计算机科学
COMPUTER SCIENCE

一种基于国密算法的区块链无证书加密机制

向宴颉，黄晓芳，向科峰，郑继楠

引用本文

向宴颉，黄晓芳，向科峰，郑继楠. 一种基于国密算法的区块链无证书加密机制[J]. 计算机科学，2024，51(8)：440-446.

XIANG Yanjie, HUANG Xiaofang, XIANG Kefeng, ZHENG Ji'nan. Blockchain Certificateless Encryption Mechanism Based on National Secret Algorithm [J]. Computer Science, 2024, 51(8): 440-446.

相似文章推荐（请使用火狐或 IE 浏览器查看文章）

Similar articles recommended (Please use Firefox or IE to view the article)

基于门限签名的时间轮换公证人组模型研究

Study on Time Rotation Notary Group Model Based on Threshold Signature

计算机科学, 2024, 51(8): 403-411. https://doi.org/10.11896/jsjkx.230500060

基于节点影响力的区块链匿名交易追踪方法

Blockchain Anonymous Transaction Tracking Method Based on Node Influence

计算机科学, 2024, 51(7): 422-429. https://doi.org/10.11896/jsjkx.230400177

元宇宙中区块链技术的应用、挑战和新策略

Application,Challenge and New Strategy of Block Chain Technology in Metaverse

计算机科学, 2024, 51(7): 373-379. https://doi.org/10.11896/jsjkx.230800072

面向物联网的分布式联邦学习加密验证研究

Study on Cryptographic Verification of Distributed Federated Learning for Internet of Things

计算机科学, 2024, 51(6A): 230700217-5. https://doi.org/10.11896/jsjkx.230700217

基于联盟链的细粒度安全访问控制机制

Fine Grained Security Access Control Mechanism Based on Blockchain

计算机科学, 2024, 51(6A): 230400080-7. https://doi.org/10.11896/jsjkx.230400080

计算机科学 COMPUTER SCIENCE
http://www.jsjkx.com
DOI:10.11896/jsjkx.230400203

一种基于国密算法的区块链无证书加密机制

向宴颉[1]　黄晓芳[1]　向科峰[2]　郑继楠[1]
1 西南科技大学计算机科学与技术学院　四川 绵阳 621010
2 西南科技大学制造科学与工程学院　四川 绵阳 621010
(yanjie0697@outlook.com)

摘　要　区块链因具有分布式、不可篡改和不变性的特点而广受关注,但区块链中使用的国际密码算法存在一定的后门安全隐患。现基于国密算法SM2,结合无证书密码机制,提出了一种基于区块链的无证书公钥加密(Certificateless Public Key Encryption,CL-PKE)方案。该方案不依赖双线性配对,降低了计算成本,消除了证书管理和密钥托管问题,并且利用区块链不可篡改和可追溯的优点,实现了用户对公钥的更新与撤销,同时能够对抗无证书机制中的Type-1和Type-2型敌手。该方案基于计算性Diffie-Hellman问题(Computational Diffie-Hellman Problem,CDHP)的困难性,在随机预言模型中被证明在自适应选择密文攻击下具有不可区分性。最后进行性能分析与测试,结果表明,与现有CL-PKE方案相比,该方案的计算效率至少提升11%。

关键词:无证书;SM2;区块链;随机预言模型
中图分类号　TP309

Blockchain Certificateless Encryption Mechanism Based on National Secret Algorithm

XIANG Yanjie[1],HUANG Xiaofang[1],XIANG Kefeng[2] and ZHENG Ji'nan[1]
1 School of Computer Science and Technology,Southwest University of Science and Technology,Mianyang,Sichuan 621010,China
2 School of Manufacturing Science and Engineering,Southwest University of Science and Technology,Mianyang,Sichuan 621010,China

Abstract　The blockchain has attracted widespread attention because of its distributed,non-tamperable and inherent immutability features. However,the international cryptographic algorithm used in the blockchain has certain backdoor security risks. Based on the national secret algorithm SM2,this paper proposes a blockchain-based certificateless public key encryption(CL-PKE)scheme,which combines with the certificateless cryptographic mechanism. The scheme does not use bilinear pairing,reduces computational cost,and eliminates certificate management and key escrow issues. At the same time,due to tamper proof and traceable of blockchain,the scheme realizes the user's updating and revocation of the public key,so as to fight against Type-1 and Type-2 adversaries in the certificateless mechanism. Based on the difficulty of the computational Diffie-Hellman problem(CDHP),it is proved that the scheme is indistinguishable under the adaptive chosen ciphertext attack in the random prediction model. Finally,after analysis and testing,compared with the existing CL-PKE schemes,the computational efficiency of this scheme is increased by at least 11%.

Keywords　Certificateless,SM2,Blockchain,Random oracle model

1　引言

区块链作为数字货币的核心技术,引起了工业界和学术界的广泛关注[1]。区块链是一个分散的分布式账本,由网络中的节点共同维护和管理,当大多数节点达成共识时,交易才会被节点认可并记录到自己的账本中。同时,区块链中使用的国际密码算法存在一定的后门安全隐患[2]。2020年央行发布的《金融分布式账本技术安全规范》[3]中,明确要求国内的区块链技术必须支持国密算法。为解决基于身份的密码体制中的密钥托管问题,Al-Riyami和Paterson[4]在2003年首次给出了无证书公钥密码机制的正式定义和安全模型。在该密码机制中,用户的私钥由密钥生成中心(Key Generation

