边缘计算环境下基于PUF的多接收者匿名签密方案

李森森,刘燕江,郁 滨,李俊全
(战略支援部队信息工程大学, 河南郑州 450001)

摘 要: 边缘计算将部分云中心业务扩展至网络边缘,能够有效缓解万物互联时代海量设备和数据造成的云中心计算开销大、处理时延长等问题. 在边缘计算环境下,边缘节点和终端设备常部署于无人值守的开放环境中,使其在面临传统安全威胁的同时,也存在遭受物理攻击的风险. 为实现边缘计算环境下设备的安全通信,已有学者提出了具有较高通信效率的多接收者签密方案. 然而,现有方案应用于高安全性要求领域仍存在两个方面的不足:(1)未提供对物理攻击的防范机制;(2)未实现对发送者的匿名性保护. 针对上述问题,基于物理不可克隆函数(Physical Unclonable Function, PUF)这一硬件安全原语,提出一种高效的多接收者多消息签密方案. 方案将PUF与椭圆曲线上的无证书公钥密码体制相结合,无需使用高计算复杂度的双线性对运算且无密钥托管问题. 安全性分析表明,方案在具备机密性、不可伪造性、匿名性等安全属性的同时,能够有效防范物理攻击. 相较于同类方案,本文方案能够在不明显增加计算开销的前提下,以更低的通信开销实现更高的安全性,满足边缘计算环境下设备的安全通信需求.

关键词: 边缘计算;签密;物理不可克隆函数;多接收者;多消息;匿名性
基金项目: 国家自然科学基金(No.62302519)
中图分类号: TP309 **文献标识码:** A **文章编号:** 0372-2112(2024)12-4087-14
电子学报 URL:http://www.ejournal.org.cn **DOI:**10.12263/DZXB.20231181

PUF-Based Multi-Receiver Anonymous Signcryption Scheme in Edge Computing

LI Sen-sen, LIU Yan-jiang, YU Bin, LI Jun-quan
(*PLA Information Engineering University*, *Zhengzhou*, *Henan* 450001, *China*)

Abstract: Edge computing extends some tasks of center cloud server to the edge of the network, which can effectively alleviate the problems of high computation overhead and long processing latency caused by massive devices and data in the era of Internet of Everything. In edge computing environment, edge nodes and terminal devices are usually deployed in the unattended and open places, making them vulnerable to physical attacks while facing traditional security threats. To achieve secure communication in edge computing, several multi-receiver signcryption schemes with high communication efficiency have been proposed. However, there are still two issues with the application of existing schemes in areas with high security requirements: (1) no prevention mechanism for physical attacks is provided; (2) the anonymity protection for the senders has not been implemented. To fill this gap, we propose an efficient multi-receiver and multi-message signcryption scheme based on the hardware security primitive physical unclonable function (PUF) in this paper. Combining PUF with certificateless public key cryptography (CL-PKC) on elliptic curve, the proposed scheme does not need to use bilinear pairings with high computational complexity and is free from the key escrow problem. The security analysis shows that the scheme can effectively prevent physical attacks while possessing security attributes including confidentiality, unforgeability, and anonymity. Compared with related schemes, the proposed scheme achieves higher security with lower communication overhead without significantly increasing the computation overhead, which can better meet the requirements of secure communication in edge computing.

Key words: edge computing; signcryption; physical unclonable function (PUF); multi-receiver; multi-message; anonymity
Foundation Item(s): National Natural Science Foundation of China (No.62302519)

收稿日期:2023-12-21;修回日期:2024-06-24;责任编辑:李勇锋

1 引言

随着无线通信和智能传感技术的发展,特别是近年来以5G为代表的移动通信技术的日益成熟,物联网已被应用于各个领域,其安全问题也受到了广泛关注[1,2]. 伴随着万物互联时代的到来,海量的终端设备接入网络,数据也呈现出爆炸式增长的趋势[3]. 在传统的以云服务器为中心的"云-端"两级网络架构中,终端设备采集到的数据需上传至云服务器进行分析和存储,该方式存在处理时延长、通信开销大等问题[4],无法满足时延敏感型应用的需求. 边缘计算将云中心的计算能力迁移至网络边缘,通过在靠近终端设备的网络边缘引入边缘节点,以协助云服务器对数据进行处理,可有效缓解上述问题,在车联网、工业物联网、智慧城市等领域有着广阔的应用前景[5]. 然而,边缘计算在带来诸多便利的同时,也面临着数据安全、隐私保护等方面的挑战[6].

签密能够在一个逻辑步骤内实现对消息的加密和签名,相较于传统的先签名后加密方式,可在较大程度上降低设备的计算开销和通信开销,并且具有更高的实现效率[7],更能满足边缘计算环境的应用需求. 近年来,已有学者提出边缘计算环境下的签密方案. 文献[8]提出基于无证书公钥密码体制的签密方案,并通过离线计算与在线计算相结合的方式来降低设备开销,但该方案中签密消息验证过程需要执行计算复杂度较高的双线性对运算,不能满足资源受限设备的应用需求. 针对该问题,文献[9]提出无需使用双线性对运算的签密方案,并且提供了聚合签名验证机制来进一步降低设备开销. 针对边缘计算环境下的车联网安全通信问题,文献[10]基于无证书密码体制提出匿名签密方案,该方案无需双线性对运算,具有较高的实现效率,但该方案仅提供对设备身份标识的匿名性保护,敌手能够获取到设备的真实公钥,通过将公钥与设备绑定,敌手可以实现对设备的追踪. 文献[11]提出基于区块链的无证书签密方案,利用区块链的不可篡改特性来保证签名的不可抵赖性,并且区块链去中心化的特点使得该方案不依赖于可信第三方. 然而,上述方案仅支持单接收者的签密模式,若要向多个接收者发送消息,则需多次重复执行签密操作.

针对边缘计算环境下的多接收者签密问题,文献[12]基于隐式证书方法提出一种多接收者签密方案,能够以较低的资源开销保证消息机密性、不可伪造性、接收者匿名性等安全属性,但该方案仅支持多接收者单消息模式,不能实现多消息签密. 文献[13]提出的签密方案同样针对多接收者单消息的应用场景. 文献[14]基于椭圆曲线密码体制提出一种边缘计算环境下的多消息多接收者签密方案,该方案无需进行公钥证书管理且无密钥托管问题,在保证公开信道中所传输消息的安全性的同时,可有效实现对消息接收者的匿名性保护. 文献[15]提出一种多密钥生成中心的多接收者签密方案,具有较高的实现效率,并且该方案在密钥分配过程中无需安全信道. 文献[8]指出采用离线与在线相结合的签密方式[16]可以将大量复杂运算在离线阶段进行预计算,预处理后的数据可以用于在线阶段对消息的高效签密. 文献[8~10,17,18]均采用离线与在线相结合的方式来设计签密方案,但仅支持单接收者的签密模式. 近期,针对边缘计算环境下工业物联网的安全通信问题,文献[19]基于离线与在线签密相结合的方式,提出支持多接收者的签密方案,方案中边缘节点采用基于身份的密码体制,而终端设备采用无证书密码体制,能够实现边缘节点同时向多个终端设备安全传递消息,但仅支持以边缘节点为发送者、终端设备为接收者的场景,并且分析表明该方案不能达到声称的不可伪造性.

在隐私保护方面,上述边缘计算环境下的多接收者签密方案均未考虑对消息发送者身份信息的保护问题,不能满足部分应用场景的安全需求. 此外,上述方案基于传统密码体制实现,需要将敏感的私钥参数保存在设备存储器中. 在边缘计算环境下,边缘节点和终端设备可能部署于无人值守的开放环境中,并且终端设备通常资源受限,自我保护能力较差. 敌手可通过实施物理攻击[20,21]获取设备中存储的私钥参数,从而使传统的签密方案面临失效的风险. 因此,为满足高安全性要求领域的应用需求,面向边缘计算的签密方案既要抵抗传统安全威胁,又要提供对物理攻击的防范.

物理不可克隆函数(Physical Unclonable Function, PUF)在Pappu提出的物理单向函数[22]的基础上发展而来,其利用集成电路制造过程中的随机性工艺偏差建立起输入挑战与输出响应之间不可预测的映射关系,具有稳定性、唯一性、不可预测性等性质,为资源受限设备抵抗物理攻击提供了可行的解决方案[23,24].

综上所述,本文将PUF与椭圆曲线上的无证书公钥密码体制相结合,提出边缘计算环境下的多接收者多消息匿名签密方案. 方案基于椭圆曲线上的离散对数问题和计算性Diffie-Hellman问题设计,采用离线与在线相结合的方式,能够以较低的资源开销实现多接收者多消息签密,具备机密性、不可伪造性、发送者匿名性、接收者匿名性等安全属性,满足边缘计算环境下的安全通信需求.

2 预备知识

2.1 相关困难问题

令q为安全的大素数,$E_{a,b}$为有限域F_q上满足要求

的椭圆曲线. 循环群G的阶为素数p,$P\in E_{a,b}(F_q)$是群G的一个生成元,则有如下困难问题[9]:

(1)椭圆曲线上的离散对数(Elliptic Curve Discrete Logarithm, ECDL)问题. 给定$P,\alpha P\in G$,计算未知参数$\alpha\in Z_p^*$.

(2)椭圆曲线上的计算性Diffie-Hellman(Elliptic Curve Computational Diffie-Hellman, ECCDH)问题. 给定$P,\alpha P,\beta P\in G$,对于未知参数$\alpha,\beta\in Z_p^*$,计算$\alpha\beta P$.

ECDL假设. 对于任意概率多项式时间算法Π,其解决ECDL问题的优势可忽略不计. 该假设可表示为$\Pr[\Pi(P,\alpha P)=\alpha|\alpha\in Z_p^*]\leqslant\varepsilon_{\mathrm{ECDL}}$,其中$\varepsilon_{\mathrm{ECDL}}$为可忽略的值.

ECCDH假设. 对于任意概率多项式时间算法Π,其解决ECCDH问题的优势可忽略不计. 该假设可表示为$\Pr[\Pi(P,\alpha P,\beta P)=\alpha\beta P|\alpha,\beta\in Z_p^*]\leqslant\varepsilon_{\mathrm{ECCDH}}$,其中$\varepsilon_{\mathrm{ECCDH}}$为可忽略的值.

2.2 分叉引理

文献[25]介绍了分叉引理的具体内容,指出若概率多项式时间敌手能够以不可忽略的优势ε伪造一个签名(m,δ,r,h),其中m为待签名的消息,δ为对应的签名值,r和h分别为生成签名所选用的随机数和哈希值,则基于随机谕言机的重放,该敌手能够伪造出新签名(m,δ',r,h')的概率不少于$\left(1-\frac{1}{\mathrm{e}}\right)\frac{\varepsilon}{q_h}$,其中e为自然对数的底数,$q_h$为该敌手执行哈希询问的次数. 特别地,签名$(m,\delta,r,h)$和$(m,\delta',r,h')$的伪造所使用的随机数相同而哈希值不同.

2.3 PUF

PUF是建立在设备随机性物理差异基础上的一种特殊映射关系,可视为以物理方式嵌入设备内部的单向函数. 理想的PUF具有如下性质[24,26,27]:

(1)稳定性. 对于相同的输入挑战,特定的PUF能够以较高的概率产生相同的输出响应. 特别地,对于非理想PUF,由于温度、电压等环境因素的影响,特定的PUF对于相同输入挑战产生的多个输出响应之间可能存在少许的比特差异,该差异可以通过模糊提取器来消除[28].

(2)唯一性. 对于相同的输入挑战,两个不同PUF,即使两者采用相同的工艺流程且电路结构相同,其各自产生的输出响应在较大的概率上不同.

(3)不可预测性. 对于特定PUF,即使已知其部分挑战-响应对,预测其对新挑战的响应仍是困难的.

(4)抗篡改性. 任何针对PUF的用于获得特定挑战-响应值的非授权访问,将改变PUF的映射关系.

(5)不可区分性. PUF的响应值与等长的随机数是计算不可区分的.

2.4 模糊提取器

一个典型的模糊提取器可表示为$(\mathrm{Gen},\mathrm{Rep})$[29,30]:

(1) $\mathrm{Gen}:\{0,1\}^n\rightarrow\{0,1\}^n\times\{0,1\}^l$,该过程以序列$\omega\in\{0,1\}^n$为输入,能够提取出序列$d\in\{0,1\}^n$和对应的辅助数据$\mathrm{hd}\in\{0,1\}^l$,可表示为$(d,\mathrm{hd})\leftarrow\mathrm{Gen}(\omega)$.

