软件学报 ISSN 1000-9825, CODEN RUXUEW
Journal of Software,2014,25(10):2409−2420 [doi: 10.13328/j.cnki.jos.004506]

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

公平的基于身份的多接收者匿名签密设计与分析*

庞辽军[1,2], 李慧贤[3], 崔静静[2], 王育民[2]

[1](西安电子科技大学 生命科学技术学院,陕西 西安 710071)

[2](综合业务网理论及关键技术国家重点实验室(西安电子科技大学),陕西 西安 710071)

[3](西北工业大学 计算机学院,陕西 西安 710072)

通讯作者: 庞辽军, E-mail: ljpang@mail.xidian.edu.cn, http://www.xidian.edu.cn

摘 要: 针对现有基于身份的多接收者签密方案中存在的接收者身份泄露以及解密不公平性等问题,提出一种具有解密公平性的基于身份的多接收者匿名签密方案.新方案不仅能够解决现有方案中不能保护接收者身份隐私性的问题,并且满足解密公平性,从而有效地防止了发送者可能的欺骗行为.接着,基于双线性 Diffie-Hellman 假设和计算 Diffie-Hellman 假设,对所提方案的保密性和不可伪造性进行了证明.同时,对方案的正确性及性能进行了分析.分析发现,该方案是一个安全、有效的公钥签密方案,能够解决现有方案中存在的接收者身份暴露和解密不公平性等问题.这使得该方案具有非常重要的应用,尤其是可以用来实现安全广播,以便在不安全和开放的网络环境中安全地广播敏感信息.

关键词: 公平性;匿名性;签密;多接收者签密;基于身份的签密

中图法分类号: TP309

中文引用格式: 庞辽军,李慧贤,崔静静,王育民.公平的基于身份的多接收者匿名签密设计与分析.软件学报,2014,25(10):2409−2420. http://www.jos.org.cn/1000-9825/4506.htm

英文引用格式: Pang LJ, Li HX, Cui JJ, Wang YM. Design and analysis of a fair ID-based multi-receiver anonymous signcryption. Ruan Jian Xue Bao/Journal of Software, 2014,25(10):2409−2420 (in Chinese). http://www.jos.org.cn/1000-9825/4506.htm

Design and Analysis of a Fair ID-Based Multi-Receiver Anonymous Signcryption

PANG Liao-Jun[1,2], LI Hui-Xian[3], CUI Jing-Jing[2], WANG Yu-Min[2]

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

[2](State Key Laboratory of Integrated Services Networks (Xidian University), Xi'an 710071, China)

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

Corresponding author: PANG Liao-Jun, E-mail: ljpang@mail.xidian.edu.cn, http://www.xidian.edu.cn

Abstract: Existing ID-based multi-receiver signcryption schemes presents some security problems. For example, the identities of receivers can be revealed and the receivers do not have fairness in decryption. In order to avoid those problems, this paper proposes a fair ID-based multi-receiver anonymous signcryption scheme. The new scheme can not only solve the problem that the existing schemes can not protect the privacy of receivers, but also meet the fairness of decryption to effectively prevent possible cheating behavior of the sender. It then proves the confidentiality and unforgeability under of the scheme the bilinear Diffie-Hellman assumption and the computational Diffie-Hellman assumption. Simultaneity, the correctness and the performance of this scheme are analyzed. It concludes that this scheme is a secure and effective public-key signcryption scheme and can solve the problems of the receivers' identity exposure and unfairness decryption. Therefore, the new scheme has very important applications, especially it can be used to broadcast sensitive information in unsafe and open network environment.

* 基金项目: 国家自然科学基金(61103178, 60803151); 西安电子科技大学基本科研业务费(K5051310006)
收稿时间: 2011-06-16; 修改时间: 2013-01-25; 定稿时间: 2013-10-09

Key words: fairness; anonymity; signcryption; multi-receiver signcryption; identity-based signcryption

在网络广播传输服务中,付费服务的提供方希望只有其授权的用户才可以享受服务,同时,授权用户也不希望让没有付费的非授权用户轻易地得到相关服务.因此,需要对广播信息进行加密,确保只有授权用户才能够正确解密得到信息.另外,授权用户为了避免收到某些无聊的服务或广告信息,通常希望可以对接收到的广播消息进行认证.由于以上需要,多接收者签密思想[1]被提了出来.在一个多接收者签密方案中,签密者,即消息发送者,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签密密文进行解签密操作以获取明文信息.

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安全地发送同一消息,比传统的一对一的签密方式[2,3]更为有效和实用,因此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.在 Duan 等人[1]提出多接收者签密概念后,许多优秀的签密方案也被提了出来[4−7].现有的多接收者签密方案均能满足保密性和不可伪造性要求,保证只有授权用户可以正确解密.同时,能够验证消息发送者的身份.但是,随着对个人隐私问题的日益重视,人们渴望自己订阅某种服务的事实对他人保密.然而,现有大多数多接收者签密方案[4−7]中的密文信息完全暴露了接收者身份,因为在现有这些方案中,所有授权接收者的身份信息及其关联顺序是密文中的一部分,任何人只要获取了密文,就能够得到接收者的身份信息.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性问题.也就是说,当密文信息部分损坏后,可能会导致部分授权用户无法正确解密,而其他用户却仍然能够正确解密.这在实际应用中具有一定的局限性,也增加了发送者蓄意欺骗某些接收者的可能.

鉴于以上考虑,针对现有多接收者签密存在的接收者身份暴露和解密过程不公平等问题,提出一个新的多接收者签密方案,以确保接收者的身份隐私性和解密过程的公平性.所提方案的密文中不再需要直接给出接收者的身份列表,从而能够保护接收者的身份隐私性.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) 接收者具有匿名性.消息密文不再泄露接收者身份信息,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能正确解密,要么均无法正确解密.

本文第 1 节介绍相关工作.第 2 节介绍本文用到的数学背景以及签密方案的基本知识.第 3 节详细介绍本文所提方案.第 4 节对本文方案进行正确性分析与安全性证明,并与现有方案进行对比,以评估本文方案的性能.第 5 节总结全文.

1 相关工作

签密概念最早是由 Zheng[8]于 1997 年提出来的,其基本思想是: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和广泛研究[9−12].自 Boneh 和 Franklin[13]于 2001 年给出了第一个实际可行的基于身份的加密方案之后,基于身份的签密方案被提了出来[10].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相同的签密操作.

