基于区块链的无线体域网无证书密文等值测试签密方案

杨小东[1],周 航[1],汪志松[1],袁 森[1],王彩芬[2]
(1. 西北师范大学计算机科学与工程学院,甘肃兰州 730070; 2. 深圳技术大学大数据与互联网学院,广东深圳 518118)

摘 要: 针对无线体域网密码方案中存在的密钥管理、密文检索与依赖可信第三方等问题,本文提出了一种基于区块链的无线体域网无证书密文等值测试签密方案. 基于无证书签密机制,解决了传统方案中的密钥托管问题,保证了医疗数据的机密性与可认证性. 利用等值测试技术,实现了对云端医疗密文的检索,减少了数据用户对重复数据解密的计算开销. 引入区块链与智能合约技术,消除了等值测试操作对可信云服务器的依赖. 利用雾节点执行部分解密计算,降低了数据用户解密时的计算开销. 在随机预言模型下,基于计算性 Diffie-Hellman 困难问题证明了本文方案满足单向性. 与同类方案相比,本文方案支持更多的安全属性,并具有较低的计算开销.

关键词: 无线体域网; 区块链; 等值测试; 无证书签密; 雾计算

基金项目: 国家自然科学基金(No.61662069,No.61562077);中国博士后科学基金(No.2017M610817);兰州市科技计划(No.2013-4-22);西北师范大学青年教师科研能力提升计划(No.NWNU-LKQN-14-7)

中图分类号: TP309.7 **文献标识码:** A **文章编号:** 0372-2112(2023)04-0922-11

电子学报 URL:http://www.ejournal.org.cn **DOI:**10.12263/DZXB.20210855

Blockchain-Based Certificateless Signcryption Scheme with Equality Test for Wireless Body Area Network

YANG Xiao-dong[1], ZHOU Hang[1], WANG Zhi-song[1], YUAN Sen[1], WANG Cai-fen[2]
(1. *College of Computer Science and Engineering*, *Northwest Normal University*, *Lanzhou*, *Gansu* 730070, *China*;
2. *College of Big Data and Internet*, *Shenzhen Technology University*, *Shenzhen*, *Guangdong* 518118, *China*)

Abstract: Aiming at the problems of key management, ciphertext retrieval and dependence on trusted third party, a blockchain-based certificateless signcryption scheme with equality test for wireless body area network is proposed. The certificateless signcryption solves the problem of key escrow and ensures the confidentiality and authentication of medical data. Meanwhile, the equality test technology is used to retrieve the medical ciphertext, which reduces the computational cost of data users to decrypt duplicate data. In addition, blockchain and smart contract are used to eliminate the dependence of trusted cloud servers. The fog nodes perform part of the decryption computation, which reduces the computation overhead of data users. Furthermore, the proposed scheme is proved to achieve one-way based on the computational Diffie-Hellman problem under the random oracle model. Compared with the similar schemes, the proposed scheme supports more security properties and has lower computational overhead.

Key words: wireless body area network; blockchain; equality test; certificateless signcryption; fog computing

Foundation Item(s): National Natural Science Foundation of China (No.61662069, No.61562077); China Postdoctoral Science Foundation (No.2017M610817); Science and Technological Projects of Lanzhou (No.2013-4-22); Northwest Normal University Young Teachers Research Capacity Improvement Program (No.NWNU-LKQN-14-7)

1 引言

无线体域网(Wireless Body Area Network,WBAN)[1]通过佩戴或植入到人体的无线传感器监测患者各方面的医疗数据,并将获取的医疗数据发送给医生或医疗机构,便于对患者病情做出相应诊断或对医疗数据进行整合. 无线体域网技术拥有低时延和高灵活性的特

收稿日期:2021-07-06;修回日期:2022-02-13;责任编辑:孙瑶

点,在医疗保健、病情监控和安全防护等领域拥有广阔的应用前景.

然而,无线体域网技术的广泛应用同时也带来了许多安全问题[2]. WBAN中传输与存储的是涉及患者隐私的敏感医疗数据,这些数据在开放的无线网络中传输时必定会面临隐私泄露的风险. 为保证用户数据隐私安全,可以对WBAN中的医疗数据加密后再传输[3]. 但传统加密方案在无线体域网的实际应用中存在着一些缺陷,例如需要可信中心对用户的私钥进行托管、计算资源受限的WBAN节点难以完成较为复杂的运算、加密操作增加了数据检索的难度以及数据检索对可信云服务器的依赖等.

针对传统WBAN加密方案中存在的问题,本文提出了一种基于区块链的无线体域网无证书密文等值测试签密方案,实现了去中心化的密文检索,同时保证了WBAN中医疗数据的机密性、完整性与可认证性. 本文方案的特点如下.

(1)支持密文检索:通过等值测试技术对数据拥有者的医疗密文与数据用户的兴趣密文进行匹配,数据用户无须对密文进行解密,就可以实现对医疗密文的检索.

(2)无证书签密体制:基于无证书签密体制,消除了传统密码方案中密钥管理产生的开销,同时确保了医疗数据的机密性、完整性、可认证性与数据拥有者签名的不可伪造性.

(3)支持外包计算:数据用户将对密文的完整性验证外包给雾节点执行,降低了数据用户在对医疗密文进行解密时产生的开销.

(4)去中心化:由部署在联盟区块链平台上的智能合约执行密文等值测试,消除了对可信云服务器的依赖,实现了密文检索操作的去中心化.

1.1　相关工作

目前,已有许多国内外学者提出了适用于无线体域网的密码方案[3-6],利用加密技术保证WBAN中医疗数据的机密性. 但由于传统无线体域网中用户节点的计算资源十分有限,在对医疗数据进行加解密时难以完成复杂度较高的计算. 一些学者提出将部分复杂的计算进行外包[7-9],有效降低了无线体域网用户的计算开销. 尽管上述方案实现了医疗数据传输时的机密性,但没有考虑到对医疗数据来源的认证. 若医生对来源不明的医疗数据进行处理与诊断,不仅会导致医疗资源的浪费,还可能威胁到患者的生命安全.

基于数字签密技术[10],许多能同时保证医疗数据机密性与可认证性的方案相继被提出. Cagalaban等人[11]构造了一种基于身份的签密方案,确保医疗保健系统中数据的机密性与完整性的同时实现了对数据来源的认证,但该方案需要可信中心对用户私钥进行托管. 为消除密钥托管问题,许多适用于无线体域网的无证书签密方案[12-14]相继被提出. 尽管上述方案确保了医疗数据传输时的机密性与可认证性,但忽略了如何实现对云端医疗数据进行有效检索的问题. 医疗数据往往以加密的形式存储在云端,以保护患者的隐私,但同时增加了对云端医疗数据进行检索的难度.

为了实现对WBAN云端医疗密文的有效检索,Zhang[15]提出了支持多关键字搜索的公钥加密算法,满足了数据用户对存储于云端的医疗密文的搜索需求,但该方案仅支持对由相同公钥加密的医疗数据的搜索,在无线体域网的实际应用中存在一定的局限性. Ramadan等人[16]提出了一种具有等值测试功能的加密方案,实现了对用不同公钥加密的医疗密文的检索. 2021年,Xiong等人[17]构造了一种支持等值测试的签密技术,实现密文检索的同时确保了医疗数据的机密性与可认证性. 然而,以上方案中对密文的检索过程都由云服务器执行,半可信的云服务器在执行用户命令的同时会对处理的数据感到好奇. 若云服务器发生不可预测的故障或遭到恶意攻击而输出错误的结果,则可能导致医生对患者的病情进行错误诊断,同时患者的隐私数据也可能被泄露.