收稿日期:2023-04-28　返修日期:2023-09-27
基金项目:国家自然科学基金(62076209);国家自然科学基金青年科学基金(61702429);四川省科技厅重点研发项目(21ZDYF3119,2022YFG0321)
This work was supported by the National Natural Science Foundation of China(62076209),Young Scientists Fund of the National Natural Science Foundation of China(61702429) and Key Research and Development Projects of the Technology Department of Sichuan Province,China(21ZDYF3119,2022YFG0321).
通信作者:黄晓芳(xf.swust@qq.com)

Center，KGC）和用户共同完成，KGC 不知道用户的完整私钥，因此无证书密码系统能够有效解决密钥托管问题。另外，用户的公钥由他们的公开信息计算而来，因此无证书密码机制避免了证书管理。

在此之后，文献[5-7]相继提出改进的无证书加密方案。Zheng 等[8]给出了无证书加密方案的敌手模型和安全证明的形式化定义，设计了一个基于双线性对的无证书加密方案。Hassan 等[9]、Ma 等[10]、Senouci 等[11]、Zhang 等[12]随后也设计了基于双线性配对的无证书公钥加密方案，并在随机预言模型下证明了该方案的安全性。Qu 等[13]设计了一种基于双线性对的无证书公钥加密方案，并证明了该方案在适应性选择密文攻击下具有密文不可区分性（IND-CCA2）。但以上基于配对的无证书加密方案开销过大。之后，Luo 等[14]采用无配对操作，构造了一个无证书跨域加密方案，该方案相比文献[13]的方案计算效率提升了 11%。Zhou 等[7]和 Cheng 等[15]分别基于 Diffie-Hellman 问题（Decisional Diffie-Hellman Problem，DDHP）和 Gap Diffie-Hellman 问题（Gap Diffie-Hellman Problem，GDHP）设计了无配对的无证书加密方案，但文献[15]仅证明了不可区分非适应性选择密文安全（IND-CCA1）。基于区块链的技术在人们的生活中得到了广泛的应用[16-17]。基于区块链的防篡改与去中心化的特点，越来越多的学者将区块链应用到无证书密码体制中，设计更安全的无证书密码系统[18-20]。Eltayieb 等[21]依靠区块链技术设计了一个无证书加密方案，该方案对数据进行分布式管理，并被证明在随机预言模型下是不可区分选择明文安全（IND-CPA）的。Xu 等[6]提出了新的基于区块链的无证书加密算法，其安全性依赖于区块链的去中心化性。

本文基于国密算法 SM2，提出了一种基于区块链的无证书加密方案。该方案不含双线性对，在计算效率上有明显的优势，并在随机预言模型下证明了 IND-CCA2 安全。同时，依托区块链的去中心化和不可篡改的特点，本方案更能有效抵抗无证书密码机制中两类型敌手的攻击。最后进行分析与验证，结果表明该方案具有更高的效率和安全性。

2 预备知识

2.1 困难问题

椭圆曲线离散对数问题（Elliptic Curve Discrete Logarithm Problem，ECDLP）：令 P 是加法循环群 G 的生成元，素数 p 是 G 的阶。给定（P，$Q\in G$），求解整数 $x\in Z_p^*$，满足 $Q=xP$。

计算性 Diffie-Hellman 问题（CDHP）：令 P 是加法循环群 G 的生成元，素数 p 是 G 的阶。对于任意的 x，$y\in Z_p^*$，给定 $Q=xP$，$R=yP$ 为 G 中的两个随机元素，求解 xyP。

2.2 SM2 加密算法

SM2 加密算法详见国密标准 GM/T003[22]，具体算法流程本节不再阐述，在此简要介绍本文提出的无证书加密方案需要用到的参数，如表 1 所列。

表 1 本文方案中使用的参数

Table 1 Parameters used in the proposed scheme

参数	定义
sk_u	用户 u 的私钥
PK_u	用户 u 的公钥
$E(F_p)$	F_p 上椭圆曲线 E/F_p 的所有点（包括无穷远点 O）的集合
F_p	有限域
ID_u	用户 u 的标识
xV，xP_{pub}，xY	V，P_{pub}，Y 的 x 坐标
yV，yP_{pub}，yY	V，P_{pub}，Y 的 y 坐标
$klen$	消息 m 的比特长度
$\|$	拼接符号
$\oplus$	异或运算
KDF	密钥派生函数

2.3 区块链

区块链是数据块按时间顺序连接而成的链式结构，链长随着新区块的加入而增长[23]。区块链是一个分布式数据库系统，由多个用户共同维护，当所有节点达成一致时，数据才能被写入区块中，并且区块中的数据不能被任何节点更改。

区块链已经从早期的区块链 1.0（以比特币为代表）过渡到区块链 2.0（以以太坊为代表）。目前，区块链已经进入去中心化信托区块链 3.0 时代（社会治理与实体经济和产业的合并）。区块链因具有独特的集成和互操作架构以及能够与各种技术和设备无缝融合的特点，将成为推动工业 4.0 发展的强大工具，为社会提供高质量的产品和服务。

3 安全模型

3.1 无证书加密算法定义

无证书加密方案由以下部分组成：

系统建立：该算法输入安全参数 λ，输出主密钥 s 和系统公共参数 $params$。

部分私钥提取：该算法输入系统参数 $params$、用户身份 ID_u 和主密钥 s，输出对应的部分私钥 d_u。

设置秘密值：该算法输入用户身份 ID_u，输出用户 u 的秘密值 v_u。

设置私钥：该算法输入部分私钥 d_u 和秘密值 v_u，输出对应的私钥 sk_u。

设置公钥：该算法输入系统参数 $params$、用户身份 ID_u 和私钥 sk_u，输出用户 u 的公钥。

加密：该算法输入系统参数 $params$ 和接收者公钥 PK_R，输出密文 C。

解密：该算法输入系统参数 $params$、密文 C、接收者私钥 sk_R，输出明文 m。

3.2 无证书加密算法安全模型

无证书加密方案中主要涉及两种攻击类型。Type-1 型敌手也称外部敌手，它不能得到系统的主密钥但可以替换用户的公钥；Type-2 型敌手被称为内部敌手，它可以得到系统的主密钥但不可以替换用户的公钥。CL-PKE 方案必须保证用户只有在获得完整密钥的授权下才能被允许访问加密消息。CL-PKE 安全性定义如下：