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需要重复多次加密过程,算法效率和实时性较低,不能满足实际需求[14].因此,Bellare[2]和 Baudron[3]于 2000 年分别提出多接收者加密这一概念.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,方案中签密者对一则消息进行一次签密,其指定的多个接收者可以分别使用自己的私钥对接收到的消息密文进行解密并验证其可靠性.然而在他们的方案中,密文内容包括两部分,即,密文正文部分和接收者信息部分(但事实上,Duan 等人在文章中可能由于某种失误,没有将解密所需要的接收者身份列表信息放入密文中,使得接收者无法在接收者信息

部分找到自己所需要的信息,故方案并不完善)[4].2007 年,文献[4]中提出了一种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,又有大量的方案被提出,如文献[5−7].其中,文献[5]提出了一个无证书的多接收者签密方案,它的缺点是密文较长,故存储和通信量较大;文献[6]提出了一个基于身份的多接收者加密方案,该方案虽然在计算性能上有一定优势,但它需要保存的公开参数过多,也不利于实际应用;文献[7]所提方案的缺点在于它的双线性对计算过多,计算复杂度太大.2009 年,Lal 等人在文献[15]中提出了一个签密者匿名的基于身份的多接收者签密方案,并给出了该方案的一个应用场合.2010 年,文献[16]给出一种新的签密者匿名的设计方案.尽管设计方法不同,但上述方案均需在消息密文中设置一个指示授权接收者的身份列表.

通过上述分析可以看出,现有的大多数多接收者签密方案的密文中都需要包括接收者身份列表(文献[1]尽管没有包含,但对其解密过程进行分析可知,这应该是作者笔误或者是无意中漏掉了),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所需要的特定密文信息元素,继而对密文的正文部分进行解密.这样必然存在如下缺陷:首先会暴露接收者身份隐私.事实上,任何人都不愿把自己的隐私透漏出去.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,故存在解密不公平性问题.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验证或解密消息,而另一些用户却可以对消息进行验证和解密.更为严重的是无法避免发送者有意欺骗某接收者的攻击,比如故意给某个接收者一个错误的信息部分.

鉴于以上考虑,针对接收者匿名性和解密不公平问题,本文提出一种新的多接收者签密方案,以满足接收者的匿名性和解密公平性.在新方案中,我们采用拉格朗日插值方法将授权接收者的身份信息隐藏在密文中,从而使得密文中不再包含接收者身份列表信息以及相关的序列号,不再直接泄露授权接收者的身份.不仅使攻击者无法得到接收者的信息,而且使接收同一则消息的所有接收者都不可获得除自己以外的其他接收者的任何信息,从而解决了接收者身份暴露的问题.同时,在新方案中,每个接收者不再需要根据自身身份选择对应的密文部分进行解密,所有接收者在解密过程中所需要的密文信息为相同的密文集合.因此,当部分密文在传输过程中丢失或者发生错误时,要么所有的接收者都不能够正确解密密文信息,要么都可以正确解密密文,从而解决了现有方案解密不公平的问题.

2 背景知识

在这一节,我们对文中用到的一些数学背景知识以及相关的困难问题作一简单介绍.

2.1 拉格朗日插值多项式

设 $F(x)=\sum_{i=1}^{t}F_i(x)=\sum_{i=0}^{t-1}a_ix^i$ 为一个 $t-1$ 次多项式,且通过 t 个点$(x_1,y_1),(x_2,y_2),\ldots,(x_t,y_t)$,其拉格朗日插值基函数为

$$f_i(x)=\prod_{1\leqslant j\neq i\leqslant t}\frac{x-x_j}{x_i-x_j}=\begin{cases}1, & x=x_i\\ 0, & x\in\{x_1,x_2,...,x_t\}-\{x_i\}\end{cases}.$$

我们有:

$$F_i(x)=f_i(x)y_i=\begin{cases}y_i, & x=x_i\\ 0, & x\in\{x_1,x_2,...,x_t\}-\{x_i\}\end{cases} \tag{1}$$

2.2 双线性函数

设 G_1 和 G_2 为两个阶为 q 的循环群,其中 q 为素数.双线性映射 e:$G_1\times G_1\to G_2$ 满足以下性质:

1) 双线性:对任意 $P,Q\in G_1$ 以及 $a,b\in Z_q$,有 $e(aP,bQ)=e(P,Q)^{ab}$ 成立;
2) 非退化性:对任意 $P,Q\in G_1$,有 $e(P,Q)\neq 1$;
3) 可计算性:对任意 $P,Q\in G_1$,存在有效的算法计算 $e(P,Q)$.

2.3 困难问题

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:$G_1\times G_1\to G_2$ 为一个双线性映射:

1) 计算 Diffie-Hellman(computational Diffie-Hellman,简称 CDH)问题:已知$\langle P,aP,bP\rangle$,其中, $a,b\in Z_q^*$, 计算 abP;
2) 双线性 Diffie-Hellman(bilinear Diffie-Hellman,简称 BDH)问题:已知$\langle P,aP,bP,cP\rangle$,其中, $a,b,c\in Z_q^*$, 计算 $e(P,P)^{abc}$.

定义 1(CDH 假设). 在解决 G_1 中的计算 Diffie-Hellman 问题时,定义一个概率多项式时间算法 B 的优势为

$$Adv_B^{\mathrm{CDH}}=\Pr[B(P,aP,bP)=abP,a,b\in Z_q^*].$$

CDH 假设为:如果任意多项式时间算法 B,其优势 Adv_B^{CDH} 都是可忽略的,则 CDH 假设成立.

定义 2(BDH 假设). 在解决 G_1 中的双线性 Diffie-Hellman 问题时,定义一个概率多项式时间算法 B 的优势为

$$Adv_B^{\mathrm{BDH}}=\Pr[B(P,aP,bP,cP)=e(P,P)^{abc}, a,b,c\in Z_q^*].$$

BHD 假设为:对任意多项式时间算法 B,其优势 Adv^{BDH} 都是可忽略的,则 BHD 假设成立.

2.4 基于身份的多接收者匿名签密方案(MIBAS)

类似于基于身份的多接收者签密[1],本文提出的基于身份的匿名签密同样包括 4 种算法,分别称为 KeyGen(参数生成算法)、Extract(密钥提取算法)、Anony-signcrypt(匿名的签密算法)和 De-signcrypt(解签密算法).

