Journal of Computer Applications　ISSN 1001-9081
计算机应用　CODEN JYIIDU　http://www.joca.cn

用于实现区块链隐私保护的属性基加密方案

马海峰[1*]，李玉霞[1]，薛庆水[1]，杨家海[2]，高永福[1]
（1. 上海应用技术大学 计算机科学与信息工程学院，上海 201418；　2. 清华大学 网络科学与网络空间研究院，北京 100084）
（*通信作者电子邮箱 mahf@sit.edu.cn）

摘　要：要解决区块链账本公开带来的安全问题，关键在于对私密信息的隐藏。本文中提出使用多属性机构的属性基加密来实现区块链数据的隐私保护。相比单一属性机构，多属性机构在实现权力分散的同时避免了任何单点故障。首先方案修改了密钥组件生成算法，每个属性机构把用户身份作为参数来生成私钥组件，防止节点合谋访问无权访问的数据。然后修改了基于身份的签名技术来建立用户身份与钱包地址之间的连接，让区块链变得可监管的同时还能对非法用户进行可追溯。最后，基于DBDH（Determining the Bilinear Diffie-Hellman）假设，在随机预言模型中证明了该方案的安全性，同时实验结果表明，与基于椭圆曲线上的环签名的区块链隐私保护方案和支持关键字遗忘搜索的区块链隐私保护方案相比，在生成相同区块个数的情况下，本方案用时最少，更具可行性。

关键词：区块链；隐私保护；可监管；属性基加密；链上数据
中图分类号：TP309　　**文献标志码：**A

Attribute-based encryption scheme for blockchain privacy protection

MA Haifeng[1*]，LI Yuxia[1]，XUE Qingshui[1]，YANG Jiahai[2]，GAO Yongfu[1]
（1. *School of Computer Science & Information Engineering，Shanghai Institute of Technology，Shanghai* 201418，*China*；
2. *Institute of Network Science and Cyberspace，Tsinghua University，Beijing* 100084，*China*）

Abstract: To solve the security problems caused by the disclosure of blockchain ledgers，the key lies in the hiding of private information. using of attribute-based encryption by multi-authority organizations was proposed to achieve privacy protection of blockchain data. Compared to single-attribute institutions，multi-attribute institutions were decentralized and avoid any single point of failure. First，the scheme was modified by the key component generation algorithm，with each authority using the user′s identity as a parameter to generate private key components，preventing collusion between nodes to access unauthorized data. Then，identity-based signature technology was modified to establish a connection between user identities and wallet addresses，making the blockchain policeable while also tracing illegal users. Finally，based on the DBDH（Determining the Bilinear Diffie - Hellman）hypothesis，the safety of the scheme was proved in the stochastic prediction model，and compared with the blockchain privacy protection scheme based on ring signature on elliptic curve and the blockchain privacy protection scheme supporting keyword forgetting search，the least amount of time was taken by this solution and it was considered more feasible，in the case of generating the same number of blocks.

Key words: blockchain; privacy protection; policeable; attribute-based encryption; on-chain data

0　引言

比特币问世时，区块链通过一系列的技术为交易系统提供了一定的安全性，避免了恶意交易，双花攻击等威胁[1]。但在隐私方面，由于区块链账本是公开的，因此区块链网络中所有节点都可以查看账本内容。恶意用户可以借助爬虫技术获取区块链平台的服务信息，构建用户网络拓扑、交易网络拓扑，利用交易特征及溯源技术来获取隐私信息，这其中包括交易隐私，账户地址隐私，用户身份信息等敏感信息[2]。为了进一步确保对用户隐私的保护，近年来相关密码学技术已应用于该领域，如零知识证明，属性基加密，环签名，聚合签名等来保证链上数据隐私[3-7]。然而数据的全部隐藏为非法交易提供了可乘之机，数字货币的滥用给政府和金融监管机构带来了麻烦，然而人们对数字货币的监管呈现不同态度[8]。一些人认为用户有保留自己的隐私和自由交易的权力，因此他们认为货币系统应该全匿名且不受监管。但另一部分人认为监管必不可少，这将大大减少违法犯罪活动。实际应用中，货币系统需要在隐私性和可监管中取得某种平衡才能更好的发展。因此，设计一种在隐私保护的同时又能实现监管的区块链方案很有意义。

