私钥对密文进行验证并解签密以获取明文信息.

由于多接收者签密能够仅通过一次签密操作完成对多个接收者发送同一消息，比传统的一对一方式更有效、更实用，特别适合网络安全广播和安全组播等业务. 目前，多接收者签密已成为信息安全领域的一个研究热点. 基于 Duan 等人[1]提出的多接收者签密概念，具有签密者匿名性的签密方案被提出[2]. 随着人们对个人隐私的日益重视，不仅发送者渴望广播消息时不泄露自己的身份，接收者也希望自己收到某个消息的事实对他人保密. 分析发现，现有大多数多接收者签密方案[2-7]的密文信息暴露接收者身份，因为在这些方案中，所有授权用户的身份信息及其关联顺序是密文的一部分. 除了隐私问题外，现有方案的这种处理方式还会导致解密不公平，也就是说，当密文信息部分损坏后，可能会导致一部分授权用户能够正确解密，另一部分无法正确解密.

鉴于以上考虑，针对现有多接收者匿名签密存在的接收者身份暴露和解密不公平等问题，本文提出一个新的多接收者签密方案，以解决接收者身份隐私和解密不公平问题. 所提方案的密文中不再需要给出接收者的身份列表，从而能够保护接收者的隐私，同时，将每一个接收者所需的不同信息变换成一个公用的信息集以实现解密公平性. 因此，除了保密性和发送者不可伪造性外，相对于现有方案，本文方案具有以下优点：(1) 不仅发送者具有匿名性，接收者也具有匿名性，消息密文不再泄露任何接收者的身份信息，从而可以保护他们的隐私；(2) 具有解密公平性，使得对所有授权接收者而言都有相同的机会获得解密结果，要么所有授权接收者均正确解密，要么均无法正确解密.

本文第 2 节介绍相关工作；第 3 节介绍本论文方案用到的基本知识；第 4 节具体介绍我们的方案；第 5 节对本文方案进行分析与证明，并将其与现有方案进行对比分析；第 6 节总结全文.

2 相关工作

签密概念最早是由 Zheng[8] 于 1997 年提出的，思想是让公钥加密和数字签名同时进行，使得签密后的消息同时具有机密性和可靠性，且相较于传统的签名-加密模式，具有更小的计算和传输代价. 因此，签密得到人们的关注[7,9]. 2002 年，第一个基于身份的签密方案被提出[9]. 这些方案的特点是一对一签密，即发送者通过一次签密只能向一个接收者传输密文信息. 而当发送者需要向多个传输者传输同一消息时，上述签密方案需要对每一个接收者重复执行签密操作.

当一则消息需要向多个接收者传送时，传统的加密方案由于要重复多次加密过程，效率和实时性较低，不能满足实际应用需求[10]，因此，多接收者加密概念被提出. 融合签密概念和多接收者加密思想，Duan 等人[1]于 2006 年提出了第一个基于身份的多接收者签密方案，签密者对一则消息进行一次签密，每个接收者均可使用自己的私钥对接收到的消息的机密性和可靠性进行验证. 然而，在该方案中，密文内容包括两部分，即密文正文和接收者信息. 但实际上由于该方案密文中并没有包含接收者身份列表信息，接收者无法在密文中找到自己所需要的信息(经我们对文献[1]方案的分析，遗漏接收者身份列表信息问题可能属于作者笔误)，故方案并不完善. 2007 年，文献[3]提出了一个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. 此后，又有其它类似的方案被提出[4-5].

匿名签名的设计思想源自环签名，最初是由 Rivest 等人[11]于 2001 年提出的. 匿名方案使得接收者无法得知消息的真实签密者，但可以验证消息的签密者是一个群体中的一员，既满足了签密者的匿名性，又保证了消息来源的可靠性. Huang 等人[12]于 2005 年提出了第一个基于身份的匿名签密方案. 2009 年，文献[13]给出了一个新的高效的接收者匿名签密方案，文献[14]对其进行了改进. 基于上述匿名设计思想，Lal 等人在文献[2]中提出了第一个签密者匿名的多接收者签密方案，该方案中通

过把签密者的身份混在一个身份集合中来达到签密者匿名的目的.接收者可以验证消息的签密者是该集合中的某个人,从而相信消息来源,但不能确定究竟是谁签署了该消息.2010 年,文献[15]给出一种签密者匿名的新方案.而该方案同样存在因密文中缺少接收者身份列表而导致解密不正确的不足.此外,现有多接收者匿名签密方案[2,15]只考虑了发送者匿名问题,而没有考虑接收者的匿名问题.

通过上述分析,现有的多接收者签密方案[1-6,15],要么没有考虑匿名性,要么仅仅考虑了签密者即发送者的匿名性,而接收者的匿名性却没有被提及.事实上,以上方案的密文中都需要包括接收者身份列表(文献[1,15]中的方案由于作者笔误而遗漏),接收者需要通过列表中自己所在的序列号找到密文中自己需要的特定信息,继而对密文解密.这样必然存在如下缺陷:首先,暴露了接收者身份.此外,每个接收者所需要的特定信息只是整个签密密文中的特定部分,故存在解密不公平问题.如果密文在传送过程中出现错误,会导致部分接收者无法正确解密,而另一些接收者却可以对消息进行正确解密.更严重的是无法避免发送者有意欺骗某接收者的攻击.

鉴于以上考虑,本文提出一种新的多接收者匿名签密方案,该方案可以同时满足接收者和签密者的匿名性.此方案包含一个身份集合用来混淆真实签密者的身份,但是不包含接收者身份列表信息,故没有直观地展示授权接收者的身份,不仅使攻击者无法得到接收者的信息,而且接收同一则消息的所有接收者都不能获得除自己以外的其它接收者的任何信息,从而解决了接收者的隐私问题.此外,由于签密消息被广播出去后,任何用户都可以接收到广播消息,而仅有发送者授权的接收者才可以正确解密.方案为用户提供了一个判断方法来确定自己是否具有解密权限,避免非授权用户不必要的解密操作.而且每个接收者所需要的密文消息均为一个相同集合,一旦集合中某个元素发生错误,所有接收者都无法正确解密密文,故满足公平性.

3 背景知识

3.1 安全假设

本文所设计的多接收者匿名签密方案的安全性基于以下难题和安全假设.

设 G_1 和 G_2 为两个阶为 q 的循环群,且 P 为 G_1 的生成元,$e:G_1\times G_1\rightarrow G_2$ 为一个双线性映射.

(1) Computational Diffie-Hellman(CDH)问题.已知$\langle P,aP,bP\rangle$,其中 $a,b\in Z_q^*$,计算 abP.

