软件学报 ISSN 1000-9825, CODEN RUXUEW
Journal of Software,2018,29(2):442−455 [doi: 10.13328/j.cnki.jos.005250]
©中国科学院软件研究所版权所有.
E-mail: jos@iscas.ac.cn
http://www.jos.org.cn
Tel: +86-10-62562563

基于身份的多接收者(多消息)匿名混合签密机制*

周彦伟[1,3], 杨 波[1,3], 王青龙[2]

[1](陕西师范大学 计算机科学学院,陕西 西安 710062)

[2](长安大学 信息工程学院,陕西 西安 710064)

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

通讯作者: 杨波, E-mail: byang@snnu.edu.cn

摘 要: 为了满足广播环境下通信数据的机密性和认证性需求以及消息收发双方的匿名性,提出了基于身份的多接收者匿名混合签密机制,满足收发双方的匿名性保护需求,并且接收者具有解密独立性.正确性分析及安全性证明表明,该机制是安全、有效的多接收者匿名混合签密机制.相对于现有方案,除了具有保密性和不可伪造性之外,该机制具有更优的性能,如更高的匿名性、公开验证性等.将该机制改进后,提出了具有收发双方匿名性、公开验证性、不可否认性等安全属性的多接收者多消息混合签密机制,实现了广播通信环境下用户的多消息发送需求.

关键词: 混合签密;多接收者;多消息;匿名性;认证性;机密性

中图法分类号: TP309

中文引用格式: 周彦伟,杨波,王青龙.基于身份的多接收者(多消息)匿名混合签密机制.软件学报,2018,29(2):442−455. http://www.jos.org.cn/1000-9825/5250.htm

英文引用格式: Zhou YW, Yang B, Wang QL. Anonymous hybrid signcryption scheme with multi-receiver (multi-message) based on identity. Ruan Jian Xue Bao/Journal of Software, 2018,29(2):442−455 (in Chinese). http://www.jos.org.cn/1000-9825/5250.htm

Anonymous Hybrid Signcryption Scheme with Multi-Receiver (Multi-Message) Based on Identity

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

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

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

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

Abstract: Authentication and confidentiality, as well as sender and receiver anonymity are essential in broadcast communication. In this paper, an anonymous hybrid signcryption scheme with multi-receiver is proposed using identity-based cryptography. The proposal does not contain receiver's identity list, and the identity of sender is included in an identity set. Thus, it not only obtains the receiver's anonymity, but also achieves the sender's anonymity. Additionally, the proof of security and the analysis of correctness demonstrate that

* 基金项目: 国家重点研发计划(2017YFB0802000); 国家自然科学基金(61572303, 61772326); 信息安全国家重点实验室(中国科学院信息工程研究所)开放课题(2017-MS-03); "十三五"国家密码发展基金(MMJJ20170216); 中央高校基本科研业务费专项资金(GK201702004)

Foundation item: National Key Research and Development Program of China (2017YFB0802000); National Natural Science Foundation of China (61572303, 61772326); Foundation of State Key Laboratory of Information Security (Institute of Information Engineering, The Chinese Academy of Sciences) (2017-MS-03); National Cryptography Development Fund during the "13th Five-year Plan" Period (MMJJ20170216); Fundamental Research Funds for the Central Universities (GK201702004)

收稿时间: 2016-09-18; 修改时间: 2016-11-17; 采用时间: 2016-12-29; jos 在线出版时间: 2017-03-24

CNKI 网络优先出版: 2017-03-24 17:09:30, http://kns.cnki.net/kcms/detail/11.2560.TP.20170324.1709.010.html

© 中国科学院软件研究所 http://www.jos.org.cn

the scheme is secure and effective. Compared with the pre-existing schemes, the proposal enjoys better performances in many perspectives, including confidentiality, unforgeability, higher anonymity of sender and receiver and public verifiability. Moreover, the presented method can be improved to develop an efficient construction of hybrid signcryption scheme with multi-message and multi-receiver, which can obtain these security properties, such as sender and receiver anonymity, public verifiability and non-repudiation. Finally, the new variant can achieve the requirement of sending multi-message in broadcast communication.

Key words: hybrid signcryption; multi-receiver; multi-message; anonymity; authentication; confidentiality

为了抵抗网络通信技术快速发展造成的各种攻击,用户期望通信数据能够同时满足保密性和认证性.通常,保密性由加密操作实现,而认证性由签名机制完成.然而,传统的先签名后加密的方法将导致整体方案的计算效率较低.针对传统方式所存在的上述不足,签密的密码学原语最早在文献[1]中提出,实现了加密和签名操作的同时进行,在一定程度上提高了方案的计算效率.后来,文献[2,3]在混合加密[4]的基础上提出了混合签密的概念,继承了混合加密的优势,很好地解决了传统签密方案中消息长度受限的不足.同时,伴随着广播通信技术的发展,增强了消息传输的效率,发送者可同时向多人发送消息.多接收者签密机制实现了向多人发送同一消息的目的,比传统方式更有效、更适用于广播等通信业务.广播通信的应用需求,推进了对多接收者签密机制的研究.

随着网络环境的复杂化,用户越来越重视自身隐私信息的保护,发送者往往期望通信数据仅有其指定的用户才能获悉,并且接收者只能完成消息合法性的验证和来源可靠性的判断,根本无法掌握发送者的身份等隐私信息;对于接收者而言,更不希望自己的身份被外界所知悉.由此可见,对收发双方均匿名的多接收者混合签密机制的研究已成为该领域当前的研究热点.然而,现有的多接收者签密机制要么忽视接收者的匿名性保护需求,要么发送者的强匿名性导致发送者对已有的签密事实进行否认.

针对上述不足,本文提出了基于身份的多接收者匿名混合签密机制,其中,利用随机身份集合实现发送者的伪装混淆;接收者身份列表的删除实现接收者的身份隐藏;接收者解密过程无需除自己之外的其他接收者的相关信息,满足接收者解密独立性的要求.本文的机制在实现收发双方匿名性的同时,对发送者匿名性实现可控操作,因此,发送者无法否认已有的签密事实.同时,本文的改进机制在继承原始机制安全性及匿名性的基础上,为发送者提供多消息发送功能.

1 研究现状

1.1 多接收者签密机制

要向多个接收者发送消息时,传统签密机制[1,5,6]在执行效率和实效性等方面存在不足.为了弥补上述不足,综合签密和多接收者加密的思想,提出了多接收者签密方案[7].近年来,针对广播通信的应用需求,国内外研究者相继提出了多个多接收者(匿名)签密方案[8−20].

现有的多接收者签密机制要么不涉及匿名性的考虑,要么忽视对接收者的匿名性保护,仅提供发送者的匿名性.然而,由于匿名性是不可控的,导致发送者能够对已有的签密事实进行否认.事实上,传统方案为了确保每位接收者都能正确解密密文,在密文中均包含了接收者的身份列表,接收者身份列表的发送及匿名的不均衡性导致相关方案[11−19]存在下述不足.

(1) 接收者的匿名性保护需求被忽视.为了保证接收者对密文的正确解密,授权接收者的身份列表(部分机制采用密文标记列表)随密文发送将导致接收者身份隐私信息的泄露.

(2) 发送者的匿名性是不可控的.部分方案仅注重发送者的匿名性,但是当发送者否认已有的签密事实或存在恶意行为时,由于发送者具有强匿名性,导致任意的接收者及包括密钥生成中心在内的任何第三方都无法获知具体的发送者信息,所以发送者很容易否认已有的签密事实.

现有的多接收者匿名签密机制[11−15]存在接收者身份易暴露的不足.文献[17−19]分别提出了相应的多接收者签密机制,但是上述机制[17−19]却忽视了对发送者匿名可控性的研究.事实上,不仅发送者渴望保护个人身份、地址等隐私信息,而且接收者同样希望个人隐私信息得到保护.为满足收发双方对个人隐私信息的保护需求,文

© 中国科学院软件研究所 http://www.jos.org.cn

献[16]提出了一种新的基于身份的多接收者匿名签密方案,遗憾的是,该方案解签密时却忽略了对密文进行合法性验证;并且发送者的匿名性不具有可控性,导致该方案的实际应用性较弱.文献[20]虽然能够满足广播环境下的多消息发送需求,但是无法实现收发双方的匿名性.因此,在追求多接收者和多消息发送的同时,必须对收发双方均实施匿名性保护,并且发送者的匿名性必须是可控的.

1.2 混合签密

文献[4]在对混合密码理论形式化定义和分析的基础上,提出了著名的混合加密结构.该结构由两部分组成,即密钥封装机制(key encapsulation mechanism,简称 KEM)与数据封装机制(data encapsulation mechanism,简称 DEM).其中,KEM 部分产生一个随机密钥和对该密钥的加密密文;DEM 利用 KEM 中得到的加密密钥,用对称加密算法对真正的待加密消息进行加密.文献[21]提出了混合加密机制的新属性——公开可验证性,该属性的提出增强了混合加密机制的安全性,使其具有更广泛的应用领域.

