基于边缘计算的并行密钥隔离聚合签名方案

周利峰[1],殷新春[1,2*],宁建廷[3,4]
(1. 扬州大学信息工程学院,江苏扬州 225127;2. 扬州大学广陵学院,江苏扬州 225128;3. 福建师范大学计算机与网络空间安全学院,福建福州 350007;4. 中国科学院信息工程研究所信息安全国家重点实验室,北京 100093)

摘 要: 无线医疗传感器网络的出现为患者的治疗带来了极大的便利. 但是,无线医疗传感器网络中往往都使用不可信的公共信道进行数据通信并且只有唯一的云服务器处理大量的医疗数据,这就导致了通信安全、隐私保护、密钥泄露、云服务器计算负担过大、延迟高等问题. 此外,现有的大多数无证书聚合签名方案无法抵抗完全选择密钥攻击. 针对上述问题,本文提出一种适用于无线医疗传感器网络基于边缘计算的无证书并行密钥隔离聚合签名方案. 方案引入边缘计算的架构使得签名的验证和聚合过程在更靠近终端用户的边缘层进行,在降低中心云服务器计算负担的同时还能有效的保护患者的隐私. 本文方案继承了无证书和密钥隔离技术的优点,同时避免了复杂的证书管理、密钥托管以及密钥暴露等问题. 在随机预言模型下证明了本文方案可以抵抗完全选择密钥攻击、Type I攻击以及Type II攻击. 性能分析表明,与相关无证书签名方案相比,本文方案的计算开销至少可降低74.03%,通信开销至少可降低25%.

关键词: 无线医疗传感器网络;无证书聚合签名;并行密钥隔离;边缘计算;随机预言模型;完全选择密钥攻击
基金项目: 国家自然科学基金(No.62032005, No.61972094);信息安全国家重点实验室项目(No.2021-ZD-02)
中图分类号: TP309 **文献标识码:** A **文章编号:** 0372-2112(2024)03-1002-14
电子学报 URL:http://www.ejournal.org.cn **DOI:**10.12263/DZXB.20220673

Parallel Key Isolation Aggregate Signature Scheme Based on Edge Computing

ZHOU Li-feng[1], YIN Xin-chun[1,2*], NING Jian-ting[3,4]
(1. *College of Information Engineering*, *Yangzhou University*, *Yangzhou*, *Jiangsu* 225127, *China*;
2. *College of Guangling*, *Yangzhou University*, *Yangzhou*, *Jiangsu* 225128, *China*;
3. *College of Computer and Cyberspace Security*, *Fujian Normal University*, *Fuzhou*, *Fujian* 350007, *China*;
4. *State Key Laboratory of Information Security*, *Institute of Information Engineering*, *Chinese Academy of Sciences*, *Beijing* 100093, *China*)

Abstract: The emergence of wireless medical sensor networks has brought great convenience to the treatment of patients. However, in wireless medical sensor networks, untrusted public channels are often used for data communication and only a single cloud server processes a large amount of medical data, which leads to communication security, privacy preservation, key leakage, excessive computational burden on the cloud server, and high latency. In addition, most existing certificateless aggregate signature schemes are unable to resist fully chosen-key attacks. Therefore, to address the above problems, a certificateless parallel key isolation aggregate signature scheme based on edge computing for wireless medical sensor networks is proposed. The scheme uses the architecture of edge computing so that the verification and aggregation process of signatures is carried out at the edge layer closer to the end-user, which can reduce the computing burden of the central cloud server and ensure effective privacy protection. The proposed scheme inherits the advantages of certificateless and key isolation, while avoiding complex certificate management, key escrow, and key exposure. Under the random oracle model, it is proved that the proposed scheme can resist fully chosen-key attacks, Type I attacks, and Type II attacks. The performance analysis shows that, compared with the related certificateless signature scheme, the computational efficiency of the proposed scheme can be reduced by at least 74.03%, and the communication overhead can be reduced by at least 25%.

Key words: wireless medical sensor networks; certificateless aggregate signature; parallel key isolation; edge com-

收稿日期:2022-06-12;修回日期:2022-11-04;责任编辑:梅志强
*通讯作者:殷新春

puting; random oracle model; fully chosen-key attacks

Foundation Item(s): National Natural Science Foundation of China (No.62032005, No.61972094); Foundation of State Key Laboratory of Information Security (No.2021-ZD-02)

1 引言

据估计,到2030年,人类的平均寿命将达到75岁,到2050年,美国60岁以上的人口将达到6 000万,而中国则将达到4.3亿[1]. 人口压力的日益增长将给社会医疗卫生工作带来巨大的挑战. 而无线医疗传感器网络(Wireless Medical Sensor Networks, WMSNs)作为物联网、无线通信和云计算技术在医疗领域的衍生,正发挥着关键的作用[2]. WMSNs具有成本低、效率高、时延低等特点,可以通过移动感知设备采集患者的生理数据. 然后这些医疗数据会通过无线网络传输至云端便于医生对患者的病情进行远程的诊断和决策[3]. 然而,WMSNs在给人类生活提供便利的同时也带来了很多问题. 如何保证医疗数据的安全通信和病人的隐私保护成为了WMSNs广泛部署与应用的两大障碍[4,5]. 由于公共无线信道的开放性,医疗数据传输过程中容易受到恶意攻击者拦截、篡改、中断、窃听等安全威胁[6]. 相比于普通数据,医疗数据有着较高的敏感性,一旦传输过程中的任何医疗数据的修改都可能导致严重的后果,甚至会危及患者的生命. 因此,需要设计签名机制保证消息的完整性和认证性. 此外,在通常情况下,患者不会将自己的医疗数据透露给非授权的组织或个人. 一旦患者的医疗信息泄露,会造成很严重的隐私问题[7]. 因此,利用假身份代替身份标识保证匿名通信显得尤为重要. 然而匿名的数字签名方案存在通信开销大、计算开销大、安全性低等问题,如何在保证安全性的同时减少相应的开销是当前研究的热点问题.

随着WMSNs的不断发展,医疗传感器从患者身上收集的健康数据呈爆炸式增长[8]. 当这些大量的医疗数据上传到云服务器,给云端带来了过多的计算负担[9,10]. 此外,远程云和终端用户之间的通信往往会出现相对较高的延迟,导致数据处理任务无法得到及时解决. 而边缘计算作为5G网络的关键技术[11],能够将一些云端的任务移动至更接近终端设备的边缘层进行处理,在减轻了中心云计算负担的同时保证了医疗数据处理的实时响应[12].

为了提高签名的验证效率,Boneh等[13]首次提出了一个聚合签名方案. 该方案可以将n个签名聚合成一个短签名,从而简化签名的验证过程. 不久之后,为了解决复杂的证书管理问题,Shim等[14]提出了一个高效的基于身份的聚合签名方案. 但是,基于身份的聚合签名方案往往会带来密钥托管问题. 为了解决上述问题,Castro等[15]首次提出基于无证书公钥密码体制的聚合签名方案. 随后许多无证书聚合签名方案被广泛应用于传感器节点资源受限的医疗领域并得到了迅速发展.

为了解决医疗场景下的安全通信问题,Kumar等[16]设计了一个基于双线性配对的无证书聚合签名方案. 然而,文献[17,18]指出了该方案无法抵抗恶意的医疗服务器攻击. 为了实现身份匿名,Liu等[19]设计了一种适用于医疗场景的无证书匿名批量认证方案. 但是,Zhang等[20]指出了文献[19]存在安全性漏洞,无法抵抗Type I和Type II攻击. 为了降低通信和计算开销,Gayathri等[21]提出了一个高效无证书匿名聚合签名方案. 该方案未使用双线性配对和映射到点的哈希运算,使得计算效率大大提高. 然而,Yang等[22]证明了文献[21]的方案无法抵抗完全选择密钥攻击、Type I和Type II攻击. 不久之后,Liu等[23]设计了一种改进无证书聚合签名方案,并声称该方案能够满足WMSNs中的需求. 但是,Zhan等[24]指出文献[23]的方案仍存在无法抵抗公钥替换攻击的安全漏洞.

在WMSNs环境中,需要在不安全的设备和信道中进行频繁的签名操作,密钥暴露问题不可避免[25]. 而关键的密钥暴露往往会导致整个系统的安全不复存在. 因此,为了解决密钥暴露问题,Dodis等[26]首次提出了一个密钥隔离的签名方案,整个系统的时间周期被分成若干时间片段,用户的公钥可以保持不变,用于签名的密钥会在协助器密钥的帮助下随着时间片段的变化进行更新,即使当前时间段的密钥遭受泄露和破坏,也不会影响其他时间段的密钥安全. 然而,上述方案采用的单个协助器的机制会增加协助器密钥暴露的频率. 为了解决这个问题,Hanaoka等[27]提出了一种具有并行机制的密钥隔离方案. 在该方案中,两个独立的协助器密钥用于更新解密密钥,在允许解密密钥频繁更新的同时,减少了协助器密钥暴露的机会,从而提高了系统的安全性.

近年来,为了同时解决密钥暴露和验证效率低的问题,国内外很多学者将无证书并行密钥隔离技术与聚合签名技术相结合[28,29]. 但是,目前的无证书并行密钥隔离的聚合签名方案计算效率低下且无法适用于无线医疗传感器网络环境. 此外,完全选择密钥攻击作为聚合签名的设计漏洞一直无法得到有效解决. 即使相互合谋的医疗传感器节点生成的签名不合法,而这些无效的单个签名可以被聚合成一个有效的聚合签名. 因此,针对上述问题,本文设计了一个适用于WMSNs

的可证明安全的基于边缘计算的无证书并行密钥隔离聚合签名方案. 本文主要的研究工作如下:

(1) 提出了一个无需双线性配对的无证书并行密钥隔离聚合签名方案,且该方案能满足消息的完整性、认证性、匿名性、可追踪性、前/后向安全性、强密钥隔离安全性、密钥更新性等安全需求.

(2) 引入密钥协商的思想保证了部分私钥的传输不需要依赖安全信道,增强了方案的健壮性. 此外,基于边缘计算的架构不仅降低了中心云的负载,还提高了整个系统的效率和安全性.

(3) 为了抵抗完全选择密钥攻击,在原有的拥有两类攻击者的安全模型下提出了第三类攻击者,并在随机预言模型下证明了方案能够抵抗这三类攻击者的攻击.

(4) 性能分析结果表明,与其他相关的无证书聚合签名方案[16,19,21,30~32]相比,本文方案有较低的通信和计算开销.

2 预备知识

2.1 困难性问题

椭圆曲线离散对数问题(Elliptic Curve Discrete Logarithm Problem, ECDLP):设G椭圆曲线上阶为素数q的加法循环群,P是群G的一个生成元,给定P,$aP \in G$,ECDLP的任务是计算出$a \in Z_q^*$.

椭圆曲线计算Diffie-Hellman问题(Elliptic Curve Computational Diffie-Hellman Problem, ECCDHP):设G是椭圆曲线上阶为素数q的加法循环群,P是群G的一个生成元,给定$aP, bP \in G$,其中$a, b \in Z_q^*$,ECCDHP的任务是计算出$abP \in G$.