随着区块链数据隐私保护的研究明显增多，区块链的安全性有一定提升，但区块链应用的复杂程度在增加，很多学者陆续提出一些可监管的区块链隐私保护方案。Yuan等[9]利用密文策略属性基加密（Ciphertext Policy Attribute Based Encryption，CP-ABE）实现了一种私有链的数据隐私保护及监管机制，并应用于电子文档的管理。该方案允许任何第三方验证公开解密密钥的身份，允许审计师公开审计

收稿日期：2023-02-23；**修回日期：**2023-03-30；**录用日期：**2023-04-03。　**基金项目：**国家电网项目（SGHAXTOOWWJS2200033）。
作者简介：马海峰（1977—），男，黑龙江哈尔滨人，副教授，博士，CCF会员，主要研究方向：云计算安全、区块链安全；　李玉霞（1996—），女，河南漯河人，硕士研究生，主要研究方向：区块链、隐私保护；　薛庆水（1971—），男，山东济南人，教授，博士，CCF会员，主要研究方向：网络空间安全；　杨家海（1966—），男，浙江丽水人，教授，博士，博士生导师，主要研究方向：互联网络管理、网络测量与安全；　高永福（1998—），男，内蒙古通辽人，硕士研究生，要研究方向：区块链、隐私保护。

恶意用户或当局是否应对公开解密密钥负责，密钥滥用者不能否认。Xue等[10]集成多种加密技术，使用概率公钥加密，基于身份标识加密(Identity-Based Cryptograph, IBC)，Pedersen承诺，零知识证明等，来实现区块链隐私保护和监管功能。虽然在安全性和隐私性方面有很大的优势，但是算法的性能和效率上需要进一步提升才能实现应用。赵晓琦等[11]提出了一种可审计的区块链匿名交易方案，使用Elgamal加密实现交易数据的隐藏，用隐地址实现监管。交易金额需要审计方审计，交易越多，审计时间越长。所以应改进优化审计策略，提高审计效率。Hill等[12]设计了一种隐私保护协议，通过把密钥和文件分割来增强供应链中的数据可用性和隐私性。审计方是供应链中数据的唯一参与者，负责解决参与者之间的争议。但该协议只针对供应链，不能得到广泛应用。Feng等[13]提出了一种基于可搜索属性加密的区块链数据隐私保护访问控制方案。该方案使用基于密文策略的属性加密来加密陷门密钥，然后使用可搜索加密来加密区块链上的交易，但该方案存在威胁，那就是属性机构必须完全可信，而且用户可能合谋访问无权访问的数据。本文主要针对文献[13]中存在的属性机构权力过大和用户合谋问题，提出新的访问控制方案，同时实现区块链的可监管。本文贡献如下：

1)本文提出使用多属性机构的属性基加密方案来实现区块链的隐私保护。解密密钥不依赖于单一机构产生，更符合区块链去中心化的性质，最主要的是一个机构被攻破，非法用户也无法获取密钥解密文件。相比于单一机构必须完全可信有更大的容错空间。

2)为了防止用户合谋访问无权访问的数据，用户在请求解密密钥组件时，需将自己的身份标识符ID和属性集都发送给属性机构。由此生成的私钥组件就跟该用户绑定，只有该用户能用。同一用户的私钥组件才能合成解密密钥，用户间就不能合谋生成解密密钥来访问权限外的数据。

3)使用基于身份的签名(Identity-Based Signatures, IBS)方案的修改后的签名算法来生成交易密钥。该方案既保密了用户身份，又能建立用户身份与用户钱包地址之间的链接，以此来实现区块链的可监管。