(2) $\mathrm{Rep}:\{0,1\}^n\times\{0,1\}^l\rightarrow\{0,1\}^n$,该过程以序列$\omega'\in\{0,1\}^n$和辅助数据$\mathrm{hd}'\in\{0,1\}^l$为输入,得到序列$d'\in\{0,1\}^n$,可表示为$d'\leftarrow\mathrm{Rep}(\omega',\mathrm{hd}')$. 对于$(d,\mathrm{hd})\leftarrow\mathrm{Gen}(\omega)$,若存在$\overline{\omega}\in\{0,1\}^n$且$\mathrm{dist}(\omega,\overline{\omega})\leqslant\epsilon$,其中$\mathrm{dist}(\omega,\overline{\omega})$表示序列$\omega$和$\overline{\omega}$之间的比特距离,$\epsilon$为特定范围内可接受的值,则有$d\leftarrow\mathrm{Rep}(\overline{\omega},\mathrm{hd})$.

3 系统结构和安全模型

3.1 系统结构

采用与文献[12]相同的边缘计算网络结构,如图1所示. 该网络结构可分为云层、边缘层和终端层,网络实体主要包括管理服务器、边缘节点和终端设备. 其中,管理服务器为可信实体,主要负责网络配置、设备注册、安全参数分配等,在签密过程中作为密钥生成中心(Key Generation Center, KGC);边缘节点用于协助管理服务器对数据进行处理和分析;终端设备依托于传感器进行数据采集或执行外设控制操作等. 为有效防范物理攻击的威胁,作如下假设:

(1)终端设备和边缘节点均集成PUF模块,并且特定PUF模块与所属终端设备或边缘节点相绑定.

(2)设备控制器与其PUF模块之间的通信不能被截取[24,27].

(3)任何针对PUF的非法访问和侵入式攻击将会改变PUF的映射关系,并使其失效[24,27].

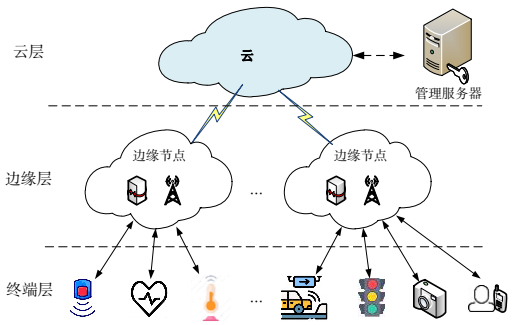

图1　边缘计算环境下的通信网络结构

为便于表示,将方案用到的主要符号定义如表1所示.

在边缘计算环境下,消息的发送者和接收者可以为终端设备或边缘节点,终端设备和边缘节点在进行安全通信前,需向KGC进行注册,以得到密钥参数. 具

表1 主要符号表示

符号	含义
κ	安全参数
params	系统公开参数
msk	系统主密钥
P_{Pub}	系统公钥
ID	设备的身份标识
t_i, t_s, t_{kgc}	时间戳
$\text{sk}_i=(x_i, y_i)$	设备ID_i的私钥
$\text{PK}_i=(X_i, R_i)$	设备ID_i的公钥
x_s^*	发送者的临时私钥
X_s^*	发送者的临时公钥
$\mathcal{M}$	待发送的消息集合
$\mathcal{L}$	消息接收者集合
PUF_i	设备ID_i的PUF
$H_i(i=1,2,3,4,5)$	哈希函数
$\|\|$	消息连接运算符

体而言,所提签密方案包括如下多项式时间算法:

(1)Setup算法. 该算法由KGC执行,输入安全参数κ,输出系统主密钥msk和系统参数params. KGC公开参数params,并秘密保存系统主密钥msk. 特别地,系统参数params中包含系统的公钥P_{Pub}.

(2)SetSecret算法. 该算法由设备(可为终端设备或边缘节点)ID_i执行,输入设备身份标识ID_i和系统参数params,输出设备随机选取的秘密值x_i以及相应的公开参数X_i.

(3)ExtractPartialKey算法. 该算法由KGC执行,用于产生设备的部分公/私钥参数. 算法的输入为设备身份标识ID_i、公开参数X_i、系统主密钥msk和系统参数params,输出KGC通过相关参数提取出的部分私钥y_i和部分公钥R_i.

(4)SetUserKey算法. 该算法由设备ID_i执行,用于产生其公钥和私钥. 算法的输入为设备身份标识ID_i、秘密值x_i、公开参数X_i、部分私钥y_i、部分公钥R_i和系统参数params,输出为设备的公钥PK_i和私钥sk_i.

(5)Offline SignCrypt算法. 该算法由消息发送者ID_s执行,用于产生预计算的签密参数. 算法的输入为消息接收者集合$\mathcal{L}=\{\text{ID}_1, \text{ID}_2, \cdots, \text{ID}_n\}$、对应的公钥集合$\mathcal{I}=\{\text{PK}_1, \text{PK}_2, \cdots, \text{PK}_n\}$以及系统参数params,输出为$\text{ID}_s$的临时公/私钥对$(X_s^*, x_s^*)$以及各个接收者对应的索引值$J_{R_i}(i=1,2,\cdots,n)$和参数$Q_i(i=1,2,\cdots,n)$.

(6)Online SignCrypt算法. 该算法由消息发送者ID_s执行,用于产生签密密文σ. 算法的输入为消息发送者身份标识ID_s及其私钥sk_s、消息接收者集合$\mathcal{L}=\{\text{ID}_1, \text{ID}_2, \cdots, \text{ID}_n\}$、待发送的消息集合$\mathcal{M}=\{M_1, M_2, \cdots, M_n\}$、系统参数params以及Offline SignCrypt算法输出参数,输出为密文σ_s.

(7)UnSignCrypt算法. 该算法由消息接收者ID_i执行,用于产生接收者ID_i对应的消息明文M_i. 算法的输入为密文σ_s、消息接收者身份标识ID_i及其公钥PK_i和私钥sk_i以及系统参数params,输出为ID_i对应的消息明文M_i.

(8)ParamsUpdate算法. 该算法由设备ID_i和KGC执行,用于更新设备ID_i的安全参数. 算法的输入为设备ID_i保存的旧安全参数,输出为设备ID_i新的安全参数.

3.2 安全模型

本文安全模型在文献[15]安全模型的基础上设计,考虑外部敌手$\mathcal{A}_{\text{I}}$和内部敌手$\mathcal{A}_{\text{II}}$的攻击,两类敌手的能力如下:

(1)$\mathcal{A}_{\text{I}}$类敌手可以看作恶意的设备,有能力查询和替换合法设备的公钥,但其无法掌握系统主密钥;

(2)$\mathcal{A}_{\text{II}}$类敌手可以看作诚实且好奇的KGC,拥有系统主密钥,但无法替换设备的公钥.

签密方案的设计既要考虑消息的机密性,又要满足签名的不可伪造性. 其中,消息的机密性是指只有授权的消息接收者能够得到消息明文,并且任意非授权接收者不能从签密密文中得到任何有用信息;签名的不可伪造性是指任意非法实体不能伪造正确的签密密文而通过验证. 为满足机密性要求,签密方案应在适应性选择密文攻击下具有不可区分性(IND-CCA2);为满足不可伪造性要求,签密方案应在适应性选择消息攻击下具有存在性不可伪造性(EUF-CMA).

3.2.1 消息机密性

通过定义游戏Game_1和Game_2来刻画两类敌手对方案机密性的攻击,具体定义如下.

Game_1(敌手$\mathcal{A}_{\text{I}}$的IND-CCA2游戏). 该游戏描述了敌手$\mathcal{A}_{\text{I}}$与挑战者C的如下交互过程.

(1)初始化阶段. 挑战者C运行Setup算法生成系统主密钥msk和公开参数params,秘密保存msk,并将params发送给$\mathcal{A}_{\text{I}}$. $\mathcal{A}_{\text{I}}$收到公开参数后,输出目标身份集合$\mathcal{L}^*=\{\text{ID}_1, \text{ID}_2, \cdots, \text{ID}_n\}$.

(2)训练阶段1. 敌手$\mathcal{A}_{\text{I}}$可多项式有界次地执行哈希询问和下述询问:

①公钥生成询问. $\mathcal{A}_{\text{I}}$将设备身份标识ID_i发送给挑战者C,C运行相关算法得到相应的公钥PK_i,并返回给$\mathcal{A}_{\text{I}}$.

②私钥生成询问. $\mathcal{A}_{\text{I}}$将ID_i发送给挑战者C,C运行相关算法得到秘密值x_i和相应的部分私钥y_i,并将私钥$\text{sk}_i=(x_i, y_i)$返回给$\mathcal{A}_{\text{I}}$.

③公钥替换询问. $\mathcal{A}_{\text{I}}$将ID_i和PK_i'发送给挑战者

C,C运行相关算法将ID_i公钥替换为PK_i'.

④签密询问. $\mathcal{A}_\mathrm{I}$选取发送者ID_s、接收者集合$\mathcal{L}$以及消息集合$\mathcal{M}$,并发送给挑战者C,C运行相关算法得到密文σ,并返回给$\mathcal{A}_\mathrm{I}$.

⑤解签密询问. $\mathcal{A}_\mathrm{I}$将签密密文σ和接收者身份标识ID_i发送给挑战者C,C运行相关算法对密文σ进行解签密,并将解签密结果返回给$\mathcal{A}_\mathrm{I}$.

(3)挑战阶段. $\mathcal{A}_\mathrm{I}$选择等长的挑战消息集合$\mathcal{M}^0=\{M_1^0,M_2^0,\cdots,M_n^0\}$和$\mathcal{M}^1=\{M_1^1,M_2^1,\cdots,M_n^1\}$及发送者身份标识$\mathrm{ID}_s$,并发送给挑战者$C$. C通过公钥生成询问查询$\mathcal{L}^*=\{\mathrm{ID}_1,\mathrm{ID}_2,\cdots,\mathrm{ID}_n\}$对应公钥$\mathcal{I}^*=\{\mathrm{PK}_1,\mathrm{PK}_2,\cdots,\mathrm{PK}_n\}$,随机选取$\theta\in\{0,1\}$,计算$\sigma^*\leftarrow\mathrm{SignCrypt}(\mathrm{ID}_s,\mathrm{sk}_s,\mathcal{L}^*,\mathcal{I}^*,\mathcal{M}^\theta,\mathrm{params})$,并将$\sigma^*$返回给敌手$\mathcal{A}_\mathrm{I}$.

(4)训练阶段2. 与训练阶段1相同,$\mathcal{A}_\mathrm{I}$可多项式有界次地执行上述询问,并得到挑战者C的响应.

(5)猜测. $\mathcal{A}_\mathrm{I}$输出对随机数θ的猜测θ',若$\theta'=\theta$且下列条件成立,则称$\mathcal{A}_\mathrm{I}$在游戏中获胜.

条件1:$\mathcal{A}_\mathrm{I}$在游戏过程中未获取到系统主密钥msk;

条件2:$\mathcal{A}_\mathrm{I}$未执行针对目标集合中任意设备$\mathrm{ID}_i\in\mathcal{L}^*$的私钥生成询问;

条件3:$\mathcal{A}_\mathrm{I}$未执行针对发送者ID_s、接收者$\mathrm{ID}_i\in\mathcal{L}^*$以及目标密文$\sigma^*$的解签密询问.

$\mathcal{A}_\mathrm{I}$赢得该游戏的优势可定义为

$$\mathrm{Adv}^{\mathrm{IND\text{-}CCA2}}(\mathcal{A}_\mathrm{I})=\left|\Pr[\theta'=\theta]-\frac{1}{2}\right|$$

Game_2(敌手$\mathcal{A}_\mathrm{II}$的IND-CCA2游戏). 该游戏描述了敌手$\mathcal{A}_\mathrm{II}$与挑战者C的如下交互过程.

(1)初始化阶段. 挑战者C运行Setup算法生成系统主密钥msk和公开参数params,并将msk和params发送给$\mathcal{A}_\mathrm{II}$. $\mathcal{A}_\mathrm{II}$收到参数后,输出目标身份集合$\mathcal{L}^*=\{\mathrm{ID}_1,\mathrm{ID}_2,\cdots,\mathrm{ID}_n\}$.

(2)训练阶段1. 与Game_1相似,敌手$\mathcal{A}_\mathrm{II}$在该阶段可多项式有界次地执行除公钥替换之外的其他询问,并获得挑战者C的响应.

