智慧医疗中基于区块链的无证书环签名方案

刘景昊[1,2],刘亚丽[1,2],陶 艺[1,2],朱河吉[1,2]

(1. 江苏师范大学 计算机科学与技术学院,江苏 徐州 221116;
2. 桂林电子科技大学 广西密码学与信息安全重点实验室,广西 桂林 541004)

摘 要: 随着物联网技术飞速发展,医疗数据传感器被广泛应用于智慧医疗场景中。在实现医疗便利的同时,由于证书颁发、验证和存储过程的复杂性,其易遭受攻击导致患者隐私泄露。无证书签名是解决智慧医疗场景中安全和隐私问题的关键技术之一。针对现有面向智慧医疗的无证书签名方案存在的传感器证书分发复杂、集中式数据库易遭受攻击、患者隐私泄露等问题,提出一种智慧医疗中基于区块链的无证书环签名方案BCLRS。首先,将传统密钥生成中心部署于区块链,将椭圆曲线公钥密码与环签名相结合,以保护患者隐私;其次,实现特殊需求患者的身份可追溯性。安全性分析表明,BCLRS方案满足正确性、匿名性的要求,相较于无证书环签名方案能抵抗中间人攻击、分布式拒绝服务攻击及密钥生成中心妥协攻击等恶意攻击。性能分析与仿真实验表明,当环成员数量大于30时,BCLRS方案的计算开销降低80%,适用于资源受限的智慧医疗场景。

关键词: 智慧医疗;无证书环签名;区块链;随机预言机模型;隐私保护
DOI: 10. 11907/rjdk. 251265 扫描二维码阅读全文:
中图分类号: TP309 **文献标识码:** A **文章编号:** 1672-7800(2026)007-0094-09

Blockchain-based Certificateless Ring Signature Scheme in Smart Healthcare

LIU Jinghao[1,2], LIU Yali[1,2], TAO Yi[1,2], ZHU Heji[1,2]

(1. *College of Computer Science and Technology*, *Jiangsu Normal University*, *Xuzhou* 221116, *China*;
2. *Guangxi Key Laboratory of Cryptography and Information Security*, *Guilin University of Electronic Technology*, *Guilin* 541004, *China*)

Abstract: With the rapid development of IoT technology, medical data sensors are widely used in smart healthcare scenarios. While achieving medical convenience, the complexity of certificate issuance, verification, and storage procedures makes it vulnerable to attacks that can lead to patient privacy breaches. Certificate free signature is one of the key technologies to address security and privacy issues in smart healthcare scenarios. Aiming at the problems of complex sensor certificate distribution, vulnerability to centralized database attacks, and patient privacy leakage in existing certificate free signature schemes for smart healthcare, a blockchain based certificate free ring signature scheme BCLRS is proposed for smart healthcare. Firstly, deploy the traditional key generation center on the blockchain and combine elliptic curve public key cryptography with ring signatures to protect patient privacy; Secondly, achieve traceability of the identity of patients with special needs. Security analysis shows that the BCLRS scheme meets the requirements of correctness and anonymity, and can resist malicious attacks such as man in the middle attacks, distributed denial of service attacks, and key generation center compromise attacks compared to unlicensed circular signature schemes. Performance analysis and simulation experiments show that when the number of ring members exceeds 30, the computational cost of the BCLRS scheme is reduced by 80%, making it suitable for resource constrained smart healthcare scenarios.

Key Words: smart healthcare; certificateless ring signature; blockchain; random oracle model; privacy-preserving

收稿日期: 2025-04-11
基金项目: 国家自然科学基金项目(61702237,62032005);徐州市科技计划项目(KC22052);广西密码学与信息安全重点实验室(桂林电子科技大学)研究课题(GCIS202114);福建省网络安全与密码技术重点实验室(福建师范大学)开放课题(NSCL-KF2021-04);江苏师范大学研究生科研与实践创新计划项目(2024XKT2589,2024XKT2632);河南省网络密码技术重点实验室研究课题(LNCT2021-A07);教育部产学合作协同育人项目(202101374001)

作者简介: 刘景昊(2000-),男,CCF会员,江苏师范大学计算机科学与技术学院硕士研究生,研究方向为信息安全、区块链与密码学及其应用的研究;刘亚丽(1981-),女,博士,江苏师范大学计算机科学与技术学院教授,研究方向为物联网安全、安全认证技术、应用密码等网络空间安全相关领域;陶艺(1999-),男,江苏师范大学计算机科学与技术学院硕士研究生,研究方向为信息安全、车联网安全和密码学及其应用;朱河吉(2000-),男,江苏师范大学计算机科学与技术学院硕士研究生,研究方向为信息安全、射频识别安全和密码学及其应用。本文通讯作者:刘亚丽。

0　引言

随着物联网、5G等技术飞速发展,医疗数据传感器被广泛应用于智慧医疗场景中,以检测患者的医疗隐私数据并发送给医院[1]。医疗数据传感器在进行证书颁发、验证和存储过程中,易遭受攻击导致患者隐私、医疗隐私数据等泄露[2]。传统基于证书的身份验证方式虽能提供一定的安全性,但其复杂的证书管理系统并不适合资源受限的智慧医疗场景。无证书环签名结合了无证书签名与环签名的优点,在解决密钥托管、证书管理问题的同时,使签名者身份匿名,可较好地解决智慧医疗场景下医疗数据传感器的认证问题及隐私保护。

现有无证书签名方案虽解决了密钥托管问题,但大多数方案需要一个集中式的密钥生成中心(Key Generation Center, KGC),用户与之进行交互以产生秘密值用于认证。然而,集中式的KGC不仅面临着单点故障问题,也会面临中间人攻击(Man-In-The-Middle attack, MITM)、KGC妥协攻击和分布式拒绝服务攻击(Distributed Denial of Service, DDOS)等。同时,因智慧医疗场景下医疗数据传感器众多,环签名虽能保护患者隐私,但计算代价会随环成员的不断增多而提升,因此需要对环成员进行合理的管理,以保证环签名的可靠性。

区块链是去中心化的分布式账本技术,在具有不可篡改性的同时赋予了区块链可编程的性质[3]。将KGC部署于区块链,可免遭受MITM、DDOS等恶意攻击。因此,研究基于区块链的无证书环签名医疗数据隐私保护方案具有广阔的应用前景与实际价值。

Al-Riyami等[4]提出无证书公钥密码体系后,众多学者相继提出了一系列无证书签名方案。Yeh等[5]提出一种基于椭圆曲线群标量乘法的无配对方案。Wang等[6]指出文献[5]的方法效率较低,设计了一个用于移动通信的签名协议,并提出另一种可用于资源受限场景的新型签名方案。Yeh等[7]证明了文献[6]的方法易受I型攻击,于是引入了安全性方案。Jia等[8]指出文献[7]的方法无法抵抗超级Type-I、Type-II攻击,且因言模型(Random Oracle Model, ROM)和映射到点(Map-To-Point, MTP)哈希函数的复杂性,文献[5-8]的方法无法应用于实际物联网场景。Karati等[9]提出一种基于配对且无需MTP和ROM的签名方案,能抵御Type-I、Type-II攻击。Pakniat等[10]指出文献[9]的方法存在安全漏洞,提出防御签名伪造攻击的解决方案。Wu等[11]提出一种车载网络无证书通信安全与隐私保护方案,但无法抵抗KGC妥协攻击等恶意攻击。Yang等[12]提出一种基于智慧医疗保健无线传感网的无证书签名方案,传感器节点可在不同消息上生成不同签名,但缺乏对患者的隐私保护,难以抵抗多种恶意攻击,不适用于隐私保护要求较高的智慧医疗场景。Li等[13]提出一种安全增强的无证书签名方案,以一个不断变化的委员会取代KGC进行系统初始化和密钥分发,虽可抵抗MITM攻击、KGC妥协攻击等攻击,但未保护患者隐私。