1 基础知识

1.1 双线性映射

取阶数为素数q的乘法循环群G_0, G_1。对于群的随机生成器，存在满足以下属性的双线性对映射：

a)双线性，对所有$u, v \in G_0$；$a, b \in Z_p$，等式$e(u^a, v^b) = e(u, v)^{ab}$成立。

b)非退化性，存在元素$g \in G_0, e(u, v) \neq 1$。

c)可计算性，对任意$u, v \in G_0$，有一种多项式时间算法用于计算$e(u, v)$。

1.2 线性秘密共享方案

密码学者已经提出了很多秘密共享方案(Linear Secret Sharing Scheme, LSSS)，且这些方案在安全性和效率上都在逐步提升。LSSS是Shamir秘密共享方案的一般性推广。线性秘密共享方案在参与组上满足以下条件：

a)各方参与者的份额来自矩阵$\boldsymbol{Z}_p$。定义一个c行d列的分享生成矩阵$\boldsymbol{M}$，该矩阵对应的秘密共享方案为$\prod$。函数ρ将$\boldsymbol{M}$第i行的参与者标记定义为$\rho(i)$，其中$i = 1, 2, \cdots, l$。本文把行向量$\boldsymbol{v} = (s, v_2, v_3, \cdots, v_c)^T \in Z_p^n$，看作共享的秘密，其中$v_2, \cdots, v_c \in \boldsymbol{Z}_p$是随机选择的。$Mv$是根据秘密共享方案$\prod$得出的秘密份额。份额$Mv_i$属于$\rho(i)$。

b)假设$\prod$是访问结构的LSSS。假设$S_u \in \mathrm{A}$是属性机构的任意子集，A是属性集合，$I \in \{1, 2, \cdots, l\}$。如果$\{\lambda_i\}$是$\prod$中的有效秘密份额，将会有一个常数$\{w_i \in Z_p\}_{i \in I}$，使$\sum_{i=1}^{l} w_i \lambda_i = S$。此外，这些常数$\{w_i\}$可以在共享生成器矩阵$\boldsymbol{M}$的时间多项式中找到。

1.3 判定性双线性Diffie-Hellman假设

设G_1和G_2是阶q为素数的乘法循环群。选择一个生成器$g \in G_1$，选择参数$a, b, c, r \in Z_q^*$，得到$g^a, g^b, g^c \in G_1, e(g, g)^{abc}, e(g, g)^r \in G_2$。判定$e(g, g)^{abc}$和$e(g, g)^r \in G_2$的关系是否相等。

定义 对于任意多项式概率时间算法敌手A，DBDH假设的优势定义为：

$$Adv_A^{\mathrm{DBDH}} = \left| \Pr\left[A\left(g^a, g^b, g^c, \mathrm{e}(g, g)^{abc}\right)\right] - \Pr\left[A\left(g^a, g^b, g^c, \mathrm{e}(g, g)^r\right)\right] \right|$$

如果测定值Adv_A^{DBDH}可以忽略不计，则将建立判定性双线性Diffie-Hellman假设。

2 系统模型

本方案提出的基于属性基加密的隐私保护方案包含的实体有：用户(user)、数据拥有者(Data Owner, DO)、多属性权威机构(Multi-attribute Authority, MA)、密钥提供商(key server)、监管节点(regulation nodes)，如图1所示：

a)用户：向系统提出注册请求，生成身份标识符，组合每个属性机构(Attribute Authority, AA)生成的私钥构件形成解密加密数据的私钥。用户ID作为生成用户属性私钥的参数，以防止用户共谋去访问无权访问的数据。

b)数据拥有者：对交易进行签名和加密。数据拥有者为区块链系统中的用户。

c)多属性权威机构：每个授权机构独立地管理着每类属性，不同授权机构生成的私钥组件共同组成用户解密密钥。监管过程中向监管节点授权属性密钥。

d)密钥提供商：根据用户提交的ID和随机值计算出用户签名公私钥对的重要组成部分并通过秘密通道发送给用户。在监管节点监测到非法用户时，向监管节点提供非法用户的真实身份。

e)监管节点：监管节点负责对交易进行监管，但不参与交易过程。该方案假定监管节点是可信的。只有在属性机构授权属性密钥后，监管节点才能解密非法交易内容，揭露用户身份，区块链账本中的正常交易信息对监管节点是不可见的。