- KeyGen:私钥生成中心(private key generator,简称 PKG)运用该算法生成主密钥 s 以及公开参数 $params$,其中,主密钥秘密保存,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 以及系统公开参数 $params$,输出相应的用户私钥 d_i,即,$d_i=Extract(ID_i,s,params)$.其中,$ID_i$ 作为用户公钥对外公开,d_i 作为其私钥秘密保存;
- Anony-signcrypt:输入 PKG 的公开参数 $params$,一个明文消息 m,发送者身份 ID_S 选取一个接收者身份集合 $L=\{ID_1,ID_2,\ldots,ID_t\}$,并输入自己的私钥 d_S,运行该算法,输出消息 m 相对应的密文消息 C,即:
$$C=Anony\text{-}signcrypt(params,m,L,d_S).$$
- De-signcrypt:输入密文 C、PKG 的公开参数 $params$、接收者的身份 $ID_i(i\in\{1,2,\ldots,t\})$及其相应的私钥 d_i,运行该算法,如果密文 C 是正确的签密消息,则接受该签名,并输出相对应的密文消息 m,即:$m=De\text{-}signcrypt(C,params,d_i)$;否则,输出$\perp$.

本文所提出的匿名多接收者签密方案的密文同样包括密文部分和接收者信息部分,但新方案的接收者信息部分不再包含具体的身份信息明文和与之相关的序列号,而是以拉格朗日插值方式将授权接收者的身份杂糅在一起,从而形成一个密文集合,该集合不暴露任何身份隐私.同时,密文的各个部分对于每个授权接收者来说都是必要的,为了解签密收到的密文,接收者需要密文的全部内容用来解密密文,以获得对应明文.

2.5 安全模型

2.5.1 消息保密性

消息保密性是指信息不被泄露给非授权的用户,即,信息只能被授权用户使用.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,Duan 等人[1]将其扩展到多接收者环境中,我们称其为多接收者签密方案在选择密文攻击下具有密文不可区分性(indistinguishability of ciphertexts under selective multi-ID, chosen ciphertext attack,简称 IND-sMIBSC-CCA),具体描述如下.

定义 3(IND-sMIBSC-CCA). 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 以及系统参数 $params$,将 $params$ 给 A,并秘密保存主密钥 s.收到系统参

数以后,A 输出 t 个目标身份 $L^* = (ID_1^*, ID_2^*, ..., ID_t^*)$.

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 $ID(ID \neq ID_i^*, i = 1,2,...,t)$ 的私钥询问时,运行算法 Extract 得到该身份相应的密钥 d=*Extract*(ID,s,*params*);
- 匿名签密询问:当 B 收到匿名签密询问(m,L,ID_s)(其中,L={ID_1,ID_2,…,ID_t})以后,计算密文:

  C=*Anony-signcrypt*(*params*,m,L,d_s),

  其中,d_s 是攻击者 ID_s 的私钥,并返回给 A;
- 解签密询问:当 B 收到解签密询问(C,ID_j,ID_s)(其中,$ID_j \in L$)以后,计算 ID_j 的私钥 d_j,如果 C 是有效的密文,就解密出 m=*De-signcrypt*(C,*params*,ID_s,ID_j,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 ID_s^*,B 计算 ID_s^* 的私钥 d_s^*,并随机选择$\beta \in \{0,1\}$,生成一个目标密文 $C^* = Anony\text{-}signcrypt(params, m_\beta, L^*, d_s^*)$,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 $(ID_1^*, ..., ID_t^*)$ 中的身份信息,解密询问时不可以询问 C^*.

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

如上所述的 A 被称为 IND-sMIBSC-CCA 攻击者,其优势定义为

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

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

2.5.2 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签名消息并发送给接收者的行为.我们对 Duan 等人[1]所提出的安全模型进行适当修改,提出称为多接收者签密方案在适应性选择消息攻击下能抗伪造性(modified existential unforgeability under selective ID, chosen message attack,简称 MEUF-sMIBSC-CMA).这里,我们提出的新安全模型描述如下.

定义 4(MEUF-sMIBSC-CMA). 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 以及系统参数 *params*,将 *params* 给 F,并秘密保存主密钥 s.收到系统参数以后,F 输出目标身份 ID_s^*.

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,就运行算法 Extract,得到:

  d=*Extract*(ID,s,*params*);
- 匿名签密询问:当 B 收到匿名签密询问(m,L,ID_s)(其中,L={ID_1,ID_2,…,ID_t})以后,计算密文:

  C=*Anony-signcrypt*(*params*,m,L,d_s),

  其中,d_s 是攻击者 ID_s 的私钥,并返回给 F.

Forgery:F 最终输出一个新的密文消息 C^*和 t 组接收者的公私钥对(ID_1,d_1),(ID_2,d_2),…,(ID_t,d_t).如果 C^*是 ID_s^*对消息 m 的签名,且可以被任何 L={ID_1,ID_2,…,ID_t}中的接收者正确解密,则 C^*是有效密文,F 赢得这场游戏.这里的限制是:F 不能对身份 ID_s^*进行私钥提取询问,且 C^*不能由 Anony-signcrypt 算法产生.F 的优势为其胜利的概率.

3 方案描述

本方案包含 KeyGen,Extract,Anony-signcrypt 和 De-signcrypt 这 4 种算法,具体描诉如下.

3.1 参数生成算法(KeyGen)

该算法由 PKG 执行,具体包括以下步骤:

1. 设 G_1 和 G_2 分别是阶为 $q\geqslant 2^k$(其中,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 $e:G_1\times G_1\to G_2$;
2. 定义 4 个单向 Hash 函数: $H_0:\{0,1\}^{\lambda_1}\to G_1, H_1:\{0,1\}^{\lambda_2}\times G_1\to Z_q^*, H_2:G_2\to\{0,1\}^{\lambda_1+\lambda_2}, H_3:\{0,1\}^{\lambda_1}\to Z_q^*$(其中,$\lambda_1=|ID|,\lambda_2=|m|$);
3. 选择一个随机数 $s\in Z_q^*$ 为主密钥,设置 $P_{pub}=sP\in G_1$ 为系统公钥;
4. 公开系统参数 $params=\langle G_1,G_2,q,e,P,P_{pub},H_0,H_1,H_2,H_3\rangle$,并安全保存主密钥 s.