2.2 系统模型

本文方案的系统模型共有6个实体:医疗传感器节点(Medical Sensor Node, MSN)、协助器(Helper)、密钥生成中心(Key Generation Center, KGC)、医疗边缘服务器(Medical Edge Server, MES)、医疗云服务器(Medical Cloud Server, MCS)和医生(Doctor),本文方案的系统模型如图1所示.

(1) 终端层:由医疗传感器节点MSN和协助器构成. MSN负责收集患者身体的医疗数据以及使用自己的秘密值和KGC分发的部分私钥生成单个签名. 两个协助器用于生成更新密钥,实现了对用户的签名密钥的交替更新.

(2) 边缘云层:由密钥生成中心KGC和医疗边缘服务器MES构成. KGC作为可信中心,负责生成系统参数以及为MSN分发部分私钥. 此外,KGC还会对MSN进行实时的监测,一旦发现有违规行为,会对恶意的MSN进行追踪并有权揭露恶意MSN的真实身份. MES负责对MSN生成的单个签名进行验证,并在验证通过后对单个签名进行聚合操作.

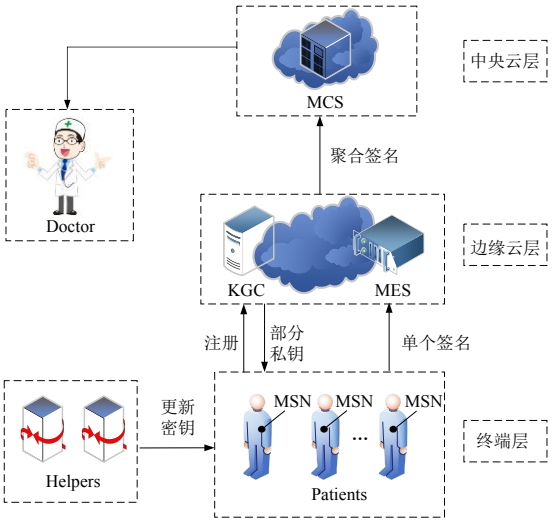

图1 基于边缘计算的无线医疗传感器网络的系统模型图

(3) 中央云层:由医疗服务器MCS构成,负责使用医疗服务器的私钥对聚合签名的合法性进行验证,若验证通过后,将医疗数据通过安全信道发送给Doctor.

(4) Doctor:负责根据医疗服务器MCS发送的医疗数据进行诊断并给出相应的治疗方案.

2.3 安全模型

这一部分展示了无证书并行密钥隔离聚合签名的安全模型,该模型考虑了3种拥有不同能力的攻击者. I类攻击者能够在不知道系统的主密钥s的情况下替换任意医疗传感器节点的公钥. II类攻击者可以获得系统的主密钥s,但是不能替换任意医疗传感器节点的公钥[33]. III类攻击者能够获得医疗传感器节点的私钥,但是它的目的并不是为了伪造签名,而是将多个无效的单个签名聚合成一个有效的聚合签名[34]. 本文通过攻击者$\delta_{\mathrm{I}}, \delta_{\mathrm{II}}, \delta_{\mathrm{III}}, \delta_{\mathrm{IV}}, \delta_{\mathrm{V}}$和挑战者的游戏交互来描述无证书并行密钥隔离聚合签名的安全模型,其中攻击者$\delta_{\mathrm{IV}}, \delta_{\mathrm{V}}$与攻击者$\delta_{\mathrm{I}}, \delta_{\mathrm{II}}$的能力相同,都分别属于I类和II类攻击者.

2.3.1 游戏I

系统初始化阶段:挑战者η_{I}执行系统初始化算法生成系统参数params和系统主密钥s. η_{I}将params发送给攻击者δ_{I},并秘密地保存s.

询问阶段:攻击者δ_{I}可执行以下询问.

(1)部分私钥询问:δ_{I}询问关于MSN身份PID_i的部分私钥,η_{I}返回d_i给δ_{I}.

(2)秘密值询问:δ_{I}询问关于MSN身份PID_i的秘密值,η_{I}返回x_i给δ_{I}.

(3)签名密钥询问:δ_{I}询问关于MSN身份PID_i的签名密钥,η_{I}返回$\mathrm{SK}_{\mathrm{PID}_i,t}$给$\delta_{\mathrm{I}}$.

(4)公钥询问:δ_{I}询问关于MSN身份PID_i的新公钥,η_{I}将(X_i, U_i)返回给δ_{I}.

(5)公钥替换询问:δ_{I}要用新公钥(X_i', U_i')替换(X_i, U_i),η_{I}记录了这次替换.

(6)签名询问:δ_{I}询问关于MSN身份PID_i的签名,η_{I}返回σ_i给δ_{I}.

伪造阶段:当完成上述查询时,若满足以下条件,攻击者δ_{I}将生成伪造签名σ_i^*.

(1) δ_{I}未对身份PID_i进行部分私钥和协助器密钥对询问.

(2) δ_{I}未对身份PID_i在消息m_i^*进行签名询问.

(3) σ_i^*是一个有效的签名.

2.3.2 游戏II

系统初始化阶段:挑战者η_{II}执行系统初始化算法生成系统参数params和系统主密钥s. η_{II}将params发送给攻击者δ_{II}.

询问阶段:δ_{II}进行的部分私钥询问、公钥询问和签名询问与游戏I中攻击者δ_{I}的询问过程相同. 此外,攻击者δ_{II}还可以进行协助器密钥对的询问,具体的询问过程如下所述.

协助器密钥对询问:攻击者δ_{II}询问关于MSN身份PID_i的协助器密钥对,η_{II}返回$(\mathrm{HSK}_0, \mathrm{HSK}_1, \mathrm{HPK}_0, \mathrm{HPK}_1)$给$\delta_{\mathrm{II}}$.

伪造阶段:当完成上述查询时,若满足以下条件,δ_{II}将生成伪造签名σ_i^*.

(1) δ_{II}未对身份PID_i^*进行秘密值和签名密钥询问.

(2) δ_{II}未对身份PID_i^*在消息m_i^*进行签名询问.

(3) σ_i^*是一个有效的签名.

2.3.3 游戏III

挑战者η_{III}执行系统初始化算法生成系统参数params和系统主密钥s. η_{III}随机选择$z \in Z_q^*$,计算$\mathrm{PK}_{\mathrm{MCS}} = zP$并分别将$z$和$\mathrm{PK}_{\mathrm{MCS}}$作为验证私钥和验证公钥. 挑战者$\eta_{\mathrm{III}}$将系统参数params和验证公钥$\mathrm{PK}_{\mathrm{MCS}}$发送给攻击者$\delta_{\mathrm{III}}$.

询问阶段:δ_{III}进行的协助器密钥对、签名密钥、部分私钥、秘密值、公钥以及签名询问的执行过程与游戏I和II的过程相同. 此外,δ_{III}聚合签名验证询问的具体过程如下所示.

聚合签名验证询问:δ_{III}询问关于MSN身份PID_i的聚合签名验证,η_{III}使用MCS的验证私钥z来执行聚合签名验证算法,并将其结果返回给δ_{III}.

伪造阶段:当完成上述查询时,若满足以下条件,δ_{III}将生成伪造聚合签名σ^*.

(1) σ^*是由所有的单个签名聚合而成的.

(2) σ^*是一个有效的聚合签名.

游戏IV和游戏V过程分别与游戏I和游戏II的过程相同,这里不重复描述.

3 本文方案

3.1 符号说明

在本文方案中所使用到的主要符号以及对应说明如表1所示.

表1 本文方案的主要符号说明

符号	含义
λ	系统安全参数
s	系统的主密钥
P_{pub}	系统的主公钥
params	系统参数
$(\mathrm{RID}_i, \mathrm{PID}_i)$	MSN的真/假身份
l_i	MSN的临时部分私钥
x_i	MSN的秘密值
d_i	MSN的部分私钥
(X_i, U_i)	MSN的公钥
$(\mathrm{HPK}_0, \mathrm{HPK}_1)$	两个协助器的公钥
$(\mathrm{HSK}_0, \mathrm{HSK}_1)$	两个协助器的私钥
t	时间片段
σ_i	消息m_i的签名
$(\mathrm{PK}_{\mathrm{MCS}}, \mathrm{SK}_{\mathrm{MCS}})$	MCS的公/私钥
$\mathrm{UK}_{\mathrm{PID}_i, t}$	时间段t内的更新密钥
$\mathrm{SK}_{\mathrm{PID}_i, t}$	时间段t内的签名密钥

3.2 方案的构造

受到文献[34]的启发,本文方案采用医疗云服务器的私钥验证聚合签名的合法性,一旦签名元素在传输过程中发生了改变,将无法通过医疗云服务器的验证,从而保证方案拥有抵抗完全选择密钥攻击的能力. 同时,本文方案引入了并行密钥隔离的思想,采用两个独立的协助器对签名密钥交替更新,使得攻击者不能判断某一时间段的签名密钥由哪一协助器进行更新,大大减小了协助器密钥泄露的影响. 此外,由于协助器对签名密钥的定时更新,即使某一时间片段中的签名密钥发生了泄漏,也不会影响到其他时间片段签名密钥的安全性. 本文方案具体的功能算法如图2所示.

3.2.1 系统初始化算法

输入安全参数λ和总时间片段数N,KGC选取椭圆曲线上阶为素数q的加法循环群G,P为群G的一个生成元. KGC随机选择$s \in Z_q^*$作为系统的主密钥,并计算$P_{\mathrm{pub}} = sP$作为系统主公钥. 选取5个安全的抗碰撞哈希函数H, H_1, H_2, H_3, H_4,其中,$H: G \to Z_q^*$,$H_1: G \times \{0,1\}^* \times G \to Z_q^*$,$H_2: \{0,1\}^* \times G \times \{0,1\}^* \to Z_q^*$,$H_3: \{0,1\}^* \times \{0,1\}^* \times G \times G \times G \times G \to Z_q^*$和$H_4: \{0,1\}^* \to Z_q^*$. 此外,MCS随机选择$z \in Z_q^*$作为私钥$\mathrm{SK}_{\mathrm{MCS}}$,并计算$\mathrm{PK}_{\mathrm{MCS}} = zP$作为公钥. 最后,