为了解决环签名所保证的无条件匿名性,Fujisaki等[14]提出可追溯环签名(Traceable Ring Signature, TRS),每条签名的消息都附加一个一次随机数,虽能确定环中的签名者,但在追溯过程中会泄露患者隐私。Liu等[15]提出一个可追溯的环签名方案,但其主密钥完全由密钥生成中心生成,易导致密钥泄露。Peng等[16]提出基于SM9算法的环签名,但随着环成员数量增加,计算代价会随之提升。Au等[17]设计了基于双线性配对的可追溯环签名方案,但计算代价过高,不适合资源受限的智慧医疗场景。Scafuro等[18]提出一次性可追溯环签名,一名成员只能对一条信息进行匿名签名,在环成员要对消息进行多次签名的场景下并不适用。

综上,目前研究工作存在以下问题:①现有智慧医疗场景中无证书签名方案基于集中式KGC,无法抵抗MITM攻击、DDOS攻击、KGC妥协攻击等,攻击者可通过攻击KGC或篡改传输的秘密值,伪造合法身份与用户通信,以获得用户身份信息及数据;②现有智慧医疗场景中无证书环签名方案未考虑签名可靠性,单纯的数字签名虽能保证数据完整性,但在签名验证过程中会暴露签名者的身份与签名信息,导致用户身份泄露;③现有智慧医疗场景中无证书环签名计算代价高,无法适用于资源受限的智慧医疗场景,具体为医疗数据传感器内存有限,无法处理复杂的身份认证过程。

为此,本文提出一种面向智慧医疗的基于区块链的无证书环签名方案(Blockchain-based Certificateless Ring Signature for Smart Healthcare, BCLRS)。主要贡献为:①身份隐私保护及追溯。通过环签名的可追溯性溯源特殊需求的患者身份,实现了患者的隐私保护;②去中心化密钥分发。提出基于区块链的无证书环签名医疗数据隐私保护模型,将KGC部署于区块链,利用区块链的去中心化性质解决传统密钥生成中心易受KGC妥协攻击等恶意攻击的问题;③提升环签名安全性及效率。利用知识签名保证环签名的认证性及完整性,并设计用户组策略提升环签名运算效率;④抵抗多种恶意攻击。在随机预言机模型下对BCLRS方案进行安全性分析;⑤降低计算开销。本文方案相较于现有典型的无证书环签名方案,当环成员数量大于30时计算开销降低了80%,更适用于资源受限的智慧医疗场景。

1　准备工作

1.1　椭圆曲线密码学

椭圆曲线密码学(Elliptic Curve Cryptography, ECC)是一种基于椭圆曲线数学理论的公钥密码算法[19]。设F_p表

示一个大素数模 P 的有限域，定义有限域 F_p 上的椭圆曲线 $E: y^2 = x^3 + ax + b \bmod p$。其中，椭圆曲线满足 $4a^3 + 27b^2 (\bmod p) \neq 0$，则 (x, y) 满足上面的方程式并且存在一个无穷点 O 就组成椭圆曲线 $E(F_P)$。

1.2 椭圆曲线离散对数问题

椭圆曲线离散对数问题（Elliptic Curve Discrete Logarithm Problem，ECDLP）：给定一个定义在有限域 F_P 上的椭圆曲线 E，以及曲线上的两个点 P、Q，找出一个整数 k，满足等式 $Q = kP$[20]。

1.3 椭圆曲线 Diffie-Hellman 问题

椭圆曲线 Diffie-Hellman 问题（Elliptic Curve Diffie-Hellman Problem，ECDHP）问题：给定一个定义在有限域 F_P 上的椭圆曲线 E，P 是椭圆曲线上的基点，已知 $aP, bP \in F_P$，计算 abP[20]。

1.4 知识签名

知识签名（Signatures of Knowledge，SoK）是一种密码学概念，签名者可直接证明知道某个秘密信息，无需暴露该秘密信息[21]。知识签名可形式化为 $Sig(S, K) = (\sigma, Verify)$。其中，$S$ 为签名者，K 为拥有的秘密信息；σ 为知识签名，代表 S 对 K 的掌握；$Verify$ 为验证过程，验证方可通过 σ 确认 S 是否掌握了 K，但不会得到 K 的具体内容。

2 方案定义与安全模型

2.1 符号定义

BCLRS 方案涉及的相关符号定义如表 1 所示。

Table 1 Symbol definition in BCLRS scheme

表 1 BCLRS 方案中的符号定义

参数	定义
ID_i	第 i 个用户的身份
h_i	哈希函数
$Addr_{ID_i}$	第 i 个用户的地址
CTR_i	第 i 个用户的请求计数
PK_i	第 i 个用户的公钥
SK_i	第 i 个用户的私钥
L_i	第 i 组 n 个用户的公钥集合
σ_{L_i}	对消息的签名

2.2 BCLRS 方案的形式化定义

本文在文献[22]的基础上给出无证书环签名方案的形式化定义。无证书环签名方案由 6 个概率多项式时间算法组成，具体算法及功能如下：

（1）初始化算法 $Setup(k) \rightarrow (s, params)$。输入安全参数 $\lambda \in Z_q^*$，KGC 输出安全参数 $params$ 和系统主密钥 s，系统参数 $params$ 对外公开，系统主密钥 s 秘密保存。

（2）部分密钥生成算法 $Gppk(ID_i, params, s) \rightarrow (ppk_i, Gp_i)$。首先，输入公共参数 $params$、系统主密钥 s、还原的用户身份 ID_i；其次，在满足用户组策略后输出签名者的部分私钥 ppk_i 和签名者的对应组数 Gp_i；最后，进行异或操作，通过不安全信道发送给用户 ID_i。

（3）设置公私钥算法 $Gpsk(sppk_i, a_i, params) \rightarrow (SK_i, PK_i)$。用户验证 ppk_i 的正确性，并随机选择秘密值 $a_i \in Z_q^*$，生成用户的私钥 $SK_i = (a_i, ppk_i)$ 及公钥 $PK_i = (A_i, R_i)$，其中 $A_i = a_i P$。

（4）签名生成算法 $Sig(M_i, ID_i, params, PK_i, SK_i) \rightarrow (\sigma_{L_i}, SoK)$。输入公共参数 $params$，消息 $M \in \{0, 1\}^*$、公钥集合 L_i 及签名者的公私钥，输出对消息的环签名 σ_{L_i} 和知识签名 SoK。

（5）签名验证算法 $VerifySig(\sigma_{L_i}, SoK, params, ID_i) \rightarrow (1, 0)$。输入参数 $(\sigma_{L_i}, SoK, params, ID_i)$，验证者输出验证结果。