3.2 私钥提取算法(extract)

向 PKG 输入参数 $params$、s 和身份 $ID\in\{0,1\}^{\lambda_1}$,算法进行以下步骤:

1. 计算 ID 的公钥 $Q_{ID}=H_0(ID)$;
2. 设置 ID 的私钥 $d_{ID}=sQ_{ID}$.

3.3 签密算法(anony-signcrypt)

签密者输入参数 $params$、消息 m,设 ID_A 是签密者,$\{ID_1,ID_2,\ldots,ID_t\}$ 是签密者从 n 个用户中选择的 t 个接收者的身份集合,ID_A 的签密过程如下:

Sign:

1. 随机选择整数 $r\in Z_q^*$,$R\in G_1$.计算 $U=rP,h=H_1(m,U),V=hd_A+rQ_A$(其中,"+"表示 G_1 中的加法运算).这里,$d_A=sQ_A$ 和 $Q_A=H_0(ID_A)$分别是签密者的私钥和公钥.

Encrypt:

1. 计算 $Y=e(rP_{pub},R),W=H_2(Y)\oplus(m||ID_A)$;
2. 计算 $x_i=H_3(ID_i),y_i=r(R+Q_i),i=1,2,\ldots,t$,其中,$Q_i=H_0(ID_i)$,从而得到 t 组数:$(x_1,y_1),(x_2,y_2),\ldots,(x_t,y_t)$,构造拉格朗日函数 $F_i(x)$满足 x_i 是 $F_i(x)=y_i$ 的根.对于 $i=1,2,\ldots,t$,计算:

$$f_i(x)=\prod_{1\leqslant j\neq i\leqslant t}\frac{x-x_j}{x_i-x_j}=a_{i,1}+a_{i,2}x+\ldots+a_{i,t}x^{t-1},\ a_{i,1},a_{i,2},\ldots,a_{i,t}\in Z_q \tag{3}$$

3. 对于 $i=1,2,\ldots,t$,计算 $T_i=\sum_{j=1}^{t}a_{j,i}y_i$;
4. 生成密文 $C=\langle T_1,T_2,\ldots,T_t,U,V,W\rangle$.

3.4 解签密算法(de-signcrypt)

接收者输入密文 $C=\langle T_1,T_2,\ldots,T_t,U,V,W\rangle$、$params$、接收者的身份 ID_i 及其私钥 d_i,为了解密 C,算法进行以下步骤的操作:

Decrypt:

1. 计算 $x_i=H_3(ID_i)$.计算 $\delta_i=T_1+x_iT_2+\ldots+(x_i^{t-1}\bmod q)T_t$.计算 $Y'=e(P_{pub},\delta_i)\cdot e(U,d_i)^{-1},(m||ID_A)=H_2(Y')\oplus W$;
2. 输出$(m||ID_A)$和$\langle U,V\rangle$进行以下验证过程:

Verify:

1. 计算 $h=H_1(m,U)$,判断 $e(P,V)=e(UP_{pub},Q_A)^h$(其中,$Q_A=H_0(ID_A)$)是否成立:如果成立,则接受消息 m;否则,输出$\perp$.

4 分析与证明

4.1 正确性分析

本文方案的正确性通过以下两个定理来加以说明.

定理 1. 第 3.4 节中所描述的解密过程(decrypt)是正确的.

证明:首先,对于每一个 $ID_i,i\in\{1,2,\ldots,t\}$,计算$\delta_i$ 如下:

$$\begin{aligned}\delta_i &= T_1 + x_iT_2 + \ldots + x_i^{i-1}T_i + \ldots + x_i^{t-1}T_t\\ &= (a_{1,1}\cdot r(R+Q_1) + \ldots + a_{t,1}\cdot r(R+Q_t)) + (x_ia_{1,2}\cdot r(R+Q_1) + \ldots + x_ia_{t,2}\cdot r(R+Q_t)) + \ldots +\\ &\quad (x_i^{i-1}a_{1,i}\cdot r(R+Q_1) + \ldots + x_i^{i-1}a_{t,i}\cdot r(R+Q_t)) + \ldots + (x_i^{t-1}a_{1,t}\cdot r(R+Q_1) + \ldots + x_i^{t-1}a_{t,t}\cdot r(R+Q_t))\\ &= (a_{1,1}+a_{1,2}x_i+\ldots+a_{1,t}x_i^{t-1})\cdot r(R+Q_1) + (a_{2,1}+a_{2,2}x_i+\ldots+a_{2,t}x_i^{t-1})\cdot r(R+Q_2) + \ldots +\\ &\quad (a_{i,1}+a_{i,2}x_i+\ldots+a_{i,t}x_i^{t-1})\cdot r(R+Q_i) + \ldots + (a_{t,1}+a_{t,2}x_i+\ldots+a_{t,t}x_i^{t-1})\cdot r(R+Q_t)\\ &= r(R+Q_i)\end{aligned} \tag{4}$$

从而,我们可以进一步得到 $e(P_{pub},\delta_i)\cdot e(U,d_i)^{-1}=e(rP_{pub},R)$,具体推导过程说明如下:

$$\begin{aligned}e(P_{pub},\delta_i)\cdot e(U,d_i)^{-1} &= e(P_{pub},r(R+Q_i))\cdot e(rP,sQ_i)^{-1}\\ &= e(P_{pub},rR)\cdot e(P_{pub},rQ_i)\cdot e(sP,rQ_i)^{-1}\\ &= e(rP_{pub},R)\end{aligned} \tag{5}$$

所以,$(m\|ID_A)=H_2(Y')\oplus W=H_2(Y)\oplus W$.证毕. □

定理 2. 第 3.4 节中所描述的验证过程(verify)是正确的.

证明:由于

$$\begin{aligned}e(P,V) &= e(P,(hd_A+rQ_A))\\ &= e(P,hsQ_A)e(P,rQ_A)\\ &= e(hsP,Q_A)e(rP,Q_A)\\ &= e(hP_{pub}\cdot rP,Q_A)\\ &= e(UP_{pub},Q_A)^h\end{aligned} \tag{6}$$

即:$e(P,V)=e(UP_{pub},Q_A)^h$,因此,验证过程是正确的.证毕. □

4.2 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 3. 在随机预言模型中,如果存在一个 IND-sMIBSC-CCA 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(这里,他最多能进行 q_{ex} 次密钥提取询问、q_s 次匿名签密询问、q_d 次解签密询问和 $q_{H_0},q_{H_1},q_{H_2},q_{H_3}$ 次对 Hash 函数 H_0,H_1,H_2,H_3 的询问),则存在一个算法 B 能够在时间 $t'\leqslant t+(2q_d+q_s)O(t_1)$内,以优势 $\varepsilon'\geqslant\varepsilon-\frac{q_{H_2}q_d}{2^k}$ 解决 BDH 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 BDH 问题.