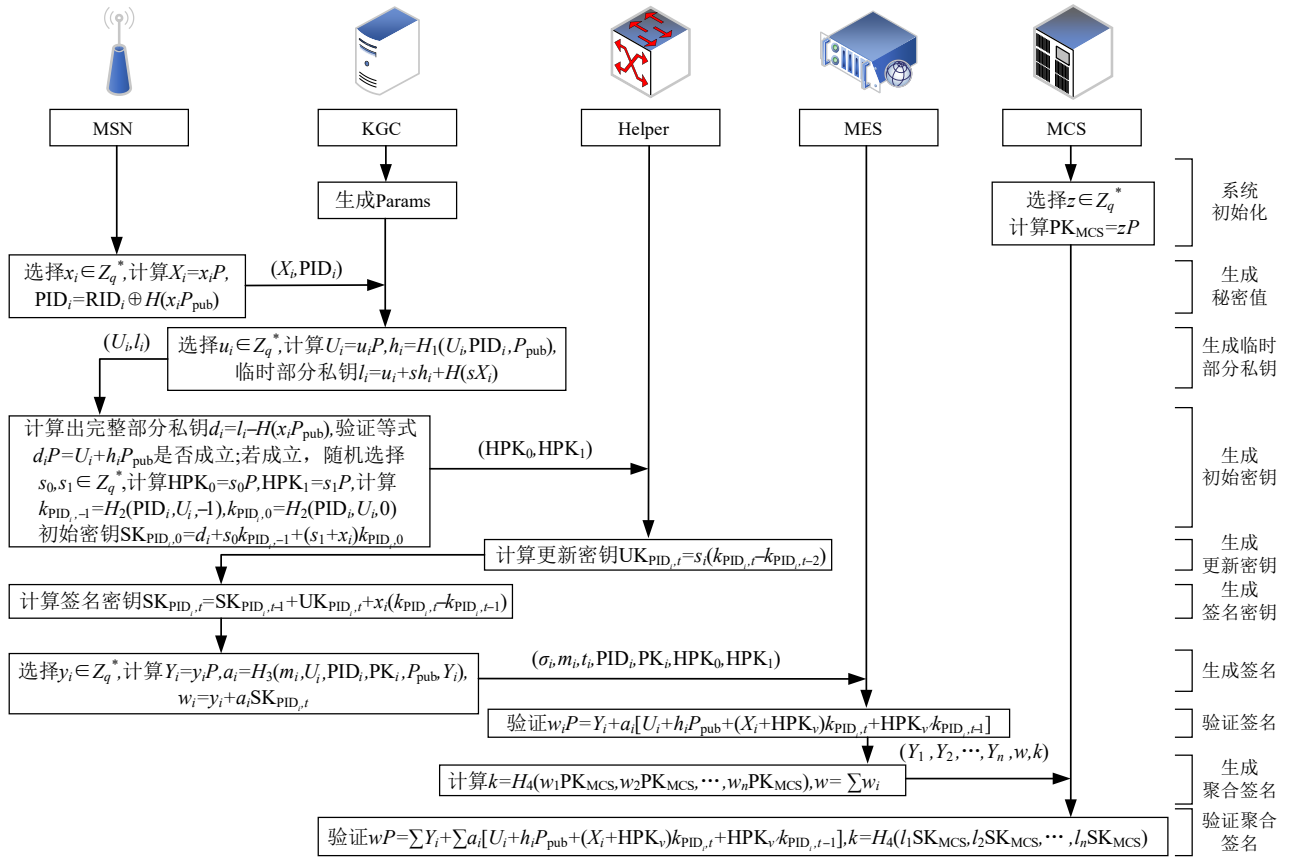

图2 本文方案的功能算法图

KGC公开系统参数$params=\{G,q,P,P_{pub},H,H_1,H_2,H_3,H_4\}$

3.2.2 秘密值生成算法

输入系统参数params,MSN的真实身份RID_i以及系统主公钥P_{pub},MSN生成秘密值和假名的步骤如下:

(1) 随机选择$x_i\in Z_q^*$作为秘密值,并计算$X_i=x_iP$.

(2) 计算$PID_i=RID_i\oplus H(x_iP_{pub})$.

(3) 将(PID_i,X_i)通过公共信道发送至KGC,并申请部分私钥.

3.2.3 部分私钥生成算法

输入系统参数params,系统主密钥s,MSN假身份PID_i和公钥X_i,KGC计算MSN临时部分私钥的步骤如下:

(1) 随机选择$u_i\in Z_q^*$,计算$U_i=u_iP$.

(2) 计算$h_i=H_1(U_i,PID_i,P_{pub})$和临时的部分私钥$l_i=[u_i+sh_i+H(sX_i)]\bmod q$.

(3) 将(U_i,l_i)通过公共信道传输给MSN.

3.2.4 初始密钥生成算法

输入元组(U_i,l_i),假身份PID_i,秘密值x_i和公钥X_i,MSN生成初始密钥的步骤如下所述:

(1) 计算$d_i=l_i-H(x_iP_{pub})\bmod q$,设置$d_i$为部分私钥,设置$(X_i,U_i)$为公钥.

(2) 验证等式$d_iP=U_i+h_iP_{pub}$是否成立,若成立,则MSN接受部分私钥d_i;否则,重新申请部分私钥.

(3) 随机选择$s_0,s_1\in Z_q^*$,设置$HSK_0=s_0$,$HSK_1=s_1$,并计算$HPK_0=s_0P$,$HPK_1=s_1P$,其中,(HSK_0,HSK_1)为两个协助器的私钥,(HPK_0,HPK_1)为两个协助器的公钥.

(4) 将(HSK_0,HSK_1)通过安全信道传输给协助器,并在MSN中删除它们.

(5) 通过计算得出$k_{PID_i,-1}=H_2(PID_i,U_i,-1),k_{PID_i,0}=H_2(PID_i,U_i,0)$以及MSN的初始密钥$SK_{PID_i,0}=d_i+s_0k_{PID_i,-1}+(s_1+x_i)k_{PID_i,0}$.

3.2.5 协助器更新密钥生成算法

输入假身份PID_i,系统参数params,时间片段t以及第i个MSN的协助器的私钥s_i. 第i个协助器计算在时间段t内的更新密钥$UK_{PID_i,t}=s_i(k_{PID_i,t}-k_{PID_i,t-2})\bmod q$,其中$i\equiv t\bmod 2$.

3.2.6 签名密钥生成算法

输入MSN的假身份PID_i,更新密钥$UK_{PID_i,t}$,系统参数params,时间片段t以及在$t-1$时间段的初始密钥$SK_{PID_i,t-1}$. MSN生成签名密钥的步骤如下所述:

(1) 通过计算得出临时的签名密钥 $SK_{PID_i,t}=SK_{PID_i,t-1}+UK_{PID_i,t}+x_i(k_{PID_i,t}-k_{PID_i,t-1})$,其中 $i\equiv t \bmod 2$.

(2) 通过上述等式可以计算出签名密钥 $SK_{PID_i,t}=d_i+(x_i+s_v)k_{PID_i,t}+s_{v'}k_{PID_i,t-1}$,其中 $v\equiv t \bmod 2$ 和 $v'\equiv(t-1) \bmod 2$.

3.2.7 签名算法

输入消息 m_i,假身份 PID_i,时间戳 T_i,时间片段 t,系统参数 params,签名密钥 $SK_{PID_i,t}$ 以及公钥 (X_i,U_i),MSN 生成签名的具体步骤如下所述:

(1) 随机选取 $y_i\in Z_q^*$,计算 $Y_i=y_iP$.

(2) 计算 $a_i=H_3(m_i,PID_i,U_i,X_i,Y_i,P_{pub},T_i)$.

(3) 计算 $\omega_i=(y_i+a_iSK_{PID_i,t}) \bmod q$.

(4) 设置 $\sigma_i=(Y_i,\omega_i)$ 作为 $m_i\|T_i$ 上的签名,并将 $\{\sigma_i,m_i,t_i,PID_i,PK_i,HPK_0,HPK_1\}$ 通过公共信道发送给 MES.

3.2.8 验证算法

输入签名 $\sigma_i=(Y_i,\omega_i)$,消息 m_i,系统参数 params,时间片段 t,公钥 (X_i,U_i),协助器公钥 (HPK_0,HPK_1) 以及 PID_i,MES 验证签名 $\sigma_i=(Y_i,\omega_i)$ 具体步骤如下所述:

(1) 计算 $a_i=H_3(m_i,PID_i,U_i,X_i,Y_i,P_{pub},T_i)$, $h_i=H_1(U_i,PID_i,P_{pub})$, $k_{PID_i,t}=H_2(PID_i,U_i,t)$ 和 $k_{PID_i,t-1}=H_2(PID_i,U_i,t-1)$.

(2) 验证等式 $\omega_iP=Y_i+a_i[U_i+h_iP_{pub}+(X_i+HPK_v)k_{PID_i,t}+HPK_{v'}k_{PID_i,t-1}]$ 是否成立,若等式成立,MES 接收签名;否则,拒绝接收签名.

3.2.9 聚合签名算法

输入在消息 m_i 上的多个签名 $\sigma_i=(Y_i,\omega_i)$,其中 $1\leqslant i\leqslant n$,MES 生成聚合签名的具体步骤如下所述:

(1) 计算 $k=H_4(\omega_1PK_{MCS},\omega_2PK_{MCS},\cdots,\omega_nPK_{MCS})$.

(2) 计算 $\omega=\sum_{i=1}^{n}\omega_i$.

(3) 输出聚合签名 $\sigma=(Y_1,Y_2,\cdots,Y_n,\omega,k)$,MES 将聚合签名 $\sigma=(Y_1,Y_2,\cdots,Y_n,\omega,k)$ 通过公共信道发送给 MCS.

3.2.10 聚合签名验证算法

输入聚合签名 $\sigma=(Y_1,Y_2,\cdots,Y_n,\omega,k)$,消息 m_i,时间片段 t,公钥 (X_i,U_i) 以及系统参数 params,MCS 验证聚合签名合法性的具体步骤如下所述:

(1) 计算 $a_i=H_3(m_i,PID_i,U_i,X_i,Y_i,P_{pub},T_i)$, $h_i=H_1(U_i,PID_i,P_{pub})$, $k_{PID_i,t}=H_2(PID_i,U_i,t)$ 和 $k_{PID_i,t-1}=H_2(PID_i,U_i,t-1)$.

(2) 计算 $l_i=Y_i+a_i[U_i+h_iP_{pub}+(X_i+HPK_v)k_{PID_i,t}+$ $+HPK_{v'}k_{PID_i,t-1}]$.

(3) 验证 $\omega P=\sum_{i=1}^{n}Y_i+\sum_{i=1}^{n}a_i[U_i+h_iP_{pub}+(X_i+HPK_v)k_{PID_i,t}+HPK_{v'}k_{PID_i,t-1}]$, $k=H_4(l_1SK_{MCS},l_2SK_{MCS},\cdots,l_nSK_{MCS})$ 是否成立. 若两个等式都成立,则接收聚合签名;否则,拒绝接收聚合签名.

3.3 正确性分析

本文方案的正确性通过以下的等式得到保证.