文献[2,3]借鉴混合加密[4]的思想提出了混合签密的概念,混合签密机制同样由 KEM 和 DEM 两部分组成,其中,对称的加密密钥由 KEM 生成,DEM 完成对通信数据的加密.文献[22]深入研究了混合签密机制,详细介绍了该机制的安全性定义及模型,在混合签密研究领域取得了重大进展.文献[23]提出了一个安全的无证书混合签密方案,并且具有密文长度短、运算速度快的优点,适用于计算资源和带宽均受限的通信环境,满足可认证性和保密性.遗憾的是,该方案不具有不可否认性和匿名性,而且无法满足其所声称的不可伪造性[24].文献[23,24]仅能完成单一接收者的混合签密操作,无法满足多接收者的消息发送需求.文献[25,26]提出了多接收者的混合签密机制,虽然具有多接收者的属性,却无法实现发送者的多消息发送需求.

综上所述,目前对多接收者多消息混合签密机制的研究较少,因此,非常有必要研究匿名混合签密机制在广播环境下实现用户的多消息发送需求.

2 预备知识

2.1 双线性映射

设 G_1 和 G_2 分别为阶是大素数 q 的循环群,P 为群 G_1 的一个生成元.当映射 $e:G_1\times G_1\to G_2$ 满足下列性质时,称 e 是一个双线性映射.

(1) 双线性:$e(aP,bQ)=e(P,Q)^{ab}$,对所有的 $P,Q\in G_1$, $a,b\in Z_q^*$ 均成立;

(2) 非退化性:对于任意的 $P,Q\in G_1$,使得 $e(P,Q)\neq 1_{G_2}$, 其中,1_{G_2} 为 G_2 的单位元;

(3) 可计算性:对于任意的 $P,Q\in G_1$,能够在多项式时间内完成 $e(P,Q)$的计算.

2.2 困难性问题

- 计算性 Diffie-Hellman(computational diffie-Hellman,简称 CDH)问题.

设 G 为阶是大素数 q 的循环群,P 为群 G 的生成元.对于任意的概率多项式时间敌手(probabilistic polynomial time,简称 PPT)算法$\mathcal{A}$,解决 CDH 问题的概率 $Adv_{\mathcal{A}}^{CDH}(k)=\Pr[\mathcal{A}(P,aP,bP)=abP]$ 是可忽略的.

- 双线性 Diffie-Hellman(bilinear diffie-Hellman,简称 BDH)问题.

设 G_1,G_2 分别为阶是大素数 q 的循环群,P 为群 G_1 的一个生成元.$e:G_1\times G_1\to G_2$ 是定义在群 G_1 和 G_2 上的双线性映射.对任意的 PPT 算法$\mathcal{A}$,解决 BDH 问题的概率 $Adv_{\mathcal{A}}^{BDH}(k)=\Pr[\mathcal{A}(P,aP,bP,cP)=e(P,P)^{abc}]$ 是可忽略的.

2.3 目标抗碰撞

令 $\mathcal{H}_I$ 是单向哈希函数 $H_i:\mathcal{X}\to\mathcal{Y}$的集合.随机选取 $H_i\in\mathcal{H}_I$,若对于任意的 PPT 敌手$\mathcal{A}$,概率 $Adv_{\mathcal{H}_I}^{TCR}(k)=\Pr[H_i(x)=H_i(x')\wedge x\neq x']$(其中,$x\leftarrow\mathcal{X},x'\leftarrow\mathcal{A}(x,H_i(x))$)在 k 范围内是可忽略的概率,则称哈希函数集合$\mathcal{H}_I$是目标抗碰撞的.

© 中国科学院软件研究所 http://www.jos.org.cn

2.4 基于身份的多接收者(多消息)混合签密机制

基于身份的多接收者(多消息)混合签密机制由下述多项式时间算法组成.

(1) 系统建立算法(Setup).输入安全参数 k,输出相应的系统公开参数 $Params$ 和主密钥 S_{msk},同时,对外公布 $Params$,秘密保存 S_{msk},则有($Params$,S_{msk})←$Setup$(1^k).其中,$Params$ 为下述 3 种算法的公共输入.

(2) 密钥生成算法(KeyGen).输入用户身份 ID,输出身份 ID 所对应的公私钥信息(PK_{ID},SK_{ID}),则有:

$$(PK_{ID},SK_{ID})\leftarrow KeyGen(Params,ID,S_{msk}).$$

(3) 混合签密算法(HSign).输入待加密消息 M、发送者身份 ID_S 和接收者身份集合 $R_{ID}=\{ID_{R_1},...,ID_{R_n}\}$,输出相应的签密密文 δ,则有 $\delta\leftarrow HSign(Params,M,ID,R_{ID})$.特别地,发送者进行多消息发送时,$M$ 是待加密消息的集合,即 $M=(M_1,\ldots,M_n)$.

(4) 解签密算法(UnHSign).输入签密密文 δ、接收者的身份 ID_{R_i} ($i\in[1,n]$) 和私钥信息 $SK_{ID_{R_i}}$,输出相应的明文 M,则有 $M\leftarrow UnHSign(Params,\delta,ID_{R_i},SK_{ID_{R_i}})$.

对于身份空间 $\mathcal{ID}$,消息空间 $\mathcal{M}$ 及所有($Params$,S_{msk})←$Setup$(1^k), $ID_S,ID_{R_i}\in\mathcal{ID}(i\in[1,n]),R_{ID}=\{ID_{R_1},...,D_{R_n}\}$, $(PK_{ID_S},SK_{ID_S})\leftarrow KeyGen(Params,ID_S,S_{msk})$, $(PK_{ID_{R_i}},SK_{ID_{R_i}})\leftarrow KeyGen(Params,ID_{R_i},S_{msk})$, $M\in\mathcal{M}$ 和 $\delta\leftarrow HSign$ ($Params$,M,ID,R_{ID}),有 $M\leftarrow UnHSign(Params,\delta,ID_{R_i},SK_{ID_{R_i}})$ 成立.

2.5 安全模型

本节分别详细介绍选择密文攻击下的保密性和选择消息攻击下的不可伪造性等安全属性的定义及游戏交互过程.当下述安全性模型推广到多消息模式时,待加密消息 M 是一个消息集合 $M=\{M_1,\ldots,M_n\}$,因此,对多消息模式的安全模型不再赘述.

2.5.1 保密性

定义 1(保密性)[16]. 在下述游戏中,若不存在 PPT 敌手 $\mathcal{A}$ 能够以不可忽略的优势获胜,则称基于身份的多接收者匿名混合签密机制具有保密性.敌手 $\mathcal{A}$ 与挑战者 $\mathcal{C}$ 间的交互过程如下所述.

初始化:$\mathcal{C}$ 运行初始化算法生成主密钥 S_{msk} 及公开参数 $Params$,将 $Params$ 发送给 $\mathcal{A}$,秘密保存 S_{msk}.

阶段 1:$\mathcal{A}$ 向 $\mathcal{C}$ 进行如下询问.

密钥生成询问:$\mathcal{C}$ 收到 $\mathcal{A}$ 关于身份 ID 的密钥生成询问后,运行密钥生成算法$\langle PK_{ID},SK_{ID}\rangle=KeyGen(Params,S_{msk},ID)$,返回相应的$\langle PK_{ID},SK_{ID}\rangle$给 $\mathcal{A}$;特别地,在方案的具体证明过程中,密钥生成询问可分解为公钥生成询问和私钥生成询问.

混合签密询问:$\mathcal{C}$ 收到 $\mathcal{A}$ 关于待加密消息 M、发送者身份 ID_S 和接收者身份集合 $R_{ID}=\{ID_{R_1},...,ID_{R_n}\}$ 的混合签密询问后,返回相应的密文 $\delta=HSign(Params,M,ID,R_{ID})$给 $\mathcal{A}$.

解混合签密询问:$\mathcal{C}$ 收到 $\mathcal{A}$ 关于密文 δ 和接收者身份 ID_{R_j} 的解签密询问后,$\mathcal{C}$ 对 ID_{R_j} 进行密钥生成询问,并获得相应的应答私钥 $SK_{ID_{R_j}}$ 后,返回相应的结果 $M/\perp=UnHSign(Params,\delta,ID_{R_j},SK_{ID_{R_j}})$ 给 $\mathcal{A}$,其中,$\perp$ 表示输入的密文无效.

挑战:$\mathcal{A}$ 选取两个等长的消息 M_0 和 M_1,发送挑战消息(M_0,M_1)、发送者身份 ID_S 和接收者身份集合 $R_{ID}=\{ID_{R_1},...,ID_{R_n}\}$ 给 $\mathcal{C}$.$\mathcal{C}$ 返回挑战密文 $\delta=HSign(Params,M_b,ID_S,R_{ID})$给 $\mathcal{A}$,其中,$b\leftarrow\{0,1\}$.

阶段 2:$\mathcal{A}$ 像阶段 1 中那样进行多次询问,但该阶段中不能对接收者身份集合 R_{ID} 中的任何信息进行私钥生成询问,并且禁止对挑战密文 δ 进行解混合签密询问;同时,不能对仅在接收者身份集合部分与挑战密文 δ 不同的密文进行解混合签密询问.

猜测:$\mathcal{A}$ 输出对随机数 b 的猜测 b',若 $b'=b$,则 $\mathcal{A}$ 赢得这场游戏.