1.2　本文主要工作

针对现有无线体域网密码方案中存在的问题,本文提出了一种基于区块链的无线体域网无证书密文等值测试签密方案. 该方案基于无证书签密体制,确保了医疗数据在传输时的机密性、完整性、可认证性与数据拥有者签名的不可伪造性. 采用等值测试技术搜索医疗密文中是否存在数据用户想要获取的数据,实现了对患者医疗密文的高效检索. 利用部署在联盟区块链中的智能合约执行测试操作,消除了测试操作对可信云服务器的依赖. 此外,该方案将解密过程中的部分复杂计算外包给半可信的雾节点执行,降低了数据用户在解密时产生的开销. 分析结果表明,本文方案满足医疗数据的机密性、数据拥有者签名的不可伪造性、外包计算的安全性、等值测试结果的可信性与测试陷门的单向性.

2　预备知识

2.1　困难问题

计算性Diffie-Hellman(Computation Diffie-Hellman, CDH)问题:设G是阶为素数p的循环乘法群,g是G的生成元,$a,b\in Z_p^*$,已知(g,g^a,g^b),计算g^{ab}.

可除计算性(Divisible Computation Diffie-Hellman, DCDH)问题:设G是阶为素数p的循环乘法群,g是G的生成元,$a,b\in Z_p^*$,已知(g,g^a,g^b),计算$g^{b/a}$.

在群G中,CDH问题与DCDH问题等价[18].

2.2 区块链与智能合约

区块链技术[19]能够通过去中心化方式，消除密码方案对可信云服务器的依赖．在区块链平台中，交易的产生、验证与记录等操作均由分布式网络执行，同时区块链采用特定的奖励机制，以激励各节点提供算力或资源，并通过共识机制和密码算法来保证交易的安全性．区块链依据开放程度的不同而分为公有链、私有链和联盟链．其中，公有链允许所有人在链上发布交易、确认交易与读取数据，是对所有人开放的共识区块链．私有链的写入与读取权限由某中心化机构掌控，其信任度相比于公有链较低，但写入权限的限制使得私有链更具灵活性．联盟链指由多个组织共同构建与维护的区块链，各个参与者之间通过契约构建共识机制以实现部分去中心化，且相比于公有链，联盟链有更强的可控性．

智能合约[20]是一段部署于区块链平台的代码，无须依赖第三方就可以进行可信交易．区块链节点通过发布交易，将预定义的规则以智能合约的形式部署于区块链上．当某一事务满足触发条件时，智能合约会自动执行相关计算，并将该事务的输入、输出以及合同状态的变化情况等信息记录在区块链中．智能合约为区块链应用层提供了各种负责存储或处理外部数据的接口，使区块链技术能够代替半可信云服务器执行密文检索[21,22]等操作．

2.3 雾计算

雾计算[23]是一种新型分布式网络计算模式，其体系架构通常分为3层：用户层、雾层和云层．其中，用户层由智能手机、平板、无线传感器等智能终端组成，这些终端设备也被称作终端节点．雾层位于用户层与云层之间，由部署在如医院、商场和酒店等应用场所的雾服务器组成，每一个雾服务器都具有一定的计算与存储能力，可以对用户外包的数据执行相应的计算．云层是雾计算架构中的核心层，处于其中的云服务器相比于雾服务器拥有更强的计算能力与存储能力．

雾计算介于个人计算与云计算之间，外包数据可以由雾节点进行处理后再上传到云端或发送给用户．雾计算的架构比云计算更加接近网络边缘，用户无须连接大型数据中心就能实现对数据的存取．雾计算具有低延迟、位置感知、分布广泛和易于实现等特性，十分适用于追求数据时效性且节点众多的无线体域网．

3 系统模型及安全目标

3.1 系统模型

本文提出的基于区块链的无证书密文等值测试签密方案的系统模型如图1所示，包括6个实体：密钥生成中心(Key Generation Center，KGC)、云服务提供商、数据拥有者、数据用户、区块链和雾节点．

(1)KGC：负责初始化系统，分别为数据拥有者和数据用户计算其部分私钥．

(2)云存储提供商：负责在云服务器存储用户上传的医疗密文．

(3)数据拥有者：即患者佩戴的无线传感设备，负责加密监测到的医疗数据，将医疗数据密文和测试陷门分别上传给云服务器和区块链平台．

(4)数据用户：即医生，对希望获取的医疗数据进行加密，将兴趣密文和测试陷门分别上传到云服务器和区块链平台．

(5)区块链平台：部署了智能合约的联盟区块链．智能合约从云端下载患者的医疗密文与医生的兴趣密文，根据双方的测试陷门对两个密文进行等值测试．

(6)雾节点：负责对从云服务器下载的医疗密文进行完整性验证的相关计算．

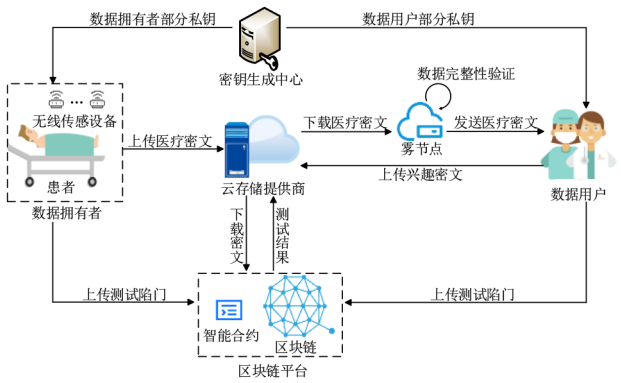


图1 系统模型

3.2 安全目标

本文提出的基于区块链的无线体域网无证书密文等值测试签密方案需要考虑4类敌手[24]，关于4类敌手的具体描述如下：I类敌手无法获取主密钥但能替换用户公钥，且无法获取用户的测试陷门；II类敌手能够获取主密钥但不能替换用户公钥，且无法获取用户的测试陷门；III类敌手无法获取主密钥但能替换用户公钥，拥有测试陷门但无法判断挑战密文对应哪个消息；IV类敌手能够获取主密钥但不能替换用户公钥，拥有测试陷门但无法判断挑战密文对应哪个消息．针对以上4类敌手，本文方案旨在达到如下5个安全目标．

(1)医疗数据的完整性和机密性：WBAN中传输与存储着大量患者敏感的隐私数据，因此需要保证患者医疗数据的安全性．本文方案通过加密技术保障医疗数据在传输和存储过程中面对I类和II类敌手时的机密性与完整性．

(2)患者签名的不可伪造性：利用签密技术能够保证无线体域网中医疗数据的机密性和可认证性．在对医疗数据的来源进行认证的过程中，需要确保针对I类

和II类类敌手时数据拥有者签名的不可伪造性.

(3)测试陷门的单向性:在区块链对密文进行等值测试的过程中,需保证测试陷门在面对III类和IV类敌手时满足单向性,即无法从测试陷门推算出与医疗数据相关的信息.

(4)等值测试结果的可信性:通过等值测试技术可以判断两个密文是否对应同一明文而无须进行解密操作. 在等值测试的过程中,需要确保输出测试结果的正确性.

(5)外包计算的安全性:雾节点是半可信的,在执行外包计算的过程中可能非法读取医疗数据相关信息,因此需要保证外包给雾节点的计算不会泄露医疗数据的相关信息.

3.3　运行流程

(1)系统初始化. 由KGC执行系统初始化操作生成系统参数,同时将智能合约代码部署在联盟区块链中.

(2)用户密钥生成. 用户与KGC共同生成密钥,通过用户选取的秘密值、KGC提供的部分私钥以及系统参数计算出用户的公私钥对.

(3)医疗数据加密及上传. 数据拥有者对无线传感器监测到的医疗数据进行签密,将密文上传到云端存储. 同时,数据用户对希望获取的兴趣数据进行加密,将兴趣密文上传到云端存储.

(4)密文等值测试. 数据拥有者与数据用户分别将用于等值测试的陷门上传给区块链平台,部署于区块链的智能合约按照预定义的规则,使用测试陷门对从云服务器下载的双方密文执行等值测试操作,并将等值测试结果返回给云服务器.