(1) MCS 通过聚合签名验证算法验证以下等式是否法:

$$\begin{aligned}\omega P&=\sum_{i=1}^{n}[y_i+a_i(d_i+(x_i+s_v)k_{PID_i,t}+s_{v'}k_{PID_i,t-1})]P\\&=\sum_{i=1}^{n}Y_i+\sum_{i=1}^{n}a_iP[d_i+(x_i+s_v)k_{PID_i,t}+s_{v'}k_{PID_i,t-1}]\\&=\sum_{i=1}^{n}Y_i+\sum_{i=1}^{n}a_i[d_iP+P(x_i+s_v)k_{PID_i,t}+HPK_{v'}k_{PID_i,t-1}]\\&=\sum_{i=1}^{n}Y_i+\sum_{i=1}^{n}a_i[U_i+h_iP_{pub}+(X_i+HPK_v)k_{PID_i,t}+HPK_{v'}k_{PID_i,t-1}]\end{aligned}$$

(2) MCS 通过聚合签名验证算法验证以下等式是否合法:

$$\begin{aligned}k&=H_4(\omega_1PK_{MCS},\omega_2PK_{MCS},\cdots,\omega_nPK_{MCS})\\&=H_4(\omega_1SK_{MCS}P,\omega_2SK_{MCS}P,\cdots,\omega_nSK_{MCS}P)\\&=H_4(\omega_1P\cdot SK_{MCS},\omega_2P\cdot SK_{MCS},\cdots,\omega_nP\cdot SK_{MCS})\\&=H_4(l_1SK_{MCS},l_2SK_{MCS},\cdots,l_nSK_{MCS})\end{aligned}$$

4 安全性证明与分析

4.1 安全性证明

定理 1 如果攻击者 δ_I 能在多项式时间内以不可忽略的概率 ε_1 成功地伪造签名(假设最多可执行 q_p 次部分私钥询问,q_v 次秘密值询问,q_h 次哈希询问,q_s 次签名询问),则存在一个挑战者 η_I 能够以 $(1-\frac{1}{e})\frac{\varepsilon_1}{q_h(q_p+q_v+q_s+1)}$ 的概率解决 ECDLP,其中 e 是自然对数基数.

证明 挑战者 η_I 能够利用攻击者 δ_I 解决 ECDLP. 给定 $(P,P_{pub}=sP)\in G\times G$,挑战者 η_I 的最终目标是计算 $s\in Z_q^*$.

系统初始化阶段:挑战者 η_I 执行系统初始化算法生成系统参数 params 和系统主密钥 s. η_I 将 params 发送给攻击者 δ_I,并秘密地保存 s. 此外,η_I 维护列表 $L_1,L_2,L_3,L_4,L_k,L_p,L_v,L_{pk},L_s$,用于跟踪攻击者 δ_I 对预言机的 H_1,H_2,H_3,H_4 哈希询问、签名密钥询问、部分私钥询问、秘密值询问、公钥询问以及签名询问的结果. 每一个列表初始时均为空.

询问阶段:攻击者 δ_I 可以在该阶段执行以下询问. 在伪造阶段之前,攻击者 δ_I 随机选择的身份不能被挑战者 η_I 捕获,因此,挑战者 η_I 能够成功猜中随机身份

PID_i^*的概率为$\rho=\dfrac{1}{q_\mathrm{p}+q_\mathrm{v}+q_\mathrm{s}+1}$.

(1) H_1 询问：当 η_I 收到攻击者 δ_I 关于 $H_1(U_i,\mathrm{PID}_i,P_\mathrm{pub})$ 的询问时，如果 L_1 中存在 $(h_i,U_i,\mathrm{PID}_i,P_\mathrm{pub})$，则 η_I 返回 h_i 给攻击者 δ_I；否则的话，η_I 随机选择 $h_i\in Z_q^*$，添加元组 $(h_i,U_i,\mathrm{PID}_i,P_\mathrm{pub})$ 到 L_1 中，并返回 h_i 给攻击者 δ_I.

(2) H_2 询问：当 η_I 收到攻击者 δ_I 关于 $H_2(U_i,\mathrm{PID}_i,t)$ 的询问时，如果 L_2 中存在 $(k_{\mathrm{PID}_i,-1},U_i,\mathrm{PID}_i,-1)$，$(k_{\mathrm{PID}_i,0},U_i,\mathrm{PID}_i,0)$，则 η_I 返回 $k_{\mathrm{PID}_i,-1}$，$k_{\mathrm{PID}_i,0}$ 给攻击者 δ_I；否则的话，η_I 随机选择 $k_{\mathrm{PID}_i,-1},k_{\mathrm{PID}_i,0}\in Z_q^*$，添加元组 $(k_{\mathrm{PID}_i,-1},U_i,\mathrm{PID}_i,-1)$，$(k_{\mathrm{PID}_i,0},U_i,\mathrm{PID}_i,0)$ 到 L_2 中，并返回给攻击者 δ_I.

(3) H_3 询问：当 η_I 收到攻击者 δ_I 关于 $H_3(m_i,\mathrm{PID}_i,U_i,X_i,Y_i,P_\mathrm{pub},T_i)$ 的询问时，如果 L_3 中存在 $(a_i,m_i,\mathrm{PID}_i,U_i,X_i,Y_i,P_\mathrm{pub},T_i)$，则 η_I 返回 a_i 给攻击者 δ_I；否则的话，η_I 随机选择 $a_i\in Z_q^*$，添加元组 $(a_i,m_i,\mathrm{PID}_i,U_i,X_i,Y_i,P_\mathrm{pub},T_i)$ 到 L_3 中，并返回 a_i 给攻击者 δ_I.

(4) H_4 询问：当 η_I 收到攻击者 δ_I 关于 $H_3(\omega_1\mathrm{PK}_\mathrm{MCS},\omega_2\mathrm{PK}_\mathrm{MCS},\cdots,\omega_n\mathrm{PK}_\mathrm{MCS})$ 的询问时，如果 L_4 中存在 $(k,\omega_1\mathrm{PK}_\mathrm{MCS},\omega_2\mathrm{PK}_\mathrm{MCS},\cdots,\omega_n\mathrm{PK}_\mathrm{MCS})$，则 η_I 返回 k 给攻击者 δ_I；否则的话，η_I 随机选择 $k\in Z_q^*$，添加元组 $(k,\omega_1\mathrm{PK}_\mathrm{MCS},\omega_2\mathrm{PK}_\mathrm{MCS},\cdots,\omega_n\mathrm{PK}_\mathrm{MCS})$ 到 L_4 中，并返回 k 给攻击者 δ_I.

(5) 签名密钥询问：当 η_I 收到攻击者 δ_I 关于 (PID_i,t) 签名密钥询问时，η_I 维护列表 $L_\mathrm{k}=(\mathrm{PID}_i,\mathrm{HSK}_0,\mathrm{HSK}_1,\mathrm{HPK}_0,\mathrm{HPK}_1)$. 然后，检查在 L_k 中是否存在 PID_i. 如果不存在，η_I 随机选择 $s_0,s_1\in Z_q^*$，设置 $\mathrm{HSK}_0=s_0$，$\mathrm{HSK}_1=s_1$，$\mathrm{HPK}_0=s_0P$，$\mathrm{HPK}_1=s_1P$，并添加元组 $(\mathrm{HSK}_0,\mathrm{HSK}_1,\mathrm{HPK}_0,\mathrm{HPK}_1)$ 到 L_k 中. 然后 η_I 执行上述的 H_1,H_2,H_3,H_4 询问. 当 $t\equiv 0 \bmod 2$ 时，挑战者 η_I 计算 $\mathrm{SK}_{\mathrm{PID}_i,t}=d_i+s_0k_{\mathrm{PID}_i,1}+(x_i+s_1)k_{\mathrm{PID}_i,2} \bmod q$. 最后，$\eta_\mathrm{I}$ 返回 $\mathrm{SK}_{\mathrm{PID}_i,t}$ 给攻击者 δ_I.

(6) 部分私钥询问：当 η_I 收到攻击者 δ_I 关于身份 PID_i 的部分私钥询问时，如果 L_p 中存在 (d_i,PID_i,U_i)，则 η_I 返回 d_i 给攻击者 δ_I；否则的话，η_I 随机选择 $d_i\in Z_q^*$，添加元组 (d_i,PID_i,U_i) 到 L_p 中，并返回 d_i 给攻击者 δ_I.

(7) 秘密值询问：当 η_I 收到攻击者 δ_I 关于身份 PID_i 的秘密值询问时，如果 L_v 中存在 (x_i,PID_i)，则 η_I 返回 x_i 给攻击者 δ_I；否则的话，η_I 随机选择 $x_i\in Z_q^*$，添加元组 (x_i,PID_i) 到 L_v 中，并返回 x_i 给攻击者 δ_I.

(8) 公钥询问：当 η_I 收到攻击者 δ_I 关于身份 PID_i 的公钥询问时，执行以下步骤：

(a) 如果 L_pk 中存在 $(X_i,U_i,\mathrm{PID}_i,c)$，则 η_I 返回 (X_i,U_i) 给攻击者 δ_I，其中 $c\in\{0,1\}$.

(b) 如果 L_pk 中不存在 $(X_i,U_i,\mathrm{PID}_i,c)$，则 η_I 从 c 中选一个值. 如果 c 为 0，则 η_I 随机选择 $x_i,d_i,h_i\in Z_q^*$，计算 $X_i=x_iP$，$U_i=d_iP-h_iP_\mathrm{pub}$，添加元组 $(X_i,U_i,\mathrm{PID}_i,c)$ 到 L_pk 中，并返回 (X_i,U_i) 给攻击者 δ_I. 如果 c 为 1，则 η_I 随机选择 $x_i,u_i,h_i\in Z_q^*$，计算 $X_i=x_iP$，$U_i=u_iP$，添加元组 $(X_i,U_i,\mathrm{PID}_i,c)$ 到 L_pk 中，并返回 (X_i,U_i) 给攻击者 δ_I.

(9) 公钥替换询问：攻击者 δ_I 选择一个关于身份 PID_i 的新的公钥 (X_i',U_i') 替换原来的公钥，当 η_I 收到攻击者 δ_I 关于身份 PID_i 的公钥替换询问时，η_I 将 L_pk 更新为 $(\mathrm{PID}_i,X_i',U_i')$.

(10) 签名询问：当 η_I 收到攻击者 δ_I 关于身份 PID_i 的签名询问时，如果 L_s 中存在 $(m_i,\mathrm{PID}_i,\sigma_i)$，则 η_I 随机选择 $y_i\in Z_q^*$，计算 $Y_i=y_iP$，$a_i=H_3(m_i,\mathrm{PID}_i,U_i,X_i,Y_i,P_\mathrm{pub},T_i)$ 和 $\omega_i=(y_i+a_i\mathrm{SK}_{\mathrm{PID}_i,t})$，并返回 σ_i 给攻击者 δ_I；否则，η_I 随机选择 $\omega_i\in Z_q^*$，计算 $Y_i=\omega_iP-a_i[U_i+h_iP_\mathrm{pub}+(X_i+\mathrm{HPK}_v)k_{\mathrm{PID}_i,t}+\mathrm{HPK}_{v'}k_{\mathrm{PID}_i,t-1}]$，并添加 σ_i 到 L_s 中返回给攻击者 δ_I.