如上所述,$\mathcal{A}$ 赢得上述游戏的优势是 $Adv_{IT,\mathcal{A}}(k)=\left|\Pr[b=b']-\frac{1}{2}\right|$.

© 中国科学院软件研究所 http://www.jos.org.cn

2.5.2 不可伪造性

定义 2(不可伪造性)[16]. 下述游戏中,若不存在 PPT 敌手$\mathcal{A}$能够以不可忽略的优势获胜,则称基于身份的多接收者匿名混合签密机制具有不可伪造性.敌手$\mathcal{A}$与挑战者$\mathcal{C}$间的交互过程如下所述.

初始化:$\mathcal{C}$运行初始化算法生成主密钥 S_{msk} 和公开参数 *Params*,将 *Params* 发送给$\mathcal{A}$,秘密保存 S_{msk}.

询问:$\mathcal{A}$向$\mathcal{C}$进行一系列询问,具体询问过程如定义 1 所述.

伪造:$\mathcal{A}$输出关于加密消息 M、发送者身份 ID_S 和接收者身份列表 $R_{ID}=\{ID_{R_1},...,ID_{R_n}\}$ 的伪造密文δ.若δ是关于 M 的有效密文,则$\mathcal{A}$赢得游戏.特别地,$\mathcal{A}$不能对 ID_S 和 ID_{R_j} $(j=1,2,...,n)$ 进行密钥生成询问,并且δ不能是混合签密询问的应答.$\mathcal{A}$的优势为其伪造密文成功的优势.

3 本文机制

本文中假设所有的通信过程都是安全的,通信过程中数据被篡改或破坏的情况本文忽略不予考虑,即所有接收者都将收到完整的密文.

3.1 方案构造

3.1.1 初始化

初始化算法由密钥生成中心(private key generation,简称 PKG)负责执行,具体操作如下.

(1) 选择阶是大素数 q 的循环群 G_1 和 G_2,P 是群 G_1 的一个生成元,定义群 G_1 和 G_2 上的双线性映射 $e:G_1\times G_1\to G_2$.令$\mathcal{ID}$是身份空间;设 $Enc(K,\cdot)$和 $Dec(K,\cdot)$是密钥空间为$\mathcal{K}$的对称加密/解密算法.

(2) 定义抗碰撞的哈希函数:$H_1:\mathcal{ID}\to G_1$,$H_2:G_1\times G_2\to\mathcal{K}$, $H_3:G_1\times Z_q^*\to Z_q^*$,$H_4:\{0,1\}^*\to Z_q^*$,其中,$\{0,1\}^*$表示任意长度的字符串(为方便表述,将多个变量的拼接视为字符串).

(3) 定义索引函数 $f_{Index}:\mathcal{ID}\to Z_q^*$,$f_{Index}(ID)$将身份标识 ID 映射到 Z_q^*,本文机制中,f_{Index}的作用是协助接收者从密文集合中准确定位相应的密文,即,$f_{Index}(ID)$生成参数的下标.

(4) 随机选取主密钥 $S_{msk}\in Z_q^*$ 并秘密保存,计算系统公钥 $P_{Pub}=S_{msk}P$,随机选取 $P_0\in G_1$,设置系统公开参数 $Params=\{q,P,G_1,G_2,e,P_0,P_{Pub},H_1,H_2,H_3,H_4,f_{index},Enc,Dec\}$是下述 3 种算法的公共输入.

3.1.2 密钥生成

收到用户 ID 的密钥生成请求后,PKG 执行下述操作.

计算 $PK_{ID}=H_1(ID)$和 $SK_{ID}=S_{msk}PK_{ID}$,输出用户 ID 的公私钥对$\langle PK_{ID},SK_{ID}\rangle$,同时,PKG 保存元组$\langle ID,SK_{ID},PK_{ID}\rangle$到本地数据库以实现用户匿名的可控性.特别地,本文中使用身份哈希值作为公钥.

3.1.3 混合签密

令 M 是待签密的消息,ID_{Alice} 是发送者 Alice 的身份, $R_{ID}=\{ID_{R_1},ID_{R_2},...,ID_{R_n}\}$ 是授权接收者集合.具体过程如下所述.

(1) 从身份空间$\mathcal{ID}$中随机选取 $m-1$ 个互不相同的身份 $ID_l(l=1,\ldots,m-1)$,对于任意的索引 $l\in[1,m-1]$,有 $ID_l\notin R_{ID}$ 和 $ID_l\neq ID_{\text{Alice}}$ 成立;使用选取的随机身份 $ID_l(l=1,\ldots,m-1)$和发送者身份 ID_{Alice} 构造发送者伪装集合 $S_{ID}=\{ID_1,ID_2,\ldots,ID_m\}$,即 $ID_{\text{Alice}}\in S_{ID}$.特别地,令 I_{Alice} 为 Alice 在集合 S_{ID} 中的位置下标,对任意的接收者和敌手而言,I_{Alice} 是完全隐藏的,即 I_{Alice} 具有完全匿名性.此外,发送者身份伪装集合和授权接收者身份集合是不相交的,即有 $S_{ID}\cap R_{ID}=\varnothing$成立.

(2) 选取随机数 $r_{\text{Alice}}\in Z_q^*$,对于任意满足条件 $i\neq I_{\text{Alice}}$ 的索引 $i\in[1,m]$,选取相应的随机数 $R_i\in Z_q^*$,计算:

$$R_{I_{\text{Alice}}}=r_{\text{Alice}}-\sum_{i=1,i\neq I_{\text{Alice}}}^{m}(R_i+h_i),$$

其中,$h_i=H_3(PK_i,R_i)$,$PK_i=H_1(ID_i)$是伪装身份 ID_i 的公钥,构造集合$\mathcal{R}=\{R_1,R_2,\ldots,R_m\}$;

计算 $Q_{\text{Alice}}=r_{\text{Alice}}+h_{\text{Alice}}$,其中, $h_{\text{Alice}}=H_3(PK_{\text{Alice}},R_{I_{\text{Alice}}})$, $PK_{\text{Alice}}=H_1(ID_{\text{Alice}})$是 Alice 的公钥;对于满足条件 $i\neq I_{\text{Alice}}$ 的索引 $i\in[1,m]$,选取任意的随机值 $c_i\in G_1$,构造集合$\mathcal{C}=\{c_1,c_2,\ldots,c_m\}$,其中,

© 中国科学院软件研究所 http://www.jos.org.cn

$$c_{I_{\text{Alice}}}=h_{\text{Alice}}PK_{\text{Alice}}-\sum_{i=1,i\neq I_{\text{Alice}}}^{m}(c_i+h_iPK_{S_i}).$$

(3) 选取秘密随机数 $d\in Z_q^*$,计算 $U=e(P_{Pub},dP_0)$,$D=dP$ 和 $\omega=Enc(K,M)$,其中,$K=H_2(U,D)$为数据封装密钥.

(4) 对于每个授权接收者 $ID_j\in R_{ID}(j=1,\ldots,n)$,生成相应的索引 $R_j=f_{Index}(ID_j)$后,分别计算 $Z_{R_j}=e(P_{Pub},dPK_j)$ 和 $N_{R_j}=d(P_0+PK_j)$, 其中,$PK_j=H_1(ID_j)$为接收者 ID_j 的公钥,构造集合 $\mathcal{Z}=\{Z_{R_1},\ldots,Z_{R_n}\}$ 和 $\mathcal{N}=\{N_{R_1},\ldots,N_{R_n}\}$.

(5) 计算发送者身份的匿名控制信息 $T=e(Q_{\text{Alice}}P,h_{\text{Alice}}SK_{\text{Alice}})$和消息签名 $V=dP_{Pub}+f_Hh_{\text{Alice}}SK_{\text{Alice}}$,其中,$f_H=H_4(\omega\|D\|T\|\mathcal{R}\|\mathcal{C}\|\mathcal{Z}\|\mathcal{N}\|S_{ID})$(本文中符号"‖"表示拼接操作);最后,输出相应的密文 $\delta=\langle\omega,V,D,T,\mathcal{R},\mathcal{C},\mathcal{Z},\mathcal{N},S_{ID}\rangle$.

特别地,收到广播密文 δ 后,对于任意的敌手和接收者而言,获知发送者的具体索引 I_{Alice} 是不可能的,因此无法通过重新构造集合 $\mathcal{R}$ 的方式伪造发送者的合法签密密文.本文机制中,索引 I_{Alice} 的保密性可保证任何敌手都无法重构集合 $\mathcal{R}$.

3.1.4 解签密

令 ID_{Bob} 是接收者 Bob 的身份信息,SK_{Bob} 是 Bob 的私钥.收到密文 $\delta=\langle\omega,V,D,T,\mathcal{R},\mathcal{C},\mathcal{Z},\mathcal{N},S_{ID}\rangle$后,具体的解签密过程如下所述.