(5)医疗数据解密及验证. 如果等值测试结果显示云端存储的数据中有医生希望获取的医疗数据,则云服务器将患者相关的医疗数据密文发送给雾节点进行完整性验证. 验证通过后,由医生对密文进行解密与消息来源的验证.

4　本文方案

4.1　方案详细构造

(1)系统初始化

KGC执行系统初始化算法,生成系统参数与主密钥,KGC具体操作如下.

(*a*)随机选择两个足够大的素数 p 和 q,其中 $q|(p-1)$,q 为群 Z_p^* 的阶,循环群 G 是 Z_p^* 的子群,g 是 G 的生成元,选择7个满足如下映射的哈希函数:

$$H_1:\{0,1\}^*\times Z_p^*\to Z_q^*$$
$$H_2:\{0,1\}^{l_0}\times\{0,1\}^{l_1}\to Z_q^*$$
$$H_3:G\to\{0,1\}^{l_0+l_1}$$
$$H_4:\{0,1\}^*\to Z_q^*$$
$$H_5:\{0,1\}^{l_1}\to Z_q^*$$
$$H_6:Z_q^*\to\{0,1\}^{l_0}$$
$$H_7:\{0,1\}^{l_0}\to\{0,1\}^{l_0}$$

其中,l_0 和 l_1 是安全参数,定义消息空间为 $\{0,1\}^{l_0}$;

(*b*)随机选择 $s\in Z_q^*$ 作为主密钥秘密保存,计算系统公钥 $P_{\text{pub}}=y=g^s$. 输出系统参数 $\text{params}=\{p,q,g,G,P_{\text{pub}},H_1,H_2,H_3,H_4,H_5,H_6,H_7\}$.

(2)密钥生成

KGC根据系统参数与用户身份标识为用户计算部分私钥,用户利用KGC发送的部分私钥计算完整密钥. 用户与KGC具体操作如下.

(*a*) KGC选择随机数 $k_{i,1},k_{i,2}\in Z_q^*$,分别计算 $u_{i,1}=g^{k_{i,1}}$,$u_{i,2}=g^{k_{i,2}}$,$e_{i,1}=H_1(\text{ID}_i,u_{i,1})$ 及 $e_{i,2}=H_1(\text{ID}_i,u_{i,2})$;

(*b*)KGC计算 $D_{i,1}=k_{i,1}-se_{i,1}$ 与 $D_{i,2}=k_{i,2}-se_{i,2}$,生成用户部分私钥 $\text{ppk}_i=(D_{i,1},D_{i,2})$;

(*c*)用户随机选取 $x_i\in Z_q^*$ 作为秘密值,计算 $\text{SK}_i=(\text{SK}_{i,1},\text{SK}_{i,2})=(x_i-D_{i,1},x_i-D_{i,2})$ 作为私钥,计算 $\text{PK}_i=(\text{PK}_{i,1},\text{PK}_{i,2})=(g^{\text{SK}_{i,1}},g^{\text{SK}_{i,2}})$ 作为公钥.

(3)医疗数据加密及上传

给定数据拥有者的公钥与私钥分别为 PK_A 与 SK_A,数据拥有者执行如下操作对医疗数据 m_A 进行签密:

(*a*)随机选择 $w_\text{A}\in\{0,1\}^{l_1}$,计算 $r_\text{A}=H_2(m_\text{A},w_\text{A})$;

(*b*)随机选择 $t_\text{A}\in Z_q^*$,计算

$$C_{\text{A},1}=H_3(g^{r_\text{A}})\oplus(m_\text{A}\|w_\text{A})$$
$$C_{\text{A},2}=t_\text{A}H_7(m_\text{A})\oplus H_6(g^{r_\text{A}})$$
$$C_{\text{A},3}=\text{PK}_{\text{A},2}^{r_\text{A}}$$
$$C_{\text{A},4}=g^{t_\text{A}}$$
$$C_{\text{A},5}=\text{PK}_{\text{B},1}^{t_\text{A}}$$
$$C_{\text{A},6}=\text{PK}_{\text{B},1}^{r_\text{A}}$$
$$C_{\text{A},7}=t_\text{A}+r_\text{A}H_4(C_{\text{A},1},C_{\text{A},5},C_{\text{A},6})$$
$$C_{\text{A},8}=r_\text{A}\text{SK}_{\text{A},1}+H_5(w_\text{A});$$

(*c*)将生成的医疗密文 $C_\text{A}=(C_{\text{A},1},C_{\text{A},2},C_{\text{A},3},C_{\text{A},4},C_{\text{A},5},C_{\text{A},6},C_{\text{A},7},C_{\text{A},8})$ 上传到云服务器存储.

给定数据用户的公钥 PK_B 与私钥 SK_B,数据用户执行如下操作对希望获取的医疗数据 m_B 加密:

(*a*)随机选择 $t_\text{B}\in Z_q^*$ 和 $w_\text{B}\in\{0,1\}^{l_1}$,并计算出 $r_\text{B}=H_2(m_\text{B},w_\text{B})$;

(*b*)计算 $C_{\text{B},1}=H_3(g^{r_\text{B}})\oplus(m_\text{B}\|w_\text{B})$,$C_{\text{B},2}=t_\text{B}H_7(m_\text{B})\oplus H_6(g^{r_\text{B}})$,$C_{\text{B},3}=\text{PK}_{\text{B},2}^{r_\text{B}}$ 与 $C_{\text{B},4}=g^{t_\text{B}}$;

(*c*)将生成的兴趣密文 $C_\text{B}=(C_{\text{B},1},C_{\text{B},2},C_{\text{B},3},C_{\text{B},4})$ 上传到云服务器.

(4)密文等值测试

数据拥有者与数据用户分别生成用于密文等值测试的陷门并上传到区块链平台,智能合约按照预定义

的规则，利用测试陷门对从云端下载双方密文执行如下等值测试操作：

①用户计算测试陷门 $\mathrm{td}_i=H_6\left(C_{i,3}^{1/\mathrm{SK}_{i,2}}\right)$ 并上传到区块链平台；

②智能合约根据双方密文 C_A，C_B 与测试陷门 td_A，td_B 计算 $X_\mathrm{A}=C_{\mathrm{A},2}\oplus\mathrm{td}_\mathrm{A}$ 与 $X_\mathrm{B}=C_{\mathrm{B},2}\oplus\mathrm{td}_\mathrm{B}$；

③智能合约检查 $C_{\mathrm{A},4}^{X_\mathrm{B}}=C_{\mathrm{B},4}^{X_\mathrm{A}}$ 是否成立，成立则向云服务器输出等值测试结果为“1”，否则返回“0”.

(5)医疗数据解密及验证

若云服务器接收到测试结果为“1”，代表云端存在与医生的兴趣相匹配的医疗数据，云服务器将相应的医疗密文发送给雾节点进行完整性验证. 验证通过后雾节点将密文发送给数据用户，由数据用户对医疗密文进行解密并验证数据来源. 雾节点与数据用户具体操作如下：

①雾节点检查 $\mathrm{PK}_{\mathrm{B},1}^{C_{\mathrm{A},7}}=C_{\mathrm{A},6}^{H_4(C_{\mathrm{A},1},C_{\mathrm{A},5},C_{\mathrm{A},6})}C_{\mathrm{A},5}$ 是否成立，若成立则将 C_A 发送给数据用户，否则返回“⊥”；

②数据用户计算 $m'_\mathrm{A}\|w'_\mathrm{A}=C_{\mathrm{A},1}\oplus H_3\left(C_{\mathrm{A},6}^{1/\mathrm{SK}_{\mathrm{B},1}}\right)$ 与 $r'=H_2(m'_\mathrm{A},w'_\mathrm{A})$；

③数据用户检查 $g^{H_5(w'_\mathrm{A})}=g^{C_{\mathrm{A},8}}\mathrm{PK}_{\mathrm{A},1}^{-r'}$ 是否成立，若成立则接受并输出医疗数据 m'_A，否则返回“⊥”.