伪造阶段：经过多项式有界次询问后，攻击者 δ_I 输出关于身份 PID_i^* 在消息 m_i^* 上伪造的签名 $\sigma_i^*=(Y_i^*,\omega_i^*)$. 根据分叉引理[35]可知，攻击者 δ_I 可以得到另外一个新的伪造签名 $\sigma_i^{*(2)}=(Y_i^{*(2)},\omega_i^{*(2)})$. 因此，通过以下的两个等式计算 $\omega_i^*P=Y_i^*+a_i^*[U_i^*+h_i^*P_\mathrm{pub}+\mathrm{HPK}_{v'}k_{\mathrm{PID}_i,t-1}{}^*+(X_i^*+\mathrm{HPK}_v)k_{\mathrm{PID}_i,t}{}^*]$，$\omega_i^{*(2)}P=Y_i^{*(2)}+a_i^{*(2)}[U_i^{*(2)}+h_i^{*(2)}P_\mathrm{pub}+\mathrm{HPK}_{v'}k_{\mathrm{PID}_i,t-1}{}^{*(2)}+(X_i^{*(2)}+\mathrm{HPK}_v)k_{\mathrm{PID}_i,t}{}^{*(2)}]$，可得出 ECDLP 的有效解 s.

如果攻击者 δ_I 要赢得该游戏，则需要满足以下条件：

(1) T_1：δ_I 从未对关于身份 PID_i^* 进行部分私钥询问和协助器密钥对询问.

(2) T_2：δ_I 从未对关于身份 PID_i^* 在消息 m_i^* 上进行签名询问.

(3) T_3：σ_i^* 是一个有效的签名.

由上述可知，$\Pr[T_1]\geqslant\dfrac{1}{q_\mathrm{h}}$，$\Pr[T_1|T_2]\geqslant\dfrac{c}{q_\mathrm{h}}$，$\Pr[T_1|T_2\wedge T_3]\geqslant(1-\dfrac{1}{\mathrm{e}})\dfrac{\varepsilon_1}{q_\mathrm{h}(q_\mathrm{p}+q_\mathrm{v}+q_\mathrm{s}+1)}$，因此，挑战者 η_I 解决 ECDLP 的优势为 $(1-\dfrac{1}{\mathrm{e}})\dfrac{\varepsilon_1}{q_\mathrm{h}(q_\mathrm{p}+q_\mathrm{v}+q_\mathrm{s}+1)}$.

证毕.

定理 2 如果攻击者 δ_II 能在多项式时间内以不可忽略的概率 ε_2 成功地伪造签名（假设最多可执行 q_v 次秘密值询问，q_h 次哈希询问，q_s 次签名询问），则存在一

个挑战者 η_{II} 能够以 $(1-\frac{1}{\mathrm{e}})\frac{\varepsilon_2}{q_{\mathrm{h}}(q_{\mathrm{v}}+q_{\mathrm{s}}+1)}$ 的概率解决ECDLP,其中e是自然对数基数.

证明　挑战者 η_{II} 能够利用攻击者 δ_{II} 解决ECDLP. 给定 $(P,X_i=x_iP)\in G\times G$,挑战者 η_{II} 的最终目标是计算出 $x_i\in Z_q^*$.

系统初始化阶段:挑战者 η_{II} 执行系统初始化算法生成系统参数params和系统主密钥 s. η_{II} 将params发送给攻击者 δ_{II}. 此外,η_{II} 维护列表 $L_1,L_2,L_3,L_4,L_{\mathrm{k}},L_{\mathrm{p}},L_{\mathrm{v}},L_{\mathrm{pk}},L_{\mathrm{s}}$,用于跟踪攻击者 δ_{II} 对预言机的 H_1,H_2,H_3,H_4 哈希询问、协助器密钥对询问、部分私钥询问、秘密值询问、公钥询问以及签名询问的结果. 每一个列表初始时均为空.

询问阶段:攻击者 δ_{II} 对预言机的 H_1,H_2,H_3,H_4、秘密值、公钥以及签名询问的执行过程与定理1中攻击者 δ_{II} 的询问过程相同. 而唯一不同的协助器密钥对询问的具体过程如下所示. 在伪造阶段之前,攻击者 δ_{II} 随机选择的身份不能被挑战者捕获. 因此,挑战者 η_{II} 能够成功猜中随机身份 PID_i^* 的概率为 $\rho=\frac{1}{q_{\mathrm{v}}+q_{\mathrm{s}}+1}$.

协助器密钥对询问:当 η_{II} 收到攻击者 δ_{II} 关于身份 PID_i 协助器密钥对询问时,如果 L_{h} 中存在 $(\mathrm{PID}_i,\mathrm{HSK}_0,\mathrm{HSK}_1,\mathrm{HPK}_0,\mathrm{HPK}_1)$,则 η_{II} 返回 $(\mathrm{HSK}_0,\mathrm{HSK}_1,\mathrm{HPK}_0,\mathrm{HPK}_1)$ 给攻击者 δ_{II};否则的话,η_{II} 随机选择 $s_0,s_1\in Z_q^*$,设置 $\mathrm{HSK}_0=s_0$,$\mathrm{HSK}_1=s_1$,$\mathrm{HPK}_0=s_0P$,$\mathrm{HPK}_1=s_1P$,添加元组 $(\mathrm{HSK}_0,\mathrm{HSK}_1,\mathrm{HPK}_0,\mathrm{HPK}_1)$ 到 L_{h} 中,并返回给攻击者 δ_{II}.

伪造阶段:经过多项式有界次询问后,攻击者 δ_{II} 输出关于身份 PID_i^* 在消息 m_i^* 上伪造的签名 $\sigma_i^*=(Y_i^*,\omega_i^*)$. 根据分叉引理[35]可知,攻击者 δ_{II} 可以得到另外一个新的伪造签名 $\sigma_i^{*(2)}=(Y_i^{*(2)},\omega_i^{*(2)})$. 因此,通过以下等式计算 $\omega_i^*P=Y_i^*+a_i^*[U_i^*+h_i^*P_{\mathrm{pub}}^*+\mathrm{HPK}_{v'}k_{\mathrm{PID}_i,t-1}^*+(X_i+\mathrm{HPK}_v)k_{\mathrm{PID}_i,t}^*]$,$\omega_i^{*(2)}P=Y_i^{*(2)}+a_i^{*(2)}[U_i^{*(2)}+h_i^{*(2)}P_{\mathrm{pub}}^{*(2)}+\mathrm{HPK}_{v'}k_{\mathrm{PID}_i,t-1}^{*(2)}+(X_i+\mathrm{HPK}_v)k_{\mathrm{PID}_i,t}^{*(2)}]$,可得出ECDLP的有效解 x_i.

如果攻击者 δ_{II} 要赢得该游戏,则需要满足以下条件:

(1) T_1:δ_{II} 从未对关于身份 PID_i^* 进行秘密值询问和签名密钥询问.

(2) T_2:δ_{II} 从未对关于身份 PID_i^* 在消息 m_i^* 上进行签名询问.

(3) T_3:σ_i^* 是一个有效的签名.

由上述可知,$\Pr[T_1]\geqslant\frac{1}{q_{\mathrm{h}}}$,$\Pr[T_1|T_2]\geqslant\frac{c}{q_{\mathrm{h}}}$,$\Pr[T_1|T_2\wedge T_3]\geqslant(1-\frac{1}{\mathrm{e}})\frac{\varepsilon_2}{q_{\mathrm{h}}(q_{\mathrm{v}}+q_{\mathrm{s}}+1)}$,因此,挑战者 η_{II} 解决ECDLP的优势为 $(1-\frac{1}{\mathrm{e}})\frac{\varepsilon_2}{q_{\mathrm{h}}(q_{\mathrm{v}}+q_{\mathrm{s}}+1)}$.

证毕.

定理3　如果哈希函数 H_4 是抗碰撞的,那么本文方案能够抵抗由攻击者 δ_{III} 发起的完全选择密钥攻击.

证明　如果完全选择密钥攻击者 δ_{III} 能以不可忽略的概率 ε_3 破坏聚合签名算法可靠性,则存在一个挑战者 η_{III} 能够破坏哈希函数 H_4 的抗碰撞性.

系统初始化阶段:挑战者 η_{III} 执行系统初始化算法生成系统参数params和系统主密钥 s. 然后,η_{III} 随机选择 $z\in Z_q^*$,并计算 $\mathrm{PK}_{\mathrm{MCS}}=zP$ 分别作为验证私钥和验证公钥. η_{III} 将params和 $\mathrm{PK}_{\mathrm{MCS}}$ 发送给攻击者 δ_{III}.

询问阶段:攻击者 δ_{III} 对预言机的 H_1,H_2,H_3,H_4、协助器密钥对、签名密钥、部分私钥、秘密值、公钥以及签名询问的执行过程与攻击者 δ_{I} 的询问过程相同. 唯一不同的聚合签名验证询问的具体过程如下.

聚合签名验证询问:当 η_{III} 收到攻击者 δ_{III} 关于元组 $(\mathrm{PID}_i,m_i,\mathrm{PK}_i)$ 的聚合签名验证询问时,η_{III} 使用MCS的验证私钥 z 来执行聚合签名验证算法,并将其结果返回给攻击者 δ_{III}.

伪造阶段:经过多项式有界次询问后,攻击者 δ_{III} 输出元组 $(\mathrm{PID}_i,m_i,\mathrm{PK}_i,\sigma_i)$ 和在消息 m_i^* 上伪造的聚合签名 $\sigma^*=(Y_i^*,\omega^*)$.

如果攻击者 δ_{III} 要赢得该游戏,则需要满足以下条件:

(1) T_1:σ^* 是由所有的单个签名聚合而成的. 因此,可知 $k=H_4(\omega_1\mathrm{PK}_{\mathrm{MCS}},\omega_2\mathrm{PK}_{\mathrm{MCS}},\cdots,\omega_n\mathrm{PK}_{\mathrm{MCS}})$.

(2) T_2:σ^* 是一个有效的聚合签名. 因此,可知 $k=H_4(l_1\mathrm{SK}_{\mathrm{MCS}},l_2\mathrm{SK}_{\mathrm{MCS}},\cdots,l_n\mathrm{SK}_{\mathrm{MCS}})$,其中 $l_i=Y_i+a_i[U_i+h_iP_{\mathrm{pub}}+(X_i+\mathrm{HPK}_v)k_{\mathrm{PID}_i,t}+\mathrm{HPK}_{v'}k_{\mathrm{PID}_i,t-1}]$.

(3) T_3:单个签名 $(\sigma_1,\sigma_2,\cdots,\sigma_n)$ 中至少有一个签名是无效的. 设 σ_i^* 为无效的签名. 可知 $\omega_i^*P\neq Y_i^*+a_i[U_i^*+h_i^*P_{\mathrm{pub}}+(X_i^*+\mathrm{HPK}_v^*)k_{\mathrm{PID}_i,t}^*+\mathrm{HPK}_{v'}^*k_{\mathrm{PID}_i,t-1}^*]$. 等式两边同乘 $\mathrm{SK}_{\mathrm{MCS}}$ 可以得到 $\omega_i^*\mathrm{PK}_{\mathrm{MCS}}\neq\mathrm{SK}_{\mathrm{MCS}}l_i$. 而由上述结果可知,$T_1$ 和 T_2 中有着两个不同的输入的哈希函数却可以得到相同的散列值. 因此,挑战者 η_{III} 找到了破坏哈希函数 H_4 的一对碰撞值.