（6）追溯算法 $Trace(M, M') \rightarrow (PK_k)$。追溯者先计算一系列安全参数，并发送新消息 M' 让签名者重新签名，再根据 $TraceList$ 中的公钥数量决定最终输出：如果仅有一个 PK_k 则输出 PK_k；当 $TraceList = \Phi$ 时输出 $independent$。

2.3 BCLRS 方案的安全定义

本文在文献[22]的基础上，给出无证书环签名安全模型的相关定义，若方案满足以下性质，则称无证书环签名方案是安全的。

（1）正确性。若签名者根据正确的签名形式化定义生成签名，且签名的有效性可通过签名验证算法进行验证，则称此签名满足正确性。

（2）匿名性。如果验证者及第三方参与者只能确认环签名由该环生成，但无法确定签名者在环中的位置，且对实际签名者的猜测概率不超过 $1/n$，则称此方案具备匿名性。

（3）不可伪造性。方案在随机预言机模型下被证明可抵御Ⅰ型攻击者 A_1 和Ⅱ型攻击者 A_2 的攻击。Ⅰ型攻击者 A_1：假设挑战者 C 期望由Ⅰ型攻击者 A_1 以不可忽略的优势 ε 破坏 ECDLP。除了在证明阶段的请求查询外，A_1 需遵循如下规则：①A_1 无法访问系统主密钥；②A_1 可选择随机整数替换环中的公钥。Ⅱ型攻击者 A_2：Ⅱ型攻击者 A_2 的请求查询与Ⅰ型攻击者类似，仍需遵循如下规则：①A_2 可访问系统主密钥；②A_2 无法获得任何用户的秘密值和私钥；③A_2 不能替换用户的公钥。

游戏Ⅰ：Ⅰ型攻击者 A_1 与挑战者 C 进行多次交互，目的是伪造环签名通过签名验证算法，详细步骤如下：

步骤 1：初始化。给定一个安全参数 λ，挑战者 C 运行初始化算法 $Setup()$ 生成系统主密钥 s 和系统公共参数集 $params$，挑战者 C 自己保存系统主密钥 s，并将系统公共参数 $params$ 发送给攻击者 A_1。

步骤 2：查询。攻击者 A_1 执行多项式有限次查询，每次查询可能依赖于之前的查询结果。①哈希查询，攻击者 A_1 向挑战者 C 询问输入的哈希值，挑战者 C 经过计算后将相应的哈希值返回给攻击者 A_1；②部分私钥查询，攻击者

A_1请求用户的部分私钥,挑战者C运行部分密钥生成算法$Gppk()$,用部分私钥进行响应;③秘密值查询,攻击者A_1请求用户的秘密值,挑战者C将相应的秘密值返回给A_1,但如果用户的公钥被替换,则A_1无法请求相应的秘密值;④用户公钥查询,攻击者A_1请求用户公钥,挑战者C运行公钥生成算法,并将相应的公钥PK_i返回给A_1;⑤公钥替换,攻击者A_1为用户提供一个新的公钥PK',挑战者C将当前用户的公钥PK替换为PK';⑥签名查询,攻击者A_1提供n个用户的公钥集$L_i=\{PK_1,PK_2,...,PK_n\}$和消息,挑战者$C$运行签名算法并返回环签名$\sigma_{L_i}$给$A_1$。

步骤3:伪造。攻击者A_1输出签名σ_{L_i},如果验证算法$VerifySig()$验证通过且输出1,且能同时满足以下3个条件则攻击者A_1获胜:①伪造签名σ_{L_i}是一个有效的环签名,且$Verify(\sigma_L(M),M)=1$;②伪造签名σ_{L_i}来自于伪造阶段,而非来自签名查询阶段;③攻击者A_1不能查询公钥集中任何用户的部分私钥信息。

游戏Ⅱ:Ⅱ型攻击者A_2与挑战者C进行交互。

步骤1:初始化。给定一个安全参数λ,挑战者C运行初始化算法$Setup()$生成系统主密钥s和系统公共参数$params$,挑战者C将系统主密钥s和系统公共参数$params$发送给攻击者A_2。

步骤2:查询。A_2进行多项式有限次查询,查询操作与游戏Ⅰ中一致,且返回的响应相同,但A_2可通过系统主密钥计算任何用户的部分私钥。

步骤3:伪造。攻击者A_2输出签名,如果验证算法$VerifySig()$验证通过且输出1,并能同时满足以下4个条件则攻击者A_2获胜:①σ_{L_i}为一个有效的环签名;②伪造的环签名σ_{L_i}不来自签名查询阶段;③攻击者A_2不能查询L_i中任何用户的秘密值;④攻击者A_2不能替换L_i中任何用户的公钥。

3　方案构造

为了解决智慧医疗场景中医疗数据传感器证书分发复杂、缺乏患者隐私保护的问题,以及传统集中式KGC易遭受恶意攻击的问题。本文提出一种面向智慧医疗的基于区块链的无证书环签名方案BCLRS。

3.1　系统模型

图1为基于区块链的无证书环签名系统模型,包含KGC、医疗数据传感器和医院3个实体,三者之间的通信信道都假定为不安全信道。系统实体功能如下:①KGC部署在区块链上负责初始化系统,为医疗数据传感器生成对应身份的部分私钥,完成用户组策略;②医疗数据传感器负责收集患者医疗数据,完成环签名及知识签名;③医院用于验证环签名及知识签名,并对有特殊需求的患者进行追溯。

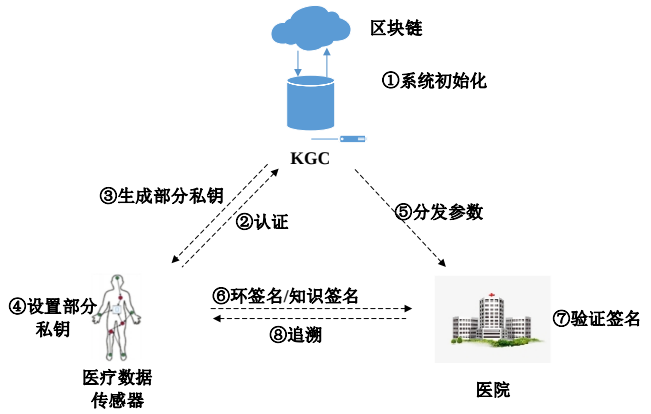

Fig. 1　BCLRS system model

图1　BCLRS系统模型

3.2　用户组策略

BCLRS方案设计了一种用户组策略:将新认证用户划分到组Gp_i,每组设置阈值j,当组Gp_i到达阈值上限则新增组Gp_{i+1},以保证组成员数量恒定,降低计算代价。

3.3　BCLRS方案

BCLRS方案由以下6个阶段组成,分别为系统初始化阶段$Setup()$、部分密钥生成阶段$Gppk()$、设置公私钥阶段$Gpsk()$、签名生成阶段$Sig()$、签名验证阶段$VerifySig()$和追溯阶段$Trace()$。具体流程如下:

3.3.1　*系统初始化阶段* $Setup(\lambda)\rightarrow(s,params)$

系统管理员$Admin$通过以下步骤进行KGC初始化。

步骤1:输入安全参数$\lambda\in Z_q^*$且选择阶为q,生成元为P的加法群G。

步骤2:KGC计算$P_{pub}=sP$,随机选择$s\in Z_q^*$作为系统主密钥。

步骤3:KGC构造安全的哈希函数$h_v=\{0,1\}^*\rightarrow Z_q^*$,$v=1$、2、3、4、5。

步骤4:KGC在区块链上公开公共参数$params=\{G,P,P_{pub},q,h_v\}$,系统主密钥$s$设置为私有。

3.3.2　*部分密钥生成算法:* $Gppk(ID_i,params,s)\rightarrow(ppk_i,Gp_i)$

当用户U_i调用$Gppk()$时,KGC为U_i自动生成部分私钥ppk_i。

步骤1:U_i计算$P_{ID_i}=ID_iP$,$E_{ID_i}=ID_i-ID_iP_{pub}$,其中$ID_i\in\{0,1\}^*$。

步骤2:KGC接受到P_{ID_i}、E_{ID_i}时,调用$Gppk()$。

步骤3:KGC首先检查$CTR_i<n$是否成立,CTR_i为区块链中的一个计数器,$Addr_{ID_i}$为U_i在区块链平台上的地址,n为一个自定义阈值。如果符合上述不等式,KGC计算$ID_i=E_{ID_i}+P_{ID_i}s$并检查ID_i是否在$List$当中,$List$负责记录认证通过的用户ID。如果$List$中不存在新认证的ID_i,则通过用户组策略生成用户组Gp_i,否则立即拒绝该次请求。

步骤4:KGC随机选择r_i、$l\in Z_q^*$、h,并公开参数$R_i=r_iP$、$CL_i=h^lP^{Gp_i}$、h、l。

步骤 5：KGC 计算 $H_1 = h_1(P_{pub}, ID_i, R_i, Gp_j)$，以及部分私钥 $ppk_i = (r_i + sH_1) \bmod q$。

步骤 6：KGC 隐藏部分私钥 $sppk_i = ppk_i \oplus ID_i$，并将隐藏组数 $sGp_i = Gp_i \oplus ID_i$ 返回给用户 U_i。

3.3.3 设置公私钥阶段 $Gpsk(sppk_i, a_i, params) \rightarrow (SK_i, PK_i)$

步骤 1：U_i 计算 $ppk_i = sppk_i \oplus ID_i$，$Gp_i = sGp_i \oplus ID_i$。

步骤 2：U_i 通过验证 $ppk_i P = R_i + H_i P_{pub}$ 是否成立来确认部分私钥的有效性。如果等式成立，说明发送方为可信 KGC，U_i 为合法用户，U_i 将根据秘密值生成公私钥；否则，说明消息发送方非可信 KGC，即拒绝接受消息。

步骤 3：U_i 随机选择 $a_i \in \boldsymbol{Z}_q^*$ 作为其秘密值，并计算 $A_i = a_i P$。

步骤 4：U_i 设置其公私钥为 $PK_i = (A_i, R_i)$、$SK_i = (a_i, ppk_i)$。

3.3.4 签名生成阶段 $Sig(M, ID_i, params, PK_i, SK_i) \rightarrow (\sigma_{L_i}, SoK)$

用户 U_i 为消息 $M \in \{0,1\}^*$ 生成环签名 σ_{L_i} 及知识签名 SoK。假设用户组 Gp_i 对应的公钥集为 $\boldsymbol{L}_i = \{PK_1, PK_2, ..., PK_n\}$，签名者为 $u_k \in \boldsymbol{L}_i$，其公私钥对为 $PK_k = (A_k, R_k)$、$SK_k = (a_k, ppk_k)$。

步骤 1：u_k 计算 $H_2 = h_2(L_i)$、$R = a_k \cdot H_2$、$C_0 = h_3(L_i, M)$、$C_1 = (R/C_0)^{1/n}$。

步骤 2：u_k 计算 $T = {H_2}^{ppk_k}$，选择随机数 r、s_i、$c_i \in \boldsymbol{Z}_q^*$，$i \in [1, ..., k-1, k+1, ..., n]$。

步骤 3：签名者 u_k 计算 $(x_i, z_i) = s_i G + c_i PK_i$、$y_i = {H_2}^{s_i} T^{c_i} \bmod q$、$(x_k, z_k) = rG$、$y_k = {H_2}^r \bmod q$。其中，$i \neq k$。

步骤 4：签名者 u_k 计算 $c_k = h_4(M, T, x_1, ..., x_n, y_1, ..., y_n) - \sum_{i=1}^{n} c_i \bmod q$、$s_k = r - c_k ppk_k \bmod q$。其中，$i \neq k$。

步骤 5：输出环签名 $\sigma_{L_i} = (C_1, T, s_1, ..., s_n, c_1, ..., c_n)$。

步骤 6：签名者 u_k 随机选取 $f \in \boldsymbol{Z}_q^*$ 且计算 $e = h_5(M, L_i, P, h, l, h^l P^f)$、$g = (r - eGp_i) \bmod q$、知识签名 $SoK = (e, g)$。

3.3.5 签名验证阶段 $VerifySig(\sigma_{L_i}, SoK, params, ID_i) \rightarrow (1, 0)$

验证者 V 通过以下等式验证用户 U_i 发送的环签名 σ_{L_i} 及知识签名 SoK 的正确性，如果等式成立则签名合法输出 1；否则输出 0。

步骤 1：V 从 KGC 获取公共参数及 U_i 所发送的 CT_1、L_i、C_1。

步骤 2：V 验证 $CTR_i < n$ 是否成立，CTR_i 为 V 设置的计数器，如果不等式成立则验证 $|CT_2 - CT_1| < \Delta t$，CT_2 为当前的时间戳，Δt 为预定义的最大传输延迟；否则，拒绝接受信息。

步骤 3：V 计算 $H_2 = h_2(L_i)$、$(x_i, z_i) = s_i G + c_i PK_i$、$y_i = {H_2}^{s_i} T^{c_i} (i = 1, 2, ..., n)$。

步骤 4：V 验证 $\sum_{i=1}^{n} c_i = h_4(M, T, x_1, ..., x_n, y_1, ..., y_n)$、$e' = h_5(M_i, CL_i, P, h, l, CL_i{}^e h^{l(1-e)} P^g)$。

3.3.6 追溯阶段 $Trace(M, M') \rightarrow (PK_k)$

对于有特殊需求的患者，追溯者 T 通过环签名进行追溯。首先，T 向消息所属的组 Gp_i 发送消息 M'，要求环成员对消息 M' 利用环公钥集 L_i 再次签名；其次，根据 $TraceList$ 中的公钥数量决定最终输出。其中，PK_k 代表追溯用户的公钥；$Independent$ 表示追溯用户不在此公钥集 L_i。

步骤 1：T 计算 $H_2 = h_2(L_i)$。

步骤 2：T 计算 $C_0 = h_3(L_i, M)$、$C_2 = C_0 C_1{}^i$。其中，$i = 1, 2, .., n$。

步骤 3：T 计算 $C_0' = h_3(L_i, M')$、$C_2' = C_0 C_1{}^i$，其中，$i = 1, 2, .., n$。

步骤 4：对于 $i = 1, 2, .., n$，检查是否 $C_2 = C_2'$，如果成立，则将 PK_k 存储在 $TraceList$ 中。

步骤 5：最终的输出由 $TraceList$ 中的公钥数量决定：如果仅有一个 PK_k，输出 PK_k；如果 $TraceList = \Phi$ 则输出 $Independent$。