4.2 智能合约算法设计

当数据拥有者与数据用户的测试陷门被上传到区块链平台后，智能合约会按照预定义的规则对双方的密文执行等值测试操作. 定义算法1与算法2来完成等值测试操作.

算法1中给出了3种用于存储用户相关信息的结构体的定义，其中Ciphertext_Tuple定义了密文的存储格式；User_Info用于存储用户的身份标识和公钥；Test_Tuple用于存储等值测试所需的用户信息，包括用户身份标识、测试密文和测试陷门. 算法2中定义了3个用于执行等值测试操作的接口，其中接口Query通过索引值来查询存储在区块链上的数据；接口Update负责更新用户密文与用户陷门；接口Test负责执行密文等值测试操作.

算法1 数据结构定义

输入: 数据结构定义方法
输出: Ciphertext_Tuple、User_Info与Test_Tuple
Structure Ciphertext_Tuple{
$C_1,C_2,C_3,C_4,C_5,C_6,C_7,C_8$ string}
Structure User_Info{
ID string
PK string}
Structure Test_Tuple{
Role string
Cipher Ciphertext_Tuple
Trapdoor string}

算法2 密文等值测试

输入: 用户的身份标识、测试陷门与密文
输出: 密文等值测试结果
Query(key string):
Return M[key] or ⊥.
%M是形如(key, value)的映射
Update(id, data string, counter, flag int):
Retrieve the Test_Tuple $x=M$[id||counter] of the user by (id, counter) from M.
IF flag == 0 THEN
  Convert the string data to the Ciphertext_Tuple structure cdata.
  Set x.Cipher = cdata.
ELSE
  Set x.Trapdoor = data.
END IF
Set M[id||counter]=x.
Test(id_i, id_j string, td_i, td_j tring):
Retrieve the Test_Tuple $x_i=M[\mathrm{id}_i]$ of the data owner i and the Test_Tuple $x_j=M[\mathrm{id}_j]$ of the data user j from the map M.
IF $x_i==\perp\|x_j==\perp$ THEN
  return null
END IF
Parse x_i.Cipher into $(C_{i,1},C_{i,2},C_{i,3},C_{i,4},C_{i,5},C_{i,6},C_{i,7},C_{i,8})$
Parse x_j.Cipher into $(C_{j,1},C_{j,2},C_{j,3},C_{j,4},C_{j,5},C_{j,6},C_{j,7},C_{j,8})$
Computes $X_i=C_{i,2}\oplus\mathrm{td}_i$
Computes $X_j=C_{j,2}\oplus\mathrm{td}_j$
IF $(C_{i,4})^{X_j}=(C_{j,4})^{X_i}$ THEN
  return 1
END IF

5 方案分析与安全性证明

5.1 正确性分析

5.1.1 密文解密等式的正确性

数据用户通过计算 $m'_\mathrm{A}\|w'_\mathrm{A}=C_{\mathrm{A},1}\oplus H_3\left(C_{\mathrm{A},6}^{1/\mathrm{SK}_{\mathrm{B},1}}\right)$ 对密文进行解密，其中 $\mathrm{SK}_{\mathrm{B},1}$ 是数据用户的私钥. 由于 $\mathrm{PK}_{\mathrm{B},1}=g^{\mathrm{SK}_{\mathrm{B},1}}$，从而有

$$\begin{aligned}m'_\mathrm{A}\|w'_\mathrm{A}&=C_{\mathrm{A},1}\oplus H_3\left(C_{\mathrm{A},6}^{1/\mathrm{SK}_{\mathrm{B},1}}\right)\\&=H_3(g^{r_\mathrm{A}})\oplus(m_\mathrm{A}\|w_\mathrm{A})\oplus H_3\left(\mathrm{PK}_{\mathrm{B},1}^{r_\mathrm{A}/\mathrm{SK}_{\mathrm{B},1}}\right)\\&=m_\mathrm{A}\|w_\mathrm{A}\end{aligned}$$

即 $m'_\mathrm{A}\|w'_\mathrm{A}=m_\mathrm{A}\|w_\mathrm{A}$. 因此，本文所提新方案满足密文解密等式的正确性.

5.1.2 签名验证等式的正确性

数据用户通过检查等式 $g^{H_5(w'_\mathrm{A})}=g^{C_{\mathrm{A},8}}\mathrm{PK}_{\mathrm{A},1}^{-r'}$ 是否成立以验证签名的合法性，其中 $r'=H_2(m'_\mathrm{A},w'_\mathrm{A})$，由于 $m'_\mathrm{A}\|w'_\mathrm{A}=m_\mathrm{A}\|w_\mathrm{A}$，则有

$$r'=H_2(m'_\mathrm{A},w'_\mathrm{A})=H_2(m_\mathrm{A}\|w_\mathrm{A})=r_\mathrm{A}$$

即 $r'=r_\mathrm{A}$，结合数据拥有者的公钥 $\mathrm{PK}_{\mathrm{A},1}=g^{\mathrm{SK}_{\mathrm{A},1}}$，从而有

$$g^{C_{A,8}}\mathrm{PK}_{A,1}^{-r'}=g^{r_A\mathrm{SK}_{A,1}+H_5(w_A)}g^{-r'\mathrm{SK}_{A,1}}$$
$$=g^{H_5(w_A)}$$
$$=g^{H_5(w'_A)}$$

因此,本文方案满足签名验证等式的正确性.

5.1.3 等值测试结果的正确性

智能合约通过检查等式 $C_{A,4}^{X_B}=C_{B,4}^{X_A}$ 是否成立以判断双方密文是否对应同一明文,等式中 X_A 与 X_B 的计算结果如下:

$$X_A=C_{A,2}\oplus \mathrm{td}_A$$
$$=t_A H_7(m_A)\oplus H_6(g^{r_A})\oplus H_6\left(\mathrm{PK}_{A,2}^{r_A/\mathrm{SK}_{A,2}}\right)$$
$$=t_A H_7(m_A)$$
$$X_B=C_{B,2}\oplus \mathrm{td}_B$$
$$=t_B H_7(m_B)\oplus H_6(g^{r_B})\oplus H_6\left(\mathrm{PK}_{B,2}^{r_B/\mathrm{SK}_{B,2}}\right)$$
$$=t_B H_7(m_B)$$

假设 $m_A=m_B$,则 $H_7(m_A)=H_7(m_B)$,从而有

$$C_{A,4}^{X_B}=g^{t_A t_B H_7(m_B)}=g^{t_B t_A H_7(m_A)}=C_{B,4}^{X_A}$$

即 $C_{A,4}^{X_B}=C_{B,4}^{X_A}$. 由智能合约输出的密文等值测试结果可知,当 $C_{A,4}^{X_B}=C_{B,4}^{X_A}$ 成立时,代表 $m_A=m_B$,与假设相符. 因此,本文方案满足等值测试结果的正确性.

5.2 安全性分析

5.2.1 等值测试结果的可信性分析

在联盟区块链平台中,一旦密文等值测试的交易被发布,智能合约就会按照预定义的规则执行等值测试操作并将测试结果作为合约状态值公开记录在联盟区块链中,参与该联盟链的所有人都可以对测试结果进行验证. 因此本文方案满足等值测试结果的可信性.

5.2.2 外包计算的安全性分析

雾节点通过检查 $\mathrm{PK}_{B,1}^{C_{A,7}}=C_{A,6}^{H_4(C_{A,1},C_{A,5},C_{A,6})}C_{A,5}$ 是否成立来验证从云服务器下载的医疗密文的完整性,其中 $\mathrm{PK}_{B,1}$ 是公开的数据用户公钥,$C_{A,1}$,$C_{A,5}$,$C_{A,6}$ 与 $C_{A,7}$ 是加密数据,雾节点无法从这些数据中推算出其他相关信息. 因此,本文方案保证雾节点在对外包数据执行计算的过程中无法获取医疗数据明文的相关信息.