(2) Decisional Bilinear Diffie-Hellman(DBDH)问题.已知$\langle P,aP,bP,cP,Z\rangle$,其中 $a,b,c\in Z_q^*$,$Z\in G_2$,判断 $Z=e(P,P)^{abc}$ 是否成立.

定义 1. CDH 假设.定义一个概率多项式时间算法 B,其输出为 $\beta\in\{0,1\}$,解决 CDH 问题的优势定义为 $Adv_B^{\mathrm{CDH}}=Pr[B(P,aP,bP)=abP:a,b\in Z_q^*]$.如果对于任何多项式时间算法,优势 Adv_B^{CDH} 都是可忽略的,则称之为满足 CDH 假设.

定义 2. DBDH 假设.定义一个概率多项式时间算法 B,其输出为 $\beta\in\{0,1\}$,其解决 DBDH 问题的优势定义为 $Adv_B^{\mathrm{DBDH}}=Pr[B(P,aP,bP,cP,e(P,P)^{abc})=1]-Pr[B(P,aP,bP,cP,Z)=1]$,这里 $a,b,c\in Z_q^*$ 且 $Z\in G_2$.如果对于任何多项式时间算法,优势 Adv_B^{DBDH} 都是可忽略的,则称之为满足 DBDH 假设.

3.2 基于身份的多接收者匿名签密方案(MIBAS)

基于现有多接收者匿名签密模型[1-6,15],这里给出本文方案的算法模型,包括 4 个算法,分别为参数生成算法 KeyGen,私钥提取算法 Extract,匿名签密算法 Anony-signcrypt 和解签密算法 De-signcrypt.本文方案就是基于该算法模型,结合所选取的困难问题和安全假设,对每个算法模块进行具体的设计和实现.

KeyGen:私钥生成中心(Private Key Generator,PKG)运用该算法生成主密钥 s_0 以及公开参数 $params$,其中主密钥需秘密保存,公开参数对外公布.

Extract:该算法用于提取用户私钥.输入用户的身份 ID_i,PKG 的私钥 s_0 以及系统公开参数 $params$,输出相应的用户私钥 d_i,即 $d_i=\mathrm{Extract}(ID_i,s_0,params)$.其中 ID_i 作为用户公钥对外公开,d_i 为其私钥秘密保存.

Anony-signcrypt:输入 PKG 的公开参数 $params$,明文消息 M,发送者选取一个身份集合 $L=\{ID_1,ID_2,\cdots,ID_m\}$,其中包含发送者的身份信息 ID_S,即 $ID_S\in L$,以及接收者的身份信息集合 $L'=\{ID_1',ID_2',\cdots,ID_n'\}$,并输入自己的私钥 d_S,运行该算法,输出消息 M 对应的不包含接收者身份信息集合 L' 的密文 C,即 $C=\text{Anony-signcrypt}(params,M,L',L,d_S)$,满足 $L'\notin C$.

De-signcrypt:输入密文 C,PKG 的公开参数 $params$,接收者的身份 $ID_i'(i\in\{1,2,\cdots,n\})$及其相应的私钥 d_i',运行该算法,首先判断 ID_i' 是否是授权

的接收者. 如果不是，则退出算法，否则，执行对密文 C 的解密过程. 如果密文 C 是正确的签密消息，则输出相应的明文消息 M，即 $M=\text{De-signcrypt}(C, params, L, d_i')$，否则输出⊥.

3.3　安全模型

安全模型用来刻画安全方案所能达到的安全级别以及对所设计方案安全性进行分析和证明. 本文将基于以下安全模型对本文所提方案的安全性给出随机预言模型下的安全证明.

3.3.1　消息保密性

提起保密性，最广泛被接受的是选择密文攻击下(CCA)的密文不可区分性安全模型. 最初是在文献[9]中被提出的，Duan 等人[1]将其扩展到多接收者环境中，并称其为 indistinguishability of ciphertexts under selective multi-ID, chosen ciphertext attack (IND-sMIBSC-CCA)，后来 Lal 等人[2]又将其推广到匿名的签密环境中，并称其为 indistinguishable against chosen ciphertext attacks (IND-sMIBAS-CCA2)，描述如下.

定义 3.　IND-sMIBAS-CCA2 假设. 假设 A 是一个攻击者(Attacker)，定义 Π 是一个基于身份的多接收者匿名签密方案. 考虑 A 与一个挑战者(Challenger) B 进行以下互动：

Setup：B 运行该算法，生成主密钥 s_0 以及系统参数 $params$，将 $params$ 给 A，并秘密保存主密钥 s_0. A 收到 $params$ 以后，输出 n 个目标身份 $L'^{*}=\{ID_1'^{*}, ID_2'^{*}, \cdots, ID_n'^{*}\}$.

Phase 1：A 向 B 进行如下询问.

私钥提取询问：当 B 接收到关于身份 $ID(ID\neq ID_i'^{*}, i=1,2,\cdots,n)$ 的私钥询问时，运行算法 Extract 得到 $d_{ID}=\text{Extract}(ID, s_0, params)$，并返回给 A.

匿名签密询问：A 给出一个身份信息集合 $L=\{ID_1, ID_2, \cdots, ID_m\}$，一个目标明文 M，n 个接收者身份信息 $L'=\{ID_1', ID_2', \cdots, ID_n'\}$. B 随机选择一个身份信息 $ID_i\in L$，计算其私钥 d_i，并计算密文 $C=\text{Anony-signcrypt}(params, M, L', L, d_i)$，然后将 C 返回给 A.

解签密询问：A 生成身份信息集合 $L=\{ID_1, ID_2, \cdots, ID_m\}$，接收者的身份信息集合 $L'=\{ID_1', ID_2', \cdots, ID_n'\}$ 和一个密文 C. B 随机选择一个接收者 $ID_j'\in L'$，计算其私钥 d_j'. 如果 C 是有效的密文，解密出 $M=\text{De-signcrypt}(C, params, L, d_j')$，并返回给 A，否则输出⊥.

Challenge：A 选择一对等长的消息 (M_0, M_1) 和一个身份集合 $L^{*}=\{ID_1^{*}, ID_2^{*}, \cdots, ID_m^{*}\}$，其中没有对 $ID_i^{*}(i=1,2,\cdots,m)$ 进行过私钥提取询问. 当 B 收到 (M_0, M_1) 后，随机选择 $\beta\in\{0,1\}$，计算目标密文 $C^{*}=\text{Anony-signcrypt}(params, M_\beta, L'^{*}, L^{*}, d_i^{*})$，并将 C^{*} 返回给 A，其中 d_i^{*} 为 L^{*} 中随机选择的身份 ID_i^{*} 所对应的私钥.