4 BCLRS 方案安全性证明和分析

本文对 BCLRS 方案的正确性、匿名性、可追溯性进行安全性证明，其安全性基于 ECDLP 问题和 ECDHP 问题[19,20]。

4.1 安全性证明

定理 1 BCLRS 方案具备正确性。

证明 1 如果 (M, σ_{L_i}, SoK) 是签名者，具有消息 M 的正确签名，则有：

$$c_k = h_4(M, T, x_1, ..., x_n, y_1, ..., y_n) - \sum_{i=1}^{n} c_i \bmod q, i \neq k \quad (1)$$

当 $(x_i, z_i) = s_i P + c_i PK_i$，$y_i = {H_2}^{s_i} T^{c_i}$，$i \neq k$，且 $s_k = r - c_k ppk_k$，则：

$$x_k = s_k P + c_k PK_k, y_k = {H_2}^{s_k + c_k a_k} = {H_2}^{s_k} T^{c_k} \quad (2)$$

$$\sum_{i=1}^{n} c_i = h_4(M, T, x_1, ..., x_n, y_1, ..., y_n) \quad (3)$$

当 $e = h_5(M_i, CL_i, P, h, l, h^l P^f)$ 成立时，可得到 $CL_i{}^e h^{l(1-e)} P^g = (h^l P^{Gp_i})^e h^{l(1-e)} P^g = h^{le + l(1-e)} P^{e\,Gp_i + g} = h^l P^r$，因此，$e' = h_5(M_i, CL_i, P, h, l, CL_i{}^e h^{l(1-e)} P^g)$ 成立，签名验证成功。

定理 2 无证书环签名具备匿名性。

证明 2 假设签名 σ_{L_i} 是由签名者生成的一个合法签名。

对于环签名 $\sigma_{L_i} = (C_1, T, s_1, ..., s_n, c_1, ..., c_n)$。其中，$s_i \in \boldsymbol{Z}_q^* (i = 1, 2, ..., k-1, k+1, ..., n)$；$s_k = r - c_k ppk_k$；$c_k = h_4(M, T, x_1, ..., x_n, y_1, ..., y_n) - \sum_{i=1}^{n} c_i$。

除s_k需要验证者计算,其他的s_i都由签名者随机选择,所以c_k不可预测。综上可知,除了消息M,其他每个参数都由签名者随机选择。因此,攻击者无法推测实际签名者的真实身份,猜测签名者实际身份的概率对于实际签名者而言等于$1/n$。

定理3　无证书环签名具备可追溯性。

证明3　在追溯阶段,环中所有成员需要使用同一个环L_i重新对消息M、M'进行签名。首先,追溯者计算$H_2 = h_2(L_i)$、$C_0 = h_3(L_i, M)$、$C_2 = C_0 C_1^{\ i}, i = 1, 2, .., n$,且$C_1 = (R/C_0)^{1/i}$;其次,计算$C_0' = h_3(L_i, M')$、$C_2' = C_0' C_1^{\ i}, i = 1, 2, .., n$;最后,判断$C_2$与$C_2'$是否相等,即判断新签名是否等于旧签名,如果$C_2 = C_2'$则追溯成功,输出签名者的对应公钥。

定理4　无证书环签名具备不可伪造性。

游戏Ⅲ　Ⅰ型攻击者A_1与挑战者C之间进行交互。

步骤1:初始化。当攻击者A_1请求初始化预言机时,挑战者C初始化KGC。A_1选择两个随机数q、P分别作为群G的阶和生成元。C根据输入的安全参数λ随机选择一个系统主密钥s,同时计算系统主公钥$P_{pub} = sP$。最后,C将系统公共参数$params = \{G, P, P_{pub}, q, h_v\}$发送给$A_1$,挑战者$C$保存系统主密钥$s$。

(1)哈希查询。攻击者A_1执行多项式有限次查询,每次查询依赖于之前的查询结果。

①$h_1(P_{pub}, ID_i, R_i, Gp_i)$。当攻击者$A_1$请求哈希查询$h_1$列表时,挑战者$C$先检查本地列表$\boldsymbol{L}_{h1}$,如果列表中存有此请求,便将$H_1$发送给$C$,否则计算$H_1 = h_1(P_{pub}, ID_i, R_i, Gp_i\}$并将其保存于$\boldsymbol{L}_{h1}$。最后,$C$将$H_1$发送给$A_1$。

②$h_2(L_i)$。当攻击者A_1请求哈希查询h_2列表时,挑战者C先检查本地列表$\boldsymbol{L}_{h2}$,如果H_2存在,挑战者C将其发送给攻击者A_1,否则C计算$H_2 = h_2(L_i)$,并将其存储在本地列表$\boldsymbol{L}_{h2}$后发送给A_1。

③$h_3(L_i, M)$。当攻击者A_1请求哈希查询h_3列表时,挑战者C先检查本地列表$\boldsymbol{L}_{h3}$,如果H_3存在,挑战者C将其发送给攻击者A_1,否则C计算$C_0 = h_3(L_i, M)$,并将其存储在本地列表L_{h3}后发送给A_1。

④$h_4(M, T, x_1, ..., x_n, y_1, ..., y_n)$。当攻击者$A_1$请求哈希查询$h_4$列表时,挑战者$C$先检查本地列表$\boldsymbol{L}_{h4}$,如果$H_4$存在,挑战者$C$将其发送给攻击者$A_1$,否则$C$计算$h_4(M, T, x_1, ..., x_n, y_1, ..., y_n)$,并将其存储在本地列表$\boldsymbol{L}_{h4}$后发送给$A_1$。

⑤$h_5(M, CL_i, P, h, l, h^l P^f)$。当攻击者$A_1$请求哈希查询$h_5$列表时,挑战者$C$先检查本地列表$\boldsymbol{L}_{h5}$,如果$e$存在,挑战者$C$将其发送给攻击者$A_1$,否则$C$计算$e = h_5(M, CL_i, P, h, l, h^l P^f)$,并将其存储在本地列表$\boldsymbol{L}_{h5}$后发送给$A_1$。

(2)部分私钥查询。当挑战者C收到查询请求后,C在部分私钥列表$\boldsymbol{L}_{ppk}$中查询(ID_i, ppk_i)。如果$\boldsymbol{L}_{ppk}$中不存在此请求,C将持续请求用户公钥以查询a_i、H_1。随后,C计算$ppk_i = (r_i + sH_1) \bmod q$,将其保存后发送给攻击者$A_1$,否则$C$将已保存的部分私钥发送给$A_1$。

(3)秘密值查询。因秘密值a_i在公钥列表$\boldsymbol{L}_{PK}$中,如果攻击者A_1发送请求,挑战者C先在$\boldsymbol{L}_{PK}$中搜索ID_i,并将其秘密值a_i发送给A_1;如果不存在ID_i,C随机选择秘密值$a_i \in \boldsymbol{Z}_q^*$,计算$PK_i = \left(A_i, R_i\right)、ID_i、a_i$,并将其存储在$\boldsymbol{L}_{PK}$中,再将$PK_i$发送给$A_1$。

(4)用户公钥查询。当挑战者C收到请求,检查公钥列表$\boldsymbol{L}_{PK}$中是否有用户ID_i。如果存在,C发送PK_i给攻击者A_1,否则C选择随机值$a_i \in \boldsymbol{Z}_q^*$,计算$PK_i = \left(A_i, R_i\right)、ID_i、a_i$,并将其存储在$\boldsymbol{L}_{PK}$中,再将$PK_i$发送给$A_1$。