5.3 安全性证明

本文所提方案满足面对I类和II类敌手时医疗数据的机密性、完整性与数据拥有者签名的存在不可伪造性,同时满足面对III类和IV类敌手选择密文攻击下的单向性(One-Way against Chosen Ciphertext Attack, OW-CCA). 机密性与不可伪造性的证明可分别参考文献[25,26]方案. 以下通过定理1和定理2证明本文方案在面对III类和IV类敌手时满足OW-CCA安全.

定理1 假设CDH问题困难,则本文方案在随机预言模型下对III类敌手是OW-CCA安全的.

证明 假设 $\mathcal{C}$ 是拥有解决CDH问题能力的人,以III类敌手 $\mathcal{A}_3$ 为子程序充当以下游戏中的挑战者. 若敌手 $\mathcal{A}_3$ 拥有以不可忽略的优势在概率多项式时间内在此游戏中获胜的能力,则 $\mathcal{C}$ 能够在概率多项式时间内解决CDH问题.

初始化阶段:CDH问题的输入为 (g,g^a,g^b),其中 $a,b\in Z_p^*$,$\mathcal{C}$ 的目标是计算出CDH问题的解 g^{ab}. $\mathcal{C}$ 初始化系统,生成系统参数 $\mathrm{params}=\{p,q,g,G,P_{\mathrm{pub}},H_1,H_2,H_3,H_4,H_5,H_6,H_7\}$ 与主密钥 s,$\mathcal{C}$ 将 s 秘密保存并发送 params 给 $\mathcal{A}_3$.

询问阶段:为了响应 $\mathcal{A}_3$ 的询问,$\mathcal{C}$ 维持列表 $L_1,L_2,L_3,L_4,L_5,L_6,L_7,L_D,L_{\mathrm{PK}},L_{\mathrm{td}},L_S$ 和 L_V 分别用于跟踪 $\mathcal{A}_3$ 对预言机 $H_1,H_2,H_3,H_4,H_5,H_6,H_7$ 部分私钥提取、密钥提取、测试陷门、签名和验证签名询问,开始每个列表都为空.

(1)H_1 哈希询问:当 $\mathcal{C}$ 收到 $\mathcal{A}_3$ 对 $H_1(\mathrm{ID}_i,u_i)$ 的查询后,若 L_1 中已有 (ID_i,u_i,e_i),则返回 e_i 给 $\mathcal{A}_3$;否则,$\mathcal{C}$ 选取 $e_i\in Z_q^*$,将 (ID_i,u_i,e_i) 加入到 L_1 中并输出 e_i.

(2)H_2 哈希询问:当 $\mathcal{C}$ 收到 $\mathcal{A}_3$ 对 $H_2(m_i,w_i)$ 的查询后,若 L_2 中已有 (m_i,w_i,r_i),则返回 r_i 给 $\mathcal{A}_3$;否则,$\mathcal{C}$ 选取 $r_i\in Z_q^*$,将 (m_i,w_i,r_i) 加入到 L_2 中并输出 r_i.

(3)H_3 哈希询问:当 $\mathcal{C}$ 收到 $\mathcal{A}_3$ 对 $H_3(R_i)$ 的查询后,若 L_3 中已有 $(R_i,H_3(R_i))$,则返回 $H_3(R_i)$ 给 $\mathcal{A}_3$;否则,$\mathcal{C}$ 选取 $H_3(R_i)\in\{0,1\}^{l_0+l_1}$,将 $(R_i,H_3(R_i))$ 加入到 L_3 中并输出 $H_3(R_i)$.

(4)H_4 哈希询问:当 $\mathcal{C}$ 收到 $\mathcal{A}_3$ 对 $H_4(C_{A,1},C_{A,5},C_{A,6})$ 的查询后,若 L_4 中已经有 $(C_{A,1},C_{A,5},C_{A,6},H_4(C_{A,1},C_{A,5},C_{A,6}))$,则返回 $H_4(C_{A,1},C_{A,5},C_{A,6})$ 给 $\mathcal{A}_3$;否则,$\mathcal{C}$ 随机选取 $H_4(C_{A,1},C_{A,5},C_{A,6})\in Z_q^*$,将 $(C_{A,1},C_{A,5},C_{A,6},H_4(C_{A,1},C_{A,5},C_{A,6}))$ 加入到 L_4 中并输出 $H_4(C_{A,1},C_{A,5},C_{A,6})$.

(5)H_5 哈希询问:当 $\mathcal{C}$ 收到 $\mathcal{A}_3$ 对 $H_5(w_i)$ 的查询后,若 L_5 中已有 $(w_i,H_5(w_i))$,则返回 $H_5(w_i)$ 给 $\mathcal{A}_3$;否则,$\mathcal{C}$ 选取 $H_5(w_i)\in Z_q^*$,将 $(w_i,H_5(w_i))$ 加入到 L_5 中并输出 $H_5(w_i)$.

(6)H_6 哈希询问:当 $\mathcal{C}$ 收到 $\mathcal{A}_3$ 对 $H_6(R_i)$ 的查询后,若 L_6 中已有 $(R_i,H_6(R_i))$,则返回 $H_6(R_i)$ 给 $\mathcal{A}_3$;否则,$\mathcal{C}$ 选取 $H_6(R_i)\in\{0,1\}^{l_0}$,将 $(R_i,H_6(R_i))$ 加入到 L_6 中并输出 $H_6(R_i)$.

(7)H_7 哈希询问:当 $\mathcal{C}$ 收到 $\mathcal{A}_3$ 对 $H_7(m_i)$ 的查询后,若 L_7 中已有 $(m_i,H_7(m_i))$,则返回 $H_7(m_i)$ 给 $\mathcal{A}_3$;否则,$\mathcal{C}$ 选取 $H_7(m_i)\in\{0,1\}^{l_0}$,将 $(m_i,H_7(m_i))$ 加入到 L_7 中并输出 $H_7(m_i)$.

(8)公钥提取询问:$\mathcal{C}$ 收到 $\mathcal{A}_3$ 对 $\mathrm{PK}_{i,1}$ 的询问后,若 L_{PK} 中已有 $(\mathrm{ID}_i,\mathrm{PK}_{i,1},\mathrm{SK}_{i,1})$,则返回 $\mathrm{PK}_{i,1}$ 给 $\mathcal{A}_3$;否则,$\mathcal{C}$

选取$c\in[1,q]$并执行如下操作：

（a）若$i=c$，$\mathcal{C}$随机选择$\mathrm{SK}_{i,1}\in Z_q^*$，计算出$\mathrm{PK}_{i,1}=(g^{1/a})^{\mathrm{SK}_{i,1}}$，将$(\mathrm{ID}_i,\mathrm{PK}_{i,1},\mathrm{SK}_{i,1})$加入到列表$L_{\mathrm{PK}}$中并输出$\mathrm{PK}_{i,1}$；

（b）若$i\neq c$，$\mathcal{C}$随机选择$\mathrm{SK}_{i,1}\in Z_q^*$，计算出$\mathrm{PK}_{i,1}=g^{\mathrm{SK}_{i,1}}$，将$(\mathrm{ID}_i,\mathrm{PK}_{i,1},\mathrm{SK}_{i,1})$加入到列表$L_{\mathrm{PK}}$中并输出$\mathrm{PK}_{i,1}$.