Phase 2：A 像 Phase 1 中那样进行多次询问. 注意私钥提取询问时不可以询问 L^{*} 中的身份信息，解密询问时不可以询问 C^{*}，也不可以对仅在接收者信息部分与 C^{*} 不同的密文消息进行解密询问.

Guess：最终，A 输出其猜测 $\beta'\in\{0,1\}$. 如果 $\beta'=\beta$，则 A 赢得这场游戏.

如上所述的 A 被称为 IND-sMIBSC-CCA2 攻击者，其优势定义为

$$Adv_{\Pi}^{\text{IND-sMIBSC-CCA2}}(A)=\left|Pr[\beta=\beta']-\frac{1}{2}\right| \quad (1)$$

如果对于任意的 IND-sMIBSC-CCA2 攻击者 A，在概率时间 t 内，它的猜测优势都小于 ε，则我们说方案 Π 是 (t,ε)-IND-sMIBSC-CCA2 安全的.

3.3.2　不可伪造性

签密方案需要具有不可伪造性，使得发送者不能否认对该消息签名的事实. Duan 等人[1]所提出的安全模型被称为 strong existential unforgeability under selective multi-ID, chosen message attack (SUF-sMIBSC-CMA). Lal 等人[2]将其推广到匿名环境下，并称其为 existentially unforgeable against adaptive chosen message attack (EUF-MIBAS-CMA)，描述如下.

定义 4.　EUF-MIBAS-CMA 假设. 假设 F 是一个伪造者(Forger)，定义 Π 是一个基于身份的多接收者匿名签密方案. 考虑 F 与一个挑战者(Challenger) B 进行以下互动：

Setup：B 运行该算法，生成主密钥 s_0 以及系统参数 $params$，将 $params$ 给 F，并秘密保存主密钥 s_0.

Attack：F 向 B 进行一系列询问，如定义 3 所述那样.

Forgery：F 最终输出一个新的密文消息 C^{*} 和 n 个接收者的身份信息 $L'^{*}=\{ID_1'^{*}, ID_2'^{*}, \cdots, ID_n'^{*}\}$. 如果 C^{*} 是 ID_S^{*} 对消息 M 对应于发送者身份集合 $L^{*}=\{ID_1^{*}, ID_2^{*}, \cdots, ID_m^{*}\}$ 的签名，且可以被任何 L'^{*} 中的接收者正确解密，则 C^{*} 是有效密文，F 赢得这场游戏. 注意 F 不能对 L^{*} 和 L'^{*} 中的身份进行私钥提取询问，且 C^{*} 不能由 Anony-signcrypt 算法产生. F 的优势为其成功的概率.

4 方案描述

本方案包含 KeyGen,Extract,Anony-signcrypt 和 De-signcrypt 4 个算法：PKG 通过 KeyGen 算法建立系统公开参数,并提供对其它非 PKG 成员的注册服务;非 PKG 成员(包括发送者和接收者)在进行签密和解签密之前需要向 PKG 进行注册,并通过 Extract 算法获取自己的私钥；经过注册的发送者可以使用 Anony-signcrypt 算法向一组授权接收者发送签密消息,同时不暴露发送者和接收者真实身份;授权的接收者使用 De-signcrypt 算法可以验证自己是否为授权接收者,并在自己为授权接收者的条件下正确地解密密文.具体描述如下.

参数生成算法(KeyGen)

PKG 执行以下过程：

1. 设 G_1 和 G_2 分别是阶为 $q\geq 2^k$(k 是一个长整数)的加法群和乘法群,P 是 G_1 的生成元.选择双线性映射 e 满足 $e:G_1\times G_1\rightarrow G_2$.

2. 定义 4 个单向 Hash 函数：$H_1:\{0,1\}^*\rightarrow G_1$；$H_2:G_2\rightarrow\{0,1\}^{l_0}$；$H_3:\{0,1\}^{l_0}\times G_1\rightarrow Z_q^*$；$H_4:\{0,1\}^*\rightarrow Z_q^*$,其中 l_0 表示明文和密文的长度.

3. 选择一个随机数 $s_0\in Z_q^*$ 为主密钥,设置 $P_{\text{pub}}=s_0P\in G_1$ 为系统的公钥.随机选择 $P_0\in G_1^*$,并计算 $g=e(P_{\text{pub}},P_0)$.

4. 公开系统参数 $params=\langle G_1,G_2,q,e,P,P_{\text{pub}},P_0,g,H_1,H_2,H_3,H_4\rangle$,并秘密保存主密钥 s_0.

私钥提取算法(Extract)

该算法由 PKG 执行.输入参数 $params$,s_0 和身份 $ID\in\{0,1\}^*$,算法包括以下步骤：

1. 计算 ID 的公钥 $Q_{ID}=H_1(ID)$.

2. 设置 ID 的私钥 $d_{ID}=s_0Q_{ID}$.

签密算法(Anony-signcrypt)

该算法由签密者即消息发送者执行.输入参数 $params$,消息 M.设 ID_S 是真正的签密者,$L'=\{ID_1',ID_2',\cdots,ID_n'\}$ 是签密者选择的 n 个接收者,ID_S 的签密过程如下：

1. 选择一个用户集 $L=\{ID_1,ID_2,\cdots,ID_m\}$,且 $ID_S\in L$,$L\cap L'=\varnothing$.

2. 随机选择整数 $u_i\in Z_q^*$,$i\in\{1,2,\cdots,m\}\backslash\{S\}$,并计算 $R_i=u_iP$.

3. 随机选择整数 $u_S\in Z_q^*$,并计算 $\alpha=\sum_{i=1}^{m}u_i$,$U=\alpha P$,$\sigma=g^{\alpha}$ 和 $W=H_2(\sigma)\oplus M$.

4. 计算 $h_i=H_3(W,R_i)$,$i\in\{1,2,\cdots,m\}\backslash\{S\}$.令 $R_S=u_SQ_S-\sum_{i=1,i\neq S}^{m}(R_i+h_iQ_i)$,其中 Q_S 是 ID_S 的公钥.令 $R=\{R_1,R_2,\cdots,R_m\}$.

5. 计算 $V=(u_S+h_S)\cdot d_S$,其中 $h_S=H_3(W,R_s)$,d_S 是 ID_S 的私钥.

6. 令 $x_j=H_4(ID_j')$,$y_j=\alpha(P_0+Q_j')$,$j=1,2,\cdots,n$,得到 n 对数：$(x_1,y_1),(x_2,y_2),\cdots,(x_n,y_n)$,构造拉格朗日函数 $F_j(x)$ 满足 x_j 是 $F_j(x)=y_j$ 的根,其中 Q_j' 是 ID_j' 的公钥.