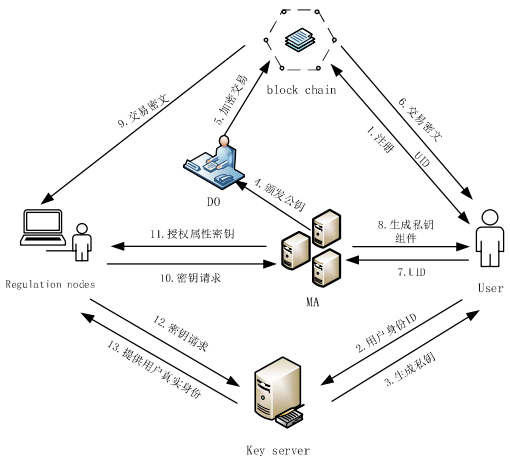


图1 系统模型

Fig. 1 System model

3 方案具体构造

方案包含两个部分：隐私保护部分和监管部分。针对隐私保护部分，基本思路是采用多属性机构的属性基加密实现对链上数据的访问控制，通过限制访问数据的用户来避免账本公开带来的安全隐患。每个属性机构根据用户的属性集为其生成私钥构件，只有满足访问结构的用户，才能解密交易密文。为了防止用户间合谋访问无

权访问的数据,本方案使用用户身份作为密钥组件的标识,只限定该密钥组件由单一用户使用。针对监管部分,基本思路是:在交易生成时,交易双方需对交易进行签名。密钥提供商为用户提供签名密钥,对交易进行签名不会泄露身份隐私。监管节点随机选择交易来验证用户身份。授权监管节点通过钱包地址和交易信息获取交易者的身份,验证其是否为诚实用户。若为非法用户,监管节点揭露非法用户的真实身份,并将其钱包地址拉入黑名单。

为了方便理解该方案,表1列出了文章中出现的部分符号。

表1 符号定义

Tab. 1 Symbol definitions

符号	含义	符号	含义
Z_p	整数集合	g	有限循环群的生成元
Z_p^*	非零整数集	S	系统属性集
p	大素数	ω_i	属性
G_0, G_1	有限循环群		

方案的两个主要部分划分为以下7个步骤:

1)初始化。

系统初始化:在群G_0中选择素数p,使用元素g生成组,在限制域中选N个元素,根据系统属性生成系统属性集$S=\{\omega_1,\omega_2,\cdots,\omega_N\}$,$\omega_1,\omega_2,\cdots,\omega_N\in Z_p$,$Z_p$是整数集合。选择两个随机值$\alpha,a\in Z_p$。公共参数$\mathrm{pp}=\{e,G_0,G_1,g_1,g_2,p\}$来定义双线性映射$e$:$G_0\times G_0=G_1$。数据所有者选择两个随机数$\mu,\eta$,计算公钥$\mathrm{PK}=\{g,g^{\mu}\}$,$g$是群$G_0$的生成元。

AA初始化:假定有x个属性机构$p\{A_1,A_2,\cdots,A_x\}$,每个属性机构管理一类属性集合,A_i运行初始化算法把公共参数pp作为输入,得到每个属性机构的公私钥对。属性机构把密钥保存,公钥公布。

密钥服务商初始化:密钥服务商选择一个随机数$a^*\in Z_q^*$,设主密钥$MK_{\mathrm{ibs}}=a^*$。系统公钥$P_{\mathrm{pub}}=a^*p$。定义两个加密哈希函数H_1:$\{0,1\}^*\times G_0\rightarrow Z_q$;$H_2$:$\{0,1\}^*\times G_0\rightarrow G_0$。系统参数$\mathrm{PK}_{\mathrm{ibs}}=\{p,p_{\mathrm{pub}},H_1,H_2\}$。

2)用户注册。

用户向系统提出注册申请,获得与用户身份相对应的身份标识和属性集$S_u=\{\omega_{u_1},\omega_{u_2},\cdots,\omega_{u_s}\}$,$S_u\in S$;$S$是系统属性集合,$\omega_i$是属性。用户提交$\{ID,r^*p\}$给密钥服务商,其中$r^*\in Z_q^*$,ID代表用户身份。密钥服务商验证ID的有效性。如果有效,则运行密钥生成算法$\mathrm{Q_{ID}}=H_2(ID,r^*p)$,$\mathrm{S_{ID}}=a^*\mathrm{Q_{ID}}=a^*H_2(ID,r^*p)$并把私钥SID通过安全通道发送给用户。签名公钥$pk_{\mathrm{sig}}=\mathrm{Q_{ID}}=H_2(ID,r^*p)$,私钥$\mathrm{sk_{sig}}=(S_{ID},r^*)=(a^*Q_{ID},r^*)$。在该方案中,用户的公钥不是真实身份,而是由随机值生成的随机化的身份散列,这就隐藏了签名者的身份。通过密钥生成算法,用户可以通过选择不同的随机值$\{a_i^*\}$生成不同的密钥对,以此来建立了用户身份和用户钱包地址之间的连接。钱包密钥对的生成如图2。