(3)挑战阶段. $\mathcal{A}_\mathrm{II}$选择等长的挑战消息集合$\mathcal{M}^0=\{M_1^0,M_2^0,\cdots,M_n^0\}$和$\mathcal{M}^1=\{M_1^1,M_2^1,\cdots,M_n^1\}$以及发送者身份标识$\mathrm{ID}_s$,并发送给挑战者$C$. C通过公钥生成询问查询集合$\mathcal{L}^*=\{\mathrm{ID}_1,\mathrm{ID}_2,\cdots,\mathrm{ID}_n\}$对应的公钥集合$\mathcal{I}^*=\{\mathrm{PK}_1,\mathrm{PK}_2,\cdots,\mathrm{PK}_n\}$,然后随机选取$\theta\in\{0,1\}$,计算密文$\sigma^*\leftarrow\mathrm{SignCrypt}(\mathrm{ID}_s,\mathrm{sk}_s,\mathcal{L}^*,\mathcal{I}^*,\mathcal{M}^\theta,\mathrm{params})$,并将$\sigma^*$返回给敌手$\mathcal{A}_\mathrm{II}$.

(4)训练阶段2. 与训练阶段1相同,敌手$\mathcal{A}_\mathrm{II}$可多项式有界次地执行上述询问,并得到挑战者C的响应.

(5)猜测. 敌手$\mathcal{A}_\mathrm{II}$输出对随机数θ的猜测θ',若$\theta'=\theta$且下列条件成立,则称$\mathcal{A}_\mathrm{II}$在游戏中获胜.

条件1:$\mathcal{A}_\mathrm{II}$未执行公钥替换询问;

条件2:$\mathcal{A}_\mathrm{II}$未执行针对目标集合中任意设备$\mathrm{ID}_i\in\mathcal{L}^*$的私钥生成询问;

条件3:$\mathcal{A}_\mathrm{II}$未执行针对发送者ID_s、接收者$\mathrm{ID}_i\in\mathcal{L}^*$以及目标密文$\sigma^*$的解签密询问.

$\mathcal{A}_\mathrm{II}$赢得该游戏的优势可定义为

$$\mathrm{Adv}^{\mathrm{IND\text{-}CCA2}}(\mathcal{A}_\mathrm{II})=\left|\Pr[\theta'=\theta]-\frac{1}{2}\right|$$

定义1　(签密方案的机密性)对于任意概率多项式时间敌手$\mathcal{A}_\mathrm{I}$和$\mathcal{A}_\mathrm{II}$,其赢得上述游戏Game_1和Game_2的优势$\mathrm{Adv}^{\mathrm{IND\text{-}CCA2}}(\mathcal{A}_\mathrm{I})$和$\mathrm{Adv}^{\mathrm{IND\text{-}CCA2}}(\mathcal{A}_\mathrm{II})$是可忽略的,则称签密方案满足机密性要求.

3.2.2　不可伪造性

通过定义游戏Game_3和Game_4来刻画两类敌手对方案不可伪造性的攻击,具体定义如下.

Game_3(敌手$\mathcal{A}_\mathrm{I}$的EUF-CMA游戏)该游戏描述了敌手$\mathcal{A}_\mathrm{I}$与挑战者C的如下交互过程.

(1)初始化阶段. 挑战者C运行Setup算法生成系统主密钥msk和公开参数params,秘密保存msk,并将params发送给$\mathcal{A}_\mathrm{I}$.

(2)询问阶段. 与Game_1的"训练阶段1"一致,敌手$\mathcal{A}_\mathrm{I}$可多项式有界次地执行哈希询问、公钥生成询问、私钥生成询问、公钥替换询问、签密询问和解签密询问.

(3)伪造阶段. 敌手$\mathcal{A}_\mathrm{I}$伪造发送者ID_s^*关于消息集合$\mathcal{M}=\{M_1,M_2,\cdots,M_n\}$和接收者集合$\mathcal{L}=\{\mathrm{ID}_1,\mathrm{ID}_2,\cdots,\mathrm{ID}_n\}$的签密密文$\sigma$,若存在接收者$\mathrm{ID}_i\in\mathcal{L}$验证$\sigma$有效并解签密得到对应的消息$M_i$,并且下列条件成立,则称$\mathcal{A}_\mathrm{I}$在游戏中获胜.

条件1:$\mathcal{A}_\mathrm{I}$在游戏过程中未获取到系统主密钥msk;

条件2:$\mathcal{A}_\mathrm{I}$未执行针对设备ID_s^*的私钥生成询问;

条件3:$\mathcal{A}_\mathrm{I}$未执行针对发送者ID_s^*、接收者$\mathrm{ID}_i\in\mathcal{L}$以及对应消息$M_i\in\mathcal{M}$的签密询问.

$\mathcal{A}_\mathrm{I}$赢得该游戏的优势可定义为

$$\mathrm{Adv}^{\mathrm{EUF\text{-}CMA}}(\mathcal{A}_\mathrm{I})=\Pr[\mathrm{UnSignCrypt}(\sigma^*)\neq\perp]$$

Game_4(敌手$\mathcal{A}_\mathrm{II}$的EUF-CMA游戏). 该游戏描述了敌手$\mathcal{A}_\mathrm{II}$与挑战者C的如下交互过程.

(1)初始化阶段. 挑战者C运行Setup算法生成系统主密钥msk和公开参数params,并将msk和params发送给$\mathcal{A}_\mathrm{II}$.

(2)询问阶段. 与Game_2的"训练阶段1"一致,敌手$\mathcal{A}_\mathrm{II}$可多项式有界次执行哈希询问、公钥生成询问、私钥生成询问、签密询问和解签密询问.

(3)伪造阶段. 敌手$\mathcal{A}_\mathrm{II}$伪造发送者ID_s^*关于消息集合$\mathcal{M}=\{M_1,M_2,\cdots,M_n\}$和接收者集合$\mathcal{L}=$

$\{\mathrm{ID}_1,\mathrm{ID}_2,\cdots,\mathrm{ID}_n\}$的签密密文$\sigma$,若存在接收者$\mathrm{ID}_i\in\mathcal{L}$验证$\sigma$有效并解签密得到对应的消息$M_i$,并且下列条件成立,则称$\mathcal{A}_{\mathrm{II}}$在游戏中获胜.

条件1:$\mathcal{A}_{\mathrm{II}}$未执行公钥替换询问;

条件2:$\mathcal{A}_{\mathrm{II}}$未执行针对设备$\mathrm{ID}_s^*$的私钥生成询问;

条件3:$\mathcal{A}_{\mathrm{II}}$未执行针对发送者$\mathrm{ID}_s^*$、接收者$\mathrm{ID}_i\in\mathcal{L}$以及对应消息$M_i\in\mathcal{M}$的签密询问.

$\mathcal{A}_{\mathrm{II}}$赢得该游戏的优势可定义为

$$\mathrm{Adv}^{\text{EUF-CMA}}(\mathcal{A}_{\mathrm{II}})=\Pr[\mathrm{UnSignCrypt}(\sigma^*)\neq\perp]$$

定义2 (签密方案的不可伪造性)对于任意概率多项式时间敌手$\mathcal{A}_{\mathrm{I}}$和$\mathcal{A}_{\mathrm{II}}$,其赢得上述游戏$\mathrm{Game}_3$和$\mathrm{Game}_4$的优势$\mathrm{Adv}^{\text{EUF-CMA}}(\mathcal{A}_{\mathrm{I}})$和$\mathrm{Adv}^{\text{EUF-CMA}}(\mathcal{A}_{\mathrm{II}})$是可忽略的,则称签密方案满足不可伪造性要求.

4 签密方案设计与正确性分析

4.1 方案设计

本文所提出的签密方案包含8个多项式时间算法,分别为初始化Setup、秘密值生成SetSecret、部分公/私钥生成ExtractPartialKey、密钥生成SetUserKey、离线签密Offline SignCrypt、在线签密Online SignCrypt、解签密UnSignCrypt和参数更新ParamsUpdate.

(1)初始化Setup

KGC选择有限域F_q上的椭圆曲线$E_{a,b}:y^2=x^3+ax+b$,其中,q($q\geqslant 2^\kappa$,κ为安全参数)为大素数,a、b满足$4a^3+27b^2\neq 0 \bmod q$,并选取阶为大素数p($p\geqslant 2^\kappa$)、生成元为$P\in E_{a,b}$的循环群G. KGC随机选取$k_M\in Z_p^*$作为系统主密钥,计算相应公钥$P_{\mathrm{Pub}}=k_MP$,并选择安全的哈希函数$H_1:\{0,1\}^*\to\{0,1\}^{L_{\mathrm{ID}}}$、$H_2:\{0,1\}^*\times G\to Z_p^*$、$H_3:\{0,1\}^{L_{\mathrm{ID}}}\times G\times G\to Z_p^*$、$H_4:\{0,1\}^*\times G\times G\to Z_p^*$、$H_5:\{0,1\}^*\times G\times G\to Z_p^*$,其中,$L_{\mathrm{ID}}$为设备身份标识的长度,$L_m$为消息$m$的长度. 然后,选择与文献[15]类似的单向索引函数$F^{\mathrm{N}}(\mathrm{ID})\to\{1\leqslant j\leqslant N,j\in Z_p^*\}$,该函数将$N$个身份标识均匀地映射到{1, 2, …, N}且不产生碰撞冲突,身份标识为ID的设备通过该函数可计算得到其对应的密文在集合中的索引值. 最后,KGC公开参数$\mathrm{params}=\{E_{a,b},q,p,P,G,P_{\mathrm{Pub}},F,H_1,H_2,H_3,H_4,H_5\}$,并秘密保存系统主密钥$\mathrm{msk}=k_M$.

(2)秘密值生成SetSecret

设备ID_i随机选取$x_i\in Z_p^*$,计算$X_i=x_iP$,并向KGC提交$<\mathrm{ID}_i,X_i>$.

(3)部分公/私钥生成ExtractPartialKey

KGC收到$<\mathrm{ID}_i,X_i>$后,随机选取$r_i\in Z_p^*$,并获取当前时间戳t_{kgc}. 然后计算$R_i=r_iP$,$h_i=H_3(\mathrm{ID}_i,X_i,R_i)$,$y_i=k_M+r_ih_i$,$z_i=y_i+H_2(t_{\mathrm{kgc}},\mathrm{ID}_i,r_iX_i)$,并向$\mathrm{ID}_i$回复$<t_{\mathrm{kgc}},z_i,R_i>$.

(4)密钥生成SetUserKey

ID_i收到$<t_{\mathrm{kgc}},z_i,R_i>$后,首先获取当前时间戳$t_i$,判断$\Delta t=|t_i-t_{\mathrm{kgc}}|$是否在可接受的时间范围内. 若可接受,则继续执行后续操作;否则,返回消息超时.

ID_i计算$h_i=H_3(\mathrm{ID}_i,X_i,R_i)$,验证等式$z_iP=P_{\mathrm{Pub}}+h_iR_i+H_2(t_{\mathrm{kgc}},\mathrm{ID}_i,x_iR_i)P$是否成立. 若上述等式成立,$\mathrm{ID}_i$计算$y_i'=z_i-H_2(t_{\mathrm{kgc}},\mathrm{ID}_i,x_iR_i)$,并继续执行后续操作;否则,$\mathrm{ID}_i$终止操作. 特别地,$y_i'$的正确性由等式$y_i'=z_i-H_2(t_{\mathrm{kgc}},\mathrm{ID}_i,x_iR_i)=z_i-H_2(t_{\mathrm{kgc}},\mathrm{ID}_i,x_ir_iP)=z_i-H_2(t_{\mathrm{kgc}},\mathrm{ID}_i,r_iX_i)=y_i$可知. 至此,$\mathrm{ID}_i$得到其公钥$\mathrm{PK}_i=(X_i,R_i)$和私钥$\mathrm{sk}_i=(x_i,y_i)$. 在此基础上,$\mathrm{ID}_i$随机选取$c_i\in Z_p^*$,利用其PUF和模糊提取器得$\omega_i\leftarrow\mathrm{PUF}_i(c_i)$,$(d_i,\mathrm{hd}_i)\leftarrow\mathrm{Gen}(\omega_i)$. 然后,$\mathrm{ID}_i$计算$\tilde{x}_i=H_2(d_i,X_i)\oplus x_i$,$\tilde{y}_i=H_2(d_i,R_i)\oplus y_i$,令$\tilde{s}=(\tilde{x}_i,\tilde{y}_i)$,并保存参数$<\mathrm{PK}_i=(X_i,R_i),\tilde{s}=(\tilde{x}_i,\tilde{y}_i),c_i,\mathrm{hd}_i>$.