7. 对于 $j=1,2,\cdots,n$,计算

$$f_j(x)=\prod_{1\leq j\neq j'\leq n}\frac{x-x_{j'}}{x_j-x_{j'}}=a_{j,1}+a_{j,2}x+\cdots+a_{j,n}x^{n-1},$$

其中 $a_{j,1},a_{j,2},\cdots,a_{j,n}\in Z_q$.

8. 对于 $j=1,2,\cdots,n$,计算 $T_j=\sum_{j'=1}^{n}a_{j',j}y_{j'}$.令 $T=\{T_1,T_2,\cdots,T_n\}$.

9. 密文为 $C=\langle U,V,W,T,R,L\rangle$.

解签密算法(De-signcrypt)

该算法由解签密者即消息接收者执行.输入密文 $C=\langle U,V,W,T,R,L\rangle$,$params$,接收者身份 ID_j' 及其私钥 d_j',对 C 进行解密,具体算法如下：

Verify：

1. 计算 $K=\sum_{i=1}^{m}(R_i+h_iQ_i)$,这里 $h_i=H_3(W,R_i)$,$i=1,2,\cdots,m$.

2. 判断等式 $e(V,P)=e(K,P_{\text{pub}})$ 是否成立.如果成立,则签密者是集合 L 中的成员之一,否则退出.

Judge：

1. 判断等式 $V\cdot Q_j'=K\cdot d_j'$ 是否成立.如果成立,ID_j' 可以对消息进行解密,否则退出.

Decrypt：

1. 计算 $\delta_j=T_1+x_jT_2+\cdots+(x_j{}^{n-1}\bmod q)T_n$,其中 $x_j=H_4(ID_j')$.

2. 计算 $\sigma'=e(P_{\text{pub}},\delta_j)\cdot e(U,d_j')^{-1}$,$M=H_2(\sigma')\oplus W$,$M$ 则为解密后所得到的消息明文.

5 分析与证明

5.1 正确性分析

定理 1. Verify 算法正确性.解密算法中对发送者身份的验证过程(Verify)是正确的.

证明.

$$\begin{aligned}e(V,P)&=e((u_S+h_S)d_S,P)=e(u_SQ_S+h_SQ_S,P_{\text{pub}})\\&=e\Big(\sum_{i=1,i\neq S}^{m}(R_i+h_iQ_i)+R_S+h_SQ_S,P_{\text{pub}}\Big)\\&=e\Big(\sum_{i=1}^{m}(R_i+h_iQ_i),P_{\text{pub}}\Big)\\&=e(K,P_{\text{pub}})\end{aligned}\tag{2}$$

即 $e(V,P)=e(K,P_{\text{pub}})$. 证毕.

定理 2. Judge 算法正确性.解密算法的接收者解密权限判断过程(Judge)是正确的.

证明. 对于每一个 ID_j',$j\in\{1,2,\cdots,n\}$,有

$$V\cdot Q'_j=(u_S+h_S)d_S\cdot Q'_j=(u_SQ_S+h_SQ_S)\cdot d'_j$$
$$=\Big(\sum_{i=1,i\neq S}^{m}(R_i+h_iQ_i)+R_S+h_SQ_S\Big)\cdot d'_j$$
$$=\sum_{i=1}^{m}(R_i+h_iQ_i)\cdot d'_j=K\cdot d'_j \quad (3)$$

即 $V\cdot Q'_j=K\cdot d'_j$. 证毕.

定理 3. Decrypt 算法正确性. 解密算法的解密过程(Decrypt)是正确的.

证明. 对于每一个 ID'_j, $j\in\{1,2,\cdots,n\}$, 计算 δ_j 如下:

$$\begin{aligned}\delta_j&=T_1+x_jT_2+\cdots+x_j^{j-1}T_j+\cdots+x_j^{n-1}T_n\\&=(a_{1,1}\alpha(P_0+Q'_1)+\cdots+a_{n,1}\alpha(P_0+Q'_n))+\\&\quad(x_ja_{1,2}\alpha(P_0+Q'_1)+\cdots+x_ja_{n,2}\alpha(P_0+Q'_n))+\cdots+\\&\quad(x_j^{j-1}a_{1,j}\alpha(P_0+Q'_1)+\cdots+x_j^{j-1}a_{n,j}\alpha(P_0+Q'_n))+\cdots+\\&\quad(x_j^{n-1}a_{1,n}\alpha(P_0+Q'_1)+\cdots+x_j^{n-1}a_{n,n}\alpha(P_0+Q'_n))\\&=(a_{1,1}+a_{1,2}x_j+\cdots+a_{1,n}x_j^{n-1})\alpha(P_0+Q'_1)+\\&\quad(a_{2,1}+a_{2,2}x_j+\cdots+a_{2,n}x_j^{n-1})\alpha(P_0+Q'_2)+\cdots+\\&\quad(a_{i,1}+a_{i,2}x_j+\cdots+a_{j,n}x_j^{n-1})\alpha(P_0+Q'_j)+\cdots+\\&\quad(a_{n,1}+a_{n,2}x_j+\cdots+a_{n,n}x_j^{n-1})\alpha(P_0+Q'_n)\\&=\alpha(P_0+Q'_j)\end{aligned} \quad (4)$$

因此, 我们可以得到 $\sigma'=e(P_{pub},\delta_j)\cdot e(U,d'_j)^{-1}$, 具体过程如下:

$$\begin{aligned}\sigma'&=e(P_{pub},\delta_j)\cdot e(U,d'_j)^{-1}\\&=e(P_{pub},\alpha(P_0+Q'_j))\cdot e(\alpha P,s_0Q'_j)^{-1}\\&=e(P_{pub},\alpha P_0)\cdot e(P_{pub},\alpha Q'_j)\cdot e(s_0P,\alpha Q'_j)^{-1}\\&=e(P_{pub},P_0)^{\alpha}\cdot e(P_{pub},\alpha Q'_j)\cdot e(P_{pub},\alpha Q'_j)^{-1}\\&=g^{\alpha}=\sigma\end{aligned} \quad (5)$$

所以, $M=H_2(\sigma')\oplus w$. 证毕.

5.2 安全性证明

下面我们分别对方案的消息保密性和不可否认性给出随机预言模型下的安全证明.