系统初始化：输入安全参数 k，挑战者运行系统建立算法，生成系统参数 $params$ 和主密钥 s，挑战者秘密保存主密钥

并把公共参数返回给敌手 A。

哈希查询：对于敌手 A 要查询的任意值，挑战者返回相应的哈希值。

部分私钥查询：对于敌手 A 要查询的部分私钥，挑战者返回相应的部分密钥 d_u。

私钥查询：对于敌手 A 要查询的私钥，挑战者返回相应的私钥 sk_u。

公钥查询：对于敌手 A 要查询的公钥，挑战者返回相应的公钥 pk_u。

公钥替换查询：敌手 A 可以为任意用户提交一个新的公钥 pk_u'，挑战者将 pk_u' 替换为用户的当前公钥 pk_u。

解密查询：A 输入身份 ID_u 和密文 C，C 返回明文消息 m 或 $\perp$。

下文将介绍 CL-PKE 下不可区分适应性选择密文安全性。

定义 1 在多项式时间内，如果没有攻击者 $A\in\{A_1,A_2\}$ 能以不可忽略的概率在下面的游戏中获胜，则无证书加密算法是适应性选择密文攻击语义不可区分的。

游戏 1 描述挑战者 B 与 Type-1 型敌手 A_1 之间的交互，但受上述定义限制。

初始化：B 运行系统建立算法获得公共参数 $params$ 和主密钥 s，秘密保存 s 将 $params$ 返回给 A_1。

阶段 1 攻击者 A_1 可以进行以下查询：系统初始化、哈希查询、部分私钥查询、私钥查询、公钥查询、公钥替换查询、解密查询。

挑战：A_1 输出两个等长明文信息 (m_0,m_1) 和挑战身份 ID^*，并将它们发送给挑战者 B。随后，B 随机选择 $\beta\in\{0,1\}$，计算挑战密文 $C^*=$加密$(params,PK_u,m_\beta)$ 并返回给 A_1。

阶段 2 A_1 像阶段 1 一样发出适应性询问，但有以下约束：1）A_1 不能执行关于挑战身份 ID^* 的私钥查询；2）如果 ID^* 对应的公钥被替换，则 A_1 不能执行 ID^* 的部分私钥查询 3；）A_1 不能执行关于 C^* 的解密询问。

猜测：A_1 输出其猜测 $\beta\in\{0,1\}$，当且仅当 $\beta=\beta'$ 时，A_1 赢得游戏。获胜的优势定义为 $Adv_{A_1}^{\text{IND-CCA}}=\left|\Pr[\beta'=\beta]-\frac{1}{2}\right|$。

游戏 2 描述挑战者 B 与 Type-2 型敌手 A_2 之间的交互，也受上述定义限制。

初始化：B 运行系统建立算法获得公共参数 $params$ 和主密钥 s，将 $params$ 和 s 返回给 A_2。

阶段 1 攻击者 A_2 可以进行以下查询：系统初始化、哈希查询、私钥查询、公钥查询、解密查询。

挑战：A_2 输出两个等长明文信息 (m_0,m_1) 和挑战身份 ID^*，并将它们发送给挑战者 B。随后，B 随机选择 $\beta\in\{0,1\}$，计算挑战密文 $C^*=$加密$(params,PK_u,m_\beta)$ 并返回给 A_2。

阶段 2 A_2 像阶段 1 一样发出适应性询问，但有以下约束：1）A_2 不能执行关于挑战身份 ID^* 的私钥查询；2）A_2 不能执行关于 C^* 的解密询问。

猜测：A_2 输出其猜测 $\beta\in\{0,1\}$，当且仅当 $\beta=\beta'$ 时，A_2 赢得游戏。获胜的优势定义为 $Adv_{A_2}^{\text{IND-CCA}}=\left|\Pr[\beta'=\beta]-\frac{1}{2}\right|$。

4 方案设计

4.1 系统模型

本文基于区块链提出了一种无配对的无证书公钥加密方案，系统模型如图 1 所示。它基于联盟链网络，提供分布式的网络存储方式，包括 KGC、区块链、发送者和接收者 4 个实体。4 个实体的功能描述如下：

KGC：该实体作为半可信的第三方，为发送者和接收者生成部分私钥和系统参数；其次，作为监管节点，承担发送者和接收者的身份监管工作，并将系统参数上传至区块链。

区块链：该实体提供去中心化的存储方式，存储系统参数以及发送者和接受者的公钥。

发送者：消息的发送者，负责生成密文，并将公钥上传区块链。

接收者：消息的接受者，负责解密密文，并将公钥上传区块链。

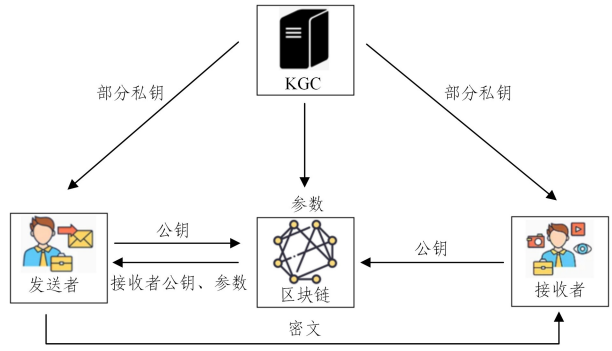

图 1 系统模型图

Fig. 1 Diagram of system model

区块结构如图 2 所示。该区块通过区块头中父区块哈希值与上一个区块链接，形成一个链式结构，若修改某个区块上的信息，则后面所有区块上的信息都需修改，这对于攻击者而言攻击代价是巨大的。区块中的交易数据包含系统参数 $params$、用户的身份 ID_u 及部分公钥 P_u，用户对公钥的每一次操作都会被记录在区块链上，恶意节点不能替换修改链上的任何数据。