证毕.

定理4　如果攻击者 δ_{IV} 能在多项式时间内以不可忽略的概率 ε_4 攻破本文方案的强密钥隔离性(假设最多可执行 q_{p} 次部分私钥询问,q_{v} 次秘密值询问,q_{h} 次哈希询问,q_{s} 次签名询问),则存在一个挑战者 η_{IV} 能够以 $(1-\frac{1}{\mathrm{e}})\frac{\varepsilon_4}{q_{\mathrm{h}}(q_{\mathrm{p}}+q_{\mathrm{v}}+q_{\mathrm{s}}+1)}$ 的概率解决ECDLP,其中e是自然对数基数.

证明　挑战者 η_{IV} 能够利用攻击者 δ_{IV} 解决

ECDLP. 给定$(P,P_{\text{pub}}=sP)\in G\times G$,挑战者$\eta_{\text{IV}}$的最终目标是计算出$s\in Z_q^*$.

系统初始化阶段:挑战者η_{IV}执行系统初始化算法生成系统参数params和系统主密钥s. η_{IV}将params发送给攻击者δ_{IV},并秘密地保存s. 此外,η_{IV}维护列表$L_1,L_2,L_3,L_4,L_{\text{k}},L_{\text{p}},L_{\text{v}},L_{\text{pk}},L_{\text{s}}$,用于跟踪攻击者$\delta_{\text{IV}}$对预言机的$H_1,H_2,H_3,H_4$哈希询问、签名密钥询问、部分私钥询问、秘密值询问、公钥询问以及签名询问的结果. 每一个列表初始时均为空.

询问阶段:攻击者δ_{IV}在该阶段的询问与定理1中询问的相同.

伪造阶段:经过多项式有界次询问后,攻击者δ_{IV}输出关于身份PID_i^*在消息m_i^*上伪造的签名$\sigma_i^*=(Y_i^*,\omega_i^*)$. 根据分叉引理[35]可知,攻击者$\delta_{\text{IV}}$可以输出另外一个新的伪造签名$\sigma_i^{*(2)}=(Y_i^{*(2)},\omega_i^{*(2)})$. 因此,通过以下两个等式$\omega_i^*P=Y_i^*+a_i^*[U_i^*+h_i^*P_{\text{pub}}+\text{HPK}_v k_{\text{PID}_i,t-1}^*+(X_i^*+\text{HPK}_v)k_{\text{PID}_i,t}^*]$,$\omega_i^{*(2)}P=Y_i^{*(2)}+a_i^{*(2)}[U_i^{*(2)}+h_i^{*(2)}P_{\text{pub}}+\text{HPK}_v k_{\text{PID}_i,t-1}^{*(2)}+(X_i^{*(2)}+\text{HPK}_v)k_{\text{PID}_i,t}^{*(2)}]$,可得出ECDLP的有效解$s$.

如果攻击者δ_{IV}要赢得该游戏,则需要满足以下条件:

(1) T_1:δ_{IV}从未对关于身份PID_i^*进行部分私钥询问和协助器密钥对询问.

(2) T_2:δ_{IV}从未对关于身份PID_i^*在消息m_i^*上进行签名询问.

(3) T_3:σ_i^*是一个有效的签名.

由上述可知,$\Pr[T_1]\geqslant\frac{1}{q_{\text{h}}}$,$\Pr[T_1|T_2]\geqslant\frac{c}{q_{\text{h}}}$,$\Pr[T_1|T_2\wedge T_3]\geqslant(1-\frac{1}{\text{e}})\frac{\varepsilon_4}{q_{\text{h}}(q_{\text{p}}+q_{\text{v}}+q_{\text{s}}+1)}$,因此,挑战者$\eta_{\text{IV}}$解决ECDLP的优势为$(1-\frac{1}{\text{e}})\frac{\varepsilon_4}{q_{\text{h}}(q_{\text{p}}+q_{\text{v}}+q_{\text{s}}+1)}$.

证毕.

定理5 如果攻击者δ_{V}能在多项式时间内以不可忽略的概率ε_5破坏本文方案的强密钥隔离性(假设最多可执行q_{v}次秘密值询问,q_{h}次哈希询问,q_{s}次签名询问),则存在一个挑战者η_{V}能够以$(1-\frac{1}{\text{e}})\frac{\varepsilon_5}{q_{\text{h}}(q_{\text{v}}+q_{\text{s}}+1)}$的概率解决ECDLP,其中e是自然对数基数.

证明 挑战者η_{V}能够利用攻击者δ_{V}解决ECDLP. 给定$(P,X_i=x_iP)\in G\times G$,挑战者$\eta_{\text{V}}$的最终目标是计算出$x_i\in Z_q^*$.

系统初始化阶段:挑战者η_{V}执行系统初始化算法生成系统参数params和系统主密钥s. η_{V}将params发送给攻击者δ_{V}. 此外,η_{V}维护列表$L_1,L_2,L_3,L_4,L_{\text{k}},L_{\text{p}},L_{\text{v}},L_{\text{pk}},L_{\text{s}}$,用于跟踪攻击者$\delta_{\text{V}}$对预言机的$H_1,H_2,H_3,H_4$哈希询问、协助器密钥对询问、部分私钥询问、秘密值询问、公钥询问以及签名询问的结果. 每一个列表初始时均为空.

询问阶段:攻击者δ_{V}对预言机的H_1,H_2,H_3,H_4、秘密值、协助器对密钥、公钥以及签名询问的执行过程与定理2中的询问过程相同.

伪造阶段:经过多项式有界次询问后,攻击者δ_{V}输出关于身份PID_i^*在消息m_i^*上伪造的签名$\sigma_i^*=(Y_i^*,\omega_i^*)$. 根据分叉引理[35]可知,攻击者$\delta_{\text{V}}$可以输出另外一个新的伪造签名$\sigma_i^{*(2)}=(Y_i^{*(2)},\omega_i^{*(2)})$. 因此,通过以下两个等式$\omega_i^*P=Y_i^*+a_i^*[U_i^*+h_i^*P_{\text{pub}}+\text{HPK}_v k_{\text{PID}_i,t-1}^*+(X_i+\text{HPK}_v)k_{\text{PID}_i,t}^*]$,$\omega_i^{*(2)}P=Y_i^{*(2)}+a_i^{*(2)}[U_i^{*(2)}+h_i^{*(2)}P_{\text{pub}}+\text{HPK}_v k_{\text{PID}_i,t-1}^{*(2)}+(X_i+\text{HPK}_v)k_{\text{PID}_i,t}^{*(2)}]$,可得出ECDLP的有效解$x_i$.

如果攻击者δ_{V}要赢得该游戏,则需要满足以下条件:

(1) T_1:δ_{V}从未对关于身份PID_i^*进行秘密值询问和签名密钥询问.

(2) T_2:δ_{V}从未对关于身份PID_i^*在消息m_i^*上进行签名询问.

(3) T_3:σ_i^*是一个有效的签名.

由上述可知,$\Pr[T_1]\geqslant\frac{1}{q_{\text{h}}}$,$\Pr[T_1|T_2]\geqslant\frac{c}{q_{\text{h}}}$,$\Pr[T_1|T_2\wedge T_3]\geqslant(1-\frac{1}{\text{e}})\frac{\varepsilon_5}{q_{\text{h}}(q_{\text{v}}+q_{\text{s}}+1)}$,因此,挑战者$\eta_{\text{V}}$解决ECDLP的优势为$(1-\frac{1}{\text{e}})\frac{\varepsilon_5}{q_{\text{h}}(q_{\text{v}}+q_{\text{s}}+1)}$.

证毕.

4.2 安全性分析

(1) 消息完整性与认证性:由定理1和定理2可知,本文方案具有签名的不可伪造性,即Type I和Type II这两类攻击者都无法通过伪造签名的方式成功通过签名的验证. 因此,本文方案具有消息完整性与认证性.

(2) 匿名性:医疗数据通信时都以假身份PID_i作为身份标识. 而真实身份RID_i只有医疗传感器节点自己和KGC所知. 医疗传感器节点的假身份为$\text{PID}_i=\text{RID}_i\oplus H(x_iP_{\text{pub}})$,其中$x_iP_{\text{pub}}=sX_i$是基于ECCDHP的困难性. 因此,本文方案具有通信的匿名性.

(3) 可追踪性:KGC是一个权威机构,能够对医疗数据传输过程进行监管,如果发现恶意的数据源,KGC可以迅速追查其身份. KGC拥有系统主密钥s,通过计算$x_iP_{\text{pub}}=x_isP=sX_i$,从而还原出真实身份$\text{RID}_i=\text{PID}_i\oplus H(sX_i)$. 因此,本文的方案可实现高效的追踪性.

(4) 强密钥隔离性:由定理4和定理5可知,即使攻击者获得了时间段t内协助器的私钥,但是它们无法获得上一时间段的签名密钥$\text{SK}_{\text{PID}_i,t-1}$,也就无法伪造当前

时间段和其他时间段的签名密钥,从而无法成功伪造签名. 因此,本文方案满足强密钥隔离性.

(5) 安全的密钥更新:对于任意的时间周期t,更新密钥$\mathrm{UK}_{\mathrm{PID}_i,t}$可以从$\mathrm{SK}_{\mathrm{PID}_i,t-1}$和$\mathrm{SK}_{\mathrm{PID}_i,t}$推导中得出. 因此,本文方案满足安全的密钥更新.

(6) 前/后向安全性:本文方案中签名密钥为$\mathrm{SK}_{\mathrm{PID}_i,t}=\mathrm{SK}_{\mathrm{PID}_i,t-1}+\mathrm{UK}_{\mathrm{PID}_i,t}+x_i(k_{\mathrm{PID}_i,t}-k_{\mathrm{PID}_i,t-1})$,由于签名密钥是在两个协助器交替更新的,即使攻击者获得了当前时间段的密钥$\mathrm{SK}_{\mathrm{PID}_i,t}$,但如果得不到协助器的更新密钥$\mathrm{UK}_{\mathrm{PID}_i,t}$,攻击者无法猜测出前一时间段和后一时间段的密钥. 因此,本文方案满足前/后向安全性.

(7) 可抵抗多类攻击:一个相对健壮的无证书聚合签名方案要能够抵抗完全选择密钥攻击、中间人攻击、重放攻击等.

① 抗完全选择密钥攻击:由定理3可知,任意无效单个签名$(\sigma_1,\sigma_2,\cdots,\sigma_n)$都无法聚合成合法的聚合签名. 如果$H_4(\omega_1\mathrm{PK}_{\mathrm{MCS}},\omega_2\mathrm{PK}_{\mathrm{MCS}},\cdots,\omega_n\mathrm{PK}_{\mathrm{MCS}})$中的任意一个元素发生变化,都会直接导致输出散列值发生变化,从而无法通过医疗云服务器MCS的验证. 因此,本文方案能够的抵抗完全选择密钥攻击.