首先,B 得到一个 BDH 问题实例 $C=\langle P,aP,bP,Q=cP\rangle$,其目标为计算出 $e(P,P)^{abc}$ 或 $e(P,Q)^{ab}$.B 模拟一个挑战者如定义 3 中所述进行每一步过程.

Setup:B 设定 $P_{pub}=bP$,将 $params=\langle G_1,G_2,q,e,P,P_{pub},H_0,H_1,H_2,H_3\rangle$作为系统参数给 A.收到系统参数以后,A 输出 t 个目标身份 $L^*=(ID_1^*,ID_2^*,\ldots,ID_t^*)$.

其中,H_0,H_1,H_2 和 H_3 由 B 如下控制:

对 H_0,H_1,H_2 和 H_3 询问的结果分别存储在 H_0-list,H_1-list,H_2-list 和 H_3-list 中.

H_0-query:向 H_0 输入一个身份 $ID_j,j\in\{1,2,\ldots,n\}$,如果 H_0-list 中存在(ID_j,l_j,Q_j),则返回 Q_j;否则,进行以下步骤:

1) 若 $ID_j=ID_i^*$,$i\in\{1,2,\ldots,t\}$,随机选择一个整数 $l_j\in Z_q^*$,计算 $Q_j=l_jP-Q$;否则,随机选择一个整数 $l_j\in Z_q^*$,计算 $Q_j=l_jP$.
2) 将(ID_j,l_j,Q_j)存入 H_0-list,返回 Q_j.

H_1-query:向 H_1 输入一组数 (m_j,U_j), $j\in\{1,2,\ldots,q_{H_1}\}$,若 H_1-list 中存在(m_j,U_j,h_j),则返回 h_j;否则,进行以下步骤的操作:

1) 随机选择一个整数 $h_j \in Z_q^*$;

2) 将(m_j,U_j,h_j)存入 H_1-list,返回 h_j.

H_2-query:向 H_2 输入一个元素 $Y_j \in G_2, j \in \{1,2,...,q_{H_2}\}$,若 H_2-list 中存在(Y_j,ρ_j),则返回ρ_j;否则,进行以下步骤的操作:

1) 随机选择一个字符串 $\rho_j \in \{0,1\}^{\lambda_1+\lambda_2}$;

2) 将(Y_j,ρ_j)存入 H_2-list,返回ρ_j.

H_3-query:向 H_3 输入一个身份 $ID_j,j\in\{1,2,\ldots,n\}$,如果 H_3-list 中存在(ID_j,x_j),则返回 x_j;否则,进行以下步骤的操作:

1) 随机选择一个整数 $x_j \in Z_q^*$;

2) 将(ID_j,x_j)存入 H_3-list,返回 x_j.

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 $ID_j(ID_j \neq ID_i^*, i=1,2,...,t)$ 的私钥询问时,就在 H_0-list 中寻找(ID_j, l_j,Q_j),计算 $d_j=bl_jP$,并返回给 A;
- 匿名签密询问:B 收到匿名签密询问(m,L,ID_A)(其中,$L=\{ID_1,ID_2,\ldots,ID_t\}$)时,这里 $ID_A \neq ID_i^*(i=1,2,...,t)$, B 随机选择 $r',h,l \in Z_p^*$,计算 $U=r'P-hbP, V=r'(l_i^*P-Q)$, $R=lP$,得到(m,U,R,h),并在 H_1-list 中查找,使得(m,U)没有在 H_1-list 中出现;否则,重新选择 $r',h,l \in Z_p^*$,进行以上过程,B 将符合条件的(m,U,h)加入到 H_1-list 中.B 计算 $Y=e(r'bP,lP)$,在 H_2-list 中查找(Y,ρ),计算出 $W=\rho\oplus(m||ID_A)$,然后,B 在 H_3-list 中查找(ID_i,x_i),计算 $y_i=(l+l_i)U,i=1,2,\ldots,t$,并由此得到 $T_i(i=1,2,\ldots,t)$.最终,B 得到密文 C,并返回给 A;
- 解签密询问:当 B 收到一个密文为 $C=\langle T_1,T_2,\ldots,T_t,U,V,W\rangle$和一个身份 $ID_i,i\in\{1,2,\ldots,t\}$的解签密询问以后,寻找$(ID_i,x_i)\in H_3$-list,并计算 $\delta_i=T_1+x_iT_2+\ldots+(x_i^{t-1} \bmod q)T_t$.在 H_0-list 中寻找(ID_i,l_i,Q_i),并计算 $d_i=bl_iP, Y'=e(P_{pub},\delta_i)\cdot e(U,d_i)^{-1}$,从而可以得到$(m||ID_A)=H_2(Y')\oplus W$.再在 H_0-list 中寻找(ID_A,l_A,Q_A),得到 Q_A.最后验证 $e(P,V)=e(UP_{pub},Q_A)^{h_i}$ 是否成立:如果成立,则 C 是有效的密文,返回 m 给 A;否则,输出$\perp$.

Challenge:A 选择一对等长的消息(m_0,m_1)和一个签密者的身份 ID_A.当 B 收到(m_0,m_1)和 ID_A 以后,随机选择 $\beta\in\{0,1\}$,对消息 m_β进行签密.首先,B 查找 H_0-list 获得与 $ID_i^*, i\in\{1,...,t\}$ 相对应的 l_i^*,并得到它们的公钥 $Q_i^*=l_i^*P$,计算出 $y_i^*=rR+rQ_i^*=r(l+l_i^*)P$,继而得到 $T_i^*, i\in\{1,...,t\}$. B 最终生成一个目标密文 $C^*=\langle T_1^*,T_2^*,...,T_t^*,U^*,V^*,W^*\rangle$,其中,$U^*=aP, V^*=(bh+r)l_AP, R^*=Q=cP$ 且 $W^*=H_2(e(P,P)^{abc})\oplus(m_\beta||ID_A)$.最后,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 $(ID_1^*,ID_2^*,...,ID_t^*)$ 中的身份信息,解密询问时不可以询问 C^*.