定理 4. 消息保密性. 在安全模型中, 如果存在一个 IND-sMIBSC-CCA2 敌手 A 能够在时间 t 内, 以一个不可忽略的优势 ε 赢得定义 3 中的游戏(此处他最多能进行 q_e 次私钥提取询问, q_s 次签密询问, q_d 次解签密询问和 $q_{H_1},q_{H_2},q_{H_3},q_{H_4}$ 次对 Hash 函数 H_1,H_2,H_3,H_4 的询问), 则存在一个算法 B 能够在时间 $t'\leq t+4q_dO(t_1)$ 内, 以优势 $\varepsilon'\geq\varepsilon-\frac{nq_d}{2^k}$ 解决 DBDH 问题(其中 t_1 是双线性对运算 e 的运算时间).

证明. 下面我们给出算法 B 如何利用 A 在时间 t' 内以概率 ε' 解决 DBDH 问题.

首先, B 得到一个 DBDH 问题实例 $\langle P,aP,bP,cP,Z\rangle$, 其目标为判定 $Z=e(P,P)^{abc}$ 是否成立. B 模拟一个挑战者如定义 3 中所述那样进行每一步过程. 此过程中 A 分别进行签密询问, 解密询问以及对 H_i, $i=1,2,3,4$ 的询问, 其中对 H_i 的询问结果被存放在 H_i-list 中.

Setup: B 设定 $P_0=bP$ 和 $P_{pub}=cP$, 那么 $g=e(P_0,P_{pub})=e(bP,cP)=e(P,P)^{bc}$, 将 $params=\langle G_1,G_2,q,e,P,P_{pub},P_0,g,H_1,H_2,H_3,H_4\rangle$ 作为系统参数给 A. 收到系统参数后, A 输出 n 个目标身份 $L'^*=(ID'^*_1,ID'^*_2,\cdots,ID'^*_n)$.

Phase 1: A 向 B 进行如下询问.

H_1-query: 向 H_1 输入一个身份 ID_k, 如果 H_1-list 中存在 (ID_k,l_k,Q_k), 则返回 Q_k. 否则, 进行以下步骤:

1. 如果 $ID_k=ID'^*_j$, $j\in\{1,2,\cdots,n\}$, 随机选择一个整数 $l'^*_j\in Z_q^*$, 计算 $Q'^*_j=l'^*_jP-P_0$. 否则随机选择一个整数 $l_k\in Z_q^*$, 计算 $Q_k=l_kP$.

2. 将 (ID_k,l_k,Q_k) 存入 H_1-list, 返回 Q_k.

H_i-query, $i\in\{2,3,4\}$: 为回答这些询问, B 首先查找相应的列表 H_i-list, $i\in\{2,3,4\}$, 如果询问目标已经存在, 则返回相应的回答给 A. 否则, B 随机选择一个恰当的元素作为询问结果返回给 A, 并将该询问和结果添加到相应的列表中.

私钥提取询问: 当 B 接收到关于身份 ID_k (此处 $ID_k\neq ID'^*_j$) 的私钥询问时, 在 H_1-list 中寻找 (ID_k,l_k,Q_k), 计算 $d_k=l_kP_{pub}=cl_kP$, 并将 d_k 返回给 A.

匿名签密询问: B 收到匿名签密询问 (M,L,L') (其中 $L=\{ID_1,ID_2,\cdots,ID_m\}$, $L'=\{ID'_1,ID'_2,\cdots,ID'_n\}$) 时, 此处存在两种情况, 描述如下:

1. B 随机选择 $ID_S\in L$. 如果对于任意 $j\in\{1,2,\cdots,n\}$ 有 $ID_S\neq ID'^*_j$, 则 B 可以在 H_1-list 中查找并计算出 ID_S 的私钥 $d_S=l_SP_{pub}=cl_SP$. B 以 (M,d_S,L,L') 作为匿名签密算法的输入, 计算出密文 C, 并将其返回给 A.

2. B 随机选择 $ID_S\in L$. 如果对于某个 $j\in\{1,2,\cdots,n\}$ 有 $ID_S=ID'^*_j$, 则令 $Q_S=l_SP-P_0$. 随机选择 $u_1,u_2,\cdots,u_S,\cdots,u_m\in Z_q^*$, 并计算 $\alpha=\sum_{i=1}^{m}u_i$, $\sigma=g^{\alpha}$ 以及 $W=H_2(\sigma)\oplus M$. 对于 $i\in\{1,2,\cdots,m\}\backslash\{S\}$, 分别计算 $R_i=u_iP$, 得到 $h_i=H_3(M,R_i)$, 并保存到 H_3-list. 计算 $U=\alpha P$ 和 $x_j=H_0(ID'_j)$, $y_j=\alpha(P_0+Q'_j)$, $j=1,2,\cdots$, 对 n 构造拉格朗日插值函数 $F_j(x)$ 满足 x_j 是函数 $F_j(x)=y_j$ 的根. 对于 $j=1,2,\cdots,n$, 计算 $f_j(x)=\prod_{1\leq j\neq j'\leq n}\frac{x-x_{j'}}{x_j-x_{j'}}=a_{j,1}+a_{j,2}x+\cdots+a_{j,n}x^{n-1}$, 得到 $a_{j,1},a_{j,2},\cdots,a_{j,n}\in Z_q$, 再计算 $T_j=\sum_{j'=1}^{n}a_{j',j}y_j$. 对于 $i=S$, 随机选择 $h_S\in Z_q^*$, 设 $R_S=u_SP-h_SQ'^*_S-\sum_{i=1,i\neq S}^{m}(R_i+h_iQ'^*_i)$ 和 $V=u_SP_{pub}$, 将 (W,R_S,h_S) 保存到 H_3-list. 最终, B 输出密文

C,并将其返回给 A.

解签密询问:A 输出一个密文 $C=\langle U,V,W,T,R,L\rangle$ 和一个接收者身份 $ID'_j, j\in\{1,2,\cdots,n\}$,向 B 进行解签密询问.

如果 $ID'_j\in L'^*$,则 B 不知道 ID'_j 的私钥,只能返回密文 C 无效.如果密文 C 本身是有效的,B 拒绝 C 的概率不多于 $n/2^k$.如果 $ID'_j\notin L'^*$,且 B 验证 $e(V,P)=e\left(\sum_{i=1}^{m}(R_i+h_iQ_i),P_{\text{pub}}\right)$ 成立,则 B 通过 H_1-list 得到 ID'_j 的私钥 d'_j,再计算出 δ_j.计算 $\sigma'=e(P_{\text{pub}},\delta_j)\cdot e(U,d'_j)^{-1}$,$M=H_2(\sigma')\oplus W$,返回 M 给 A.否则密文 C 无效,输出 $\perp$.