(1) 验证密文的合法性

基于等式(1)验证密文 δ 中签名的正确性:若该等式成立,则 δ 是完整的密文;否则,退出并输出无效信息⊥,拒绝解密 δ.同时,等式(1)也验证了密钥参数 D 的合法性.

$$e(V,P)=e\left(\frac{f_H}{2}\sum_{i=1}^{m}(c_i+h_iPK_i)+D,P_{Pub}\right) \tag{1}$$

其中,$f_H=H_4(\omega\|D\|T\|\mathcal{R}\|\mathcal{C}\|\mathcal{Z}\|\mathcal{N}\|S_{ID})$,$PK_i=H_1(ID_i)$是身份 $ID_i\in S_{ID}$ 的公钥,$h_i=H_3(PK_i,R_i)$.

(2) 验证发送者的身份合法性

若等式(2)成立,则发送者是伪装集合 S_{ID} 中的有效成员之一;否则,退出并输出无效信息⊥,拒绝解密 δ.同时,该等式验证了匿名性控制参数 T 的合法性.对任意的敌手和接收者而言,成功猜测真实发送者身份的概率是 $\frac{1}{m}$.

$$T=e\left(P_{Pub}\sum_{i=1}^{m}(R_i+h_i),\frac{1}{2}\sum_{i=1}^{m}(c_i+h_iPK_i)\right) \tag{2}$$

(3) 验证接收者身份的合法性

若 $Z_{\text{Bob}}=e(E,SK_{\text{Bob}})\notin\mathcal{Z}$,则 Bob 不是合法的授权接收者,则退出并输出无效信息⊥,拒绝解密 δ;否则,Bob 是授权接收者,可进行解密操作.

(4) 解密密文

① 计算索引 $J_{\text{Bob}}=f_{index}(ID_{\text{Bob}})$,根据索引,$J_{\text{Bob}}$ 从 $\mathcal{N}$ 中获知相应参数 $N_{J_{\text{Bob}}}=d(P_0+PK_{\text{Bob}})$ 后,计算:

$$U=e(P_{Pub},N_{J_{\text{Bob}}})e(D,SK_{\text{Bob}})^{-1};$$

② 输出明文消息 $M=Dec(K,\omega)$,其中,$K=H_2(U,D)$.

3.1.5 匿名的可控性

在传统方案中,由于发送者具有强匿名性,致使密文接收者无法从发送者伪装集合中准确定位发送者的具体身份;而本文机制中,当密文发送者对签密事实进行否认或发送者进行恶意签密操作时,接收者可基于发送者匿名控制策略撤销发送者的匿名性.当发送者 Alice 否认其所进行的签密操作或有恶意行为发生时,接收者 Bob 可向 PKG 申请撤销 Alice 的匿名性.具体操作过程如下.

Bob 将 $\delta=\langle\omega,V,D,T,\mathcal{R},\mathcal{C},\mathcal{Z},\mathcal{N},S_{ID}\rangle$发送给 PKG,向 PKG 提出撤销 Alice 匿名性的申请.

PKG 首先评估 Bob 匿名性撤销请求的合法性(撤销请求的合法性检测并非本文的核心研究内容,此处不再赘述),有效杜绝 Bob 非法撤销行为的发生;撤销请求的合法性验证通过后,根据伪装集合 S_{ID} 记录的相关身份信息计算相应的参数 $\sum_{i=1}^{m}(R_i+h_i)$;最后,根据 S_{ID} 中的身份信息 ID_j 搜索本地数据库的相应记录 $\langle ID_j,SK_{ID_j},PK_{ID_j}\rangle$,

© 中国科学院软件研究所 http://www.jos.org.cn

并计算 $T=e(h_jSK_{ID_j},\sum_{i=1}^{m}(R_i+h_i)P)$ 是否成立(其中, $h_j=H_3(PK_{ID_j},R_j)$, $R_j\in\mathcal{R}$).

由于发送者 Alice 的私钥信息 SK_{Alice} 满足等式关系 $T=e(h_{\text{Alice}}SK_{\text{Alice}},\sum_{i=1}^{m}(R_i+h_i)P)$, 则 PKG 返回相应的 ID_{Alice} 给 Bob.虽然发送者具有强匿名性,但匿名的可控性确保任何发送者都无法否认已有的签密事实.

3.2 正确性分析

声称 1. 密文合法性验证过程是正确的.

证明:由 $c_{\text{Alice}}=h_{\text{Alice}}PK_{\text{Alice}}-\sum_{i=1,i\neq I_{\text{Alice}}}^{m}(c_i+h_iPK_i)$ 可知:

$$\sum_{i=1}^{m}(c_i+h_iPK_i)=\sum_{i=1,i\neq I_{\text{Alice}}}^{m}(c_i+h_iPK_i)+c_{\text{Alice}}+h_{\text{Alice}}PK_{\text{Alice}}=2h_{\text{Alice}}PK_{\text{Alice}}.$$

由于 $e(V,P)=e(f_Hh_{\text{Alice}}SK_{\text{Alice}},P)e(dP_{Pub},P)=e(f_Hh_{\text{Alice}}PK_{\text{Alice}},P_{Pub})e(D,P_{Pub})=e\left(\frac{f_H}{2}\sum_{i=1}^{m}(c_i+h_iPK_i)+D,P_{Pub}\right)$,

因此 $e(V,P)=e\left(\frac{f_H}{2}\sum_{i=1}^{m}(c_i+h_iPK_i)+D,P_{Pub}\right)$ 成立,即接收者可验证密文的合法性. □

声称 2. 发送者身份合法性验证过程是正确的.

证明:由等式 $\sum_{i=1}^{m}(R_i+h_i)=\sum_{i=1,i\neq I_{\text{Alice}}}^{m}(R_i+h_i)+(R_{\text{Alice}}+h_{\text{Alice}})$ 和 $R_{\text{Alice}}=r_{\text{Alice}}-\sum_{i=1,i\neq I_{\text{Alice}}}^{m}(R_i+h_i)$ 可知:

$$\sum_{i=1}^{m}(R_i+h_i)=r_{\text{Alice}}+h_{\text{Alice}}=Q_{\text{Alice}},$$

则 $T=e\left(P_{Pub}\sum_{i=1}^{m}(R_i+h_i),\frac{1}{2}\sum_{i=1}^{m}(c_i+h_iPK_i)\right)=e(Q_{\text{Alice}}P_{Pub},h_{\text{Alice}}PK_{\text{Alice}})=e(Q_{\text{Alice}}P,h_{\text{Alice}}SK_{\text{Alice}})$,因此,接收者可验证发送者身份的合法性. □

声称 3. 授权接收者拥有正确的数据封装密钥.

证明:由 $e(P_{Pub},N_{J_{\text{Bob}}})=e(P_{Pub},d(P_0+PK_{\text{Bob}}))=e(P_{Pub},dP_0)e(S_{msk}P,dPK_{\text{Bob}})=e(P_{Pub},dP_0)e(D,SK_{\text{Bob}})$ 可知:

$$U=e(P_{Pub},N_{J_{\text{Bob}}})e(D,SK_{\text{Bob}})^{-1}=e(P_{Pub}dP_0).$$

因此,授权接收者能正确计算数据封装密钥 $K=H_3(U,D)$. □

定理 1. 合法的授权接收者可解密出正确的明文.

证明:由声称 1~声称 3 可知,合法的授权接收者可解密出正确的明文.其中,声称 1 保证了密文是合法的签密密文,声称 2 保证了发送者身份的合法性,声称 3 保证了授权接收者可正确还原数据封装密钥. □

4 安全性证明

4.1 机密性

定理 2. 假设对称加密/解密算法 $Enc(K,\cdot)$和 $Dec(K,\cdot)$具有机密性.在随机预言机模型下,若存在 PPT 敌手$\mathcal{A}$能够以不可忽略的优势ε赢得定义 1 中的游戏(游戏中,$\mathcal{A}$至多进行 q_D 次解混合签密询问),那么存在算法$\mathcal{C}$,至少能够以优势 $\varepsilon\left(1-\frac{q_D}{2^{|ID|}}\right)$解决 BDH 问题.

证明:算法$\mathcal{C}$的输入是 BDH 问题的挑战实例$\langle aP,bP,cP\rangle$,其中, $a,b,c\in Z_q^*$ 且未知,其目标是计算 $e(P,P)^{abc}$.$\mathcal{C}$把敌手$\mathcal{A}$作为子程序并充当定义 1 游戏中的挑战者,此过程中,$\mathcal{A}$分别进行混合签密询问,解混合签密询问和对预言机 H_1 的询问.同时,$\mathcal{C}$维护列表 L_1,L_2 和 L_{SK} 记录相应的询问,初始化时,上述列表均为空,其中,L_1 用于跟踪公钥生成询问(也是跟踪$\mathcal{A}$对预言机 H_1 的询问),L_2 用于跟踪$\mathcal{A}$对预言机 H_2 的询问,L_{SK} 用于跟踪私钥生成询问.

初始化:$\mathcal{C}$令 $P_0=bP$ 和 $P_{Pub}=cP$(隐含设置了 $S_{msk}=c$,对于$\mathcal{C}$而言,S_{msk} 是未知的),生成相应的公开参数 *Params* 发送给$\mathcal{A}$.