（9）部分私钥提取询问：当$\mathcal{C}$收到$\mathcal{A}_3$对$D_{i,1}$的查询后，若$(\mathrm{ID}_i,D_{i,1},x_i)$已经在$L_D$中，则返回$D_{i,1}$给$\mathcal{A}_3$；否则，$\mathcal{C}$执行以下操作：

（a）若$\mathcal{A}_3$在某个时刻能够替换ID_i的公钥，但无法请求相应的部分私钥，则$\mathcal{C}$操作如下：若$i=c$，$\mathcal{C}$输出“$\perp$”并终止模拟；若$i\neq c$，$\mathcal{C}$首先从列表L_{PK}中恢复对应的$(\mathrm{ID}_i,\mathrm{PK}_{i,1},\mathrm{SK}_{i,1})$，随机选取$x_i\in Z_q^*$，计算$D_{i,1}=x_i-\mathrm{SK}_{i,1}$，最后$\mathcal{C}$将$(\mathrm{ID}_i,D_{i,1},x_i)$加入到列表$L_D$中并输出$D_{i,1}$.

（b）若$\mathcal{A}_3$可以在某个时刻询问ID_i的部分私钥，但不能对相应公钥进行替换，则$\mathcal{C}$执行部分私钥提取算法生成$D_{i,1}$发送给$\mathcal{A}_3$.

（10）私钥提取询问：当$\mathcal{C}$收到$\mathcal{A}_3$对$\mathrm{SK}_{i,1}$的查询后，若$i=c$，$\mathcal{C}$输出“$\perp$”后终止模拟；若$i\neq c$，$\mathcal{C}$首先从列表L_{PK}中恢复对应的$(\mathrm{ID}_i,\mathrm{PK}_{i,1},\mathrm{SK}_{i,1})$并返回相应的$\mathrm{SK}_{i,1}$给$\mathcal{A}_3$.

（11）公钥替换询问：当$\mathcal{C}$收到$\mathcal{A}_3$对$(\mathrm{ID}_i,\mathrm{PK}_{i,1})$的查询后，若$i=c$，且$\mathcal{A}_3$可以在某个时刻询问$\mathrm{ID}_i$对应的$D_{i,1}$，但不能替换对应的$\mathrm{PK}_{i,1}$，则$\mathcal{C}$输出“$\perp$”后终止模拟；否则，$\mathcal{C}$设置$\mathrm{PK}_{i,1}=\mathrm{PK}_{c,1}$，将$(\mathrm{ID}_i,\mathrm{PK}_{i,1},\mathrm{SK}_{i,1})$加入到列表$L_{\mathrm{PK}}$中.

（12）解密询问：当$\mathcal{A}_3$以$(\mathrm{PK}_{i,1},C_i)$作为输入发起询问时，若$i\neq c$，则$\mathcal{C}$执行解密算法输出C_i对应的明文m_i并返回给$\mathcal{A}_3$；否则，$\mathcal{C}$检查等式$\mathrm{PK}_{\mathrm{B},1}^{C_{i,7}}=C_{i,5}\cdot C_{i,6}^{H_4(C_{i,1},C_{i,5},C_{i,6})}$是否成立，若不成立则返回“$\perp$”，否则返回$C_i=(C_{i,1},C_{i,6})$.

（13）测试陷门询问：当$\mathcal{C}$收到$\mathcal{A}_3$对消息σ_i对应的td_i询问后，若$i=c$，则$\mathcal{C}$输出“$\perp$”后终止模拟；否则，$\mathcal{C}$从列表L_{PK}中取出$(\mathrm{ID}_i,\mathrm{PK}_{i,1},\mathrm{SK}_{i,1})$，计算$\mathrm{td}_i=H_6\left(C_{i,3}^{1/\mathrm{SK}_{i,2}}\right)$并返回$\mathrm{td}_i$.

挑战阶段：$\mathcal{A}_3$选择两个相等长度的消息m_0和m_1与希望挑战的身份ID_i^*，其中ID_i^*是没有执行过部分私钥提取询问或私钥提取询问的用户身份，$\mathcal{C}$执行以下操作.

（1）$\mathcal{C}$随机选择$\gamma^*\in Z_q^*$与$C_{i,7}^*\in Z_q^*$，设置$H_4(C_{\mathrm{A},1}^*,C_{\mathrm{A},5}^*,C_{\mathrm{A},6}^*)=\gamma^*$并计算

$$\begin{aligned}C_{i,5}^*&=(g^b)^{-\gamma^*\mathrm{SK}_{i,1}^*}(g^{1/a})^{\mathrm{SK}_{i,1}^*C_{i,7}^*}\\&=(g^{\mathrm{SK}_{i,1}^*/a})^{C_{i,7}^*-ab\gamma^*}\\&=(\mathrm{PK}_{i,1}^*)^{C_{i,7}^*-ab\gamma^*}\\C_{i,6}^*&=(g^b)^{\mathrm{SK}_{i,1}^*}\\&=(g^{\mathrm{SK}_{i,1}^*/a})^{ab}\\&=(\mathrm{PK}_{i,1}^*)^{ab}\end{aligned}$$

（2）$\mathcal{C}$选择$\theta\in\{0,1\}$与$w^*\in\{0,1\}^{l_1}$，其中θ与w^*满足$H_2(m_\theta,w^*)=ab$，随机选择$C_{i,1}^*\in\{0,1\}^{l_0+l_1}$，其中$C_{i,1}^*=H_3(g^{ab})\oplus(m_\theta,w^*)$.

（3）$\mathcal{C}$设置$t^*=C_{i,7}^*-ab\gamma^*$，$r^*=ab$，计算

$$\begin{aligned}C_{i,7}^*&=(C_{i,7}^*-ab\gamma^*)+ab\gamma^*\\&=t^*+r^*H_4(C_{\mathrm{A},1}^*,C_{\mathrm{A},5}^*,C_{\mathrm{A},6}^*)\end{aligned}$$

并返回$C_i^*=(C_{i,1}^*,C_{i,5}^*,C_{i,6}^*,C_{i,7}^*)$给$\mathcal{A}_3$.

猜测阶段：$\mathcal{A}_3$输出一个对θ的猜测$\theta'\in\{0,1\}$，如果$\theta'=\theta$，则$\mathcal{A}_3$在以上游戏中获胜. $\mathcal{C}$在列表L_3中随机选取一个元组$(R_i,H_3(R_i))$并以$R_i=g^{ab}$作为CDH困难问题的解，这与目前公认的CDH问题的难解性相矛盾. 因此，本文方案在面对III类敌手时，满足选择OW-CCA安全.

证毕

定理2 假设CDH问题困难，则本文方案在随机预言模型下对Ⅳ类敌手是OW-CCA安全的.

证明 假设$\mathcal{C}$是拥有解决CDH问题能力的人，以IV类敌手$\mathcal{A}_4$为子程序充当以下游戏中的挑战者. 若敌手$\mathcal{A}_4$拥有以不可忽略的优势在概率多项式时间内在此游戏中获胜的能力，则$\mathcal{C}$能够在概率多项式时间内解决CDH困难问题.

初始化阶段：CDH问题的输入为(g,g^a,g^b)，其中$a,b\in Z_p^*$，$\mathcal{C}$的目标是给出CDH问题的解g^{ab}. $\mathcal{C}$对系统初始化生成s和$\mathrm{params}=\{p,q,g,G,P_{\mathrm{pub}},H_1,H_2,H_3,H_4,H_5,H_6,H_7\}$，将$s$和params一并发送给$\mathcal{A}_4$.

询问阶段：$\mathcal{A}_4$可以执行证明定理1时定义的游戏中除了“部分私钥提取询问”和“用户公钥替换”之外的所有操作.

挑战阶段：与定理1的证明过程类似.

猜测阶段：$\mathcal{A}_4$输出一个$\theta'\in\{0,1\}$作为对θ的猜测，如果$\theta'=\theta$，则$\mathcal{A}_4$在以上游戏中获胜. $\mathcal{C}$在列表L_3中随机选取一个元组$(R_i,H_3(R_i))$并以$R_i=g^{ab}$作为CDH困难问题的解，这与目前公认的CDH问题的难解性相矛盾. 因此本文方案在面对IV类敌手时，满足选择OW-CCA安全.