(5)公钥替换。当挑战者C收到请求,检查公钥列表$\boldsymbol{L}_{PK}$中的(PK_i, ID_i, a_i)。如果$\boldsymbol{L}_{PK}$存有(PK_i, ID_i, a_i),C通过PK_i'、a_i'替换用户的原始公钥PK_i和秘密值a_i,否则C返回未知值。在此请求中,Ⅰ型攻击者A_1可用PK_c'替换用户的原始公钥PK_c。

(6)签名查询。当攻击者A_1提交消息$M \in \{0, 1\}^*$和n个用户的公钥集时,挑战者C输出环签名σ_{L_i}的步骤如下:如果存在用户的公钥$PK_k \in \boldsymbol{L}_i$且满足$PK_k \neq \boldsymbol{L}_i$,则挑战者$C$通过调用签名算法返回环签名$\sigma_{L_i}$,其中$u_k$为实际签名者;否则,挑战者$C$执行以下操作:①计算$T = H_2^{a_k}$,随机选择$r、s_i、c_i \in \boldsymbol{Z}_q^*, i \in [1, ..., k-1, k+1, .., n]$。②挑战者$C$通过计算等式$(x_i, z_i) = s_i G + c_i PK_i、y_i = H_2^{s_i} T^{c_i} \bmod q、(x_k, z_k) = rG、y_k = H_2^r \bmod q, i \neq k$。③挑战者$C$验证等式$c_k = h_4(M, T, x_1, ..., x_n, y_1, ..., y_n) - \sum_{i=1}^{n} c_i \bmod q, i \neq k$是否成立,并计算$s_k = r - c_k a_k \bmod q$。④输出签名$\sigma_{L_i} = (C_1, T, s_1, ..., s_n, c_1, ..., c_n)$。

步骤2:伪造。攻击者A_1如果满足以下条件,则输出用户ID_C在消息M_C上的环签名σ_{L_i}*:①伪造签名σ_{L_i}*是一个有效的环签名,$VerifySig(\sigma_{L_i}, params, ID_i) \rightarrow 1$;②伪造签名$\sigma_{L_i}$*来自于伪造阶段,而非来自签名查询阶段;③攻击者$A_1$不能查询$\boldsymbol{L}_i$中任何用户的部分私钥。

$$\sigma' = (C_1, T', s_1, ..., s_k', ..., s_n, c_1, ..., c_k', ..., c_n) \tag{4}$$

$$\sigma'' = (C_1, T'', s_1, ..., s_k'', ..., s_n, c_1, ..., c_k'', ..., c_n) \tag{5}$$

因$s_k' = r - c_k' ppk_k、s_k'' = r - c_k'' ppk_k$,由式(4)、式(5)可得$abP = a_k = (s_k' - s_k'')^{-1}(c_k'' - c_k')$。

根据分叉引理可知,攻击者A_1在游戏Ⅲ中计算出abP的值,即可解决ECDHP问题,与ECDHP困难问题矛盾。因此,BCLRS方案在ROM下不可伪造[23]。

游戏Ⅳ　Ⅱ型攻击者A_2与挑战者C之间交互。

攻击者A_2除了无法调用公钥替换请求外,与上述攻击者A_2所能调用的请求相同,因此A_2的安全证明过程与游戏Ⅲ类似。由于A_2有能力窃取系统主密钥s,因此A_2可伪造一个挑战用户的签名。当A_2试图伪造一个签名时,必须

首先伪造 R_c，如果伪造成功，意味着在区块链系统中成功发起了51%攻击（任意用户都可通过KGC访问 R_c）。

$$H_{A_2}/H_t \leqslant 51\% \tag{6}$$

式中：H_{A_2} 表示 A_2 的可用计算能力；H_t 表示系统的总计算能力。

由于区块链的防篡改能力，A_2 不可能具有足够大的哈希算力发起攻击[24]。由 $s_k' = r - c_k' ppk_k$、$s_k'' = r - c_k'' ppk_k$ 可得 $s = s_k' - s_k''/H_1\left(c_k'' - c_k'\right) - R_i/H_1 P$。因此，攻击者 A_2 的成功概率为：

$$s_k' - s_k''/H_1\left(c_k'' - c_k'\right) - R_i/H_1 P + P\left(H_{A_2}/H_t \leqslant 51\%\right) \tag{7}$$

根据ECDLP假设，攻击者 A_2 在游戏Ⅳ中计算出 s 的值与ECDLP问题矛盾。因此，BCLRS方案在ROM下是不可伪造的。

4.2 安全性分析

本文从抵抗恶意攻击方面对BCLRS方案进行安全性分析。

（1）抗KGC妥协攻击。在传统的无证书环签名方案中，集中式KGC负责密钥生成。当集中式KGC被入侵后，将泄露用户密钥及身份。BCLRS方案以部署在区块链的KGC取代集中式KGC。如果攻击者试图攻击或篡改KGC，需要对区块链系统进行51%的攻击。由于区块链的不可篡改性质，攻击者难以获取秘密值并更改参数。因此，BCLRS方案可抵御KGC妥协攻击。

（2）抗重放攻击。假设攻击者窃听用户和验证者之间的通信信道，用户生成或传输的签名都有可能被攻击者捕获。BCLRS方案在签名发送时增加时间戳 CT_1，验证者在验证签名时需验证 CT_1 的有效性，即验证 $|CT_2 - CT_1| < \Delta t$ 是否成立，其中 CT_2 为验证者接收到签名时的时间戳，Δt 为验证者预定义的最大传输延迟，只有满足上述不等式时验证者才会接收签名；否则，立刻拒绝接受消息。因此，BCLRS方案可抵御重放攻击。

（3）抗DDOS攻击。区块链用户都必须有一个用于交易的地址，BCLRS方案设置了两个计数器 $Addr_{ID_i}$、CTR_i，用于检测用户发送请求及发送签名的频率。当KGC接受用户请求时，先验证 $CTR_i < n$ 是否成立，n 为KGC设定的自定义阈值，如果用户的请求频率大于规定阈值，请求将被阻塞一段时间。因此，BCLRS方案可抵御DDOS攻击。

（4）抗MITM攻击。为了防止攻击者拦截和修改信道中传输的信息，BCLRS方案利用椭圆曲线加密算法构造密钥生成算法，隐藏用户 ID_i。用户在传输 ID_i 时，根据KGC公开的参数 P、P_{pub} 计算 $P_{ID_i} = ID_i P$、$E_{ID_i} = ID_i - ID_i P_{pub}$，并发送给KGC。假设攻击者截获了消息，但因系统主密钥 s 仅由KGC拥有，攻击者无法求解用户的 ID_i。同时，在传输部分密钥及环签名组数时，利用异或操作实现秘密值隐藏。假设攻击者截获消息，但因发送的部分密钥 $sppk_i$ 和发送的组数 sGp_i 与 ID_i 进行了异或操作，攻击者无法得知 ID_i、ppk_i、Gp_i。因此，BCLRS方案可抵御MITM攻击。

5 性能分析

本文从安全性和计算开销两个方面对BCLRS方案进行性能分析，并与文献[12,13,25,26]的无证书环签名方案进行比较。此外，通过仿真实现BCLRS方案、文献[26-28]的无证书环签名方案，根据实验结果比较计算开销。