阶段 1:敌手$\mathcal{A}$向$\mathcal{C}$进行如下询问:

H_2 询问:当收到$\mathcal{A}$关于$\langle U_j,D_j\rangle$的 H_2 询问时,若存在$\langle U_j,D_j,K_j\rangle\in L_2$,则$\mathcal{C}$返回相应的 K_j 给$\mathcal{A}$;否则,$\mathcal{C}$选取满足关

© 中国科学院软件研究所 http://www.jos.org.cn

系$\langle\cdot,\cdot,K_j\rangle\notin L_2$(避免哈希函数碰撞的产生)的随机值$K_j\in\mathcal{K}$作为询问应答返回给$\mathcal{A}$,并添加$\langle U_j,D_j,K_j\rangle$到$L_2$中.

公钥生成询问(H_1询问):当$\mathcal{C}$收到$\mathcal{A}$关于ID_i的公钥生成询问时,若存在$\langle ID_i,x_i,PK_{ID_i}\rangle\in L_1$,则$\mathcal{C}$返回相应的$PK_{ID_i}$给$\mathcal{A}$;否则,$\mathcal{C}$选取随机数$x_i\in Z_q^*$,使得列表$L_1$中不存在相应的元组$\langle ID_i,x_i,PK_{ID_i}\rangle\notin L_1$,计算$PK_{ID_i}=x_iP$,添加$\langle ID_i,x_i,PK_{ID_i}\rangle$到$L_1$中,并返回相应的$PK_{ID_i}$给$\mathcal{A}$.

私钥生成询问:当$\mathcal{C}$收到$\mathcal{A}$关于ID_i的私钥生成询问时,若L_{SK}中存在$\langle ID_i,SK_{ID_i}\rangle\in L_{SK}$,则返回相应的$SK_{ID_i}$给$\mathcal{A}$;否则,对$ID_i$进行公钥生成询问,并获得相应的应答$\langle ID_i,x_i,PK_{ID_i}\rangle$,计算$SK_{ID_i}=x_iP_{Pub}$;将$SK_{ID_i}$返回给$\mathcal{A}$,并添加$\langle ID_i,SK_{ID_i}\rangle$到$L_{SK}$中.

混合签密询问:当收到$\mathcal{A}$对关于$\langle M,ID_S R_{ID}\rangle$的混合签密询问时(其中,$R_{ID}=\langle ID_{R_1},...,ID_{R_n}\rangle$是接收者身份集合),$\mathcal{C}$运行混合签密算法$\delta=HSign(M,ID_S,R_{ID})$获知相应的密文$\delta$,并返回$\delta$给$\mathcal{A}$.

解签密询问:当收到$\mathcal{A}$关于$\langle\delta,ID_{R_j}\rangle$的解签密询问时,$\mathcal{C}$对$ID_{R_j}$进行私钥生成询问,获得相应的应答私钥$SK_{ID_{R_j}}$后,运行解签密算法$M/\perp=UnHSign(M,ID_{R_j},SK_{ID_{R_j}})$,并返回结果$M/\perp$给$\mathcal{A}$,其中,$\perp$表示输入的密文$\delta$无效.

挑战:$\mathcal{A}$向$\mathcal{C}$发送挑战信息(M_0,M_1,ID_S,R_{ID}),其中,M_0和M_1是两个等长的挑战消息,ID_S是发送者身份,$R_{ID}=(ID_{R_1},...,ID_{R_n})$是接收者身份集合.$\mathcal{C}$收到$\mathcal{A}$的挑战后,选取随机比特$b\leftarrow\{0,1\}$,按下述步骤生成消息$M_b$所对应的签密密文$\delta=\langle\omega,D,T,\mathcal{R},\mathcal{C},\mathcal{Z},\mathcal{N},S_{ID}\rangle$.

(1) 构造满足条件$ID_S\in S_{ID}$和$S_{ID}\cap R_{ID}=\varnothing$的发送者伪装集合$S_{ID}=(ID_{S_1},...,ID_{S_m})$,选取随机数$r_S\in Z_q^*$,对于满足条件$i\neq I_S$($I_S$为$ID_S$在$S_{ID}$中的位置索引)的索引$i\in[1,m]$,选取随机数$R_i\in Z_q^*$,并计算$R_{I_S}=r_S-\sum_{i=1且i\neq I_S}^{m}(R_i+h_i)$(其中,$h_i=H_3(PK_{S_i},R_i)$),构造集合$\mathcal{R}=\{R_1,\ldots,R_m\}$;对发送者身份$ID_S$进行公钥生成询问,获知相应的应答$PK_{ID_S}$;计算$Q_S=r_S+h_S$(其中,$h_S=H_3(PK_{ID_S},R_{I_S})$);随机选取$c_i\in G_1$(其中,$i\in[1,m]$且$i\neq I_S$),并计算$c_{I_S}=h_SPK_{ID_S}-\sum_{i=1且i\neq I_S}^{m}(c_i+h_iPK_{ID_{S_i}})$,构造集合$\mathcal{C}=\{c_1,\ldots,c_m\}$;令$D=aP$,选取群$G_1$中满足关系$e(W,P)=e(D,P_{Pub})$的元素$W\in G_1$(暗含了$W=aP_{Pub}$),计算$U=e(W,P_0)$,$K=H_2(U,D)$和$\omega=Enc(K,M_b)$.

(2) 分别对授权接收者$ID_{R_j}\in R_{ID}$计算索引$J_{R_j}=f_{index}(ID_{R_j})$后,对$ID_{R_j}$进行公钥生成询问,获知相应的公钥$PK_{ID_{R_j}}$,然后计算$Z_{J_{R_j}}=e(W,PK_{ID_{R_j}})$;选取群$G_1$中满足条件$e(W,P_0)=e(X,P_{Pub})$和$e(W,PK_{ID_{R_j}})=e(Y,P_{Pub})$的元素$X,Y\in G_1$(这意味着$X=aP_0$和$Y=aPK_{ID_{R_j}}$);计算$N_{J_{R_j}}=X+Y$(暗含了$N_{J_{R_j}}=a(P_0+PK_{ID_{R_j}})$),构造集合$\mathcal{Z}=\{Z_{R_1},...,Z_{R_n}\}$和$\mathcal{N}=\{N_{R_1},...,N_{R_n}\}$.

(3) 计算$T=e(Q_SP,h_SSK_{ID_S})$和$V=W+f_Hh_SSK_{ID_S}$,其中,$f_H=H_4(\omega\|ID\|T\|\mathcal{R}\|\mathcal{C}\|\mathcal{Z}\|\mathcal{N}\|S_{ID})$,返回挑战密文$\delta=\langle\omega,D,T,\mathcal{R},\mathcal{C},\mathcal{Z},\mathcal{N},S_{ID}\rangle$给$\mathcal{A}$.

阶段2:该阶段与阶段1相类似,敌手$\mathcal{A}$进行多次相关询问,但该阶段不能对接收者集合R_{ID}中的任何身份信息进行私钥生成询问,并且禁止对挑战密文δ进行解签密询问;同时,不能对仅在接收者身份集合部分与挑战密文δ不同的密文进行解签密询问.

猜测:最后,敌手$\mathcal{A}$输出$b'\leftarrow\{0,1\}$作为对随机数b的猜测.若$b'=b$,$\mathcal{C}$输出1,并从列表L_1中选取身份$ID_j\in R_{ID}$对应的元组$\langle ID_j,x_j,PK_{ID_j}\rangle$,返回BDH问题的有效解$e(N_{J_{R_j}}-x_jD,P_{Pub})$;否则,$\mathcal{C}$输出0,表示未解决BDH问题.

已知$D=aP$,$P_0=bP$,$P_{Pub}=cP$和$PK_{J_{R_j}}=x_jP$,若$\mathcal{A}$猜测成功,则有$N_{J_{R_j}}=abP+ax_jP$.

因此,$e(N_{J_{R_j}}-x_jD,P_{Pub})=e(P,P)^{abc}$就是BDH问题的有效解.

当且仅当解签密询问中有效密文被拒绝时,导致$\mathcal{C}$的模拟不够完美;$\mathcal{A}$在整个模拟过程中总共进行了q_D次解签密询问,则在q_D次解签密询问中,$\mathcal{C}$拒绝有效密文δ的最大概率为$\frac{q_D}{2^{|ID|}}$,其中,$|ID|$为用户的身份长度;则攻击本文机制成功的优势至少为$\varepsilon\left(1-\frac{q_D}{2^{|ID|}}\right)$.

© 中国科学院软件研究所 http://www.jos.org.cn

若敌手$\mathcal{A}$在多项式时间内能够以ε的优势赢得定义 1 中的游戏,则$\mathcal{C}$至少能够以优势$\varepsilon\left(1-\frac{q_D}{2^{|ID|}}\right)$解决 BDH 问题.已知 BDH 问题是困难的,因此,本文机制在自适应选择密文攻击下具有保密性. □

4.2 不可伪造性

定理 3. 假设对称加密/解密算法 $Enc(K,\cdot)$和 $Dec(K,\cdot)$具有不可伪造性.在随机预言机模型下,若存在 PPT 敌手$\mathcal{A}$能够以不可忽略的优势ε赢得定义 2 中的游戏(游戏中$\mathcal{A}$至多进行 q_D次解签密询问),则存在算法$\mathcal{C}$,至少以优势$\varepsilon\left(1-\frac{q_D}{2^{|ID|}}\right)$解决 CDH 困难性问题.