Guess:最终,A 输出其猜测$\beta'\in\{0,1\}$,如果$\beta'=\beta$,B 从 H_2-list 选取(Y,ρ),并输出 V 作为 BDH 问题的解.

分析:在签密询问中,$U=r'P-hbP=(r'-bh)P$,故 $r=r'-bh$.又

$$V=r'(l_i^*P-Q)=(r'-bh)(l_i^*P-Q)+bh(l_i^*P-Q)=(r'-bh)Q_{ID_i^*}+bhQ_{ID_i^*}=rQ_{ID_i^*}+hd_{ID_i^*},$$

且

$$y_i=(l+l_i)U=(l+l_i)(rP)=r(lP+l_iP)=r(R+Q_i)=rR+rQ_i, i=1,2,\ldots,t,$$

由此计算出 T_i,从而可以得到目标密文.

在挑战过程中,我们设置 $U^*=aP, R=Q=cP$.已知 $Q_{ID_i^*}=H_0(ID_i^*)=l_i^*P-Q$, 可以得到:

$$y_i'=l_i^*(U^*)=al_i^*P=a(l_i^*P-Q+Q)=a(Q_{ID_i^*}+R').$$

再通过拉格朗日插值函数得到 T_i^*.因此,C^*与实际攻击过程中描述的相同.如果 A 的猜测正确,它需要询问随机预言函数 H_2 得到 $Y=e(rP_{pub},R)^{ab}=e(abP,Q)=e(P,Q)^{ab}$,并将$(Y,\rho)$存入 H_2-list,B 可以从中提取出 $e(P,Q)^{ab}$.

由以上讨论可知,攻击环境的模拟几乎完美,唯一不足的情况是:一个合理的密文在解签密询问时可能遭到

拒绝.显然,对于 H_2-list 中的每一对(Y_i,ρ_i),在 H_1-list 中恰好存在一个 h_i 提供一个合法的密文.拒绝一个合理密文的概率不大于 $\frac{q_{H_2}}{2^k}$.在攻击阶段,A 进行了 q_d 次解签密询问,B 从 H_2-list 中随机选择 Y 作为 BDH 困难问题的结果,我们有 $\varepsilon' \geqslant \varepsilon - \frac{q_{H_2}q_d}{2^k}$, 且 $t' \leqslant t+(2q_d+q_s)O(t_1)$(其中,$t_1$ 是对运算 e 的运算时间). □

定理 4. 在随机预言模型中,如果存在一个 MEUF-sMIBSC-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(这里,他最多能进行 q_{ex} 次密钥提取询问、q_s 次匿名签密询问和 $q_{H_0},q_{H_1},q_{H_2},q_{H_3}$ 次对 Hash 函数 H_0,H_1,H_2,H_3 的询问),则存在一个算法 B 能够在时间 $t' \leqslant t+q_sO(t_1)$内,以优势 $\varepsilon' \geqslant \varepsilon - \frac{q_{H_1}q_s}{2^k}$ 解决 CDH 问题(其中,t_1 是对运算 e 的运算时间).

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$\langle P,bP,Q=cP\rangle$,其目标为计算出 bcP 或 bQ.B 模拟一个挑战者如定义 4 中所述进行每一步过程.

Setup:B 设定 $P_{pub}=bP$,将 $params=\langle G_1,G_2,q,e,P,P_{pub},H_0,H_1,H_2,H_3\rangle$作为系统参数给 F.收到系统参数以后,F 输出目标身份 ID_s^*.其中,对 H_0,H_1,H_2 和 H_3 的询问如定理 3 中所描述.

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_0-list 中寻找(ID,l,Q),计算 $d=blP$,并返回给 F;
- 匿名签密询问:对于一个关于(m,L,ID_s)(其中,$L=\{ID_1,ID_2,\ldots,ID_t\}$)的签密询问,$B$ 随机选择 $r' \in Z_p^*$ 和 $R' \in G_1$,计算 $U'=r'P$.在 H_1-list 中查找(m,U',h'),得到 h',若未找到,就选择一个 $h' \in Z_q^*$,并将(m,U',h')存入 H_1-list.在 H_0-list 中查找(ID_A,l_A,Q_A),得到 Q_A,如果找不到,就选择一个 $l_A \in Z_q^*$,计算 $Q_A=l_AP$,并将(ID_A,l_A,Q_A)存入 H_0-list,计算 $V'=h'S_A+r'Q_A=l_Abh'P+l_Ar'P=l_A(bh'+r')P$.接下来计算 $Y'=e(br'P+R')$,在 H_2-list 中查找(Y',ρ'),若未找到,就选择一个$\rho' \in \{0,1\}^{l+k}$,并将(Y',ρ')存入 H_2-list,计算 $W'=\rho' \oplus (m\|ID_A)$.$B$ 在 H_3-list 中查找(ID_i,l_i),并计算 $y_i=(l+l_i)U,i=1,2,\ldots,t$,由此得到 $T_i,i \in \{1,2,\ldots,t\}$,最终,$B$ 得到密文 C,并返回给 F.

Forgery:F 生成一个目标密文 $C^*=\langle T_1^*,T_2^*,\ldots,T_t^*,U^*,V^*,W^*\rangle$,如果这个伪造是成功的,则有:

$$e(P,V^*)=e(U^*P_{pub},Q_A)^h.$$

定义 $c=l_Ah$,则 $V^*=hS_h+rQ_A=l_AbhP+rQ_A=bcP+rQ_A$,这样就很容易提取出 CDH 问题的解:$bcP=V^*-rQ_A$.

下面我们考虑 B 成功的优势.由于匿名签密询问中至多进行了 q_{H_1} 次 H_1 询问,故 B 对一个签密询问回答失败的概率不大于 $\frac{q_{H_1}q_s}{2^k}$,所以我们得到 $\varepsilon' \geqslant \varepsilon - \frac{q_{H_1}q_s}{2^k}$, 且 $t' \leqslant t+q_sO(t_1)$(其中,t_1 是对运算 e 的运算时间). □

4.3 性能比较与效率分析

4.3.1 性能比较

与现有的基于身份的多接收者签密方案进行比较,本文提出的方案实现了更为完善的性能,见表 1(部分优缺点分析见第 4.3.2 节).