Challenge:A 输出一对等长的消息 (M_0,M_1) 和一个身份集合 $L^*=\{ID_1^*,ID_2^*,\cdots,ID_m^*\}$.接收者身份集合 $L'^*=\{ID'^*_1,ID'^*_2,\cdots,ID'^*_n\}$ 是被攻击对象.B 随机选择 $\beta\in\{0,1\}$,对消息 M_β 进行签密.首先,B 令 $U^*=aP,\sigma=Z$,查找 H_1-list 获得与 ID'^*_j,$i\in\{1,2,\cdots,n\}$ 相对应的 l'^*_j,计算出 $y_j^*=l'^*_jU^*$,继而得到 $T'^*_j, j\in\{1,2,\cdots,n\}$.$B$ 最终生成一个目标密文 $C^*=\langle U^*,V^*,W^*,T^*,R^*,L^*\rangle$,并将 C^* 返回给 A.

Phase 2:A 像 Phase 1 中一样进行多次询问,注意私钥提取询问时不可以询问 L^* 中的身份信息,解密询问时不可以询问 C^*,也不可以对仅在接收者信息部分与 C^* 不同的密文消息进行解密询问.

Guess:最终,A 输出其猜测 $\beta'\in\{0,1\}$,如果 $\beta'=\beta$,B 输出 DBDH 问题的解,因为

$$\begin{aligned}Z&=e(P_{\text{pub}},y_j^*)e(U^*,d'^*_j)^{-1}\\&=e(cP,l'^*_jU^*)e(U^*,d'^*_j)^{-1}\\&=e(cP,l'^*_jaP)e(aP,l'^*_jcP-cdP)^{-1}\\&=e(cP,l'^*_jaP)e(aP,l'^*_jcP)^{-1}e(aP,-cbP)^{-1}\\&=e(P,P)^{abc}\end{aligned}\tag{6}$$

分析:下面开始分析 B 的优势.对于 q_d 次解密询问,B 拒绝有效密文的概率不超过 $\frac{nq_d}{2^k}$.若 A 赢得 IND-sMIBAS-CCA2 游戏,则 B 的优势为 $\varepsilon'=|Pr[B(aP,bP,cP,Z)=1]-Pr[B(aP,bP,cP,e(P,P)^{abc})=1]|\geq\left|\varepsilon+\frac{1}{2}-\frac{nq_d}{2^k}-\frac{1}{2}\right|=\varepsilon-\frac{nq_d}{2^k}$,且 $t'\leq t+4q_dO(t_1)$(其中 t_1 是双线性对函数 e 的运算时间).

定理 5. 不可伪造性.在安全模型中,如果存在一个 EUF-MIBAS-CMA 敌手 F 能够在时间 t 内,以一个不可忽略的优势 ε 赢得定义 4 中的游戏(此处他最多能进行 q_e 次密钥提取询问,q_s 次签密询问和 $q_{H_1},q_{H_2},q_{H_3},q_{H_4}$ 次对 Hash 函数 H_1,H_2,H_3,H_4 的询问),则存在一个算法 B 能够在时间 $t'\leq t$ 内,以优势 $\varepsilon'\geq\varepsilon-\frac{q_s}{2^k}$ 解决 CDH 问题.

证明. 下面我们给出算法 B 如何利用 F 在时间 t' 内以概率 ε' 解决 CDH 问题.

首先,B 得到一个 CDH 问题实例 $\langle P,aP,bP\rangle$,其目标为计算出 abP.B 模拟一个挑战者如定义 4 中所述那样进行每一步过程.

Setup:B 设定 $P_{\text{pub}}=bP$,将 $params=\langle G_1,G_2,q,e,P,P_{\text{pub}},P_0,g,H_1,H_2,H_3,H_4\rangle$ 作为系统参数给 F.收到系统参数后,F 输出目标身份 ID_S^*.其中对 H_1,H_2,H_3 和 H_4 的询问如定理 3 中所述.

Attack:F 向 B 进行如下询问.

私钥提取询问:当 B 接收到关于身份 $ID(ID\neq ID_S^*)$ 的私钥询问时,就在 H_1-list 中寻找 (ID,l,Q),计算私钥 $d=blP$,并将其返回给 F.

匿名签密询问:对于一个关于 (m,L',L,ID_S)(其中 $ID_S\in L=\{ID_1,ID_2,\cdots,ID_m\}$,$L'=\{ID'_1,ID'_2,\cdots,ID'_n\}$)的签密询问,$B$ 随机选择 $x_i\in Z_p^*$,$i\in\{1,2,\cdots,m\}$,计算 $R_i=x_iP, i\in\{1,2,\cdots,m\}\backslash\{S\}$,$\alpha=\sum_{i=1}^{m}x_i$,$\omega=g^\alpha$ 和 $R_S=x_SQ_S-\sum_{i=1,i\neq s}^{m}(R_i+h_iQ_i)$.再计算 $U=\alpha P$ 和 $W=H_2(\omega)\oplus M$.在 H_3-list 中查找 (W,R_S),得到 h_S.如果不存在,就随机选择 $h_S\in Z_q^*$,并将 (W,R_S,h_S) 保存在 H_3-list 中,计算 $V=(x_S+h_S)d_S=(x_S+h_S)l_SbP$.$B$ 在 H_4-list 中查找 ID'_j 对应的结果 x_j,并计算 $y_j=\alpha(P_0+Q'_j)$,$j=1,2,\cdots,n$,由此得到 $T_j, j\in\{1,2,\cdots,n\}$.最终,$B$ 得到密文 C,并将其返回给 F.

Forgery:F 生成一个目标密文 $C^*=\langle U^*,V^*,W^*,T^*,R^*,L^*\rangle$,如果这个伪造是成功的,我们就有 $e(Z^*,P)=e\left(P_{\text{pub}},\sum_{i=1}^{m}(R_i^*+h_i^*Q_i^*)\right)$.定义 $Q_S^*=l_S^*P=aP$,则有 $V^*=(x_S^*+h_S^*)d_S^*=(x_S^*+h_S^*)l_S^*bP=(x_S^*+h_S^*)abP$,这样就很容易提取出 CDH 问题的解 $abP=V^*(x_S^*+h_S^*)^{-1}$.

下面我们考虑 B 成功的优势.由于签密询问中,B 对签密询问回答失败的概率不大于 $\frac{q_S}{2^k}$,所以我们得到优势 $\varepsilon'\geq\varepsilon-\frac{q_S}{2^k}$,且 $t'\leq t$. 证毕.

5.3 性能比较与效率分析

5.3.1 性能比较

与现有基于身份的多接收者签密方案进行比较,我们的方案性能更好,如表 1 所示(部分性能分析参见 5.3.2 小节).