(5)离线签密Offline SignCrypt

消息发送者ID_s执行如下步骤:

①为实现对发送者身份隐私的保护,在每次进行签密时,发送者随机选取$x_s^*\in Z_p^*$作为其临时私钥,并计算对应的临时公钥$X_s^*=x_s^*P$.

②对于消息接收者集合$\mathcal{L}=\{\mathrm{ID}_1,\mathrm{ID}_2,\cdots,\mathrm{ID}_n\}$中的每个接收者$\mathrm{ID}_i(i=1,2,\cdots,n)$,发送者$\mathrm{ID}_s$计算索引值$J_{R_i}=F^n(\mathrm{ID}_i)$,$h_i=H_3(\mathrm{ID}_i,X_i,R_i)$,$Q_i=x_s^*(X_i+h_iR_i+P_{\mathrm{Pub}})$.

(6)在线签密Online SignCrypt

对于待发送的消息集合$\mathcal{M}=\{M_1,M_2,\cdots,M_n\}$,发送者$\mathrm{ID}_s$执行如下步骤:

①ID_s利用其PUF和模糊提取器得到$\bar{\omega}_s\leftarrow\mathrm{PUF}_s(c_s)$,$d_s\leftarrow\mathrm{Rep}(\bar{\omega}_s,\mathrm{hd}_s)$,计算$x_s=H_2(d_s,X_s)\oplus\tilde{x}_s$,$y_s=H_2(d_s,R_s)\oplus\tilde{y}_s$,并获取当前时间戳$t_s$.

②对于接收者$\mathrm{ID}_i(i=1,2,\cdots,n)$,分别计算$\alpha_i=H_4(t_s,\mathrm{ID}_i,X_s^*,Q_i)$,$\gamma_i=\alpha_i\oplus M_i$以及临时身份标识$\mathrm{pid}_i=\mathrm{ID}_s\oplus H_1(\alpha_i\|M_i)$,其中符号"‖"为消息连接符,并将$(\mathrm{pid}_i,\gamma_i)$存入集合$\Gamma_s$,即$\Gamma_s[J_{R_i}]\leftarrow(\mathrm{pid}_i,\gamma_i)$.

③ID_s计算$\eta_s=y_s+(x_s+x_s^*)H_5(t_s,\mathrm{ID}_s,\Gamma_s,X_s,R_s,X_s^*)$,构造签密密文$\sigma_s=(t_s,\eta_s,\Gamma_s,X_s^*)$,并通过广播信道将$\sigma_s$发送给各个接收者.

(7)解签密UnSignCrypt

接收者$\mathrm{ID}_i(i=1,2,\cdots,n)$收到密文后,执行如下操作:

①获取当前时间戳t_i,判断$\Delta t'=|t_i-t_s|$是否在可接受的时间范围内. 若可接受,则继续执行后续操作;否则,返回消息超时.

②利用其PUF和模糊提取器得到$\bar{\omega}_i\leftarrow\mathrm{PUF}_i(c_i)$,$d_i\leftarrow\mathrm{Rep}(\bar{\omega}_i,\mathrm{hd}_i)$,并计算$x_i=H_2(d_i,X_i)\oplus\tilde{x}_i$,$y_i=H_2(d_i,R_i)$

$\oplus\tilde{y}_i$. 然后计算索引值$J_{R_i}=F^n(\mathrm{ID}_i)$,并利用$J_{R_i}$在集合$\Gamma_s$中查找对应的参数$(\mathrm{pid}_i,\gamma_i)$.

③分别计算$Q_i'=(x_i+y_i)X_s^*$,$\alpha_i=H_4(t_s,\mathrm{ID}_i,X_s^*,Q_i')$,$M_i=\alpha_i\oplus\gamma_i$,$\mathrm{ID}_s=\mathrm{pid}_i\oplus H_1(\alpha_i\|M_i)$. 在此基础上,接收者可以得到发送者的真实公钥$(X_s,R_s)$,并计算$h_s=H_3(\mathrm{ID}_s,X_s,R_s)$. 特别地,$Q_i'$的正确性由等式$Q_i'=(x_i+y_i)X_s^*=x_s^*(x_i+y_i)P=x_s^*(X_i+h_iR_i+P_{\mathrm{Pub}})=Q_i$可知.

④验证等式$\eta_sP=P_{\mathrm{Pub}}+h_sR_s+H_5(t_s,\mathrm{ID}_s,\Gamma_s,X_s,R_s,X_s^*)(X_s+X_s^*)$是否成立. 若成立,则接受消息$M_i$;否则,返回验证失败.

(8)参数更新ParamsUpdate

设备ID_i可根据通信环境条件灵活选择合适的时机来执行参数更新算法,该过程由ID_i与KGC交互完成,具体操作如下:

①ID_i利用其PUF和模糊提取器得到$\bar{\omega}_i'\leftarrow\mathrm{PUF}_i(c_i)$,$d_i\leftarrow\mathrm{Rep}(\bar{\omega}_i',\mathrm{hd}_i)$,并计算$x_i=H_2(d_i,X_i)\oplus\tilde{x}_i$,$y_i=H_2(d_i,R_i)\oplus\tilde{y}_i$. ID_i随机选取$x_i'\in Z_p^*$,并获取当前时间戳t_i',计算$X_i'=x_i'P$,$u_i=H_4(t_i',X_i',x_i'P_{\mathrm{Pub}})$,$\psi_i=y_i+(x_i+x_i')H_5(t_i',\mathrm{ID}_i,X_i,R_i,X_i')$以及临时身份标识$\mathrm{TID}_i=\mathrm{ID}_i\oplus H_1(u_i)$,并向KGC发送$<t_i',\mathrm{TID}_i,\psi_i,X_i'>$作为参数更新请求.

②KGC收到消息后,首先验证时间戳t_i'是否可接受. 若可接受,则继续执行后续操作;否则,返回消息超时. KGC计算$u_i'=H_4(t_i',X_i',k_MX_i')$,$\mathrm{ID}_i=\mathrm{TID}_i\oplus H_1(u_i')$,$h_i=H_3(\mathrm{ID}_i,X_i,R_i)$,并验证$\psi_iP=P_{\mathrm{Pub}}+h_iR_i+H_5(t_i',\mathrm{ID}_i,X_i,R_i,X_i')(X_i+X_i')$是否成立. 若成立,则继续执行后续操作;否则,返回验证失败. KGC随机选取$r_i'\in Z_p^*$,获取当前时间戳t_{kgc}',计算$R_i'=r_i'P$,$h_i'=H_3(\mathrm{ID}_i,X_i',R_i')$,$y_i'=k_M+r_i'h_i'$,$z_i'=y_i'+H_2(t_{\mathrm{kgc}}',\mathrm{ID}_i,r_i'X_i')$,并向$\mathrm{ID}_i$回复$<t_{\mathrm{kgc}}',z_i',R_i'>$.

③ID_i收到消息后,首先验证时间戳t_{kgc}'是否可接受. 若可接受,则继续执行后续操作;否则,返回消息超时. ID_i计算$h_i'=H_3(\mathrm{ID}_i,X_i',R_i')$,验证等式$z_i'P=P_{\mathrm{Pub}}+h_i'R_i'+H_2(t_{\mathrm{kgc}}',\mathrm{ID}_i,x_i'R_i')P$是否成立. 若上述等式成立,$\mathrm{ID}_i$计算$y_i'=z_i'-H_2(t_{\mathrm{kgc}}',\mathrm{ID}_i,x_i'R_i')$,得到新的公/私钥$<\mathrm{PK}_i'=(X_i',R_i')\ \mathrm{sk}_i'=(x_i',y_i')>$,并继续执行后续操作;否则,$\mathrm{ID}_i$终止操作. 在此基础上,$\mathrm{ID}_i$随机选取$c_i'\in Z_p^*$,利用其PUF和模糊提取器得到$\omega_i'\leftarrow\mathrm{PUF}_i(c_i')$,$(d_i',\mathrm{hd}_i')\leftarrow\mathrm{Gen}(\omega_i')$,然后计算$\tilde{x}_i'=H_2(d_i',X_i')\oplus x_i'$,$\tilde{y}_i'=H_2(d_i',R_i')\oplus y_i'$,令$\tilde{s}=(\tilde{x}_i',\tilde{y}_i')$,并将保存的参数更新为$<\mathrm{PK}_i'=(X_i',R_i')\ \tilde{s}=(\tilde{x}_i',\tilde{y}_i')\ c_i',\mathrm{hd}_i'>$.

4.2　正确性分析

(1)密钥生成的正确性

设备ID_i通过密钥生成算法得到其完整公/私钥$\mathrm{PK}_i=(X_i,R_i)$和$\mathrm{sk}_i=(x_i,y_i)$,其中X_i和x_i由该设备产生,而部分公/私钥R_i和y_i由KGC计算得到. 因而,ID_i在收到KGC向其分配的参数$<z_i,R_i>$时应对其正确性进行验证. 由于$z_iP=(y_i+H_2(t_{\mathrm{kgc}},\mathrm{ID}_i,r_iX_i))P=(k_M+r_ih_i+H_2(t_{\mathrm{kgc}},\mathrm{ID}_i,r_ix_iP))P=P_{\mathrm{Pub}}+h_iR_i+H_2(t_{\mathrm{kgc}},\mathrm{ID}_i,x_iR_i)P$,其中$h_i=H_3(\mathrm{ID}_i,X_i,R_i)$,则当等式$z_iP=P_{\mathrm{Pub}}+h_iR_i+H_2(t_{\mathrm{kgc}},\mathrm{ID}_i,x_iR_i)P$成立时,$\mathrm{ID}_i$可知其收到的参数$<z_i,R_i>$为KGC产生的合法参数. 在此基础上,$\mathrm{ID}_i$可计算得到部分私钥$y_i=z_i-H_2(t_{\mathrm{kgc}},\mathrm{ID}_i,x_iR_i)$,并且$y_i$与$R_i$满足关系$y_iP=P_{\mathrm{Pub}}+h_iR_i$.

(2)签密消息验证的正确性

在签密过程中,消息发送者ID_s计算(X_s^*,x_s^*)作为其临时公/私钥对,其中,$x_s^*\in Z_p^*$为ID_s选取的随机数且$X_s^*=x_s^*P$. 对于消息接收者ID_i,由于$\eta_sP=(y_s+(x_s+x_s^*)\cdot H_5(t_s,\mathrm{ID}_s,\Gamma_s,X_s,R_s,X_s^*))P=P_{\mathrm{Pub}}+h_sR_s+H_5(t_s,\mathrm{ID}_s,\Gamma_s,H_5(t_s,\mathrm{ID}_s,\Gamma_s,X_s,R_s,X_s^*)(X_s+X_s^*)[Xs,Rs,X^*s)(Xs+X^*s)]$,则当等式$\eta_sP=P_{\mathrm{Pub}}+h_sR_s+H_5(t_s,\mathrm{ID}_s,\Gamma_s,X_s,R_s,X_s^*)\cdot(X_s+X_s^*)$成立时,接收者$\mathrm{ID}_i$可以确认收到的消息由合法设备产生.

5　安全性分析

5.1　形式化证明

本节基于第3.2节所述安全模型,通过定理1和定理2证明签密方案在随机谕言机模型下的机密性和不可伪造性.

定理1　若ECCDH问题是困难的,则针对敌手$\mathcal{A}_{\mathrm{I}}$和$\mathcal{A}_{\mathrm{II}}$,方案是IND-CCA2安全的.

定理1可通过如下引理1和引理2进行形式化证明.

引理1　若敌手$\mathcal{A}_{\mathrm{I}}$在多项式时间内能够以不可忽略的优势ϵ_1赢得游戏$\mathrm{Game}_{\mathrm{I}}$(在该游戏过程中,$\mathcal{A}_{\mathrm{I}}$最多进行$q_{h_i}$次哈希$H_i(i=3,4,5)$询问、$q_{\mathrm{pk}}$次公钥生成询问、$q_{\mathrm{sk}}$次私钥生成询问、$q_{\mathrm{pkr}}$次公钥替换询问、$q_s$次签密询问和$q_{\mathrm{us}}$次解签密询问),则存在敌手$C$能在多项式时间内以不可忽略优势$\frac{\epsilon_1}{\mathrm{e}(1+q_{\mathrm{sk}}+q_s+q_{\mathrm{us}})}\left(1-\frac{n}{2^{L_{\mathrm{ID}}}}\right)^{q_{\mathrm{sk}}+q_s+q_{\mathrm{us}}+1}\left(1-\frac{q_{\mathrm{pkr}}}{2^{L_{\mathrm{ID}}}}\right)^{q_{\mathrm{us}}}\left(1-q_{\mathrm{us}}\left(\frac{1}{2^{L_m}}+\frac{1}{2^{\kappa}}\right)\right)$解决ECCDH问题,其中e为自然对数的底数.