基于 CDH 假设可完成对定理 3 的证明,思路与定理 2 类似,限于篇幅,本文不再赘述.

5 机制分析

5.1 匿名性

5.1.1 发送者匿名性

发送者的身份信息 ID_{Alice} 没有直接发送给接收者,而是通过伪装集合 S_{ID} 对其进行了隐藏,使用多个“假身份”掩盖了发送者的真实身份.收到相应的密文后,任何接收者(要么是授权接收者,要么是非授权接收者)都无法准确获知发送者的具体身份信息,仅能通过相应的验证操作判断发送者是伪装集合 S_{ID} 中的一员,具体是哪一个,接收者无法确定.因此,本文机制中除发送者之外的任何用户都无法关联密文及其对应的发送者.由于发送者伪装集合 S_{ID} 中的身份都是从$\mathcal{ID}$中均匀随机选取的,故接收者获知真实发送者身份的概率是 $\frac{1}{m}$.

文献[8,13,15,19]中,接收者会收到发送者的真实身份,因此,这将威胁到发送者隐私信息的匿名性,无法满足发送者对自身隐私信息的保护需求;而文献[12,16,17]及本文机制将发送者的身份信息隐藏于伪装集合中,而伪装集合中各身份信息均被接收者所信任,因此,任意接收者仅能判断密文来源的可靠性,而无法准确定位具体的发送者.然而,上述机制[12,16,17]对发送者匿名性未给出形式化证明,并且发送者的匿名性是不可控的,易产生发送者否认已有签密事实的行为.

5.1.2 接收者匿名性

本文机制中,由于密文中不再包含授权接收者身份列表的相关信息,因此,任意的接收者仅能验证密文的正确性,无法从密文中获悉其他接收者的身份等隐私信息.在文献[8,12−15,19]中,为了保证各接收者能够正确解密密文,在密文中必须包含接收者身份组成的标识信息,导致接收者隐私信息的泄露,因此,上述方案不具备接收者匿名性.而本文机制中.由集合$\mathcal{Z}$和$\mathcal{N}$承担标识的作用,并且$\mathcal{Z}$和$\mathcal{N}$中不包含接收者的任何隐私信息,为接收者提供了匿名性保护.

5.2 安全性分析

本节对方案的公开验证性和不可否认性等安全属性进行理论分析.

5.2.1 公开验证性

任何可信第三方无需获知接收者秘密信息,在公开信息的作用下,可独自完成密文的合法性验证操作.在本文机制中,可信第三方 PKG 通过验证等式(1)和等式(2)是否成立,即可完成对密文合法性的验证,验证过程无需接收者的秘密信息,也无需明文的参与,因此,本文机制具有密文的公开验证性.

5.2.2 不可否认性

当发送者否认已有的签密操作时,由于本文机制中发送者具有强匿名性,使得接收者不具备确认发送者身份的功能,但是由于发送者的匿名性是可控的,接收者可向 PKG 申请撤销发送者的匿名性.PKG 首先对接收者撤销申请的合法性进行判断,并响应合法的申请,即 PKG 通过相应计算可返回发送者的详细身份信息.由于密文具有不可伪造性,同时,发送者的匿名性是可控的,因此,发送者对签密事实无法进行否认.

© 中国科学院软件研究所 http://www.jos.org.cn

5.2.3 提前判断性

由于消息的广播传输,导致多个用户都能收到广播消息,一旦收到消息就解密,在一定程度上增加了用户的操作负载.因此,任何接收者解密之前,都可以验证自己是否是授权接收者,避免了不必要的计算开销.

5.3 性能分析

由于混合签密与签密具有相似的功能,并且目前对多接收者混合签密方案的研究较少,因此,将本文机制与相应的多接收者签密方案进行比较分析.

表 1 所示为本文机制与传统多接收者签密方案的性能比较结果.传统多接收者签密方案[7,11−19]在匿名性及完整性验证方面存在不足.文献[7]中,密文中缺失接收者身份列表,并且无法满足发送者的匿名性需求.文献[11]无法满足接收者的匿名性需求.文献[12–14]缺乏对收发双方的匿名性保护.文献[15]中,由于笔误造成签密密文缺失接收者身份列表,并且无法满足接收者的匿名性需求.文献[16]中,签密发送者和接收者具有较强的匿名性,并且签密运算计算量较少,但遗憾的是,文献[17]指出,文献[16]无法满足其所声称的接收者匿名性,并且该机制中解签密运算缺乏对签密密文合法性的验证,同时,发送者不具有匿名的可控性,易产生发送者否认签密事实的现象.文献[17]提出的改进机制解决了原始方案[16]中接收者匿名性方面的不足,却无法满足发送者匿名的可控性.文献[18]中,发送者不具有匿名性,并且该机制不具有公开验证性.文献[19]中,收发双方都不具有匿名性,并且接收者只有在获知所有发送者身份信息(身份信息对应公钥)的前提下才能正确解密.虽然文献[7,13–15]中密文长度较短,但对收发双方不提供匿名性保护.

Table 1 Comparison of performance

表 1 性能比较

方案	基础理论	设计特点	不足
文献[7]	双线性理论	提出多接收者签密	密文缺失接收者身份列表,易暴露发送者和发送者的身份
文献[11]	双线性理论	提出发送者匿名	易暴露接收者身份
文献[12]	双线性理论	使用接收者列表	易暴露发送者和接收者的身份
文献[13]	插值多项式理论	密文短,传输效率高	易暴露发送者和接收者的身份
文献[14]	双线性理论和插值多项式理论	公开参数少	易暴露发送者和接收者的身份
文献[15]	双线性理论	标准模型下安全	密文缺失接收者身份列表;易暴露接收者身份信息
文献[16]	双线性理论和拉格朗日插值多项式理论	提出收发双方匿名性的需求	缺乏对密文的正确性验证,由于发送者的匿名性是不可控的,发送者可否认已有的签密操作,且不满足发送者匿名性
文献[17]	双线性理论和拉格朗日插值多项式理论	收发双方均匿名	发送者的匿名性是不可控的,发送者可否认已有的签密操作
文献[18]	双线性理论和拉格朗日插值多项式理论	提供接收者匿名性	发送者不具有匿名性,不满足公开验证性
文献[19]	双线性理论	多发送者参与发送同一个消息	收发双方均不具有匿名性,并且接收者需获知所有发送者的身份信息才能解密
本文机制	双线性理论	收发双方均匿名,且发送者的匿名性是可控的,可验证密文的合法性	与文献[7,11–19]相比尚无

多数机制[7,11−15]为了确保接收者正确完成解密操作,通常在密文中增加接收者身份列表,导致接收者的身份信息遭泄露;个别机制[18]虽然为接收者提供了匿名性,却忽视了发送者的匿名性保护需求;部分机制[16,17]虽然实现了收发双方的匿名性保护,却无法完成对发送者匿名性的控制操作.然而本文机制中,任何接收者无法获知除自身之外的其他任何接收者的隐私信息;并且所有的接收者仅能验证该密文消息来自一个合法的发送者,而无法确定发送者的具体身份,有效保护了发送者的隐私信息;虽然发送者具有强匿名性,但本文机制中匿名性是可控的,当发送者否认签密操作或有恶意行为发生时,接收者能够在可信第三方 PKG 的协助下撤销发送者的匿名性.因此,相对于现有基于身份的多接收者签密方案[7,11−19]而言,本文机制的性能更优.

© 中国科学院软件研究所 http://www.jos.org.cn

5.4 效率分析

计算效率由(混合)签密算法和解(混合)签密算法的计算量来衡量,传输效率由密文长度决定;并且表 2 中仅对计算复杂度较高的双线性映射、指数运算等进行了统计,对运算量较小的哈希、异或等运算并未统计.

表 2 中,相关符号的具体含义为:E_B 表示双线性映射运算;E_M 表示群上的乘运算;E_E 表示单指数运算,如 $\forall r \in Z_q^*, g \in G$,计算 g^r;E_D 表示双指数运算,如 $\forall r_1, r_2 \in Z_q^*, g_1, g_2 \in G$,计算 $g_1^{r_1} g_2^{r_2}$;$|G|$表示群 G 中元素的长度;$|Z_q^*|$表示有限域 Z_q^* 中元素的长度;l_m 表示明文消息的长度.