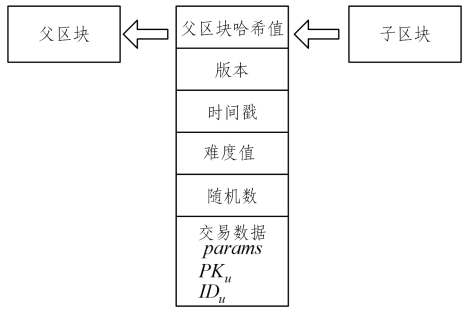

图 2 区块的数据结构

Fig. 2 Data structure of blocks

4.2 方案构造

系统模型的详细描述如下：

(1)系统建立。输入系统安全参数 k，KGC 生成 $kbit$ 素数

p 和定义在有限域 F_p 上的椭圆曲线 E/F_p。$E(F_p)$是由 E/F_p 上的点组成的阶为 q 的加法群,G 是群 $E(F_p)$上的生成元。KGC 随机选择 $s\in Z_q^*$ 为系统主密钥,计算主公钥 $P_{\text{pub}}=sG$。KGC 选择哈希函数,$H_1:\{0,1\}^*\rightarrow Z_q^*$,$H_2:\{0,1\}^*\rightarrow\{0,1\}^n$。公开系统参数 $params=\{F_p,E/F_p,E(F_p),G,p,q,P_{\text{pub}},H_1,H_2\}$,KGC 秘密保存 s 并上传 $params$ 到区块链。

(2)用户秘钥生成。用户 u 随机选择 $v_u\in Z_q^*$,计算 $V=v_uG$,得到用户的公私钥对(V,v_u)。

(3)部分私钥提取。KGC 随机选择 $w\in Z_q^*$,计算 $Y=wG$,$d_u=w+qs$,$q=H_1(xY\parallel ID_u\parallel yY\parallel xP_{\text{pub}}\parallel xV\parallel yP_{\text{pub}}\parallel yV)$,通过安全通道将$(d_u,Y)$发送给 u。同时,KGC 上传部分公钥 $P_u=(Y,V)$至区块链。用户 u 验证 $d_uG=Y+qP_{\text{pub}}$是否成立,若成立则接受部分私钥 d_u。

(4)设置私钥。用户 u 将部分私钥 d_u 和秘密值 v_u 结合,得到私钥 $sk_u=d_u+v_u$。

(5)设置公钥。用户 u 设置公钥 $PK_u=Y+V+qP_{\text{pub}}$。

(6)加密。发送者 *Sen* 从区块链获取接收者 *Rec* 的部分公钥 $P_u=(Y,V)$和系统参数 $params$,验证 *Rec* 公钥 PK_u'的正确性。发送者 *Sen* 验证 $PK_u'=Y+V+qP_{\text{pub}}$是否成立,若成立,则随机选择 $r\in Z_q^*$,计算 $C_1=rG$,$Q=rPK_u$,$f=KDF(xQ\parallel yQ,klen)$,$C_2=m\oplus f$$C_2=m\oplus f$,$C_3=H_2(xQ\parallel m\parallel yQ)$,生成密文 $C=(C_1,C_2,C_3)$发送给接收者 *Rec*。

(7)解密。接收者 *Rec* 从 C 中取出 C_1,计算 $Q=sk_uC_1$,$f=KDF(xQ\parallel yQ,klen)$,从 C 中取出 C_2 并计算 $m=C_2\oplus f$,$C_3=H_2(xQ\parallel m\parallel yQ)$,如果 $C_3=C'_3$,则输出消息 m,否则输出$\perp$。

4.3 密钥更新

当用户需要将已有公钥 PK_u 更新为 PK_u'时,首先计算 $U=sk_uP_{\text{pub}}$,然后向 KGC 发送密钥更新请求 $Req=(ID_u,U)$。KGC 收到用户的密钥更新请求后验证 $U=sPK_u$ 是否成立,若成立,则与用户合作执行 4.2 节密钥生成操作,KGC 将新部分公钥 $P'_u=(Y',V')$上传至区块链,更新用户的部分公钥。由于用户在查询公钥时只查询最新的有效公钥,因此用户的旧密钥在新密钥生效后自动失效,变为无效公钥。

4.4 密钥撤销

在该系统结构中,若用户的私钥泄露或用户不需要公钥服务,需撤销公钥时,KGC 设置 $P_u=null$,使用最新的有效公钥签名信息,在区块链上更新公钥。其他用户也在自己的账本中进行同步更新,最终实现密钥的撤销。