证明　敌手C从ECCDH困难问题的挑战者处获得公开参数$(E_{a,b},q,p,P,G)$和挑战元组$(P,\alpha P,\beta P)$,并作为挑战者与敌手$\mathcal{A}_{\mathrm{I}}$执行$\mathrm{Game}_{\mathrm{I}}$的交互过程.

(1)初始化阶段. C运行初始化算法得到$\mathrm{params}=\{E_{a,b},q,p,P,G,P_{\mathrm{Pub}},F,H_1,H_2,H_3,H_4,H_5\}$和系统主密钥$\mathrm{msk}=k_M$,其中,$H_1$和$H_2$为安全的单向哈希函数,$H_i(i=$

3,4,5)为随机谕言机. C将params发送给$\mathcal{A}_1$,并秘密保存msk. 此外,C维持列表$L_{H_i}(i=3,4,5)$、L_{pk}和L_{sk}用于分别记录哈希$H_i(i=3,4,5)$询问、公钥生成询问以及私钥生成询问. $\mathcal{A}_1$收到公开参数后,输出目标身份集合$\mathcal{L}^*=\{\text{ID}_1,\text{ID}_2,\cdots,\text{ID}_n\}$.

(2)训练阶段1. 敌手$\mathcal{A}_1$可多项式有界次地执行下述询问:

公钥生成询问:敌手$\mathcal{A}_1$输入ID_i进行公钥生成询问时,若存在$(\text{ID}_i,X_i,R_i,\rho_i)\in L_{\text{pk}}$,则$C$返回相应的$(X_i,R_i)$给$\mathcal{A}_1$;否则,$C$随机选取$\rho_i\leftarrow\{0,1\}$且$\Pr[\rho_i=1]=\delta$,并进行如下操作:

①若$\text{ID}_i\notin\mathcal{L}^*$且$\rho_i=0$,$C$随机选取$x_i,y_i,h_3^i\in Z_p^*$,计算$X_i=x_iP$和$R_i=(h_3^i)^{-1}(y_iP-P_{\text{Pub}})$. 上述参数需满足条件$(*,X_i,R_i,*)\notin L_{\text{pk}}$、$(*,x_i,y_i)\notin L_{\text{sk}}$以及$(*,*,*,h_3^i)\notin L_{H_3}$(若参数不满足条件,$C$需重新选取随机数并计算相关参数). 然后,$C$将$(\text{ID}_i,X_i,R_i,\rho_i)$添加至列表$L_{\text{pk}}$,将$(\text{ID}_i,x_i,y_i)$添加至列表$L_{\text{sk}}$,将$(\text{ID}_i,X_i,R_i,h_3^i)$添加至列表$L_{H_3}$,并将$(X_i,R_i)$返回给$\mathcal{A}_1$.

②若$\text{ID}_i\notin\mathcal{L}^*$且$\rho_i=1$,$C$随机选取$\xi_i,y_i,h_3^i\in Z_p^*$,计算$X_i=\xi_i(\alpha P)$(隐含地设置$x_i=\xi_i\alpha$,由于$C$不掌握参数$\alpha$,将$\xi_i\alpha$记为$\perp$)和$R_i=(h_3^i)^{-1}(y_iP-P_{\text{Pub}})$. 上述参数需满足条件$(*,X_i,R_i,*)\notin L_{\text{pk}}$、$(*,\perp,y_i)\notin L_{\text{sk}}$以及$(*,*,*,h_3^i)\notin L_{H_3}$. 然后,$C$将$(\text{ID}_i,X_i,R_i,\rho_i)$添加至列表$L_{\text{pk}}$,将$(\text{ID}_i,\perp,y_i)$添加至列表$L_{\text{sk}}$,将$(\text{ID}_i,X_i,R_i,h_3^i)$添加至列表$L_{H_3}$,并将$(X_i,R_i)$返回给$\mathcal{A}_1$.

③若$\text{ID}_i\in\mathcal{L}^*$,$C$随机选取$x_i,\zeta_i,h_3^i\in Z_p^*$,计算$X_i=x_iP$和$R_i=(h_3^i)^{-1}(\zeta_i(\beta P)-P_{\text{Pub}})$(隐含地设置$y_i=\zeta_i\beta$,由于$C$不掌握参数$\beta$,将$\zeta_i\beta$记为$\perp$). 上述参数需满足条件$(*,X_i,R_i,*)\notin L_{\text{pk}}$、$(*,x_i,\perp)\notin L_{\text{sk}}$以及$(*,*,*,h_3^i)\notin L_{H_3}$. 然后,$C$将$(\text{ID}_i,X_i,R_i,\rho_i)$添加至列表$L_{\text{pk}}$,将$(\text{ID}_i,x_i,\perp)$添加至列表$L_{\text{sk}}$,将$(\text{ID}_i,X_i,R_i,h_3^i)$添加至列表$L_{H_3}$,并将$(X_i,R_i)$返回给$\mathcal{A}_1$.

H_3询问:敌手$\mathcal{A}_1$输入参数(ID_i,X_i,R_i)对H_3进行询问时,C查询列表L_{H_3}中是否存在元组$(\text{ID}_i,X_i,R_i,h_3^i)$. 如果存在,则$C$将$h_3^i$返回给$\mathcal{A}_1$;否则,$C$对$\text{ID}_i$进行公钥生成询问后返回相应参数$h_3^i$给$\mathcal{A}_1$.

H_4询问:敌手$\mathcal{A}_1$输入参数$(t_s,\text{ID}_i,X_s^*,Q_i)$对$H_4$进行询问时,$C$查询列表$L_{H_4}$中是否存在元组$(t_s,\text{ID}_i,X_s^*,Q_i,h_4^i)$. 如果存在,则$C$将$h_4^i$返回给$\mathcal{A}_1$;否则,$C$选取满足条件$(*,*,*,*,h_4^i)\notin L_{H_4}$的随机数$h_4^i\in\{0,1\}^{L_m}$,将$(t_s,\text{ID}_i,X_s^*,Q_i,h_4^i)$添加至列表$L_{H_4}$,并将参数$h_4^i$返回给$\mathcal{A}_1$.

H_5询问:敌手$\mathcal{A}_1$输入参数$(t_s,\text{ID}_s,\Gamma_s,X_s,R_s,X_s^*)$对$H_5$进行询问时,$C$查询列表$L_{H_5}$中是否存在元组$(t_s,\text{ID}_s,\Gamma_s,X_s,R_s,X_s^*,h_5^i)$. 如果存在,则$C$将$h_5^i$返回给$\mathcal{A}_1$;否则,$C$选取满足条件$(*,*,*,*,*,*,h_5^i)\notin L_{H_5}$的随机数$h_5^i\in Z_p^*$,将$(t_s,\text{ID}_s,\Gamma_s,X_s,R_s,X_s^*,h_5^i)$添加至列表$L_{H_5}$,并将参数$h_5^i$返回给$\mathcal{A}_1$.

私钥生成询问:敌手$\mathcal{A}_1$输入ID_i进行私钥生成询问时,C查询列表L_{sk}中是否存在元组(ID_i,x_i,y_i). 如果存在,则C将(x_i,y_i)返回给$\mathcal{A}_1$;如果不存在,C对ID_i进行公钥生成询问后获得元组$(\text{ID}_i,X_i,R_i,\rho_i)$,若$\text{ID}_i\notin\mathcal{L}^*$且$\rho_i=0$,则在公钥生成询问过程中已经生成了相应的私钥,$C$查询列表$L_{\text{sk}}$并返回相应参数$(x_i,y_i)$给$\mathcal{A}_1$;否则,$C$停止模拟并退出.

公钥替换询问:敌手$\mathcal{A}_1$输入(ID_i,X_i',R_i')进行公钥替换询问时,C查询列表L_{pk}中是否存在元组(ID_i,X_i,R_i). 如果存在,则C将(ID_i,X_i,R_i)替换为(ID_i,X_i',R_i');否则,C对ID_i进行公钥生成询问后将(ID_i,X_i,R_i)替换为(ID_i,X_i',R_i').

签密询问:敌手$\mathcal{A}_1$输入$(\text{ID}_s,\mathcal{L},\mathcal{M})$(其中,$\mathcal{L}=\{\text{ID}_1,\text{ID}_2,\cdots,\text{ID}_n\}$为接收者集合,$\mathcal{M}=\{M_1,M_2,\cdots,M_n\}$为消息集合)进行签密询问时,$C$输入$\text{ID}_s$进行公钥生成询问,并从列表$L_{\text{pk}}$获得对应元组$(\text{ID}_s,X_s,R_s,\rho_s)$. 若$\text{ID}_s\in\mathcal{L}^*$或$\rho_s=1$,$C$停止模拟并退出;否则,$C$输入$\text{ID}_s$进行私钥生成询问得到$(\text{ID}_s,x_s,y_s)$,对接收者集合$\mathcal{L}$中身份$\text{ID}_i(i=1,2,\cdots,n)$进行公钥生成询问得到$(\text{ID}_i,X_i,R_i,\rho_i)$,并执行如下操作:

①随机选取$x_s^*\in Z_p^*$,计算$X_s^*=x_s^*P$.

②对于接收者$\text{ID}_i(i=1,2,\cdots,n)$,计算索引值$J_{R_i}=F^n(\text{ID}_i)$,然后输入参数$(\text{ID}_i,X_i,R_i)$对$H_3$进行询问得到$h_3^i$,计算$Q_i=x_s^*(X_i+h_3^iR_i+P_{\text{Pub}})$,并输入参数$(t_s,\text{ID}_i,X_s^*,Q_i)$对$H_4$进行询问得到$h_4^i$. 令$\alpha_i=h_4^i$,分别计算$\gamma_i=\alpha_i\oplus M_i$,$\text{pid}_i=\text{ID}_s\oplus H_1(\alpha_i\|M_i)$,并将$(\text{pid}_i,\gamma_i)$存入集合$\Gamma_s$,即$\Gamma_s[J_{R_i}]\leftarrow(\text{pid}_i,\gamma_i)$.

③输入参数$(t_s,\text{ID}_s,\Gamma_s,X_s,R_s,X_s^*)$对$H_5$进行询问得到$h_5^s$,计算$\eta_s=y_s+(x_s+x_s^*)h_5^s$,构造签密密文$\sigma_s=(t_s,\eta_s,\Gamma_s,X_s^*)$,并返回参数$\sigma_s$给$\mathcal{A}_1$.

解签密询问:敌手$\mathcal{A}_1$输入签密密文$\sigma_s=(t_s,\eta_s,\Gamma_s,X_s^*)$和身份$\text{ID}_i$进行解签密询问,$C$输入$\text{ID}_i$进行公钥生成询问得到元组$(\text{ID}_i,X_i,R_i,\rho_i)$. 若$\text{ID}_i\in\mathcal{L}^*$或$\rho_i=1$,$C$停止模拟并退出;否则,$C$以$\text{ID}_i$为索引检索列表$L_{\text{sk}}$得到元组$(\text{ID}_i,x_i,y_i)$,并进行如下操作:

①计算索引值$J_{R_i}=F^n(\text{ID}_i)$,并利用J_{R_i}在集合Γ_s中查找对应的参数(pid_i,γ_i). 若对应参数不存在,则拒绝密文,停止模拟并退出;否则,得到(pid_i,γ_i).

②计算$Q_i=(x_i+y_i)X_s^*$,以$(t_s,\text{ID}_i,X_s^*,Q_i)$为索引检

索列表L_{H_4},若不存在元组$(t_s,\mathrm{ID}_i,X_s^*,Q_i,h_4^i)$,则拒绝密文,停止模拟并退出;否则,得到$h_4^i$.

③令$\alpha_i=h_4^i$,计算消息$M_i=\alpha_i\oplus\gamma_i$以及发送者身份标识$\mathrm{ID}_s=\mathrm{pid}_i\oplus H_1(\alpha_i\|M_i)$,并输入$\mathrm{ID}_s$进行公钥生成询问得到元组$(\mathrm{ID}_s,X_s,R_s,\rho_s)$.

④以(ID_s,X_s,R_s)为索引检索列表L_{H_3},若L_{H_3}中不存在元组$(\mathrm{ID}_s,X_s,R_s,h_3^s)$,则表明$\mathrm{ID}_s$对应的公钥被替换,停止模拟并退出;否则,得到$h_3^s$.