Table 2 Comparison of efficiency

表 2 效率比较

方案	签密算法	解签密算法	密文长度
文献[7]	$3E_E+(n+2)E_D+1E_B$	$1E_D+4E_B$	$(n+3)\|G_1\|+\|ID\|+l_m$
文献[11]	$(2n+m+2)E_M+1E_E$	nE_M+4E_E	$(m+n+2)\|G_1\|+(m+n)\|ID\|+l_m$
文献[12]	$(2m+2)E_M+1E_D+1E_B$	$1E_M+1E_D+3E_B$	$(n+2)\|G_1\|+\|G_2\|+n\|ID\|+l_m$
文献[13]	$(n+3)E_M+1E_E$	$3E_B$	$3\|G_1\|+n\|ID\|+l_m$
文献[14]	$(4n+4)E_M+1E_E+1E_B$	nE_E+2E_B	$(m+3)\|G_1\|+(n+1)\|ID\|+l_m$
文献[15]	$(m+n+1)E_M+(2m+n+3)E_E+1E_B$	$(n+5)E_B$	$(m+n+2)\|G_1\|+m\|Z_q^*\|+l_m$
文献[17]	$(2m+1)E_M+1E_E$	$(m+2)E_M+4E_B$	$(m+n+2)\|G_1\|+m\|ID\|+l_m$
文献[18]	$(2m+1)E_M+1E_E$	$(m+2)E_M+4E_B$	$(n+2)\|G_1\|+(m+n)\|Z_q^*\|+m\|ID\|+l_m$
本文机制	$(m+n+3)E_M+(n+2)E_B$	$(m+2)E_M+6E_B$	$(m+n+1)\|G_1\|+(n+1)\|G_2\|+m\|Z_q^*\|+m\|ID\|+l_m$

由表 1 可知:本文机制中,收发双方均具有匿名性,且发送者的匿名性是可控的,同时满足接收者解密独立性的需求;相对于现有的多接收者签密方案[7,11−19],由于本文机制的安全性更高,且性能更优,导致效率相对较低(相应安全性能的实现会增加一定的计算量).通常,在安全性与计算效率之间仅能寻求平衡,很难同时兼顾安全性与计算效率,从机制的安全性和性能出发,本文机制计算效率的降低在可容忍的范围之内.

特别地,本文机制为了实现密文的合法性验证、接收者的匿名性以及发送者匿名的可控性等安全性能,在密文中增添了部分额外的参数,致使方案密文的长度较长.但在实际应用中,用户可根据实际环境和安全性需求选择方案的相关功能,删除密文中相应的辅助参数,缩短密文长度,同时提升计算效率.

6 改进机制

第 3 节的方案在广播环境下将相同的消息发送给了不同的接收者,即单消息通信模式;然而,广播环境下存在同一用户期望将不同的消息发送给不同的接收者,即多消息通信模式.本节将改进上文提出的机制,使得改进后的机制满足广播环境下发送者的多消息发送需求.

6.1 改进机制

多接收者多消息匿名混合签密机制的初始化、密钥生成和匿名控制操作与第 3 节原始方案中的相关算法一致,此处不再赘述;具体混合签密和解签密算法的过程如下所述.

(1) 混合签密算法

令 $M=\{M_1,\ldots,M_n\}$是待加密的消息集合,ID_{Alice} 是发送者 Alice 的身份信息,$R_{ID}=\{ID_{R_1},ID_{R_2},\ldots,ID_{R_n}\}$ 是授权接收者集合.具体操作如下所述.

① 从身份空间$\mathcal{ID}$中选取 $m-1$ 个随机身份 $ID_i \in \mathcal{ID}$与 ID_{Alice} 一起构造满足条件 $S_{ID} \cap R_{ID}=\varnothing$的发送者伪装集合 $S_{ID}=\{ID_{S_1},\ldots,ID_{S_m}\}$,其中,$I_{\text{Alice}}$ 为 ID_{Alice} 在 S_{ID} 中的位置索引.

② 选取随机数 $r_{\text{Alice}} \in Z_q^*$, 对满足条件 $i \neq I_{\text{Alice}}$ 的索引 $i \in [1,m]$,选取 $R_i \in Z_q^*$ 和 $c_i \in G_1$,计算 $R_{I_{\text{Alice}}}=r_{\text{Alice}}-\sum_{i=1,i\neq i_{\text{Alice}}}^{m}(R_i+h_i)$(其中,$h_i=H_3(PK_{S_i},R_i)$),构造集合$\mathcal{R}=\{R_1,\ldots,R_m\}$;计算 $Q_{\text{Alice}}=r_{\text{Alice}}+h_{\text{Alice}}$(其中,$h_{\text{Alice}}=H_3(PK_{\text{Alice}},R_{\text{Alice}})$)和 $c_{I_{\text{Alice}}}=h_{\text{Alice}}PK_{\text{Alice}}-\sum_{i=1,i\neq i_{\text{Alice}}}^{m}(c_i+h_iPK_{S_i})$, 构造集合$\mathcal{C}=\{c_1,\ldots,c_m\}$;选取秘密随机数 $d,t \in Z_q^*$, 计算 $D=dP$

© 中国科学院软件研究所 http://www.jos.org.cn

和 $E=tP$,通过计算,将秘密随机数 d 和 t 安全擦除.

③ 对每个接收者 $ID_{R_j} \in ID_R$ 计算索引 $J_{R_j}=f_{Index}(ID_{R_j})$ 后,分别计算 $U_{J_{R_j}}=e(dP_{Pub},PK_{ID_{R_j}})$ 和 $Z_{J_{R_j}}=e(tP_{Pub},PK_{ID_{R_j}})$ (其中, $PK_{R_j}=H_1(ID_{R_j})$ 为接收者 ID_{R_j} 的公钥),构造集合 $\mathcal{Z}=\{Z_{J_{R_1}},...,Z_{J_{R_n}}\}$; 计算数据封装密钥 $K_{J_{R_j}}=H_2(U_{J_{R_j}},D)$ 后,计算密文 $\omega_{J_{R_j}}=Enc(K_{J_{R_j}},M_{J_{R_j}})$, 生成密文集合 $\omega=\{\omega_{J_{R_1}},...,\omega_{J_{R_n}}\}$.

④ 计算匿名控制信息 $T=e(Q_{\text{Alice}}P,h_{\text{Alice}}SK_{\text{Alice}})$和消息签名 $V=dP_{Pub}+f_Hh_{\text{Alice}}SK_{\text{Alice}}$,其中,$f_H=H_4(\omega\|\|D\|\|E\|\|T\|\|\mathcal{R}\|\|\mathcal{C}\|\|\mathcal{Z}\|\|S_{ID})$;输出密文 $\delta=\langle\omega,V,D,E,T,\mathcal{R},\mathcal{C},\mathcal{Z},S_{ID}\rangle$.

(2) 解签密算法

令 ID_{Bob} 是授权接收者 Bob 的身份,SK_{Bob} 是 Bob 的私钥.收到密文 $\delta=\langle\omega,V,D,E,T,\mathcal{R},\mathcal{C},\mathcal{Z},S_{ID}\rangle$后,Bob 的具体解签密过程如下所述.

① 验证密文的合法性

通过等式(1)是否成立,验证密文 δ 中签名的正确性:若等式(1)成立,则密文 δ 为完整的签密密文;否则,退出该算法并输出无效信息$\perp$,拒绝解密;同时,等式(1)验证了密钥参数 D 的合法性.

② 验证发送者的身份合法性

Bob 判断等式(2)是否成立:若成立,则发送者是发送者身份伪装集合 S_{ID} 中的有效成员之一;否则,退出该算法并输出无效信息$\perp$,拒绝解密;同时,等式(2)验证了匿名控制参数 T 的合法性.

③ 验证接收者身份的合法性

若 $Z_{\text{Bob}}=e(E,SK_{\text{Bob}})\notin\mathcal{Z}$,其中,$e(E,SK_{\text{Bob}})=e(tP,S_{msk}PK_{\text{Bob}})=e(tS_{msk}P,PK_{\text{Bob}})=e(tP_{Pub},PK_{\text{Bob}})$,则 Bob 不是合法的授权接收者,退出该算法并输出无效信息$\perp$,拒绝解密;否则,Bob 进行密文解密操作.

④ 解密密文

若验证均成立,则密文是完整的混合签密密文,发送者和接收者的身份都是合法的.

Bob 计算索引 $J_{\text{Bob}}=f_{index}(ID_{\text{Bob}})$,根据 J_{Bob} 从集合$\mathcal{C}$中准确定位密文 $C_{J_{\text{Bob}}}$; 计算 $U_{J_{\text{Bob}}}=e(D,SK_{\text{Bob}})$ 和 $K_{J_{\text{Bob}}}=H_2(U_{J_{\text{Bob}}},D)$ 后,对密文 $\omega_{J_{\text{Bob}}}$ 进行解密 $M_{J_{\text{Bob}}}=Dec(K_{J_{\text{Bob}}},\omega_{J_{\text{Bob}}})$, 并输出相应的消息 $M_{J_{\text{Bob}}}$.

6.2 正确性和安全性

与原始方案相比,改进机制的正确性与定理 1 的证明相类似;改进机制对密钥参数的计算方式进行了改变,上述改变并不影响原始方案的安全性,因此,改进后的方案与原始方案具有相同的安全性,并且改进机制具有原始机制的所有安全性能,如公开验证性、匿名性等.限于篇幅,具体过程不再赘述.

6.3 性能分析

本节将改进机制与功能相似的相关签密(混合签密)机制[20,25,26]就性能进行分析比较,其中,文献[20]实现了广播环境下的多消息发送需求,文献[25]提出了基于身份密码系统的多接收者混合签密机制,文献[26]提出了无证书环境下多接收者混合签密机制.

表 3 为相应的性能分析结果,其中,本文改进机制中收发双方均匿名,且发送者的匿名性是可控的,可公开验证密文的合法性,并且本文改进机制具有不可否认性等安全属性.文献[20]满足广播环境下的多消息发送需求,但对收发双方不提供匿名性保护.文献[25]中收发双发均不具有匿名性,并且该机制无法满足发送者的多消息发送需求.文献[26]中发送者不具有匿名性,而接收者仅对攻击者具有匿名性,即任何合法的接收者均能获知其他接收者的身份信息.