5.1 安全性能分析

无证书环签名方案能否抵御恶意攻击是安全性能评判的重要指标之一。表2给出了BCLRS方案及文献[12,13,25,26]的无证书签名方案的安全性能。其中，√表示文献可抵抗对应的攻击；×表示文献无法抵抗对应的攻击。

Table 2 Comparison of safety performance of BCLRS solutions

表2 BCLRS方案安全性能比较

方案	身份隐私保护	可追溯性	KGC妥协攻击	DDOS攻击	MITM攻击
文献[12]	×	×	×	×	√
文献[13]	×	×	√	√	√
文献[25]	×	√	×	×	×
文献[26]	×	×	×	×	×
BCLRS方案	√	√	√	√	√

在身份隐私保护方面，文献[12,13,25,26]均未保护用户隐私，在智慧医疗场景中难以满足用户对隐私保护的需求，特别是涉及大量互联医疗传感器的数据传输场景，身份隐私暴露可能增加患者数据被滥用或被非法追踪的风险。相较而言，BCLRS方案通过无证书环签名技术、环签名的匿名特性，可成功隐藏签名者身份，确保患者信息在数据传输和认证过程中不被泄露。

在可追溯性方面，文献[12,13,26]缺乏对用户身份的追溯性，在智慧医疗场景中难以满足医疗机构对特殊患者身份追溯的需要。BCLRS方案通过环签名的匿名性和可追溯性设计，在保护患者隐私的同时，为医疗机构提供了可追踪患者特定身份的机制。

在抵抗恶意攻击方面，文献[12,25,26]均依赖传统的集中式KGC，易遭受KGC妥协攻击、DDOS攻击和MITM攻击。如果攻击者成功攻破KGC，即可获取用户部分私钥或身份信息，导致整个系统的安全性和隐私性彻底崩溃。文献[12,25,26]缺乏有效的防御机制，医疗数据传感器一旦受到DDOS攻击将无法正常工作，严重影响了医疗数据传输的可靠性。同时，这些方案在不可信信道传输中的安全性不够，未能有效抵御MITM攻击，攻击者可在数据传输过程中拦截或篡改医疗数据，危及患者安全和系统完整性。BCLRS方案将KGC部署在区块链，以消除集中式KGC可能出现的单点故障问题，通过区块链的去中心化和不可篡改特性抵御KGC妥协攻击，并引入请求计数器和时间戳抵御重放攻击和DDOS攻击。

综上，BCLRS方案可很好地抵御无证书环签名方案中

常见的KGC妥协攻击、DDOS攻击等恶意攻击,相较于文献[12,13,25,26]安全性更高,能应用于隐私保护要求更高的智慧医疗场景。

5.2　BCLRS方案计算开销分析及比较

BCLRS在个人电脑(Windows10操作系统、英特尔i5-8300H处理器,主频2.30 GHz,8 GB内存),使用MIRACL库实行以下密码运算的运行时间如表3所示。

Table 3　Symbolic representation of password operation time

表3　密码运算时间的符号表示

符号	密码运算名称	时间/ms
T_P	双线性配对运算	7.396 8
T_M	标量乘法运算	1.315 1
T_A	标量加法运算	0.023 6
T_W	幂指数运算	0.259 0
T_H	哈希函数运算	0.000 1

由于本文利用的是椭圆曲线公钥加密技术,而文献[28]是双线性配对技术。为了实现相同的测试环境,对BCLRS方案及文献[26-28]采用了支持双线性配对的椭圆曲线群 $E: y^2 = x^3 - 3x(\mathrm{mod}\,p)$。其中,$P = 2$;$p$ 为1 536 bit的素数;q 为256 bit的素数。BCLRS方案及文献[26-28]的计算开销如表4所示。

Table 4　Comparison of calculation costs for BCLRS scheme

表4　BCLRS方案计算开销比较

方案	签名生成阶段	签名验证阶段	总时间
文献[26]	$(3T_H + 4T_A + 3T_M) \times n - (T_H + 3T_A + T_M)$	$2nT_H + (2n + 1)T_A + (2n + 2)T_M$	$(5n - 1)T_H + (6n - 2)T_A + (5n + 1)T_M$
文献[27]	$(3n + 2)T_M + T_H$	$(3n + 3)T_M + T_H$	$(6n + 5)T_M + 2T_H$
文献[28]	$(2n + 2)T_M + nT_A$	$nT_M + 2T_P$	$(3n + 2)T_M + nT_A + 2T_P$
BCLRS方案	$(2n - 1)T_M + T_H + 2T_w$	$2(nT_M + T_H)$	$(4n - 1)T_M + 3T_H + 2T_W$

图2、图3描述了BCLRS方案及文献[26-28]的签名生成、签名验证阶段的计算开销,单位为 ms。其中,横坐标表示签名生成及验证的环成员数量;纵坐标表示各个方案签名生成及验证的计算开销。如图2所示,当环成员数量为10时,BCLRS方案的计算开销低于文献[26-28],且

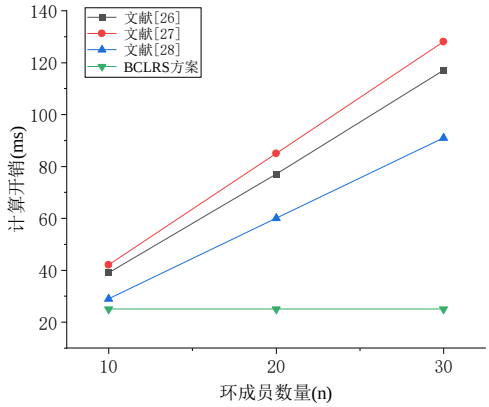

Fig. 2　Signature generation comparison

图2　签名生成对比较

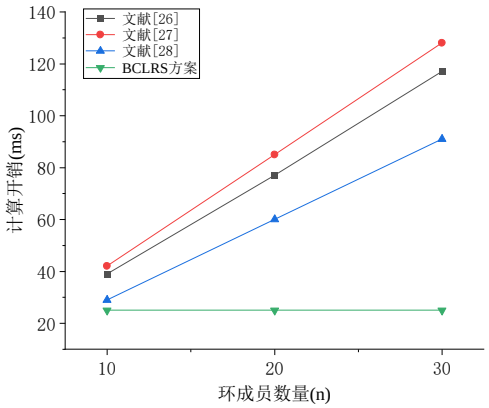

Fig. 3　Signature verification comparison

图3　签名验证比较

BCLRS方案在签名生成阶段生成的知识签名 SoK,保证了环签名的安全性与完整性。随着环成员数量增加,由于BCLRS方案采用用户组策略,环成员数量限制为固定值,因此计算开销固定。在环成员数量为30时,BCLRS方案的签名生成算法的计算开销仅为文献[27]的19.5%。

如图3所示,当环成员数量为10时,BCLRS方案与文献[26,28]的计算开销相近,但文献[26,28]未保证环签名的可靠性。同时,BCLRS方案在签名验证时额外验证了知识签名 SoK,在保证环签名可靠性的同时还能保护用户隐私。随着环成员数量增加,BCLRS方案计算开销固定。在环成员数量为30时,BCLRS方案签名验证算法的计算开销仅为文献[27]的20.8%。