⑤以$(t_s,\mathrm{ID}_s,\Gamma_s,X_s,R_s,X_s^*)$为索引检索列表$L_{H_5}$,若不存在元组$(t_s,\mathrm{ID}_s,\Gamma_s,X_s,R_s,X_s^*,h_5^s)$,则拒绝密文,停止模拟并退出;否则,得到$h_5^s$.

⑥验证等式$\eta_sP=P_{\mathrm{Pub}}+h_3^sR_s+h_5^s(X_s+X_s^*)$是否成立. 若等式成立,则将消息$M_i$返回给$\mathcal{A}_{\mathrm{I}}$;否则,拒绝密文,停止模拟并退出.

(3)挑战阶段. 敌手$\mathcal{A}_{\mathrm{I}}$选择两个等长的挑战消息集合$\mathcal{M}^0=\{M_1^0,M_2^0,\cdots,M_n^0\}$和$\mathcal{M}^1=\{M_1^1,M_2^1,\cdots,M_n^1\}$以及发送者身份$\mathrm{ID}_s$,$C$输入$\mathrm{ID}_s$进行公钥生成询问得到元组$(\mathrm{ID}_s,X_s,R_s,\rho_s)$. 若$\mathrm{ID}_s\in\mathcal{L}^*$或$\rho_s=0$,则$C$终止并退出;若$\mathrm{ID}_s\notin\mathcal{L}^*$且$\rho_s=1$,$C$以$\mathrm{ID}_s$为索引检索列表$L_{\mathrm{sk}}$得到元组$(\mathrm{ID}_s,\perp,y_s)$,随机选取$\theta\in\{0,1\}$,对接收者集合$\mathcal{L}^*$中身份$\mathrm{ID}_i(i=1,2,\cdots,n)$进行公钥生成询问得到$(\mathrm{ID}_i,X_i,R_i,\rho_i)$,并按如下步骤生成签密密文:

①以(ID_s,X_s,R_s)为索引检索列表L_{H_3},若不存在元组$(\mathrm{ID}_s,X_s,R_s,h_3^s)$,则表明$\mathrm{ID}_s$对应的公钥被替换,$C$终止并退出;否则,$C$得到$h_3^s$.

②C选取满足$(*,*,*,*,*,*,h_5^s)\notin L_{H_5}$的随机数$h_5^s\in Z_p^*$,然后随机选取$l_s\in Z_p^*$,并令$X_s^*=l_sP-X_s$.

③对于接收者$\mathrm{ID}_i(i=1,2,\cdots,n)$,计算索引值$J_{R_i}=F^n(\mathrm{ID}_i)$,然后输入参数$(\mathrm{ID}_i,X_i,R_i)$对$H_3$进行询问得到$h_3^i$,并选取满足$(*,*,*,*,h_4^i)\notin L_{H_4}$的随机数$h_4^i\in\{0,1\}^{L_m}$,将$(t_s,\mathrm{ID}_i,X_s^*,*,h_4^i)$加入列表$L_{H_4}$. 然后令$\alpha_i=h_4^i$,$\gamma_i=\alpha_i\oplus M_i^{\theta}$,$\mathrm{pid}_i=\mathrm{ID}_s\oplus H_1(\alpha_i\|M_i^{\theta})$,并将$(\mathrm{pid}_i,\gamma_i)$存入集合$\Gamma_s$,即$\Gamma_s[J_{R_i}]\leftarrow(\mathrm{pid}_i,\gamma_i)$.

④C将元组$(t_s,\mathrm{ID}_s,\Gamma_s,X_s,R_s,X_s^*,h_5^s)$加入列表$L_{H_5}$,并计算$\eta_s=y_s+h_5^sl_s$. 显然,等式$\eta_sP=y_sP+h_5^sl_sP=P_{\mathrm{Pub}}+h_sR_s+h_5^s(X_s+X_s^*)$成立. 在此基础上,构造签密密文$\sigma^*=(t_s,\eta_s,\Gamma_s,X_s^*)$,并返回参数$\sigma^*$给$\mathcal{A}_{\mathrm{I}}$.

(4)训练阶段2. 与训练阶段1相同,敌手$\mathcal{A}_{\mathrm{I}}$可多项式有界次地执行上述询问,并得到C的响应. 特别地,敌手$\mathcal{A}_{\mathrm{I}}$不能执行针对任意设备$\mathrm{ID}_i\in\mathcal{L}^*$和目标密文$\sigma^*$的解签密询问.

(5)猜测. $\mathcal{A}_{\mathrm{I}}$输出对随机数θ的猜测值θ',若$\theta'=\theta$,则$\mathcal{A}_{\mathrm{I}}$以极大概率提交了$H_4(t_s,\mathrm{ID}_i,X_s^*,Q_i)$询问且$\mathrm{ID}_i\in\mathcal{L}^*$. 通过检索列表$L_{H_4}$,$C$可得到参数$Q_i$,并且以$\mathrm{ID}_i$为索引检索列表$L_{\mathrm{sk}}$可得到元组$(\mathrm{ID}_i,x_i,\perp)$. 由于$Q_i=(x_i+y_i)X_s^*$,$X_s^*=l_sP-X_s$,$X_s=\xi_s(\alpha P)$,$y_i=\zeta_i\beta$且$C$掌握参数$l_s$、$\xi_s$和$\zeta_i$,$C$可计算得到$\alpha\beta P=(\xi_s\zeta_i)^{-1}(x_il_sP+\zeta_il_s(\beta P)-x_i\xi_s(\alpha P)-Q_i)$,即$C$能够解决ECCDH困难问题. 相反,若$\theta'\neq\theta$,则$C$终止并退出,即$C$未解决ECCDH困难问题.

C为$\mathcal{A}_{\mathrm{I}}$模拟了真实的攻击环境,若C在模拟过程中未终止,且$\mathcal{A}_{\mathrm{I}}$能够以不可忽略的优势ϵ_1攻击签密方案的机密性,则C能够以不可忽略的优势解决ECCDH困难问题. 具体而言,当敌手$\mathcal{A}_{\mathrm{I}}$成功攻击签密方案,并且下列事件不发生时,C能够解决ECCDH困难问题.

事件E_1:在私钥生成询问中,C终止模拟并退出;

事件E_2:在签密询问中,C终止模拟并退出;

事件E_3:在解签密询问中,C终止模拟并退出;

事件E_4:在解签密询问中,C拒绝有效的签密密文;

事件E_5:在挑战阶段,C终止并退出.

对于事件E_1,当敌手$\mathcal{A}_{\mathrm{I}}$用于私钥生成询问的身份$\mathrm{ID}_i\in\mathcal{L}^*$或$\rho_s=1$时,该事件发生,其概率$\Pr[E_1]=1-\left(1-\frac{n}{2^{L_{\mathrm{ID}}}}\right)^{q_{\mathrm{sk}}}(1-\delta)^{q_{\mathrm{sk}}}$;对于事件$E_2$,当敌手用于签密询问的发送者身份$\mathrm{ID}_s\in\mathcal{L}^*$或$\rho_s=1$时,该事件发生,其概率$\Pr[E_2]=1-\left(1-\frac{n}{2^{L_{\mathrm{ID}}}}\right)^{q_s}(1-\delta)^{q_s}$;对于事件$E_3$,当敌手用于解签密询问的接收者身份$\mathrm{ID}_i\in\mathcal{L}^*$或$\rho_s=1$,或者发送者的公钥被替换时,该事件发生,其概率$\Pr[E_3]=1-\left(1-\frac{n}{2^{L_{\mathrm{ID}}}}\right)^{q_{\mathrm{us}}}(1-\delta)^{q_{\mathrm{us}}}\left(1-\frac{q_{\mathrm{pkr}}}{2^{L_{\mathrm{ID}}}}\right)^{q_{\mathrm{us}}}$;对于事件$E_4$,当敌手$\mathcal{A}_{\mathrm{I}}$未访问随机谕言机而通过猜测得到$H_i(i=4,5)$的值时,该事件发生,其概率$\Pr[E_4]=q_{\mathrm{us}}\left(\frac{1}{2^{L_m}}+\frac{1}{2^{\kappa}}\right)$;对于事件$E_5$,当敌手用于挑战的发送者身份$\mathrm{ID}_s\in\mathcal{L}^*$或$\rho_s=0$时,该事件发生,其概率$\Pr[E_5]=1-\left(1-\frac{n}{2^{L_{\mathrm{ID}}}}\right)\delta$.

可知,若$\mathcal{A}_{\mathrm{I}}$能够以不可忽略的优势ϵ_1攻击签密方案的机密性,则C解决ECCDH问题的优势

$$\begin{aligned}\epsilon_1'&=\epsilon_1\big(1-\Pr[E_1]\big)\big(1-\Pr[E_2]\big)\big(1-\Pr[E_3]\big)\\&\quad\cdot\big(1-\Pr[E_4]\big)(1-\Pr[E_5])=\epsilon_1\left(1-\frac{n}{2^{L_{\mathrm{ID}}}}\right)^{q_{\mathrm{sk}}+q_s+q_{\mathrm{us}}+1}\\&\quad\cdot\left(1-\frac{q_{\mathrm{pkr}}}{2^{L_{\mathrm{ID}}}}\right)^{q_{\mathrm{us}}}\left(1-q_{\mathrm{us}}\left(\frac{1}{2^{L_m}}+\frac{1}{2^{\kappa}}\right)\right)(1-\delta)^{q_{\mathrm{sk}}+q_s+q_{\mathrm{us}}}\delta\end{aligned}.$$

由不等式知识可知,当$\delta=\frac{1}{1+q_{\mathrm{sk}}+q_s+q_{\mathrm{us}}}$时,$(1-\delta)^{q_{\mathrm{sk}}+q_s+q_{\mathrm{us}}}\delta$取得最大值,并且当$q_{\mathrm{sk}}+q_s+q_{\mathrm{us}}$足够大时,$(1-\delta)^{q_{\mathrm{sk}}+q_s+q_{\mathrm{us}}}=\left(\frac{q_{\mathrm{sk}}+q_s+q_{\mathrm{us}}}{1+q_{\mathrm{sk}}+q_s+q_{\mathrm{us}}}\right)^{q_{\mathrm{sk}}+q_s+q_{\mathrm{us}}}$趋近于$\mathrm{e}^{-1}$,其中

e为自然对数的底数. 因此,在游戏过程中,C可令$\delta=\frac{1}{1+q_{\mathrm{sk}}+q_s+q_{\mathrm{us}}}$,此时$C$解决ECCDH困难问题的优势

$$\epsilon_1'=\frac{\epsilon_1}{\mathrm{e}(1+q_{\mathrm{sk}}+q_s+q_{\mathrm{us}})}\left(1-\frac{n}{2^{L_{\mathrm{ID}}}}\right)^{q_{\mathrm{sk}}+q_s+q_{\mathrm{us}}+1}\cdot\left(1-\frac{q_{\mathrm{pkr}}}{2^{L_{\mathrm{ID}}}}\right)^{q_{\mathrm{us}}}\left(1-q_{\mathrm{us}}\left(\frac{1}{2^{L_m}}+\frac{1}{2^{\kappa}}\right)\right)$$

引理2 若敌手$\mathcal{A}_{\mathrm{II}}$在多项式时间内能够以不可忽略的优势$\epsilon_2$赢得游戏$\mathrm{Game}_2$(在该游戏过程中,$\mathcal{A}_{\mathrm{II}}$最多进行$q_{h_i}$次哈希$H_i(i=3,4,5)$询问、$q_{\mathrm{pk}}$次公钥生成询问、$q_{\mathrm{sk}}$次私钥生成询问、$q_s$次签密询问和$q_{\mathrm{us}}$次解签密询问),则存在敌手$C$能够在多项式时间内以不可忽略的优势$\frac{\epsilon_2}{\mathrm{e}(1+q_{\mathrm{sk}}+q_s+q_{\mathrm{us}})}\left(1-\frac{n}{2^{L_{\mathrm{ID}}}}\right)^{q_{\mathrm{sk}}+q_s+q_{\mathrm{us}}+1}\left(1-q_{\mathrm{us}}\left(\frac{1}{2^{L_m}}+\frac{1}{2^{\kappa}}\right)\right)$**解决**ECCDH问题,其中e为自然对数底数.

该引理的证明思路与引理1相似,此处不再赘述.

综上所述,方案的机密性可归约为ECCDH问题的困难性,即若ECCDH问题是困难的,则方案是IND-CCA2安全的.

定理2 若ECDL问题是困难的,则针对敌手$\mathcal{A}_{\mathrm{I}}$和$\mathcal{A}_{\mathrm{II}}$,方案是EUF-CMA安全的.

定理2可通过如下引理3和引理4进行形式化证明.