② 抗中间人攻击:在本文方案中,采用密钥协商的思想使得部分私钥的安全传输得到了保障. 此外,各参与实体相互通信时都会彼此进行身份的验证. 因此,攻击者不能冒充合法实体发送验证消息,因此本文方案可以抵抗中间人攻击.

③ 抗重放攻击:由于本文方案在签名阶段哈希函数H_3中增加了时间戳T_i. 因此,在验证签名时,验证者要检查每一个签名的时间戳T_i是否在有效的时间窗口内. 因此,本文方案实现了的抗重放攻击.

5　性能分析

在本节中,为了展现本文方案的性能优势,我们将和文献[16,19,21,30~32]中的方案在计算开销、通信开销以及安全特性3个方面进行性能分析的比较. 本文使用MIRACL密码学库,并通过实验仿真来衡量方案的计算开销. 具体的环境如下:Windows 10操作系统,Intel i7-1195G7处理器,主频2.9 GHz,内存16 GB. 通过仿真得到各类密码学相关基本运算的运行时间如表2所示.

5.1　计算开销

为了展现边缘计算的优势,我们将本文方案引入边缘计算和不引入边缘计算的两种情况进行计算效率的对比. 如表3所示,当本文方案不引入边缘计算时,医疗云服务器需要执行$(5n+7)$次基于椭圆曲线的乘法运算和$(7n+3)$次基于椭圆曲线的加法运算. 当引入边缘计算后,单个签名的验证和聚合操作可以由边缘层的医疗边缘服务器完成. 在单个签名验证阶段,医疗边缘服务器需执行6次基于椭圆曲线的乘法运算和5次基于椭圆曲线的加法运算;同时,医疗边缘服务器需要在签名聚合阶段执行n次基于椭圆曲线的乘法运算和$(n-1)$次的基于椭圆曲线的加法运算. 而医疗云服务器只需要在聚合签名验证阶段执行$(4n+1)$次基于椭圆曲线的乘法运算和$(6n-1)$次基于椭圆曲线的加法运算. 如图3所示,不使用边缘计算技术时医疗云服务器的负载程度要明显高于基于边缘计算的方案. 与此同时,随着签名数量的增加,医疗云服务器的负载程度也随之线性增大,因而基于边缘计算的方案在签名数量较多时性能的优势更为明显. 边缘计算的引入,使得本文方案在面临大量的医疗数据时能够实现更高效、更快速的响应与处理.

表2　密码学基本运算的运行时间

符号	含义	运行时间/ms
T_{SM}	基于双线性配对的乘法运算	2.256 0
T_{PA}	基于双线性配对的加法运算	0.173 2
T_{P}	双线性配对运算	4.602 8
T_{H}	映射到点的哈希运算	5.124 0
T_{ESM}	基于椭圆曲线的乘法运算	0.764 8
T_{EPA}	基于椭圆曲线的加法运算	0.043 5

如表4所示,在签名的生成和验证阶段,文献[16]中的方案共需要执行4次双线性配对乘法运算,3次双线性配对加法运算,3次双线性配对运算,3次映射到点的哈希运算;文献[19]中的方案共需要执行3次双线性配对乘法运算,2次双线性配对加法运算,2次双线性配对运算,1次映射到点的哈希运算;文献[30]中的方案共需要执行3次双线性配对乘法运算,1次双线性配对加法运算,3次双线性配对运算,3次映射到点的哈希运算;文献[32]中的方案共需要执行2次映射到点的哈希运算,6次双线性配对乘法运算,4次双线性配对运算;而本文方案未使用到复杂的双线性配对和映射到点的哈希运算. 如图4所示,与上述方案[16,19,30,32]相比,本文方案所需的计算开销分别减少了82.97%,74.03%,84.58%,86.79%. 虽然文献[21,31]的计算开销略低于本文方案,但是他们的方案存在安全性问题,文献[21]无法抵抗Type I和Type II两类攻击者的攻击,文献[31]无法抵抗完全选择密钥攻击. 当系统安全性出现问题时,方案的性能优势将不复存在. 因此,总体而言,与相关方案相比,本文方案在计算开销方面具有一定的优势.

表3　本文方案引入边缘计算的开销对比

是否引入边缘计算	医疗边缘服务器	医疗云服务器
否	—	$(5n+7)T_{\mathrm{ESM}}+(7n+3)T_{\mathrm{EPA}}$
是	$(n+6)T_{\mathrm{ESM}}+(n+4)T_{\mathrm{EPA}}$	$(4n+1)T_{\mathrm{ESM}}+(6n-1)T_{\mathrm{EPA}}$

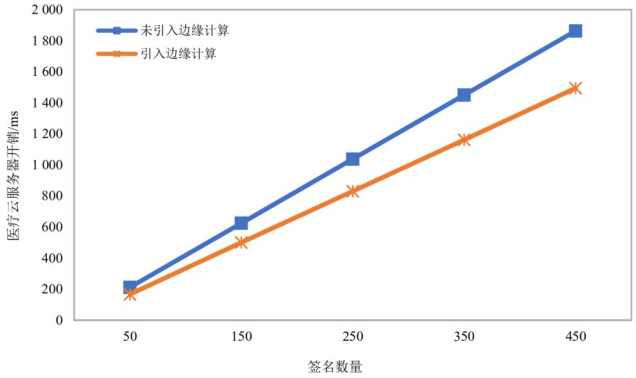

图3 医疗云服务器开销负载的对比图

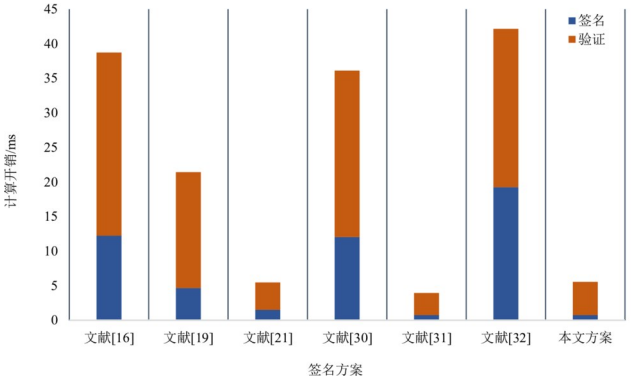

图4 不同方案计算开销的对比图

表4 不同方案计算开销和通信开销的对比

方案	签名阶段/ms	验证阶段/ms	总的时间消耗/ms	单个签名长度/bit	n个签名长度/bit
文献[16]	$3T_{SM}+2T_{PA}+T_H$	$3T_P+T_{SM}+T_{PA}+2T_H$	32.708 3	$2\|G_1\|$	$(n+1)\|G_1\|$
文献[19]	$2T_{SM}+T_{PA}$	$2T_P+T_{SM}+T_{PA}+T_H$	21.444 0	$2\|G_1\|$	$3\|G_1\|$
文献[21]	$2T_{ESM}$	$5T_{ESM}+3T_{EPA}$	5.484 1	$\|G\|+2\|Z_q^*\|$	$2\|G\|+\|Z_q^*\|$
文献[30]	$3T_{SM}+T_{PA}+T_H$	$3T_P+2T_H$	36.121 6	$2\|G_1\|$	$(n+1)\|G_1\|$
文献[31]	T_{ESM}	$4T_{ESM}+3T_{EPA}$	3.954 5	$\|G\|+2\|Z_q^*\|$	$(n+1)\|G\|+n\|Z_q^*\|$
文献[32]	$2T_H+4T_{SM}$	$4T_P+2T_{SM}$	42.159 2	$2\|G_1\|$	$2\|G_1\|$
本文方案	T_{ESM}	$6T_{ESM}+5T_{EPA}$	5.571 1	$\|G\|+\|Z_q^*\|$	$n\|G\|+2\|Z_q^*\|$

5.2 通信开销

如表5所示，我们列出了在双线性对和椭圆曲线中各个参数以及长度规格. 此外，整数域上的群元素大小$|Z_q^*|$规定为160 bits. 根据表4，在单个签名的阶段，文献[16,19,21,30~32]中的方案分别所需要的通信开销为$2|G_1|$=2 048 bits，$2|G_1|$=2 048 bits，$|G|+2|Z_q^*|$=640 bits，$2|G_1|$=2 048 bits，$|G|+2|Z_q^*|$=640 bits，$2|G_1|$=2 048 bits. 而本文方案签名的形式为(Y_i,ω_i)，其中$Y_i\in G,\omega_i\in Z_q^*$. 因此，本文方案在单个签名阶段的通信开销只需要$|G|+|Z_q^*|$=480 bits，分别比文献[16, 19, 21, 30~32]降低了76.57%，76.57%，25%，76.57%，25%，76.57%. 很显然，在单个签名的阶段，本文方案的通信开销具有很大的优势.

表5 双线性对和椭圆曲线中的参数和长度规格

方案类型	曲线类型	配对	循环群	群元素/bit
双线性对	$E:y^2=x^3+x \bmod q$	$e:G_1\times G_1\to G_T$	$G_1(P)$	$\|G_1\|=1024$
椭圆曲线	$E:y^2=x^3+ax+b \bmod q$	—	$G(P)$	$\|G\|=320$

如图5所示，在n个签名的阶段，随着医疗传感器节点数量和签名的增加，文献[16,30,31]中方案的通信开销会以较快的趋势增加，且增长的幅度都明显高于本文方案. 虽然文献[19,21,32]中的方案所需通信开销略低于本文方案，但是他们的方案构造仍存在安全缺陷. 因此，本文方案的通信开销在各类方案中处于中上游水平，能够很好地适用于资源受限的无线医疗传感器网络.

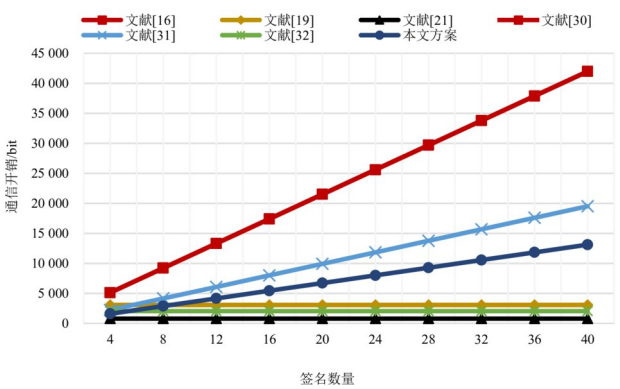

图5 不同方案通信开销的对比图

5.3 安全特性

在安全特性方面，如表6所示，文献[16,19,21]中的方案无法抵抗无线医疗传感器网络中Type I攻击和Type II攻击. 此外，文献[16,19,21,31,32]中的方案忽略了恶意传感器节点之间的相互合谋，使得这些方案都无法抵抗完全选择密钥攻击. 而本文方案在随机预言模型下证明了能够抵抗这三类攻击者的攻击. 同时，文献[16,19,21,30~32]中的方案未考虑到无证书签名系统中密钥泄露问题的严重性，导致这些方案的安全性较低. 由于文献[16,19,

30]中的方案无法满足可追踪性,因而无法很好地适用于无线医疗传感器网络. 此外,文献[16,19,21,30~32]中的方案都是假设在安全的信道传输部分私钥,但是在实际的医疗场景下,完全的安全信道是无法保证的. 医疗数据在信道传输过程中遭受中间人攻击的事件时常发生. 而本文方案通过密钥协商的思想保护了部分私钥的传输. 因此,与上述方案相比,本文方案有更高的安全级别.