Table 1 Performance comparison of our scheme with the exiting ones

表 1 本文方案与现有方案的性能比较

方案	加密算法	设计思想	优点	缺点
文献[1]方案	基于身份的加密	双线性技术	提出多接收者签密方案	丢失接收者身份列表;不公平
文献[4]方案	基于身份的加密	双线性技术	添加接收者身份列表	密文长;身份暴露;不公平
文献[5]方案	无证书加密	签密过程无双线性对	高效签密	密钥长;身份暴露;不公平
文献[6]方案	基于身份的加密	多项式技术	短密文	公开参数多;身份暴露;不公平
文献[7]方案	基于身份的加密	双线性技术	公开参数少	密文长;解密过程效率低;身份暴露;不公平
本方案	基于身份的加密	拉格朗日插值多项式	接收者匿名;解密公平;高效	不存在已知安全问题

对表 1 的解释如下:

1) 接收者身份列表

接收者身份列表是现有方案密文中必须要包含的信息,用于指示每个授权接收者根据自己在列表中的位置查找自己所需要的密文信息.

文献[1]中缺少此部分内容(但通过分析,文献[1]的方案事实上是需要接收者身份列表信息的),会导致接收者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.此后的文章中都补充了该列表信息,虽然解决了文献[1]中存在的问题,但却会引发下面 2)和 3)中所描述的安全问题.

2) 接收者匿名性

接收者匿名性要求每一个接收者的身份对攻击者以及其他接收者是匿名的.

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[4−7],密文需要包含一个标志信息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列表,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$\{T_1,T_2,\ldots,T_t\}$中,每个接收者都得不到其他授权的接收者的任何信息,从而使得该方案具有接收者匿名性.

3) 解密公平性

解密公平性要求,一旦消息在传输过程中出错或者被破坏,所有接收者都将以相同的概率得到正确明文信息,要么所有的接收者都不能够正确解密密文信息,要么都可以正确解密密文.

现有方案中,每个接收者需要通过密文中身份列表中自己所在的序列号找到密文信息部分中自己所需要的特定信息后,才可以对密文进行解密,然而一旦传输过程中部分密文信息发生错误,会直接导致部分接收者无法对消息进行解密,而其余接收者却可以解密,故不具有解密公平性.在我们提出的方案中,密文为 $C=\langle T_1,T_2,\ldots,T_t,U,V,W\rangle$,解密过程中所有出现的元素对于每个接收者解密都是必须的,故任何一个元素出错,所有接收者都无法解密得到正确的消息,从而对所有授权的接收者而言解密过程是公平的.

4.3.2 效率分析

下面,我们主要从计算成本和通信量两个方面来比较现有的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) 通信量分析

本文所提出的方案中密文 $C=\langle T_1,T_2,\ldots,T_t,U,V,W\rangle$的长度为$(t+2)|G_1|+|ID|+|m|$.文献[1]中方案的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$(t+3)|G_1|+(t+1)|ID|+|m|$,大于本文所提出的方案.文献[6]中方案虽然密文长度较短,但其系统公开参数至少为$(t+9)$个,数量太多而不利于存储.文献[7]中所提方案虽然系统公开参数较少,但其密文长度为$(t+2)|G_1|+|m|+t|ID|+|Z_q|$,长度过长而不便于传送.综合上述分析,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,而且系统公开参数适中,利于存储.

2) 计算量分析

本文方案中,计算 $f_i(x)=\prod_{1\leqslant j\neq i\leqslant t}\frac{x-x_j}{x_i-x_j}=a_{i,1}+a_{i,2}x+\ldots+a_{i,t}x^{t-1}$, $a_{i,1},a_{i,2},\ldots,a_{i,t}\in Z_q$ 和 $T_i=\sum_{j=1}^{t}a_{j,i}y_i$,$i\in\{1,2,\ldots,t\}$需要一定的计算代价,但是 $f_i(x)$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,它们是本方案中实现相关功能的重要计算步骤;且当选定接收者后,上述运算可以预计算.如果不统计这两步的计算量,则本文方案仅需 1 次双线性对计算、$(t+1)$次加运算、$(t+4)$次乘运算和 3 次 Hash 运算,无需指数运算(这里的加运算、乘运算和指数运算分别指 G_1,G_2 和 Z_q 中的加运算、乘运算和指数运算次数的总和).所以,计算量与文献[1,4−7]中方案比较起来也具有很大的优势.具体比较结果见表 2.

Table 2 Signcryption efficiency comparison of our scheme with the exiting ones

表 2 本文方案与现有方案的签密效率比较

方案	对运算	加法运算	乘法运算	指数运算	Hash运算	密文长度	公开参数
文献[1]方案	1	0	6	t+4	3	(t+3)$\|G_1\|$+$\|ID\|$+$\|m\|$	10
文献[4]方案	1	t+1	t+5	1	2	(t+2)$\|G_1\|$+$\|G_2\|$+$\|m\|$+$t\|ID\|$	10
文献[5]方案	0	t+1	t+3	t+1	4	$2t\|G_1\|$+$\|m\|$+$t\|ID\|$+$t\|Z_q\|$	12
文献[6]方案	0	t+1	t+3	1	2	$3\|G_1\|$+$\|m\|$+$t\|ID\|$	t+9
文献[7]方案	2	t+1	t+4	2	2	(t+2)$\|G_1\|$+$\|m\|$+$t\|ID\|$+$\|Z_q\|$	8
本方案	1	t+1	t+4	0	3	(t+2)$\|G_1\|$+$\|ID\|$+$\|m\|$	10

$|G_1|$:G_1 中元素的长度,$|ID|$:身份信息 ID 的长度,$|m|$:明文消息 m 的长度,$|Z_q|$:Z_q 中元素的长度,t:指定接收者的人数

5 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,以安全且可认证的方式广播消息给多个授权用户.本文针对现有的多接收者签密方案中存在的接收者身份暴露和解密不公平性等问题,提出了一个新的基于身份的多接收者签密方案.该方案不仅满足保密性和不可伪造性,还满足接收者匿名性以及解密公平性.同时,给出了在随机预言模型下的 IND-sMIBSC-CCA 和 MEUF-sMIBSC-CMA 安全性证明,并通过与现有方案的对比,分析了本方案的性能与效率,从而证明该方案是安全、有效的.

致谢 衷心感谢匿名审稿专家对本文提出的问题与质疑以及所提供的修改建议.