引理3 若敌手$\mathcal{A}_{\mathrm{I}}$在多项式时间内能够以不可忽略的优势ϵ_3赢得游戏Game_3(在该游戏过程中,$\mathcal{A}_{\mathrm{I}}$最多进行q_{h_i}次哈希$H_i(i=3,4,5)$询问、q_{pk}次公钥生成询问、q_{sk}次私钥生成询问、q_{pkr}次公钥替换询问、q_s次签密询问和q_{us}次解签密询问),则存在敌手C能够在多项式时间内至少以不可忽略的优势$\left(1-\frac{1}{\mathrm{e}}\right)\frac{\epsilon_3}{\mathrm{e}(1+q_{\mathrm{sk}}+q_s+q_{\mathrm{us}})q_{h_5}}$解决ECDL问题,其中$e$为自然对数的底数.

引理4 若敌手$\mathcal{A}_{\mathrm{II}}$在多项式时间内能够以不可忽略的优势$\epsilon_4$赢得游戏$\mathrm{Game}_4$(在该游戏过程中,$\mathcal{A}_{\mathrm{II}}$最多进行$q_{h_i}$次哈希$H_i(i=3,4,5)$询问、$q_{\mathrm{pk}}$次公钥生成询问、$q_{\mathrm{sk}}$次私钥生成询问、$q_s$次签密询问和$q_{\mathrm{us}}$次解签密询问),则存在敌手$C$能够在多项式时间内至少以不可忽略的优势$\left(1-\frac{1}{\mathrm{e}}\right)\frac{\epsilon_4}{\mathrm{e}(1+q_{\mathrm{sk}}+q_s+q_{\mathrm{us}})q_{h_5}}$解决ECDL问题,其中e为自然对数的底数.

引理3和引理4的证明思路与引理1相似,结合分叉引理[25]的思想即可证明,此处不再赘述.

综上所述,方案的不可伪造性可归约为ECDL问题的困难性,即若ECDL问题是困难的,则方案是EUF-CMA安全的.

5.2 安全属性分析

在上述形式化证明的基础上,对方案的安全属性进行分析,包括机密性、不可伪造性、发送者匿名性、接收者匿名性、抗物理攻击、抗重放攻击、无密钥托管、无需安全信道等.

(1)机密性. 由定理1可知,方案的机密性可归约为ECCDH问题的困难性. 由形式化证明过程和ECCDH假设[9]可知,方案是IND-CCA2安全的,即在适应性选择密文攻击下具有不可区分性. 因此,所提出的签密方案能够保证消息的机密性.

(2)不可伪造性. 由定理2可知,方案的不可伪造性可归约为ECDL问题的困难性. 由形式化证明过程和ECDL假设[9]可知,方案是EUF-CMA安全的,即在适应性选择消息攻击下具有存在性不可伪造性. 因此,所提出的签密方案具备不可伪造性.

(3)发送者匿名性. 签密方案中发送者在每次执行签密操作时均选择新的临时公/私钥对(X_s^*,x_s^*),其中,$X_s^*=x_s^*P$且$x_s^*\in Z_p^*$为发送者选取的随机数. 由于参数x_s^*具有随机性和保密性,敌手和非授权的接收者均不能从临时公/私钥对(X_s^*,x_s^*)中获取到发送者的真实公/私钥信息,只有授权的接收者可以通过其私钥计算出相关参数,从而获得消息发送者的真实身份信息. 因此,方案能够实现对发送者的匿名性保护.

(4)接收者匿名性. 由签密过程可知,方案的签密密文中未包含消息接收者的身份信息,而将该信息隐藏于参数$\alpha_i=H_4(t_s,\mathrm{ID}_i,X_s^*,Q_i)$,其中$Q_i=x_s^*(X_i+h_iR_i+P_{\mathrm{Pub}})=(x_i+y_i)X_s^*$. 由ECCDH问题和ECDL问题的困难性[9]可知,Q_i具有保密性. 此外,由于哈希函数的单向性,敌手无法从相关参数中获得消息接收者的身份信息. 对于授权的消息接收者而言,其同样无法获取到其他接收者的身份信息. 因此,方案能够实现对接收者的匿名性保护.

(5)抗物理攻击. 敌手可通过物理攻击[20]获取到目标设备ID_i存储的全部参数$<X_i,R_i,\tilde{x}_i,\tilde{y}_i,c_i,\mathrm{hd}_i>$. 目标设备$\mathrm{ID}_i$的私钥$<x_i,y_i>$的计算方式为$x_i=H_2(d_i,X_i)\oplus\tilde{x}_i$,$y_i=H_2(d_i,R_i)\oplus\tilde{y}_i$,其中$d_i=\mathrm{Rep}(\bar{\omega}_i,\mathrm{hd}_i)$且$\bar{\omega}_i=\mathrm{PUF}_i(c_i)$. 由于PUF具有唯一性、不可预测性和抗篡改性,对PUF的非法访问和侵入式攻击将改变其映射关系并使其失效[24,27],即使敌手能够得到PUF的挑战值c_i,其仍然无法得到对应的参数d_i来计算设备的私钥. 此外,若敌手利用错误的参数d_i'计算并产生签密密文,则无法通过接收者的验证. 因此,方案能够抵抗物理攻击的威胁.

(6)抗重放攻击. 方案通过选取随机数和时间戳来保证消息的新鲜性,接收者在收到签密密文后首先通过

验证时间间隔$\Delta t=|t_i-t_s|$是否在可接受的时间范围内,以判断所收到消息的新鲜性. 由签密过程可知,方案中的时间戳通过带秘密参数的哈希函数与签密密文绑定,例如$\alpha_i=H_4(t_s,\mathrm{ID}_i,X_s^*,Q_i)$,由于参数$Q_i$的保密性,敌手无法将旧的时间戳$t_s$替换为新的时间戳$t_s'$并计算出对应的有效签密密文. 因此,方案能够抵抗重放攻击的威胁.

(7)无密钥托管. 方案基于无证书公钥密码体制提出,设备ID_i的私钥由x_i和y_i两部分组成. 由签密方案的秘密值生成过程和部分公/私钥生成过程可知,x_i由设备ID_i随机选取,KGC仅计算部分私钥y_i且无法得到x_i,即KGC无法得到设备的完整私钥. 因此,方案不存在密钥托管的问题.

(8)无需安全信道. 由签密方案的部分公/私钥生成过程可知,KGC为设备ID_i生成部分私钥y_i后,通过计算$z_i=y_i+H_2(t_{\mathrm{kgc}},\mathrm{ID}_i,r_iX_i)$来实现对$y_i$的隐藏,并将$z_i$发送给设备$\mathrm{ID}_i$. 由ECCDH问题和ECDL问题的困难性[9]可知,参数r_iX_i具有保密性,仅拥有参数r_i的KGC和拥有参数x_i的设备ID_i能够计算出该参数$r_iX_i=r_ix_iP=x_iR_i$. 因此,方案无需借助安全信道来实现注册参数的传递.

6　性能分析与对比

本节从安全属性、计算开销、通信开销等方面对所提出的签密方案进行分析,并与同类方案进行对比.

(1)安全属性

本文方案与同类方案[8,10,14,15,17,18]的安全性对比如表2所示.

表2　安全性对比

方案	机密性	不可伪造性	发送者匿名性	接收者匿名性	抗物理攻击	抗重放攻击	无密钥托管	无需安全信道	离线/在线方式	接收者数量	消息数量
文献[8]	√	√	×	√	×	×	√	×	√	单接收者	单消息
文献[10]	√	√	×	√	×	×	√	×	√	单接收者	单消息
文献[14]	√	√	×	√	×	×	√	×	×	多接收者	多消息
文献[15]	√	√	×	√	×	×	√	√	×	多接收者	多消息
文献[17]	√	√	×	√	×	×	√	×	√	单接收者	单消息
文献[18]	√	√	×	√	×	×	√	×	√	单接收者	单消息
本文	√	√	√	√	√	√	√	√	√	多接收者	多消息

由表2可知,同类方案和本文所提出的方案均能满足机密性、不可伪造性以及接收者匿名性等安全要求,并且不存在密钥托管的问题,但同类方案均未实现对发送者的匿名性保护并且无法抵抗物理攻击和重放攻击的威胁. 因此,相较于同类方案,本文所提出的签密方案具备更高的安全性.

此外,方案[8,10,17,18]仅支持单接收者单消息签密模式,若向多个接收者传递多条消息,则需重复执行签密操作;方案[14]和方案[15]虽然支持多接收者多消息签密模式,但未采用离线与在线相结合的方式.

(2)计算开销

在实验过程中,基于MIRACL函数库在内存为8 GB的Raspberry Pi 4B开发板上利用C++语言进行测试. 采用实现128-bit安全等级的椭圆曲线secp256k1[31]定义的相关参数,其中p和q均为256bit,G为512 bit. 由于文献[8]和文献[17]使用了双线性对运算,为便于分析比较,选取实现128-bit安全等级且双线性对友好(pairing-friendly)的BLS12-381曲线[32]构造Optimal ATE对[33]:$G_2\times G_1\to G_T$,其中G_1是有限域$F_{\bar{q}}$上阶为$\bar{p}$的循环群且$\bar{p}$为256 bit、$\bar{q}$为381 bit,G_2是有限域$F_{\bar{q}^2}$上的循环群,G_T是有限域$F_{\bar{q}^{12}}$上的乘法群的子群.

与文献[10]和文献[18]相同,采用复杂运算的执行次数来衡量各个方案的计算开销. 在上述实验环境的基础上,可以得到相关复杂运算的平均运行时间,如表3所示.

表3　复杂运算的符号表示及运行时间

符号	描述	运行时间/ms
$T_{\mathrm{sm}G}$	G上的点乘运算	2.35
$T_{\mathrm{sm}G_1}$	G_1上的点乘运算	2.83
$T_{\mathrm{sm}G_2}$	G_2上的点乘运算	6.02
$T_{\mathrm{e}G_T}$	G_T上的幂运算	7.76
T_{bp}	双线性对运算	24.34

由方案执行过程可知,当向n个消息接收者发送n条消息时,本文方案与同类签密方案的计算开销对比如表4所示.

利用表3中的复杂运算运行时间,可以得到签密过程和解签密过程计算开销对比示意图,如图2和图3所示.

由上图可知,文献[8]和文献[17]的计算开销明显高于其他方案,原因在于文献[8]和文献[17]采用了计算复杂度较高的双线性对运算,而本文方案与文献[10,14,15,18]的计算开销相差不大. 具体而言,本文方案的

表4 计算开销对比

方案	离线签密开销	在线签密开销	签密过程总计算开销	解签密过程总计算开销
文献[8]	$3nT_{\mathrm{sm}G_1}+nT_{\mathrm{e}G_T}$	$nT_{\mathrm{sm}G_1}$	$4nT_{\mathrm{sm}G_1}+nT_{\mathrm{e}G_T}$	$3T_{\mathrm{sm}G_1}+T_{\mathrm{bp}}$
文献[10]	$3nT_{\mathrm{sm}G}$	negligible	$3nT_{\mathrm{sm}G}$	$3T_{\mathrm{sm}G}$
文献[14]	—	$(2n+1)T_{\mathrm{sm}G}$	$(2n+1)T_{\mathrm{sm}G}$	$4T_{\mathrm{sm}G}$
文献[15]	—	$(2n+1)T_{\mathrm{sm}G}$	$(2n+1)T_{\mathrm{sm}G}$	$4T_{\mathrm{sm}G}$
文献[17]	$4nT_{\mathrm{sm}G_1}+nT_{\mathrm{e}G_T}$	negligible	$4nT_{\mathrm{sm}G_1}+nT_{\mathrm{e}G_T}$	$4T_{\mathrm{sm}G_1}+T_{\mathrm{e}G_T}+2T_{\mathrm{bp}}$
文献[18]	$2nT_{\mathrm{sm}G}$	negligible	$2nT_{\mathrm{sm}G}$	$3T_{\mathrm{sm}G}$
本文	$(2n+1)T_{\mathrm{sm}G}$	negligible	$(2n+1)T_{\mathrm{sm}G}$	$4T_{\mathrm{sm}G}$

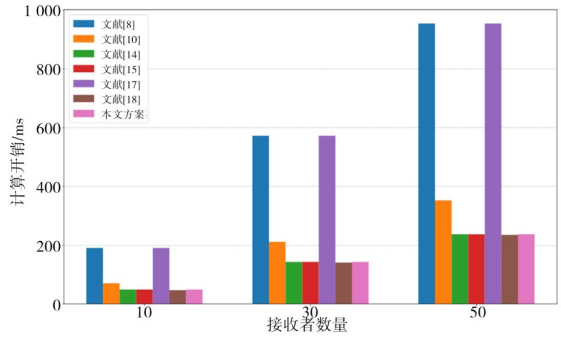

图2 签密过程计算开销对比

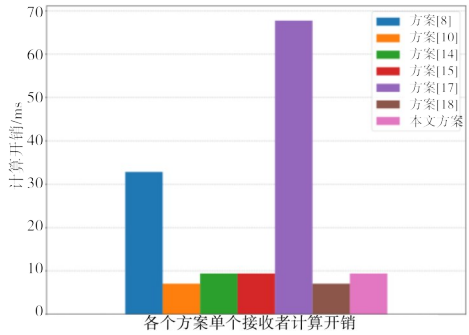

图3 解签密过程计算开销对比

总计算开销与文献[14]、文献[15]基本相同，但文献[14]、文献[15]未考虑离线/在线相结合的方式实现签密，其签密过程的运算均在线完成，而本文方案在线签密过程的计算开销可忽略；相较于文献[10]和文献[18]，本文方案签密过程计算开销优于文献[10]而略高于文献[18]，解签密过程计算开销略高于文献[10]和文献[18]，原因在于为实现对消息发送者的匿名性保护，本文方案在签密过程中引入了发送者的临时身份标识和临时公/私钥，相应地，接收方在解签密过程也需要额外计算相关参数并验证签密密文的合法性.