5 安全性证明

5.1 正确性分析

定理 1 令用户 u 的公私钥对为(V,v_u),用户 u 收到由 KGC 通过安全通道发送的部分公私钥对(d_u,Y),若验证用户部分私钥算法 $d_uG=Y+qP_{\text{pub}}$成立,则说明用户 u 的部分公私钥合法。验证用户部分私钥正确性算法如下:

$$d_uG=(w+qs)G=wG+qsG=Y+qP_{\text{pub}} \tag{1}$$

定理 2 令接收者 Rec 接收的密文为 $C=(C_1,C_2,C_3)$,该密文由发送者 *Sen* 使用接收者 *Rec* 的公钥计算而得,同时 *Rec* 的私钥为 sk_u,若 $Q'=sk_uC_1=Q$ 成立,则说明解密的明文是合法的并且解密成功。验证解密算法正确性算法如下:

$$Q'=r(Y+V+qP_{\text{pub}})=(w+v_u+qs)rG=(d_u+v_u)C_1=sk_uC_1=Q \tag{2}$$

5.2 安全性分析

区块链的安全性依赖于哈希函数,前一个区块的哈希值记录在后一个区块中,利用哈希碰撞避免攻击者篡改区块中的数据。考虑到该方案中区块链对无证书机制中两类敌手的抵抗,对于 Type-1 型敌手,它可以替换用户的公钥。在该方案中,用户的公钥 PK_u、系统参数 $params$ 存储在区块链中,由于区块链的去中心化和不可变性,用户对公钥数据操作的交易信息能够被追踪,恶意敌手不能篡改一个已存储在区块链中的用户公钥。因此,Type-1 型敌手不能替换任何用户的公钥。

对于 Type-2 敌手,系统参数 $params$ 在上传至区块链后不可更改,并且用户收到 KGC 发送的部分私钥后,通过区块链上的系统参数 $params$ 验证主密钥 s 及参数的正确性,如 5.1 节定理 1 所示。因此,Type-2 型攻击者不能修改 KGC 的主密钥。

定理 3 假设 CDH 问题是难以解决的,本文方案在随机预言机模型下是 IND-CCA2 安全的。

定理 3 由引理 1 和引理 2 分别证明。

引理 1 假定 Type-1 型敌手 A_1 最多可以发起 q_{H_2} 次 H_2 询问、q_{pri}次私钥询问和 q_{d} 次解密询问。若 A_1 能够以不可忽略的优势 ε 攻破该方案,则存在挑战者 B 能以不可忽略的优势 $\varepsilon'\geqslant\frac{1}{q_{H_3}}\left(\frac{2\varepsilon}{e(1+q_{\text{pri}})}-\frac{q_{H_4}}{q}-\frac{q_{\text{d}}}{2^{l_1}}\right)$解决 CDH 问题。

证明:给定 CDHP 实例(G,x_0G,y_0G,Q),其中 $x_0,y_0\in Z_q^*$,B 通过以下游戏计算 $x_0,y_0\in Z_q^*$。

初始化:B 生成系统参数 $params=\{F_p,E/F_p,E(F_p),G,p,q,P_{\text{pub}},H_1,H_2,H_3\}$,将 $params$ 发送给 A_1,令 $P_{\text{pub}}=x_0G$。

H_1查询:B 在 L^{H_1} 中维护列表。收到对 H_1 询问 η 时,B 首先查询(η,q)是否在列表 L^{H_1} 中,如果在,将 q 返回 A_1;否则,B 随机选择 $q\in Z_q^*$,把(η,q)插入 L^{H_1} 中并返回 q 给 A_1。

H_2查询:B 在 L^{H_2} 中维护列表(θ,C_3)。收到对 H_2 询问 θ 时,B 首先查询(θ,C_3)是否在列表 L^{H_2} 中,如果在,将 C_3 返回 A_1;否则,B 随机选择 $C_3\in\{0,1\}^n$,把(θ,C_3)插入 L^{H_3} 中并返回 C_3 给 A_1。

阶段 1 部分私钥查询:B 在 L^{par} 中维护列表(ID_u,Y,d_u)。B 收到 A_1 询问 ID_u 时,首先查询(ID_u,Y,d_u)是否在列表 L^{par} 中,如果在,将(Y,d_u)返回 A_1;否则,B 随机选择 q,$d_u\in Z_q^*$,计算 $Y=d_uP-qP_{\text{pub}}$,把(ID_u,Y,d_u)插入 L^{par} 中并返回(Y,d_u)给 A_1。

公钥查询:B 在 L^{pub} 中维护列表$(ID_u,Y,V,qP_{\text{pub}},coin)$。$B$ 收到 A_1 关于 ID_u 的询问时,首先查询$(ID_u,Y,V,qP_{\text{pub}},coin)$是否在列表 L^{pub} 中,如果在,将(PK_u)返回 A_1。否则,当 $coin=0$ 时,B 随机选择 $coin\in\{0,1\}$使得 $\Pr[coin=0]=\delta$(δ 在后文给定义)。若(ID_u,Y,d_u)存在列表 L^{par}中,B 随机选择 $v_u\in Z_q^*$,计算 $V=v_uG$,将(ID_u,d_u,v_u)和$(ID_u,Y,V,qP_{\text{pub}},coin)$分别插入 L^{pri}和 L^{pub}中,并把 L^{pub}返回给 A_1;若$(ID_u,Y,$

d_u)不在列表 L^{par} 中，则 B 执行部分私钥查询获得部分私钥(d_u，v_u)，计算 $V=v_uG$，$sk_u=v_u+d_u$，$PK_u=sk_uG$，将(ID_u，d_u，v_u)和(ID_u，Y，V，qP_{pub}，$coin$)分别插入 L^{pri} 和 L^{pub} 中，并返回(Y，V)。

当 $coin=1$ 时，B 随机选择 w，$v_u\in Z_q^*$，计算 $Y=wG$，$V=v_uG$，将(ID_u，v_u，$*$，w)和(ID_u，Y，V，qP_{pub}，$coin$)分别插入 L^{pri} 和 L^{pub} 中，并返回(ID_u，PK_u)。