证毕

6　性能分析

6.1　特性分析

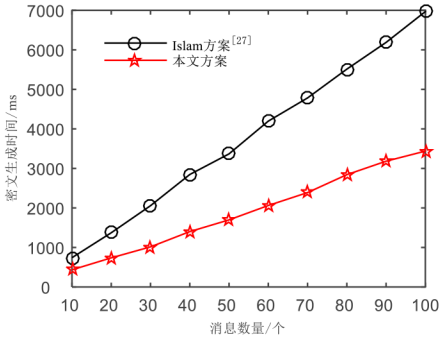
将本文提出的新方案与已有的WBAN加密方案[11,14,16]在特性方面进行比较,对比结果如表1所示.与文献[11,14]方案相比,本文方案利用等值测试实现了对WBAN云端医疗密文的检索,同时利用区块链技术消除了测试操作对可信云服务器的依赖. 与文献[11,16]方案相比,所提新方案引入无证书签密技术,保证了无线体域网中医疗数据的机密性与可认证性,消除了密钥管理问题. 文献[14,16]方案不支持外包计算,本文方案将对医疗密文的完整性验证计算外包给雾节点执行,降低了无线体域网中数据用户解密时的计算开销.

表1　特性对比

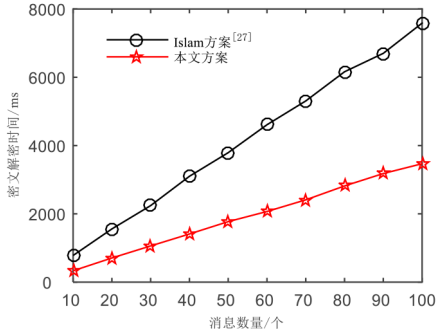
方案	等值测试	去中心化	无证书体制	签密	外包计算
Cagalaban方案[11]	×	×	×	×	√
Omala方案[14]	×	×	√	√	×
Ramadan方案[16]	√	×	×	×	×
本文方案	√	√	√	√	√

6.2　效率分析

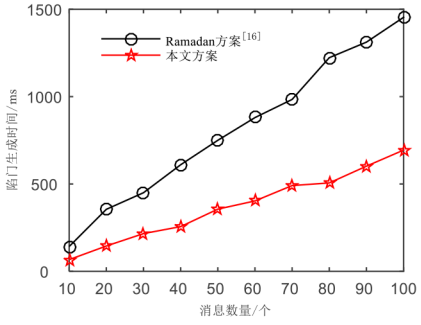
将本文提出的新方案在时间开销方面与文献[16,27]方案进行比较,设置消息的数量为10~100之间,使用i7-8750h 2.20 GHz处理器,8 GB内存和Win10操作系统在VC6.0环境下,调用基于配对的密码学(Pairing-Based Cryptography,PBC)库分别对3个方案进行了仿真模拟,对比结果如图2所示.



(a)　密文生成时间对比



(b)　密文解密时间对比



(c)　陷门生成时间对比

图2　时间开销对比

由图2(a)和图2(b)可知,当消息数量为10时,本文方案在密文生成和解密阶段的时间开销分别比文献[27]方案降低了41.43%和57.44%;同时,随着消息数量的增多,本文所提新方案在计算开销方面的优势更加显著. 当设置消息的数量为100时,本文方案比文献[27]方案密文生成阶段的时间开销降低了50.67%,在解密阶段的时间开销降低了54.29%. 由图2(c)可知,当消息数量为10时,本文方案在陷门生成阶段的时间成本比文献[16]方案减少了52.82%;消息数量为100时,新方案的陷门生成阶段时间开销比文献[16]方案减少了52.27%. 通过上述分析能够看出,新方案在加密、解密与陷门生成阶段的计算开销与相关方案相比都有所降低.

6.3　区块链成本分析

6.3.1　智能合约成本分析

本文方案利用部署在联盟区块链上的智能合约执行密文等值测试操作,保证了测试结果的可信性. 为评估智能合约在执行等值测试操作时的成本,本文采用Solidity编程语言在Remix平台上对智能合约进行编译,并将智能合约代码部署在了以太坊测试网络Rinkeby上. 智能合约在执行命令时产生的消耗以Gas作为单位,验证交易所需的计算资源以Ether作为单位. 本文方案涉及的所有交易及成本测试结果均可以通过智能合约地址"0xa626bf9a5d38837e9Bca3b32a6265cFc10ef69F3"在以太坊提供的官方网站https://rinkeby.etherscan.io/中查看,设置密文长度为64 bit,智能合约成本测试结果如表2所示.

6.3.2　引入区块链前后效率对比分析

将本文的智能合约利用Solidity编程语言在Remix-IDE集成开发环境下编译并运行,利用Remix-IDE的Solidity单元测试模块(Solidity Unit Testing)统计执行智能

表2 智能合约成本

函数	消耗成本/Gas	实际成本/Ether	成本/美元
Query	196 762	0.000 590 286	0.159 377 22
Update	167 233	0.000 501 699	0.135 458 73
Test	292 250	0.000 876 750	0.236 722 50

合约所消耗的时间. 在统计引入区块链后智能合约执行等值测试操作所消耗时间的过程中,设置挖矿时间为0以消除其他时间对测试结果的影响. 同时对比了本文方案在基于区块链与基于传统云服务器时执行相同次数等值测试所产生的时间开销,在实验过程中设置双方进行等值测试的密文长度都为64 bit,对比结果如图3所示.

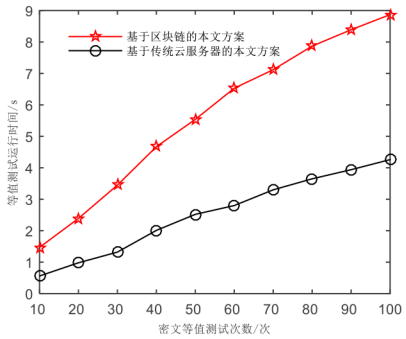


图3 引入区块链前后时间开销对比

由图3可以看出,基于区块链的本文方案执行等值测试的时间相比于基于传统云服务器有所增加,但随着等值测试次数的增多,测试时间的增长率逐步降低. 基于区块链的本文方案相比于传统云服务器下的本文方案最显著的区别就是实现了去中心化的密文检索方式,这意味着链上的每一个节点都需要对分布式账本的数据进行计算与存储,导致区块链的工作效率低于传统的中心化云服务器. 针对区块链"去中心化"这一固有特性导致其工作效率较低的问题,已有学者提出了一些相应的解决方案[28,29]. 尽管区块链执行等值测试的时间开销略高于传统云服务器,但区块链技术的引入消除了新方案对可信或半可信第三方的依赖. 链上节点的分布越呈分散趋势,单凭一个节点篡改链上等值测试结果的可能性就越小,因此相比于传统的中心化云服务器,基于区块链的等值测试结果更加安全可靠.

7 结束语

无线体域网技术具有低时延与高灵活性的特点,在医疗数据监控等领域发挥了重要的作用. 针对WBAN加密方案中密文检索困难与依赖可信云服务器等问题,本文提出了一种基于区块链的无线体域网无证书密文等值测试签密方案. 基于无证书签密技术对医疗数据进行签密,确保了医疗数据的机密性与可认证性. 利用部署在区块链中的智能合约执行测试操作,消除了对可信云服务器的依赖. 采用雾节点执行解密时的部分计算,降低了WBAN用户执行解密操作时的计算开销. 通过本文方案与现有WBAN方案的对比分析可知,本文提出的新方案支持更多的安全属性,并具有较低的计算开销. 在未来的工作中,将尝试设计抗量子计算攻击的无证书等值测试方案.

参考文献

[1] JABEEN T, ASHRAF H, ULLAH A. A survey on healthcare data security in wireless body area networks[J]. Journal of Ambient Intelligence and Humanized Computing, 2021, 12(10): 9841-9854.