(3)通信开销

利用签密过程中发送者向接收者传递的消息长度来衡量方案的通信开销. 在分析过程中，分别采用符号L_{ID}表示身份标识的长度、L_m表示明文消息的长度、$L_{Z_p^*}$表示Z_p^*中元素的长度、$L_{Z_{\tilde{p}}^*}$表示$Z_{\tilde{p}}^*$中元素的长度、L_G表示群G中元素的长度、L_{G_1}表示群G_1中元素的长度、L_T表示时间戳的长度、n表示消息接收者的数量. 此外，符号L_Π和L_{Len}分别表示文献[14]中标签$\Pi_i(i=1,2,\cdots,n)$和消息比特数$\mathrm{Len}_i(i=1,2,\cdots,n)$的长度. 由方案执行过程可知，当向$n$个消息接收者发送$n$条消息时，本文方案与同类方案的通信开销对比如表5所示.

表5 通信开销对比

方案	通信开销
文献[8]	$nL_m+2nL_{Z_p^*}+2nL_{G_1}$
文献[10]	$nL_m+nL_{Z_p^*}+nL_G$
文献[14]	$nL_m+(n+2)L_{Z_p^*}+nL_\Pi+nL_{\mathrm{Len}}$
文献[15]	$nL_m+2nL_{Z_p^*}$
文献[17]	$3nL_{Z_p^*}+3nL_{G_1}$
文献[18]	$nL_m+nL_{Z_p^*}+nL_G$
本文	$nL_{\mathrm{ID}}+nL_m+L_{Z_p^*}+L_G+L_T$

依据椭圆曲线secp256k1[31]以及曲线BLS12-381[32]定义的相关参数长度，可知$L_{Z_p^*}$为256 bit、$L_{Z_{\tilde{p}}^*}$为256 bit、L_G为512 bit、L_{G_1}为762 bit. 此外，不失一般性，将L_m定义为256 bit，将L_{ID}、L_T、L_Π、L_{Len}均定义为32 bit. 由此可得，本文方案与同类方案的通信开销对比如图4所示.

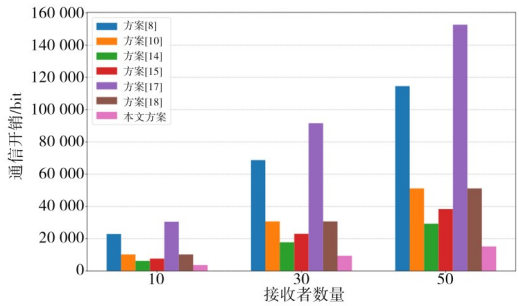

图4 通信开销对比

由图4可知，本文方案的通信开销优于同类方案，并且随着接收者数量的增多，该优势更加明显. 因而，对于终端设备数量较多的边缘计算应用场景，本文方

案在通信开销上具有更显著的优势.

7 结束语

本文基于PUF和椭圆曲线上的无证书公钥密码体制,提出面向边缘计算的多接收者多消息匿名签密方案,有效解决了现有方案存在的无法实现对消息发送者的匿名性保护、无法抵抗物理攻击等问题. 方案能够以更小的通信开销达到机密性、不可伪造性、匿名性等安全属性要求,并且可以有效防范物理攻击的威胁,满足边缘计算环境下设备的安全通信需求.

参考文献

[1] DONG S, SU H D, XIA Y J, et al. A comprehensive survey on authentication and attack detection schemes that threaten it in vehicular ad-hoc networks[J]. IEEE Transactions on Intelligent Transportation Systems, 2023, 24(12): 13573-13602.

[2] SU H, DONG S, WANG N, et al. An efficient privacy-preserving authentication scheme that mitigates TA dependency in VANETs[J]. Vehicular Communications, 2024, 45: 100727.

[3] 周俊, 沈华杰, 林中允, 等. 边缘计算隐私保护研究进展[J]. 计算机研究与发展, 2020, 57(10): 2027-2051.
ZHOU J, SHEN H J, LIN Z Y, et al. Research advances on privacy preserving in edge computing[J]. Journal of Computer Research and Development, 2020, 57(10): 2027-2051. (in Chinese)

[4] 王菲菲, 汪定. 基于雾计算的智能医疗三方认证与密钥协商协议[J]. 软件学报, 2023, 34(7): 3272-3291.
WANG F F, WANG D. Fog computing-based three-party authentication and key agreement protocol for smart healthcare[J]. Journal of Software, 2023, 34(7): 3272-3291. (in Chinese)

[5] 施巍松, 张星洲, 王一帆, 等. 边缘计算: 现状与展望[J]. 计算机研究与发展, 2019, 56(1): 69-89.
SHI W S, ZHANG X Z, WANG Y F, et al. Edge computing: State-of-the-art and future directions[J]. Journal of Computer Research and Development, 2019, 56(1): 69-89. (in Chinese)

[6] ALWARAFY A, AL-THELAYA K A, ABDALLAH M, et al. A survey on security and privacy issues in edge-computing-assisted Internet of things[J]. IEEE Internet of Things Journal, 2021, 8(6): 4004-4022.

[7] BELGUITH S, KAANICHE N, HAMMOUDEH M, et al. PROUD: Verifiable privacy-preserving outsourced attribute based signcryption supporting access policy update for cloud assisted IoT applications[J]. Future Generation Computer Systems, 2020, 111: 899-918.

[8] CHEN J, WANG L, WEN M, et al. Efficient certificateless online/offline signcryption scheme for edge IoT devices[J]. IEEE Internet of Things Journal, 2022, 9(11): 8967-8979.

[9] ALI I, CHEN Y, LI J, et al. Efficient offline/online heterogeneous-aggregated signcryption protocol for edge computing-based Internet of vehicles[J]. IEEE Transactions on Intelligent Transportation Systems, 2023, 24(12): 14506-14519.

[10] XIE Z, CHEN Y, ALI I, et al. Efficient and secure certificateless signcryption without pairing for edge computing-based Internet of vehicles[J]. IEEE Transactions on Vehicular Technology, 2023, 72(5): 5642-5653.

[11] XU G, DONG J, MA C, et al. A certificateless signcryption mechanism based on blockchain for edge computing[J]. IEEE Internet of Things Journal, 2023, 10(14): 11960-11974.

[12] YU X, ZHAO W, TANG D. Efficient and provably secure multi-receiver signcryption scheme using implicit certificate in edge computing[J]. Journal of Systems Architecture, 2022, 126: 102457.

[13] LIANG Y, YAN H, LIU Y. Unlinkable signcryption scheme for multi-receiver in VANETs[J]. IEEE Transactions on Intelligent Transportation Systems, 2023, 24(9): 10138-10154.

[14] PENG C, CHEN J, OBAIDAT M S, et al. Efficient and provably secure multireceiver signcryption scheme for multicast communication in edge computing[J]. IEEE Internet of Things Journal, 2020, 7(7): 6056-6068.

[15] WANG L, GUAN Z, CHEN Z, et al. Multi-receiver signcryption scheme with multiple key generation centers through public channel in edge computing[J]. China Communications, 2022, 19(4): 177-198.

[16] AN J H, DODIS Y, RABIN T. On the security of joint signature and encryption[M]//Lecture Notes in Computer Science. Berlin: Springer, 2002: 83-107.

[17] JIN C, ZHU H, QIN W, et al. Heterogeneous online/offline signcryption for secure communication in Internet of things[J]. Journal of Systems Architecture, 2022, 127: 102522.

[18] AN H, HE D, PENG C, et al. Efficient certificateless online/offline signcryption scheme without bilinear pairing for smart home consumer electronics[J]. IEEE Transactions on Consumer Electronics, 2024, 70(1): 4005-4015.

[19] NIU S, SHAO H, SU Y, et al. Efficient heterogeneous

signcryption scheme based on edge computing for industrial Internet of things[J]. Journal of Systems Architecture, 2023, 136: 102836.

[20] MARCHAND C, BOSSUET L, MUREDDU U, et al. Implementation and characterization of a physical unclonable function for IoT: A case study with the TERO-PUF[J]. IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, 2018, 37(1): 97-109.

[21] AMAN M N, CHUA K C, SIKDAR B. Mutual authentication in IoT systems using physical unclonable functions[J]. IEEE Internet of Things Journal, 2017, 4(5): 1327-1340.

[22] PAPPU R, RECHT B, TAYLOR J, et al. Physical one-way functions[J]. Science, 2002, 297(5589): 2026-2030.

[23] AMAN M N, BASHEER M H, SIKDAR B. Data provenance for IoT with light weight authentication and privacy preservation[J]. IEEE Internet of Things Journal, 2019, 6(6): 10441-10457.

[24] LI S, ZHANG T, YU B, et al. A provably secure and practical PUF-based end-to-end mutual authentication and key exchange protocol for IoT[J]. IEEE Sensors Journal, 2021, 21(4): 5487-5501.

[25] POINTCHEVAL D, STERN J. Security arguments for digital signatures and blind signatures[J]. Journal of Cryptology, 2000, 13(3): 361-396.

[26] LI S, HUANG Y, YU B. A practical and flexible PUF-based end-to-end anonymous authentication protocol for IoT[J]. Computer Networks, 2024, 247: 11426.

[27] SEIFELNASR M, ALTAWY R, YOUSSEF A. SKAFS: Symmetric key authentication protocol with forward secrecy for edge computing[J]. IEEE Internet of Things Journal, 2024, 11(1): 510-525.

[28] SUZUKI M, UENO R, HOMMA N, et al. Efficient fuzzy extractors based on ternary debiasing method for biased physically unclonable functions[J]. IEEE Transactions on Circuits and Systems I: Regular Papers, 2019, 66(2): 616-629.

[29] DODIS Y, OSTROVSKY R, REYZIN L, et al. Fuzzy extractors: How to generate strong keys from biometrics and other noisy data[J]. SIAM Journal on Computing, 2008, 38(1): 97-139.

[30] 张效林, 谷大武. 一种基于PUF的可证明安全消息认证算法及应用[J]. 中国科学(信息科学), 2022, 52(12): 2336-2350.
ZHANG X L, GU D W. A PUF-based provably secure message authentication algorithm and application[J]. Scientia Sinica (Informationis), 2022, 52(12): 2336-2350. (in Chinese)

[31] BROWN D R L. SEC 2: Recommended elliptic curve domain parameters[S/OL]. Standards for Efficient Cryptography. (2010-01-27)[2023-12-12]. https://www.secg.or g/sec2-v2.pdf.

[32] BOWE S. BLS12-381: New zk-SNARK elliptic curve construction[EB/OL]. (2017-03-11) [2023-12-12]. https://electriccoin.co/blog/new-snark-curve/.

[33] VERCAUTEREN F. Optimal pairings[J]. IEEE Transactions on Information Theory, 2010, 56(1): 455-461.

作者简介

李森森 男,1993年7月出生于河南省洛阳市. 现为战略支援部队信息工程大学讲师、博士研究生. 主要研究方向为物联网安全、云数据安全.
E-mail: lss589@163.com

刘燕江 男,1990年7月出生于河南省南阳市. 现为战略支援部队信息工程大学讲师. 主要研究方向为物理不可克隆函数设计及其应用.
E-mail: liuyj_1013@126.com