私钥查询：B 在 L^{pri} 中维护列表(ID_u，d_u，v_u)。B 收到 A_1 关于 ID_u 的询问时，执行公钥查询得到(ID_u，PK_u，$coin$)。当 $coin=0$ 时，B 在 L^{pri} 中查找(ID_u，d_u，v_u)，并返回(d_u，v_u)作为私钥；当 $coin=1$ 时，B 输出“Abort”并终止游戏。

替换公钥查询：A_1 可选择任意一个新的公钥替换原来的公钥。

解密查询：B 收到关于(ID_u，Y，V，qP_{pub}，$coin$)，$C=(C_1$，C_2，$C_3)$的解密查询，在列表 L^{pub} 中查找(ID_u，Y，V，qP_{pub}，$coin$)。1)若此数组存在且 $coin=0$，则 B 在列表 L^{pri} 中查找(ID_u，d_u，v_u)，计算 $Q=(d_u+v_u)C_1$，$f=KDF(xQ\parallel yQ$，$klen)$，$m=C_2\oplus f$，验证 $C^3=H_3(xQ\parallel m\parallel yQ)$是否成立。若成立，则返回 m，否则 B 输出 L^{H_2}。2)若此数组存在且 $coin=1$，B 分别在列表 L^{H_2} 上查找(θ，C_3)使得 $C_3=H_2(xQ\parallel m\parallel yQ)$，$m=f\oplus C_2$，其中 $Q=rPK_u$，$f=KDF(xQ\parallel yQ$，$klen)$，若存在，则 B 返回 m，否则 B 输出 $\perp$。3)若此数组不存在，则 B 执行 H_1 查询得到(ID_u，Y，V)，然后重复执行 2)操作。

挑战：A_1 输出两个比特长度相等的明文消息(m_0，m_1)和一个挑战身份 ID^*。当收到对(ID^*，m_0，m_1)的询问时，B 在 ID^* 上执行公钥查询，得到(ID^*，Y^*，V^*，$coin$)。若 $coin=0$，则 B 输出“Abort”并终止游戏；否则，B 随机选择 $\beta\in\{0,1\}$，$C_2^*\in\{0,1\}$，$C_3^*\in\{0,1\}^n$，令 $C_1^*=y_0G$，$\Omega=y_0Y^*$，$\Phi=y_0V^*$，定义 $Q^*=y_0PK_u^*$，$f^*=KDF(xQ^*\parallel yQ^*)$，$C_2^*=m_\beta\oplus f$，$C_3^*=H_2(xQ^*\parallel m_\beta\parallel yQ^*)$，输出($C_1^*$，$C_2^*$，$C_3^*$)作为挑战密文。

阶段 2　A_1 执行与阶段 1 相同的询问，但不能对挑战身份 ID^* 进行部分私钥询问和私钥询问，以及不能利用 ID^* 和 PK^* 对明文 m_β 进行加密后得到的密文(C_1^*，C_2^*，C_3^*)进行解密询问。

猜测：A_1 输出其猜测。若 $\beta'=\beta$，A_1 赢得游戏，则 B 输出 $\dfrac{Q^*-\Omega-\Phi}{q^*}$作为 CDHP 的解。

分析：定义 $AskH_2^*$ 为事件 A_1 用 $xQ^*\parallel m_\beta\parallel yQ^*$ 询问 H_2，$DecErr$ 为事件 B 在访问解密查询时发生模拟错误，可以得到 $\Pr[DecErr]\leqslant q_d/2^n$。令 $AskH_2^*\vee DecErr)\mid\neg Abort$，$Abort$ 为事件 B 在模拟过程中中止。如果事件 E 不发生，在猜测 β 时，A_1 得不到大于 $\frac{1}{2}$ 的任何优势，即 $\Pr[\beta'=\beta\mid\neg E]\leqslant\frac{1}{2}$，有 $\Pr[\beta'=\beta]=\Pr[\neg E]+\Pr[\beta'=\beta\mid E]\Pr[E]\leqslant\frac{1}{2}\Pr[\neg E]+\Pr[E]=\frac{1}{2}+\frac{1}{2}\Pr[E]$。由 ε 的定义知，$\varepsilon<\left|\Pr[\beta'=\beta]-\frac{1}{2}\right|\leqslant\frac{1}{2}\Pr[E]\leqslant\frac{(\Pr[AskH_2^*]+\Pr[DecErr])}{2\Pr[\neg Abort]}$。$\neg Abort$ 发生的概率为 $\delta^{q_{pri}}(1-\delta)$，当 $\delta=1-1/(q_{pri}+1)$ 时，该值取得最大值，由此可得 $\Pr[\neg Abort]=1/e(1+q_{pri})$，其中 e 表示自然对数。由此可以得到：$\Pr[AskH_2^*]\geqslant 2\varepsilon\Pr[\neg Abort]-\Pr[DecErr]\geqslant\frac{2\varepsilon}{e(1+q_{pri})}-\frac{q_d}{2^n}$。

如果 $AskH_2^*$ 发生，那么 B 能通过在列表 L^{H_2} 上搜索数组(θ，C_3)解决 CDH 问题。因此，B 能以不可忽略的优势 $\varepsilon'\geqslant\frac{1}{q_{H_2}}\Pr[AskH_2^*]\geqslant\frac{1}{q_{H_2}}\left(\frac{2\varepsilon}{e(1+q_{pri})}-\frac{q_d}{2^n}\right)$解决 CDH 问题。

引理 2　假定 Type-2 型敌手 A_1 最多可以发起 q_{H_2} 次 H_2 询问、q_{pri} 次私钥询问和 q_d 次解密询问。若 A_1 能够以不可忽略的优势 ε 攻破该方案，则存在挑战者 B 能以不可忽略的优势 $\varepsilon'\geqslant\frac{1}{q_{H_2}}Pr[AskH_2^*]\geqslant\frac{1}{q_{H_2}}\left(\frac{2\varepsilon}{e(1+q_{pri})}-\frac{q_d}{2^n}\right)$解决 CDH 问题。