References:

[1] Duan S, Cao Z. Efficient and provably secure multi receiver identity based signcryption. In: Batten L, Safavi-Naini R, eds. Proc. of the 11th Australasian Conf. on Information Security and Privacy (ACISP 2006). LNCS 4058, Heidelberg: Springer-Verlag, 2006. 195−206. [doi: 10.1007/11780656_17]

[2] Bellare M, Boldyreva A, Micali S. Public-Key encryption in a multi-user setting: Security proofs and improvements. In: Naor M, ed. Proc. of the Advances in Cryptology (Eurocrypt 2000). LNCS 1807, Heidelberg: Springer-Verlag, 2000. 259−274. [doi: 10.1007/3-540-45539-6_18]

[3] Baudron O, Pointcheval D, Stern J. Extended notions of security for multicast public key cryptosystems. In: Widmayer P, Francisco T, *et al*., eds. Proc. of the 29th Int'l Colloquium on Automata, Languages and Programming (ICALP 2000). LNCS 1853, Heidelberg: Springer-Verlag, 2000. 499−511. [doi: 10.1007/3-540-45022-X_42]

[4] Yu Y, Yang B, Huang X, Zhang M. Efficient identity-based signcryption scheme for multiple receivers. In: Xiao B, *et al*., eds. Proc. of the 4th Int'l Conf. on Autonomic and Trusted Computing (ATC 2007). LNCS 4610, Heidelberg: Springer-Verlag, 2007. 13−21. [doi: 10.1007/978-3-540-73547-2_4]

[5] Sharmila S, Shukla D, Rangan P. Efficient and provably secure certificateless multi-receiver signcryption. In: Baek J, *et al*., eds. Proc. of the 2nd Int'l Conf. on Provable Security (ProvSec 2008). LNCS 5324, Heidelberg: Springer-Verlag, 2008. 52−67. [doi: 10.1007/978-3-540-88733-1_4]

[6] Sharmila S, Sree S, Srinivasan R, Pandu C. An efficient identity-based signcryption scheme for multiple receivers. In: Takagi T, Mambo M, eds. Proc. of the 4th Int'l Workshop on Security (IWSEC 2009). LNCS 5824, Heidelberg: Springer-Verlag, 2009. 71−88. [doi: 10.1007/978-3-642-04846-3_6]

[7] Elkamchouchi H, Abouelseoud Y. MIDSCYK: An efficient provably secure multirecipient identity-based signcryption scheme. In: Hossam M, Watheq M, *et al*., eds. Proc. of the 2009 Int'l Conf. on Networking and Media Convergence (ICNM 2009). Piscataway: IEEE Press, 2009. 70−75. [doi: 10.1109/ICNM.2009.4907192]

[8] Zheng Y. Digital signcryption or how to achieve *cost*(*signature* & *encryption*)<<*cost*(*signature*)+*cost*(*encryption*). In: Burton S, ed. Proc. of the Advances in Cryptology (CRYPTO'97). LNCS 1294, Heidelberg: Springer-Verlag, 1997. 165−179. [doi: 10.1007/BFb0052234]

[9] Shin JB, Lee K, Shim K. New DSA-verifiable signcryption schemes. In: Lee P, Lim C, eds. Proc. of the 5th Int'l Conf. on Information Security and Cryptology (ICISC 2002). LNCS 2587, Heidelberg: Springer-Verlag, 2003. 35−47. [doi: 10.1007/3-540-36552-4_3]

[10] Malone-Lee J. Identity-Based signcryption. IACR Cryptology ePrint Archive: Report 2002/098 (2002), 2002. http://eprint.iacr.org/2002/098.pdf

[11] Malone-Lee J, Mao W. Two birds one stone: Signcryption schemes using RSA. In: Joye M, ed. Proc. of the Cryptographer's Track at RSA Conf. (CT-RSA 2003). LNCS 2612, Heidelberg: Springer-Verlag, 2003. 211−226. [doi: 10.1007/3-540-36563-X_14]

[12] Libert B, Quisquator J. A new identity based signcryption scheme from pairings. In: Ezio B, Vahid T, eds. Proc. of the 2003 IEEE Information Theory Workshop. Piscataway: IEEE Press, 2003. 155−158. [doi: 10.1109/ITW.2003.1216718]

[13] Boneh D, Franklin M. Identity-Based encryption from the Weil pairing. In: Kilian J, ed. Proc. of the Advances in Cryptology (CRYPTO 2001). LNCS 2139, Heidelberg: Springer-Verlag, 2001. 213−229. [doi: 10.1007/3-540-44647-8_13]

[14] Pang LJ, Li HX, Jiao LC, Wang YM. Design and analysis of a provable secure multi-recipient public key encryption scheme. Ruan Jian Xue Bao/Journal of Software, 2009,20(10):2907−2914 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/3552.htm [doi: 10.3724/SP.J.1001.2009.03552]

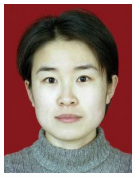
[15] Lal S, Kushwah P. Anonymous ID based signcryption scheme for multiple receivers. IACR Cryptology ePrint Archive: Report 2009/345 (2009), 2009. http://eprint.iacr.org/2009/345.pdf

[16] Zhang B, Xu QL. An ID-based anonymous signcryption scheme for multiple receivers secure in the standard model. In: Kim T, Adeli H, eds. Proc. of the AST/UCMA/ISA/ACN 2010 Conf. on Advances in Computer Science and Information Technology (AST/ UCMA/ISA/ACN 2010). LNCS 6059, Heidelberg: Springer-Verlag, 2010. 15−27. [doi: 10.1007/978-3-642-13577-4_2]

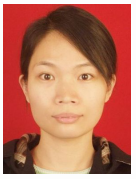
附中文参考文献:

[14] 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):2907−2914. http://www.jos.org.cn/1000-9825/3552.htm [doi: 10.3724/SP.J.1001.2009.03552]

庞辽军(1978－),男,陕西渭南人,博士,教授,博士生导师,CCF 高级会员,主要研究领域为密码学,安全协议设计与分析.
E-mail: ljpang@mail.xidian.edu.cn



李慧贤(1977－),女,博士,副教授,CCF 会员,主要研究领域为多接收者签密及应用研究.
E-mail: lihuixian@nwpu.edu.cn



崔静静(1986－),女,硕士生,主要研究领域为网络与信息安全.
E-mail: cuijj102@yahoo.com.cn

王育民(1936－),男,教授,博士生导师,主要研究领域为信息论,密码,编码.
E-mail: ymwang@xidian.edu.cn