综上,BCLRS方案相较于文献[26-28]方案具有更高的安全性和更低的计算开销。

6　结语

本文提出一种基于区块链的无证书环签名方案BCLRS。在效率方面,BCLRS方案采用安全性高、密钥短的椭圆曲线密码以降低计算开销;设计用户组策略使环签名在用户数量增加的同时,仍能保证签名生成及验证阶段的高效性,减轻了医疗数据传感器的负担。在安全性方面,解决了证书分发和管理的安全问题,实现了患者隐私保护及可追溯用户的功能;将KGC部署在区块链上实现了不可篡改性,能抵抗DDOS攻击、KGC妥协攻击等攻击。

实验表明,本文在随机预言机模型下证明了所提方案能抵抗Ⅰ/Ⅱ型等攻击,安全性较高,具有匿名性、不可伪造性等属性。相较于现有典型的无证书环签名方案,在具备更高安全性的同时,计算代价更少,适用于资源受限的智慧医疗场景。

然而,本方案仅支持医疗数据传感器与医院之间的安全认证,未充分考虑数据在多方协作场景下的隐私保护和高效处理。此外,区块链的吞吐量限制和环签名在超大规模环成员下的计算开销可能对系统实时性产生一定影响。未来,将进一步提升方案的隐私保护及效率,以更好地适

应智慧医疗场景中的共享需求。

参考文献：

[1] ZHANG Y Q, ZHOU W, PENG A N. Survey of Internet of Things security [J]. Journal of Computer Research and Development, 2017, 54(10): 2130-2143.
张玉清, 周威, 彭安妮. 物联网安全综述[J]. 计算机研究与发展, 2017,54(10):2130-2143.

[2] ZHANG X J, WANG X, LIAO W C, et al. Lightweight integrity verification scheme for outsourced medical data in cloud storage supporting conditional identity anonymity[J]. Journal of Electronics & Information Technology, 2022, 44(12): 4348-4356.
张晓均, 王鑫, 廖文才, 等. 支持条件身份匿名的云存储医疗数据轻量级完整性验证方案[J]. 电子与信息学报, 2022, 44(12): 4348-4356.

[3] DENG Y, CHEN X Q, WANG Z H, et al. Blockchain-based privacy security protection feasibility analysis[J]. Software Guide, 2019, 18(1): 166-168.
邓毅, 陈秀清, 王志豪, 等. 基于区块链的隐私安全保护可行性分析[J]. 软件导刊, 2019,18(1):166-168.

[4] AL-RIYAMI S S, PATERSON K G. Certificateless public key cryptography[C]// International Conference on the Theory and Application of Cryptology and Information Security, 2003: 452-473.

[5] YEH K H, TSAI K Y, FAN C Y. An efficient certificateless signature scheme without bilinear pairings[J]. Multimedia Tools and Applications, 2015, 74: 6519-6530.

[6] WANG L, CHEN K, LONG Y, et al. A modified efficient certificateless signature scheme without bilinear pairings[C]// International Conference on Intelligent Networking and Collaborative Systems, 2015: 82-85.

[7] YEH K H, SU C, CHOO K K R, et al. A novel certificateless signature scheme for smart objects in the Internet-of-Things[J]. Sensors, 2017, 17(5): 1001.

[8] JIA X, HE D, LIU Q, et al. An efficient provably-secure certificateless signature scheme for Internet-of-Things deployment[J]. Ad Hoc Networks, 2018, 71: 78-87.

[9] KARATI A, ISLAM S K H, KARUPPIAH M. Provably secure and lightweight certificateless signature scheme for IIoT environments[J]. IEEE Transactions on Industrial Informatics, 2018, 14(8): 3701-3711.

[10] PAKNIAT N, VANDA B A. Cryptanalysis and improvement of a pairing-free certificateless signature scheme[C]// International Conference on Information Security and Cryptology,2018: 1-5.

[11] WU Q, ZHANG L, YANG Y, et al. Certificateless signature scheme with batch verification for secure and privacy-preserving V2V communications in VANETs[J]. IEEE Transactions on Dependable and Secure Computing, 2024, 10(1): 1-12.

[12] YANG X, WEN H, DIAO R, et al. Improved security of a pairing-free certificateless aggregate signature in healthcare wireless medical sensor networks[J]. IEEE Internet of Things Journal, 2023, 10(12): 10881-10892.

[13] LI X, ZHOU L, YIN X, et al. A security-enhanced certificateless designated verifier aggregate signature scheme for HWMSNS in the YOSO model[J]. IEEE Internet of Things Journal, 2023, 11(6): 10865-10879.

[14] FUJISAKIE,SUZUKIK. Traceable ring signature[C]// International Conference on Public Key Cryptography, 2007: 181-200.

[15] LIU J K, WEI V K, WONG D S. Linkable spontaneous anonymous group signature for ad Hoc groups[C]// International Conference on Information Security and Privacy, 2004: 325-335.

[16] PENG C, HE D B, LUO M. An Identity-based ring signature scheme for SM9 algorithm[J]. Journal of Cryptologic Research, 2021, 8(4): 724-734.
彭聪, 何德彪, 罗敏. 基于SM9标识密码算法的环签名方案[J]. 密码学报, 2021,8(4):724-734.

[17] AU M H, LIU J K, SUSILO W, et al. Secure ID-based linkable and revocable-iff-linked ring signature with constant-size construction[J]. Theoretical Computer Science, 2013, 469: 1-14.

[18] SCAFURO A, ZHANG B. One-time traceable ring signatures[C]// International Conference on European Symposium on Research in Computer Security, 2021: 481-500.

[19] KOBLITZ N. Elliptic curve cryptosystems[J]. Mathematics of Computation, 1987, 48(177): 203-209.

[20] BONEH D, BOYEN X. Short signatures without random oracles[C]// International Conference on the Theory and Applications of Cryptographic Techniques,2004: 56-73.

[21] CHASE M, LYSYANSKAYA A. On signatures of knowledge[C]// International Conference on Cryptology Conference,2006: 78-96.

[22] SHIM K A. A secure certificateless signature scheme for cloud-assisted Industrial IoT[J]. IEEE Transactions on Industrial Informatics, 2024, 20(4): 6834-6843.

[23] POINTCHEVAL D, STERN J. Security proofs for signature schemes [C]// International Conference on the Theory and Applications of Cryptographic Techniques,1996: 387-398.

[24] GHARAVI H, GRANJAL J, MONTEIRO E. Post-quantum blockchain security for the Internet of Things: survey and research directions[J]. IEEE Communications Surveys & Tutorials, 2024, 26(3): 1748-1774.

[25] MA K, ZHOU Y, WANG Y, et al. An efficient certificateless signature scheme with provably security and its applications[J]. IEEE Systems Journal, 2023, 17(4): 5636-5647.

[26] WANG W, LI X, QIU X, et al. A privacy preserving framework for federated learning in smart healthcare systems[J]. Information Processing & Management, 2023, 60(1): 103167.

[27] ZHANG S, YING X, WANG B. A privacy protection scheme based on linkable ring signature for user payment of peer-to-peer uniform-price double auction transaction in the microgrid day-ahead market[J]. International Journal of Electrical Power & Energy Systems, 2023, 147: 108806.

[28] LIU Q, WANG G, YAN B, et al. BCRS-DS: a privacy-protected data sharing scheme for IOT based on blockchain and certificateless ring signature[J]. Journal of Information Security and Applications, 2024, 87: 103914.

（责任编辑：刘嘉文）