本引理证明思路同引理 1，不再赘述。

6　性能分析

6.1　性能评估

本节将从存储开销和计算开销两方面对所提出的加密算法进行对比分析。定义如下：$|q|$表示 Z_q^* 上元素的长度，$|G|$表示阶为 P 的循环群 G 上的元素长度，$|m|$表示消息长度，$|h|$表示哈希函数长度($|q|=20$ bytes，$|G|=128$ bytes，$|m|=32$ bytes，$|h|=32$ bytes)，PKT 表示公钥操作可追溯，I_1 表示 IND-CCA1，I_2 表示 IND-CCA2。表 2 列出了本文方案与其他 CL-PKE 方案的性能对比结果，可以看出，本文方案结合区块链能确保透明交易并有效防止恶意用户替换用户的公钥，用户与 KGC 对公钥操作具有可追溯性的特点。本文方案与文献[6-7，9，15]的通信开销相当，且具有 IND-CCA2。

表 2　通信开销及安全分析比较

Table 2　Comparison of communication overhead and security analysis

方案	密文长度	PKT	安全目标	
			I_1	I_2
文献[6]	$\|G\|+2\|m\|$	√	×	×
文献[7]	$2\|G\|+2\|m\|$	×		√
文献[9]	$2\|G\|+2\|q\|$	×		√
文献[15]	$\|G\|+\|m\|+\|h\|$	×	√	
本文方案	$\|G\|+\|m\|+\|h\|$	√		√

在效率对比分析中，本文采用表 3 中的符号表示本文方案的运算，计算开销数据参考文献[24]。表 4 列出了本文方案与其他 CL-PKE 方案的详细效率分析比较。由表 4 可知，本文方案总耗时约为文献[6]的 6.3%、文献[7]的 53.8%、文献[9]的 6.5%、文献[15]的 77.8%。因此，本文方案的计算效率优于其他方案。

表 3　运算符号说明及开销

Table 3　Operation symbol description and overhead

符号	计算开销/ms
双线性配对运算	$1T_P\approx4.2110$
双线性对群 G_1 的标量乘运算	$1T_{pm}\approx1.7090$
椭圆曲线上的标量乘运算	$1T_{em}\approx0.4420$
哈希运算	$1T_h\approx0.0001$
幂乘运算	$1T_e\approx0.0535$
map to point 哈希运算	$1T_{H_{mtp}}\approx4.4060$

表 4 效率比较

Table 4 Comparison of efficiency

方案	密钥生成	加密	解密	总计
文献[6]	$4T_{pm}+2T_p+T_{em}+T_h+T_{H_{mtp}}$	$T_{pm}+3T_p+T_{H_{mtp}}+2T_h$	$T_{pm}+T_p+T_{H_{mtp}}+2T_h$	$6T_{pm}+6T_p+3T_{H_{mtp}}+4T_h$
文献[7]	$4T_{em}+2T_h$	$6T_{em}+3T_h$	$3T_{em}+T_h$	$13T_{em}+6T_h$
文献[9]	$8T_{pm}+3T_h$	$6T_{pm}+2T_p+7T_h+2T_e$	$4T_{pm}+2T_p+6T_h$	$18T_{pm}+4T_p+16T_h+2T_e$
文献[15]	$5T_{em}+4T_h$	$3T_{em}+3T_h$	$T_{em}+T_h$	$9T_{em}+8T_h$
本文方法	$5T_{em}+T_h$	$2T_{em}+T_h$	$T_{em}+T_h$	$8T_{em}+3T_h$

图 3 展示了本文方案与其他 CL-PKE 方案加密与解密两阶段的耗时对比。由图 3 可知，本文方案具有更高的计算效率。并且由表 2 和表 4 可知，本文方案与其他 CL-PKE 方案相比，在通信开销相似的情况下能够抵抗自适应选择密文攻击并且具有公钥可验证性、密钥不可否认性。因此，本文方案能以最小的计算开销兼备前者优点。

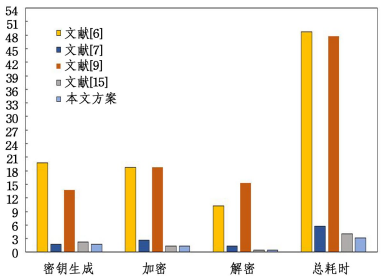

图 3 不同 CL-PKE 方案的加密与解密耗时

Fig. 3 Encryption and decryption time of different CL-PKE schemes

6.2 区块链实现

本文基于 HyperledgerFabric2.4.1 平台构建区块链平台，其中 KGC 为联盟链的监管节点。仿真实验操作系统为 ubuntu20.04，处理器 Intel(R)Core(TM)i7-7700 CPU @3.60GHz 3.60GHz，内存 4GB。实验测试数据存储上链操作和查询链上用户部分公钥操作，实验数据取 100 次操作的平均值。表 5 列出了数据上链和查询数据的平均时延。

表 5 系统平均时延

Table 5 System average delay

方案	存储平均耗时/s	查询平均耗时/s
文献[25]	0.25	0.23
本文方案	0.16	0.03

如表 5 所列，与文献[25]相比，本文在区块链上的存储数据操作和查询链上的数据操作平均时延较低，在区块链上运行的计算成本是可接受和合理的。

结束语 本文利用区块链提出了一种基于国密算法 SM2 的无证书加密方案，使区块链技术支持国密算法。系统参数和用户对公钥的操作以交易的形式记录在区块链上。由于区块链的不可篡改性和可追溯性，敌手不能对存储在区块链上的用户公钥进行替换或对系统参数进行恶意篡改。因此，该方案能够完全抵抗 Type-1 和 Type-2 两种敌手。其次，该方案也在随机预言机模型下进行了形式化分析。与其他 CL-PKE 方案相比，本文方案在计算效率上开销成本更少。虽然本文方案从区块链的角度进行了安全性证明，但其仍存在一定的局限性。如何应对密钥丢失问题仍是今后继续研究的重点。

参 考 文 献

[1] AO W, FU S, ZHANG C, et al. A secure identity authentication scheme based on blockchain and identity-based cryptography [C]// 2019 IEEE 2nd International Conference on Computer and Communication Engineering Technology (CCET). IEEE, 2019: 90-95.