© 中国科学院软件研究所 http://www.jos.org.cn

Table 3 Analysis of performance

表 3 性能分析

方案	设计特点	不足
文献[20]	广播环境下的多消息签密机制,即涉及多接收者和多消息发送	收发双方均不具有匿名性
文献[25]	基于身份的多接收者混合签密机制,使用接收者身份标记列表确保密文被正确解密	收发双方均不具有匿名性,无法满足发送者的多消息发送需求
文献[26]	基于无证书密码系统的多接收者的混合签密机制,消息不作限制;对攻击者而言,实现了接收者的匿名性,但合法接收者可掌握接收者身份列表	发送者不具有匿名性,接收者的仅对攻击者具有匿名性
本文改进机制	广播环境下的多消息签密机制,即涉及多接收者和多消息发送.收发双发均具有匿名性,并且发送者的匿名性是可控的	与文献[20,25,26]相比尚无

7 结束语

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.本文为满足收发双方隐私信息的保护需求,提出了基于身份的多接收者(多消息)匿名混合签密方案,其中,公用的信息集合确保密文解密的独立性.分析表明:除具有保密性和不可伪造性之外,本文机制的安全性能更加完善.特别地,本文仅提出了多接收者(多消息)匿名混合签密机制的设计思路,在广播环境的具体应用本文并未赘述.在具体使用时,需根据应用环境的安全性需求对方案的设计进行调整.如通信时延、合谋攻击等对方案的影响,在特定的环境中需要考虑,并调整相应方案的设计.

本文虽然实现了对收发双方的匿名性和发送者匿名性的控制操作,但是为了实现上述功能,使得密文长度和 PKG 的存储量增加(其中,发送者伪装集合随密文发送导致密文长度增长,用户注册信息的存储增加了 PKG 存储负担),并且,可控操作中涉及本地数据库的身份搜索(身份的搜索数量以发送者身份伪装集合的大小一致),因此,下一步有必要深入研究更加高效、快捷的匿名实现技术和控制策略.

References:

[1] Zheng YL. Digital signcryption or how to achieve cost(Signature & Encryption)<<cost(Signature)+cost(Encryption). In: Proc. of the Advances in Cryptology—CRYPTO'97. LNCS 1294, Berlin: Springer-Verlag, 1997. 165−179. [doi: 10.1007/BFb0052234]

[2] Dent AW. Hybrid signcryption schemes with outsider security. In: Proc. of the Int'l Conf. on Information Security (ISC 2005). 2005. 203−217. [doi: 10.1007/11556992_15]

[3] Dent AW. Hybrid signcryption schemes with insider security. In: Proc. of the Australasian Conf. on Information Security and Privacy (ACISP 2005). 2005. 253−266. [doi: 10.1007/11506157_22]

[4] Cramer R, Shoup V. Design and analysis of practical public-key encryption schemes secure against adaptive chosen ciphertext attack. Siam Journal on Computing, 2004,33(1):167−226. [doi: 10.1137/S0097539702403773]

[5] Li X, Qian H, Weng J, Yu Y. Fully secure identity-based signcryption scheme with shorter signcryptext in the standard model. Mathematical & Computer Modelling, 2013,57(3-4):503−511. [doi: 10.1016/j.mcm.2012.06.030]

[6] Ch SA, Uddin N, Sher M, Ghani A, Naqvi H, Irshad A. An efficient signcryption scheme with forward secrecy and public verifiability based on hyper elliptic curve cryptography. Multimedia Tools & Applications, 2015,74(5):1711−1723. [doi: 10.1007/s11042-014-2283-9]

[7] Duan S, Cao Z. Efficient and provably secure multi receiver identity based signcryption. In: Proc. of the 11th Australasian Conf. on Information Security and Privacy. 2006. 195−206. [doi: 10.1007/11780656_17]

[8] Han Y, Gui X. Adaptive secure multicast in wireless networks. Int'l Journal of Communication Systems, 2009,22(9):1213−1239. [doi: 10.1002/dac.1023]

[9] Wang X, Shu J, Zheng W, Liu L, Fan X. New multi-receiver ID-based ring signcryption scheme. Lecture Notes in Electrical Engineering, 2014,238:2251−2257. [doi: 10.1007/978-1-4614-4981-2_246]

[10] Wang H, Zhang Y, Qin B. Analysis and improvements of two identity based anonymous signcryption schemes for multiple receivers. In: Proc. of the IEEE Int'l Conf. on Trust, Security and Privacy in Computing and Communications. 2012. 1057−1062. [doi: 10.1109/TrustCom.2012.88]

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

© 中国科学院软件研究所 http://www.jos.org.cn

[12] Yu Y, Yang B, Huang X, Zhang M. Efficient identity based signcryption scheme for multiple receivers. In: Proc. of the 4th Int'l Conf. on Autonomic and Trusted Computing. 2007. 13−21. [doi: 10.1007/978-3-540-73547-2_4]

[13] Sharnila S, Sree S, Srinivasan R, Pandu C. An efficient identity based signcryption scheme for multiple receivers. In: Proc. of the 4th Int'l Workshop on Advances in Information and Computer Security. 2009. 71−88. [doi: 10.1007/978-3-642-04846-3_6]

[14] Qin H, Dai Y, Wang Z. Identity based multi-reveiver threshold signcryption scheme. Security and Communication Networks, 2010, 3(6):535−545. [doi: 10.1002/sec.259]

[15] Zhang B, Xu Q. An ID-based anonymous signcryption scheme for multiple receivers secure in the standard model. Int'l Journal of Advanced Science and Technology, 2010,20(7):9−24.

[16] Pang LJ, Cui JJ, Li HX, Pei QQ, Jiang ZT, Wang YM. A new multi-receiver ID-based anonymous signcryption. Chinese Journal of Computers, 2011,34(11): 2104−2112 (in Chinese with English abstract).

[17] Li HX, Ju LF. Security analysis and improvement of an anonymous multi-receiver signcryption scheme. ACTA Electronica Sinica, 2015,43(11):2187−2193 (in Chinese with English abstract).

[18] Pang LJ, Gao L, Li HX, Wang YM. Anonymous multi-receiver ID-based signcryption scheme. IET Information Security, 2015,9(3): 194−201. [doi: 10.1049/iet-ifs.2014.0360]

[19] Swapna G, Reddy PV. Efficient identity based multi-signcryption scheme with public verifiability. Journal of Discrete Mathematical Sciences & Cryptography, 2014,17(2):181−190. [doi: 10.1080/09720529.2013.867674]

[20] Din N, Umar AI, Waheed A, Amin NU. An efficient multi-message multi-receiver signcryption scheme with forward secrecy on elliptic curves. Cryptology ePrint Archive: Report 2015/655, 2015.

[21] Kang L, Tang XH, Liu JF. Tight chosen ciphertext attack (CCA)-secure hybrid encryption scheme with full public verifiability. Science China Information Sciences, 2014,57(11):1−14. [doi: 10.1007/s11432-014-5166-9]

[22] Bjørstad TE. Hybrid signcryption. In: Dent A, Zheng Y, eds. Practical Signcryption. Information Security and Cryptography. Berlin, Heidelberg: Springer-Verlag, 121−147.

[23] Sun YX, Li H. Efficient certificateless hybrid signcryption. Ruan Jian Xue Bao/Journal of Software, 2011,22(7):1690−1698 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/3825.htm [doi: 10.3724/ SP.J.1001.2011.03825]

[24] Tong RY, Meng QX, Chen M. Effective and secure identity-based hybrid signcryption scheme. Journal of Computer Applications, 2013,33(5):1382−1385, 1393 (in Chinese with English abstract). [doi: 10.3724/SP.J.1087.2013.01382]

[25] Sun YX, Li H. ID-Based signcryption KEM to multiple recipients. Chinese Journal of Electronics, 2011,20(2):317−322.

[26] Han Y, Yue Z, Fang D, Yang XY. New multivariate-based certificateless hybrid signcryption scheme for multi-recipient. Wuhan University Journal of Natural Sciences, 2014,19(5):433−440. [doi: 10.1007/s11859-014-1036-y]

附中文参考文献:

[16] 庞辽军,崔静静,李慧贤,斐庆祺,姜正涛,王育民.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):2104−2112.

[17] 李慧贤,巨龙飞.对一个匿名多接收者签密方案的安全性分析与改进.电子学报,2015,43(11):2187−2193.

[23] 孙银霞,李晖.高效无证书混合签密.软件学报,2011,22(7):1690−1698. http://www.jos.org.cn/1000-9825/3825.htm [doi: 10.3724/SP.J.1001.2011.03825]

[24] 仝瑞阳,孟庆见,陈明.高效安全的身份混合签密方案.计算机应用,2013,33(5):1382−1385,1393. [doi: 10.3724/SP.J.1087.2013.01382]

周彦伟(1986－),男,甘肃通渭人,博士生,工程师,主要研究领域为密码学,信息安全.

王青龙(1970－),男,博士,副教授,主要研究领域为密码学及其应用.

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

© 中国科学院软件研究所 http://www.jos.org.cn