表6　不同方案安全特性的对比

方案	匿名性	可追踪性	强密钥隔离性	安全的密钥更新	前/后向安全性	抗Type I攻击	抗Type II攻击	抗完全选择密钥攻击	抗中间人攻击	抗重放攻击
文献[16]	×	×	×	×	×	×	×	×	×	×
文献[19]	√	×	×	×	×	×	×	×	×	√
文献[21]	√	√	×	×	×	×	×	×	×	√
文献[30]	×	×	×	×	×	√	√	√	×	×
文献[31]	√	√	×	×	×	√	√	×	×	√
文献[32]	√	√	×	×	×	√	√	×	×	√
本文方案	√	√	√	√	√	√	√	√	√	√

“√”表示该方案能够满足功能,“×”表示该方案无法满足功能.

6　总结

本文提出了一种基于边缘计算的无证书并行密钥隔离的聚合签名方案. 本文方案通过边缘计算的架构保证了医疗数据的实时处理并缓解了中心云的计算负担. 同时,该方案引入了密钥隔离和密钥协商的技术,大大降低了密钥暴露的风险. 在随机预言模型下,证明了本文方案具有不可伪造性,且能够满足匿名性、可追踪性、强密钥隔离性、安全的密钥更新、前/后向安全性等安全需求. 此外本文方案还可以抵抗Type I攻击、Type II攻击、完全选择密钥攻击、中间人攻击以及重放攻击. 与相关无证书签名方案相比,本文方案的计算开销和通信开销更具优势. 下一个阶段,我们将结合多协助器与无证书聚合签名设计出高效且安全的签名方案来解决无线传感器网络中的安全与隐私问题.

参考文献

[1] HAJAR M S, AL-KADRI M O, KALUTARAGE H K. A survey on wireless body area networks: Architecture, security challenges and research opportunities[J]. Computers & Security, 2021, 104: 102211.

[2] MWITENDE G, Ye Y, Ali I, et al. Certificateless authenticated key agreement for blockchain-based WBANs[J]. Journal of Systems Architecture, 2020, 110: 101777.

[3] VERMA G K, SINGH B B, KUMAR N, et al. PFCBAS: Pairing free and provable certificate-based aggregate signature scheme for the e-healthcare monitoring system[J]. IEEE Systems Journal, 2020, 14(2): 1704-1715.

[4] WANG W M, HUANG H P, XIAO F. Computation-transferable authenticated key agreement protocol for smart healthcare[J]. Journal of Systems Architecture, 2021, 118: 102215.

[5] BENIL T, JASPER J. Cloud based security on outsourcing using blockchain in E-health systems[J]. Computer Networks, 2020, 178: 107344.

[6] GHAYVAT H, PANDYA S, BHATTACHARYA P, et al. CP-BDHCA: Blockchain-based confidentiality-privacy preserving big data scheme for healthcare clouds and applications[J]. IEEE Journal of Biomedical and Health Informatics, 2022, 26(5): 1937-1948.

[7] PENG C, LUO M, LI L, et al. Efficient certificateless online/offline signature scheme for wireless body area networks[J]. IEEE Internet of Things Journal, 2021, 8(18): 14287-14298.

[8] PENG C, LUO M, WANG H Q, et al. An efficient privacy-preserving aggregation scheme for multidimensional data in IoT[J]. IEEE Internet of Things Journal, 2022, 9(1): 589-600.

[9] LI Y M, ZHANG F T. An efficient certificate-based data integrity auditing protocol for cloud-assisted WBANs[J]. IEEE Internet of Things Journal, 2022, 9(13): 11513-11523.

[10] LI Y M, ZHANG F T, LIU X. Secure data delivery with identity-based linearly homomorphic network coding signature scheme in IoT[J]. IEEE Transactions on Services Computing, 2022, 15(4): 2202-2212.

[11] LI B, HE Q, CHEN F F, et al. Inspecting edge data integrity with aggregate signature in distributed edge computing environment[J]. IEEE Transactions on Cloud Comput-

ing, 2022, 10(4): 2691-2703.

[12] GARG S, SINGH A, BATRA S, et al. UAV-empowered edge computing environment for cyber-threat detection in smart vehicles[J]. IEEE Network, 2018, 32(3): 42-51.

[13] BONEH D, GENTRY C, LYNN B, et al. Aggregate and verifiably encrypted signatures from bilinear maps[M]// Lecture Notes in Computer Science. Berlin, Heidelberg: Springer Berlin Heidelberg, 2003: 416-432.

[14] SHIM K A. An ID-based aggregate signature scheme with constant pairing computations[J]. Journal of Systems and Software, 2010, 83(10): 1873-1880.

[15] CASTRO R, DAHAB R. Efficient certificateless signatures suitable for aggregation[J]. IACR Cryptology EPrint Archive, 2007, 2007: 454.

[16] KUMAR P, KUMARI S, SHARMA V, et al. A certificateless aggregate signature scheme for healthcare wireless sensor network[J]. Sustainable Computing: Informatics and Systems, 2018, 18: 80-89.

[17] XIE Y, LI X, ZHANG S S, et al. iCLAS: An improved certificateless aggregate signature scheme for healthcare wireless sensor networks[J]. IEEE Access, 2019, 7: 15170-15182.

[18] ZHAN Y, WANG B C. Cryptanalysis of a certificateless aggregate signature scheme for healthcare wireless sensor network[J]. Security and Communication Networks, 2019, 2019: 1-5.

[19] LIU J W, CAO H J, LI Q Q, et al. A large-scale concurrent data anonymous batch verification scheme for mobile healthcare crowd sensing[J]. IEEE Internet of Things Journal, 2019, 6(2): 1321-1330.

[20] ZHANG Y H, SHU J G, LIU X M, et al. Comments on "A large-scale concurrent data anonymous batch verification scheme for mobile healthcare crowd sensing"[J]. IEEE Internet of Things Journal, 2019, 6(1): 1287-1290.

[21] GAYATHRI N B, THUMBUR G, RAJESH KUMAR P, et al. Efficient and secure pairing-free certificateless aggregate signature scheme for healthcare wireless medical sensor networks[J]. IEEE Internet of Things Journal, 2019, 6(5): 9064-9075.

[22] YANG W J, WANG S P, MU Y. An enhanced certificateless aggregate signature without pairings for E-healthcare system[J]. IEEE Internet of Things Journal, 2021, 8(6): 5000-5008.

[23] LIU J H, WANG L H, YU Y. Improved security of a pairing-free certificateless aggregate signature in healthcare wireless medical sensor networks[J]. IEEE Internet of Things Journal, 2020, 7(6): 5256-5266.

[24] ZHAN Y, WANG B C, LU R X. Cryptanalysis and improvement of a pairing-free certificateless aggregate signature in healthcare wireless medical sensor networks[J]. IEEE Internet of Things Journal, 2021, 8(7): 5973-5984.

[25] LIU Z, YANG G M, WONG D S, et al. Key-insulated and privacy-preserving signature scheme with publicly derived public key[C]//2019 IEEE European Symposium on Security and Privacy (EuroS&P). Piscataway: IEEE, 2019: 215-230.

[26] DODIS Y, KATZ J, XU S H, et al. Key-insulated public key cryptosystems[C]//Advances in Cryptology - EUROCRYPT 2002. Berlin, Heidelberg: Springer Berlin Heidelberg, 2002: 65-82.

[27] HANAOKA G, HANAOKA Y, IMAI H. Parallel key-insulated public key encryption[C]//Public Key Cryptography - PKC 2006. Berlin, Heidelberg: Springer Berlin Heidelberg, 2006: 105-122.

[28] 寻甜甜, 于佳, 杨光洋, 等. 密钥隔离的无证书聚合签名[J]. 电子学报, 2016, 44(5): 1111-1116.
XUN T T, YU J, YANG G Y, et al. Key-insulated certificateless aggregate signature[J]. Acta Electronica Sinica, 2016, 44(5): 1111-1116. (in Chinese)

[29] 赵慧艳, 于佳, 李朦, 等. 并行密钥隔离聚合签名[J]. 电子学报, 2015, 43(5): 1035-1040.
ZHAO H Y, YU J, LI M, et al. Parallel key-insulated aggregate signature[J]. Acta Electronica Sinica, 2015, 43 (5): 1035-1040. (in Chinese)

[30] SHEN L M, MA J F, LIU X M, et al. A secure and efficient ID-based aggregate signature scheme for wireless sensor networks[J]. IEEE Internet of Things Journal, 2017, 4(2): 546-554.

[31] DENG L Z, YANG Y X, GAO R H. Certificateless designated verifier anonymous aggregate signature scheme for healthcare wireless sensor networks[J]. IEEE Internet of Things Journal, 2021, 8(11): 8897-8909.

[32] MEI Q, XIONG H, CHEN J H, et al. Efficient certificateless aggregate signature with conditional privacy preservation in IoV[J]. IEEE Systems Journal, 2021, 15(1): 245-256.

[33] ZHANG F T, SHEN L M, WU G. Notes on the security of certificateless aggregate signature schemes[J]. Information Sciences, 2014, 287: 32-37.

[34] WU G, ZHANG F T, SHEN L M, et al. Certificateless ag-

gregate signature scheme secure against fully chosen-key attacks[J]. Information Sciences, 2020, 514: 288-301.

[35] POINTCHEVAL D, STERN J. Security proofs for signature schemes[C]//Advances in Cryptology - EUROCRYPT' 96. Berlin, Heidelberg: Springer Berlin Heidelberg, 1996: 387-398.

作者简介

周利峰　男,1998 年 1 月出生于江苏省苏州市. 现为扬州大学信息工程学院硕士研究生. 主要从事密码学、物联网通信安全与隐私保护、无证书签名等方面的研究工作.

E-mail: lfengzhou@outlook.com

殷新春　男,1962 年 2 月出生于江苏省姜堰市. 现为扬州大学信息工程学院教授、博士生导师. 主要从事密码学、软件质量保障、高性能计算等方面的研究工作.

E-mail: xcyin@yzu.edu.cn

宁建廷　男,1988 年 6 月出生于浙江省龙游市. 现为福建师范大学计算机与网络空间安全学院教授、博士生导师. 主要从事公钥密码学、数据安全、区块链安全等方面的研究工作.

E-mail: jtning88@gmail.com