[2] YANG H Z, YUAN L Y, WANG S. Blockchain Design Based on SM2 National Secret Algorithm Optimization [J]. Computer Engineering and Design, 2021, 42(3): 622-627.

[3] PEOPLE's BANK of CHINA. Financial distributed ledger technology security specification [EB/OL]. (2020-02-05) [2022-12-07]. https://www.cfstc.org/bzgk/gk/view/yulan.jsp?i_id=1855&s_file_id=1741.

[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. Springer, 2003: 452-473.

[5] SU Y, LI Y P, CAO Q, et al. Authorized certificateless conjunctive keyword search on encrypted EHRs from WSNs [J]. Journal of Information Science & Engineering, 2020, 36(4): 881-896.

[6] XU G X, DONG J N, MA C, et al. A certificateless encryption scheme based on blockchain [J]. Peer-to-Peer Networking and Applications, 2021, 14(5): 2952-2960.

[7] ZHOU Y W, YANG B. Leakage-resilient CCA2-secure certificateless public-key encryption scheme without bilinear pairing [J]. Information Processing Letters, 2018, 130: 16-24.

[8] ZHENG X Y, ZHOU Y Y, YE Y L, et al. A cloud data deduplication scheme based on certificateless proxy re-encryption [J]. Journal of Systems Architecture, 2020, 102: 101666.

[9] HASSAN A, WANG Y, ELHABOB R, et al. An efficient certificateless public key encryption scheme with authorized equality test in healthcare environments [J]. Journal of Systems Architecture, 2020, 109: 101776.

[10] MA M M, FAN S Q, FENG D G. Multi-user certificateless public key encryption with conjunctive keyword search for cloud-based telemedicine [J]. Journal of Information Security and Applications, 2020, 55: 102652.

[11] SENOUCI M R, BENKHADDRA I, SENOUCI A, et al. An efficient and secure certificateless searchable encryption scheme against keyword guessing attacks [J]. Journal of Systems Architecture, 2021, 119: 102271.

[12] ZHANG R R, NIU H X. Security-enhanced certificateless searchable public key encryption scheme [J]. Microelectronics & Computer, 2022, 39(6): 89-98.

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

[14] LUO M, PEI Y S, CHEN A. Cross-domain encryption scheme with equality test for wireless body area networks [J]. Wireless Networks, 2022, 28(5): 2105-2114.

[15] CHENG C H. A Certificateless encryption algorithm based on SM2 [J]. Journal of Cryptologic Research, 2021, 8(1): 87-95.

[16] ODOOM J, HUANG X F, DANSO S A. COVID-19 and future pandemics: A blockchain-based privacy-aware secure borderless travel solution from electronic health records [J]. Software: Practice and Experience, 2022, 52(10): 2263-2287.
[17] PAN W, HUANG X F. Identity Management and Authentication Model Based on Smart Contracts [J]. Computer Engineering and Design, 2020, 41(4): 915-919.
[18] TOMAR A, TRIPATHI S. BCAV: Blockchain-based certificateless authentication system for vehicular network [J]. Peer-to-Peer Networking and Applications, 2022, 15(3): 1733-1756.
[19] WANG Z H, HUO R, WANG S. A Lightweight Certificateless Group Key Agreement Method without Pairing Based on Blockchain for Smart Grid [J]. Future Internet, 2022, 14(4): 119.
[20] XU G X, DONG J N, MA C, et al. A Certificateless Signcryption Mechanism Based on Blockchain for Edge Computing [J]. IEEE Internet of Things Journal, 2022, 10(14): 11960-11974.
[21] ELTAYIEB N, SUN L, WANG K, et al. A certificateless proxy re-encryption scheme for cloud-based blockchain [C]// International Conference on Frontiers in Cyber Security. Springer, 2019: 293-307.
[22] STATE CRYPTOGRAPHY ADMINISTRATION. SM2 Elliptic Curve Public Key Cryptography Algorithm [S]. Beijing: China Standard Press. 2010.
[23] MONRAT A A, SCHELÉN O, ANDERSSON K. A survey of blockchain from the perspectives of applications, challenges, and opportunities [J]. IEEE Access, 2019, 7: 117134-117151.
[24] CUI J, ZHANG J, ZHONG H, et al. An efficient certificateless aggregate signature without pairings for vehicular ad hoc networks[J]. Information Sciences, 2018, 451: 1-15.
[25] YANG X, TIAN T, WANG J, et al. Blockchain-based multi-user certificateless encryption with keyword search for electronic health record sharing[J]. Peer-to-Peer Networking and Applications, 2022, 15(5): 2270-2288.

XIANG Yanjie, born in 1996, postgraduate. Her main research interests include blockchain and cryptography.

HUANG Xiaofang, born in 1977, Ph.D, professor, master supervisor. Her main research interests include blockchain and digital signature.

（责任编辑：何杨）