表 1　本文方案与现有方案的性能比较

方案	签密算法	设计方法	优点	缺点
Duan 等人方法[1]	基于身份的签密	双线性对技术	提出多接收者签密方案	缺失接收者身份列表； 暴露发送者的身份； 解密不公平；
Lal 等人方法[2]	基于身份的签密	双线性对技术	提出发送者匿名性	暴露接收者的身份； 解密不公平；
Yu 等人方法[3]	基于身份的签密	双线性对技术	添加接收者身份列表	暴露发送者和接收者的身份； 解密不公平；
Sharmila 等人方法[4]	基于身份的签密	插值多项式技术	密文简短	暴露发送者和接收者的身份； 解密不公平；
Elkamchouchi 等人方法[5]	基于身份的签密	双线性对技术	公开参数少	暴露发送者和接收者的身份； 解密不公平；
Qin 等人方法[6]	基于身份的签密	双线性对和插值多项式技术	提出门限签密方案	暴露发送者和接收者的身份； 解密不公平；
Zhang 等人方法[15]	基于身份的签密	双线性对技术	标准模型下具有安全性	缺失接收者身份列表； 暴露接收者的身份； 解密不公平；
新方案	基于身份的签密	双线性对和拉格朗日插值多项式技术	发送者和接收者双重匿名性； 解密公平； 提前判断解密权限	与文献[1-6,15]相比尚无

对表 1 的解释如下：

(1) 接收者身份列表. 这是现有方案都必须包含的信息，用于接收者查找自己所需要的密文信息. 而本文方案无需包含接收者身份列表，从而提供了接收者匿名性.

文献[1,15]中缺少此部分(经分析可能是作者笔误)，会导致接收人无法从密文中查找自己所需要的信息，故无法对消息进行正确解密. 并且当缺少身份列表时，又没有给出接收者权限验证过程，会导致非授权用户进行不必要的解密开销.

(2) 接收者匿名性. 每一个接收者对于攻击者以及其它接收者来说都是匿名的.

由于签密者将消息进行广播，所以任何用户都可以接收到密文消息. 在许多现有文献中，如文献[1-6,15]，密文需要包含一个标志信息(文献[1,15]本身也是需要的)才能使接收者在密文中找到自己需要的信息来对密文进行解密，而标志信息就是所有授权接收者的身份信息集合，故接收者的身份会直接暴露出来，从而不具备隐私性. 但是在我们的方案中，加密过程中使用拉格朗日插值函数将所有授权接收者的身份信息 ID_i 糅合在一起，并隐藏在集合 $T=\{T_1,T_2,\cdots,T_n\}$ 中，每个接收者都得不到其它授权接收者的任何信息，从而具有接收者匿名性.

(3) 发送者匿名性. 每一个接收者只能验证消息来源于一个群组中的一员，而无法确定发送者的真实身份.

文献[1,3-6]的方案中，解密者会得到发送者的真实身份，而在一些特殊情况下，这将给发送者带来不利或负面影响，此时发送者需要匿名发布消息，以保全自己的名誉. 文献[2,15]的方案以及本文方案将发送者的身份隐藏在一组身份 $L=\{ID_1,ID_2,\cdots,ID_m\}$ 中，这组身份均是接收者所信任的，故接收者既相信了消息来源的可靠，又无法得到真实的消息来源.

(4) 解密公平性. 一旦消息在传输过程中出错或者被破坏，所有接收者都将得不到正确的消息明文.

现有方案[1-6,15]中，每个接收者需要通过列表中自己所在的序列号找到消息密文中自己所需要的特定信息，才可以对消息进行解密，然而一旦传输过程中密文信息发生错误，会直接导致部分接收者无法对消息进行解密，而其他接收者却可以解密，故不具有公平性. 在我们提出的方案中，密文为 $C=\langle U,V,W,T,R,L\rangle$，解密过程中所有出现的元素对于每个接收者而言都是必须的，故任何一个元素出错，所有接收者都无法正确解密，从而对所有授权的接收者而言解密过程是公平的.

(5) 提前判断性. 接收到广播消息的用户可以在解密前验证自己是不是授权的接收者，避免不必要的解密开销.

本方案中虽然没有直观地给出授权接收者的身份列表，但是每一个接收到签密消息的用户可以通过一步简单的判断方法来确定自己的解密权限. 如果等式 $V\cdot Q'_j=K\cdot d'_j$ 成立，则用户 ID'_j 是授权的接收者，否则无需对消息解签密.

5.3.2　效率分析

这里主要从签密过程的计算成本和通信量两个方面来比较现有基于身份的多接收者签密方案和本

文所提出的方案,具体分析如下:

(1)在本文方案中密文 $C=\langle U,V,W,T,R,L\rangle$ 的长度为 $(m+n+2)|G_1|+|M|+m|ID|$. 在文献[15]的方案中,密文信息缺少了接收者身份标志,如果添加上接收者身份标志,密文的真实长度应该为 $(m+n+2)|G_1|+|M|+(m+n)|ID|$,大于本文所提出的方案. 文献[2]的方案中,密文长度同样大于本文提出的方案. 文献[1,3-6]中,虽然密文长度较短,但是它们并没有实现发送者和接收者的匿名性这一功能. 总之,与现有匿名方案[2,15]相比,本文提出的方案不仅密文较短,在传输过程中具有一定优势,而且功能更完善.

(2)本文方案中 $f_i(x)$ 和 T_i 的功能是用于隐藏接收者的身份信息,保护接收者的隐私,且使得解密具有公平性,计算 $f_i(x)$ 和 T_i 需要一定的计算代价,但是只要选定了接收者,就可以提前对 $f_i(x)$ 和 T_i 进行计算以减少签密时的计算开销. 如果预先计算 $f_i(x)$ 和 T_i,则不统计这两步的计算量,本文的方案仅需 1 次指数计算,$3m-2$ 次加运算,$2m+1$ 次乘运算和 $m+1$ 次 Hash 运算,无需双线性对运算. 由于双线性对运算和指数运算的计算成本远大于加运算、乘运算和 Hash 运算,所以本方案的计算量与文献[1-6,15]中的方案比较起来也具有很大的优势. 具体比较结果如表 2 所示.