[2] 宫继兵, 王睿, 崔莉. 体域网BSN的研究进展及面临的挑战[J]. 计算机研究与发展, 2010, 47(5): 737-753.
GONG J B, WANG R, CUI L. Research advances and challenges of body sensor network (BSN) [J]. Journal of Computer Research and Development, 2010, 47(5): 737-753. (in Chinese)

[3] MYKLETUN E, GIRAO J, WESTHOFF D. Public key based cryptoschemes for data concealment in wireless sensor networks[C]//2006 IEEE International Conference on Communications. Istanbul: IEEE, 2006: 2288-2295.

[4] 张文娟, 吴聪, 余梅生. 利用多值和模糊属性的云辅助WBAN数据加密算法[J]. 计算机应用研究, 2016, 33(5): 1537-1541.
ZHANG W J, WU C, YU M S. Data encryption algorithm of cloud-assisted WBAN using multi-valued and ambiguous attribute[J]. Application Research of Computers, 2016, 33(5): 1537-1541. (in Chinese)

[5] MANA M, FEHAM M, BENSABER B A. Trust key management scheme for wireless body area networks[J]. International Journal of Network Security, 2011, 12(2): 75-83.

[6] TRIPATHY S. Tin-key: Effective key-establishment for wireless sensor networks[C]//2010 10th IEEE International Conference on Computer and Information Technology. Bradford: IEEE, 2010: 916-921.

[7] 张维纬, 张育钊, 黄焯, 等. 支持安全外包计算的无线体域网数据共享方案[J]. 通信学报, 2017, 38(4): 64-75.
ZHANG W W, ZHANG Y Z, HUANG Z, et al. Data sharing scheme supporting secure outsourced computation in wireless body area network[J]. Journal on Communications, 2017, 38(4): 64-75. (in Chinese)

[8] 高改梅, 彭新光, 靳黎忠. 面向云辅助WBAN的无证书公

共审计方案[J]. 计算机工程与设计, 2019, 40(2): 306-311.
GAO G M, PENG X G, JIN L Z. Certificateless public auditing scheme for cloud-assisted WBAN[J]. Computer Engineering and Design, 2019, 40(2): 306-311. (in Chinese)

[9] MUKHTAR T, CHAUDHARY S. Energy efficient cluster formation and secure data outsourcing using TEOSCC and ECDH-IBT technique in WBAN[C]//2016 International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET). Chennai: IEEE, 2016: 596-602.

[10] ZHENG Y L. Digital signcryption or how to achieve cost (signature & encryption) << cost(signature) + cost (encryption)[C]//Proceedings of the 17th Annual International Cryptology Conference on Advances in Cryptology. Berlin: Springer, 1997: 165-179.

[11] CAGALABAN G, KIM S. Towards a secure patient information access control in ubiquitous healthcare systems using identity-based signcryption[C]//Proceedings of the 13th International Conference on Advanced Communication Technology. Gangwon: IEEE, 2011: 863-867.

[12] LI F G, HONG J J. Efficient certificateless access control for wireless body area networks[J]. IEEE Sensors Journal, 2016, 16(13): 5389-5396.

[13] ULLAH I, ZEADALLY S, AMIN N U, et al. Lightweight and provable secure cross-domain access control scheme for Internet of Things (IoT) based wireless body area networks (WBAN)[J]. Microprocessors and Microsystems, 2021, 81: 103477.

[14] OMALA A A, MBANDU A S, MUTIRIA K D, et al. Provably secure heterogeneous access control scheme for wireless body area network[J]. Journal of Medical Systems, 2018, 42(6): 108.

[15] ZHANG J. Public key encryption with keyword search in wireless body area network[J]. Modern Computer, 2017, 12(1): 64-73.

[16] RAMADAN M, LIAO Y J, LI F G, et al. IBEET-RSA: Identity-based encryption with equality test over RSA for wireless body area networks[J]. Mobile Networks and Applications, 2020, 25(1): 223-233.

[17] XIONG H, HOU Y Z, HUANG X, et al. Heterogeneous signcryption scheme from IBC to PKI with equality test for WBANs[J]. IEEE Systems Journal, 2021, DOI: 10.1109/JSYST.2020.3048972.

[18] BAO F, DENG R H, ZHU H F. Variations of Diffie-Hellman problem[C]//International Conference on Information and Communications Security. Berlin: Springer, 2003: 301-312.

[19] NAKAMOTO S. Bitcoin: A Peer-to-Peer Electronic Cash System[EB/OL]. (2009)[2021]. http://bitcoin.org/bitcoin.pdf.

[20] 朱健, 胡凯, 张伯钧. 智能合约的形式化验证方法研究综述[J]. 电子学报, 2021, 49(4): 792-804.
ZHU J, HU K, ZHANG B J. Review on formal verification of smart contract[J]. Acta Electronica Sinica, 2021, 49(4): 792-804. (in Chinese)

[21] CHEN B W, HE D B, KUMAR N, et al. A blockchain-based proxy re-encryption with equality test for vehicular communication systems[J]. IEEE Transactions on Network Science and Engineering, 2021, 8(3): 2048-2059.

[22] CHEN B W, WU L B, WANG H Q, et al. A blockchain-based searchable public-key encryption with forward and backward privacy for cloud-assisted vehicular social networks[J]. IEEE Transactions on Vehicular Technology, 2020, 69(6): 5813-5825.

[23] BONOMI F, MILITO R, ZHU J, et al. Fog computing and its role in the Internet of Things[C]//Proceedings of the First Edition of the MCC Workshop on Mobile Cloud Computing. New York: ACM, 2012: 13-16.

[24] QU H P, YAN Z, LIN X J, et al. Certificateless public key encryption with equality test[J]. Information Sciences, 2018, 462: 76-92.

[25] WANG L L, CHEN K F, MAO X P, et al. Efficient and provably-secure certificateless proxy re-encryption scheme for secure cloud data sharing[J]. Journal of Shanghai Jiaotong University (Science), 2014, 19(4): 398-405.

[26] 张艳艳, 王亮亮. 新型的基于DLP的无证书签名方案[J]. 计算机工程与应用, 2011, 47(12): 62-64.
ZHANG Y Y, WANG L L. New DLP-based certificateless signature scheme[J]. Computer Engineering and Applications, 2011, 47(12): 62-64. (in Chinese)

[27] HAFIZUL ISLAM S, LI F G. Leakage-free and provably secure certificateless signcryption scheme using bilinear pairings[J]. The Computer Journal, 2015, 58(10): 2636-2648.

[28] HU Q, YAN B W, HAN Y B, et al. An improved delegated proof of stake consensus algorithm[J]. Procedia Computer Science, 2021, 187: 341-346.

[29] ZHANG E. Truechain: Highly performant decentralized

public ledger work in progress[EB/OL]. (2018) [2021]. https://www.truechain.pro/Truechain.pdf.

作者简介

杨小东 男,1981年出生,甘肃甘谷人. 现为西北师范大学教授,硕士生导师. 主要研究方向为现代密码学和云计算安全.
E-mail: y200888@163.com

周 航 女,1996年出生,河北承德人. 现为西北师范大学计算机科学与工程学院硕士研究生. 主要研究方向为密文等值测试.
E-mail: 1019164488@qq.com

汪志松 男,1998年出生,江苏盐城人. 现为西北师范大学计算机科学与工程学院硕士研究生. 主要研究方向为代理重签名.
E-mail: 1216053764@qq.com

袁 森 女,1994年出生,河南新乡人. 现为西北师范大学计算机科学与工程学院硕士研究生. 主要研究方向为代理保护签名.
E-mail: 1819989234@qq.com

王彩芬 女,1963年出生,河北安国人. 现为深圳技术大学大数据与互联网学院教授,博士生导师. 主要研究方向为大数据安全.
E-mail: wangcaifen@sztu.edu.cn