表 2 本文方案与现有方案的签密效率比较

方案	双线性对运算	指数运算	加运算	乘运算	Hash 运算	密文长度	参数个数
Duan 等人方法[1]	1	$n+4$	0	6	3	$(n+3)\|G_1\|+\|ID\|+\|M\|$	10
Lal 等人方法[2]	0	1	$3m+n-2$	$2m+n+1$	$m+1$	$(m+n+2)\|G_1\|+\|M\|+(m+n)\|ID\|$	11
Yu 等人方法[3]	1	1	$n+1$	$n+5$	2	$(n+2)\|G_1\|+\|G_2\|+\|M\|+n\|ID\|$	10
Sharmila 等人方法[4]	0	1	$n+1$	$n+3$	2	$3\|G_1\|+\|M\|+n\|ID\|$	$n+9$
Elkamchouchi 等人方法[5]	2	2	$n+1$	$n+4$	2	$(n+2)\|G_1\|+\|M\|+n\|ID\|+\|Z_q\|$	8
Qin 等人方法[6]	1	1	$2n-1$	$4n+4$	2	$(n+3)\|G_1\|+\|M\|+(n+1)\|ID\|$	9
Zhang 等人方法[15]	1	$2m+n+3$	0	$m+n+1$	2	$(m+n+2)\|G_1\|+\|M\|+m\|ID\|$	13
新方案	0	1	$3m-2$	$2m+1$	$m+1$	$(m+n+2)\|G_1\|+\|M\|+m\|ID\|$	12

6 结束语

多接收者签密将公钥加密和签名同时进行,满足了广播服务中保密性以及不可伪造性的需要,以安全且认证的方式对多个授权用户广播消息. 本文针对现有多接收者签密方案和匿名签密方案中的解签密者隐私泄露和解密不公平等问题,提出了一个基于身份的多接收者匿名签密方案,新方案满足接收者匿名性以及解密公平性. 文章最后给出了随机预言模型下本文方案的 IND-sMIBSC-CCA2 和 EUF-MIBSC-CMA 安全性证明,以及性能比较与效率分析. 结果表明本方案是一个安全有效的多接收者签密方案,可以用于不安全和开放网络环境中的敏感消息广播.

参 考 文 献

[1] 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

[2] Lal S, Kushwah P. Anonymous ID based signcryption scheme for multiple receivers. Cryptology ePrint Archive: Report 2009/345

[3] 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

[4] Sharmila S, Sree S, Srinivasan R, Pandu C. An efficient identity-based signcryption scheme for multiple receivers//Proceedings of the Advances in Information and Computer Security 4th International Workshop on Security. Toyama, Japan, 2009: 71-88

[5] Elkamchouchi H, Abouelseoud Y. MIDSCYK: An efficient provably secure multirecipient identity-based signcryption scheme//Proceedings of the International Conference on Networking and Media Convergence. Cairo, Egypt, 2009: 70-75

[6] Qin H, Dai Y, Wang Z. Identity-based multi-receiver threshold signcryption scheme. Security and Communication Networks, 2010, 3(6): 535-545

[7] 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

[8] Zheng Y. Digital signcryption or how to achieve cost (signature & encryption)≪cost (signature)+cost (encryption)//Proceedings of the 17th Annual International Cryptology Conference on Advances in Cryptology. London, UK, 1997: 165-179

[9] Malone-Lee J. Identity-based signcryption. Cryptology ePrint Archive: Report 2002/098

[10] Pang Liao-Jun, Li Hui-Xian, Jiao Li-Cheng, Wang Yu-Min. Design and analysis of a provable secure multi-recipient public key encryption scheme. Journal of Software, 2009, 20(10): 2739-2745(in Chinese)
(庞辽军，李慧贤，焦李成，王育民. 可证明安全的多接收者公钥加密方案设计与分析. 软件学报，2009，20(10)：2739-2745)

[11] Rivest R, Shamir A, Tauman Y. How to leak a secret: Theory and applications of ring signatures//Proceedings of the 7th International Conference on the Theory and Application of Cryptology and Information Security: Advances in Cryptology. London, UK, 2001: 552-565

[12] Huang X, Susilo W, Mu Y, Zhang F. Identity based ring signcryption scheme: Cryptographic primitive for preserving privacy and authenticity in the ubiquitous world//Proceedings of the 19th International Conference on Advanced Information Networking and Applications. Taipei, China, 2005: 649-654

[13] Zhang J, Gao S, Chen H, Geng Q. A novel ID-based anonymous signcryption scheme//Proceedings of the Advances in Data and Web Management Joint International Conferences. Suzhou, China, 2009: 604-610

[14] Zhang M, Zhong Y, Li P, Yang B. Analysis and enhance of anonymous signcryption model. Cryptology ePrint Archive: Report 2009/194

[15] Zhang B, Xu Q. An ID-based anonymous signcryption scheme for multiple receivers secure in the standard model//Proceedings of the Advances in Computer Science and Information Technology. Miyazaki, Japan, 2010: 15-27

PANG Liao-Jun, born in 1978, Ph. D., associate professor. His research interests include network security, information security and cryptography.

CUI Jing-Jing, born in 1986, M. S. candidate. Her research interests include network security and information security.

LI Hui-Xian, born in 1977, Ph. D., associate professor. Her research interests include multi-receiver ID-based signcryption and its application.

PEI Qing-Qi, born in 1975, Ph. D., associate professor. His research interests include network security and information security.

JIANG Zheng-Tao, born in 1976, Ph. D., associate professor. His research interest is cryptography.

WANG Yu-Min, born in 1936, professor, Ph. D. supervisor. His research interests include information theory, cryptology and coding.

Background

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 the recent years, some multi-receiver ID-based signcryption schemes have been published, but none of them has taken the privacy of the receivers into account. Although some anonymous schemes have already been proposed, they aim only at the anonymity of the sender. Actually, it can be found that there are the receiver privacy exposure and decryption unfairness problems in all the existing multi-receiver ID-based signcryption schemes.

This paper focuses on how to design a secure and fair multi-receiver ID-based signcryption scheme to support the development and application of the secure broadcasting. It proposes a new multi-receiver ID-based anonymous signcryption scheme, which can not only solve the problem that the existing schemes cannot protect the privacy of receivers, but also meet the fairness of decryption to prevent the possible cheating behavior of the sender effectively. The theoretical analyses about the security and the computation performance show that this scheme is more secure and effective than the existing ones. And thus, it can be used to broadcast sensitive information in unsafe and open network environment.

This research is supported by the National Natural Science Foundation of China under Grant Nos. 60803151, 60803150, 61103178 and 61103199, the Key Program of NSFC-Guangdong Union Foundation under Grant No. U0835004, the Research Fund for the Doctoral Program of Higher Education of China under Grant No. 20096102120045, the Open Foundation of the Key Laboratory of Network and Information Security in Xidian University, Ministry of Education of China under Grand No. 2008CNIS-07, NPU "Aoxiang Star" (2008) and Beijing Municipal Natural Science Foundation under Grand No. 4112052.