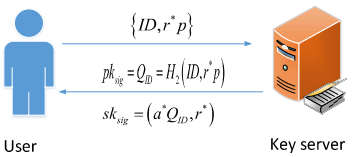


图2 钱包密钥对生成

Fig. 2 Wallet key pair generation

3)交易产生及签名。

假定A、B之间进行交易,A运行签名算法并选择钱包地址pk_{ai},使用对应的钱包密钥sk_{ai}对交易进行签名。然后生成交易TransA发送给B。A的签名为:$\sigma_A=(V_{A1},V_{A2},V_{A3},r_{ai}^*P)$,其中$V_{A1}=t^*pk_{ai}$,$V_{A2}=r_{ai}^*H_2(Trans\|ID_A,V_1)$,$V_{A3}=(t^*+V_A)pk_{ai}$,$r^*,t^*\in Z_q^*$,$V_A=H_1(m,V_{A1}+V_{A2})$。B对交易进行签名,由$V_{B1}=t^*pk_{bj}$,$V_{B2}=r_{bj}^*H_2(Trans\|ID_B,V_1)$,$V_{B3}=(t^*+V_B)pk_{bj}$,$V_B=H_1(m,V_{B1}+V_{B2})$得B的签名为$\sigma_B=(V_{B1},V_{B2},V_{B3},r_{ai}^*P)$。交易$\mathrm{Trans_{AB}}$广播到区块链要验证签名$\sigma_A$的公钥不是用户A的身份$ID_A$而是钱包地址$\mathrm{pk_{ai}}$,因此签名$\sigma_A$不会导致身份$ID_A$的隐私泄露,签名$\sigma_B$也是。

4)加密。

$(m,(\boldsymbol{M},\rho),pp)\rightarrow C_w$。数据拥有者运行加密算法,输入公共参数$pp$,访问控制策略$(\boldsymbol{M},\rho)$,交易信息$m$,得到交易密文$C_w$。

5)密钥生成。

$(\mathrm{ID},S_u,SK_i)\rightarrow\mathrm{USK_{uid}}$:用户向AA提交申请,AA根据用户标识符ID、用户属性集$S_u\in S$和主密钥生成私钥构件$\mathrm{USK_{uid}}$。用户拿到所有AA生成的私钥构件,计算出自己的私钥SKT。

6)解密。

$(\mathrm{UID},\mathrm{PK},C_w,\mathrm{SKT})\rightarrow m$:算法由数据使用者执行。该算法将用户身份UID、公共参数pp、密文C_w、用户生成的密钥SKT作为输入。当访问策略满足时,输出交易明文m,否则输出为空。

7)监管。

若对交易信息有异议,授权监管节点希望验证用户身份,它将通过输入授权属性密钥和密文来运行解密算法对交易信息进行解密,该算法返回一个身份ID′,监管节点通过计算$\mathrm{pk}=H_2(ID',r_{ai}^*P)$,并把它和钱包地址$pk_{ai}$比较来验证身份,如果相等,则$\mathrm{ID}'=\mathrm{ID_A}$,A是诚实用户。否则,监管节点向密钥提供商发送请求以得到用户的真实身份A,并把钱包地址$\mathrm{ID_A}$添加到黑名单。

4 方案分析与比较

4.1 安全模型

CP-ABE方案的安全模型与基于身份加密(Identity-Based Encrypted, IBE)方案类似,允许敌手对任意的密钥(不包括能够解密挑战密文的密钥)及逆行询问。敌手会选择挑战一个满足访问结构p^*的密文,并且能够对任何不满足p^*的属性集合S^*进行密询问。CP-ABE方案的选择明文攻击下的不可区分游戏(记为IND-CP-ABE-CPA游戏)如下:

a)初始化。由挑战者运行,产生系统参数params并将其发送给敌手。

b)阶段1。敌手发出对属性集合S^*的密钥产生询问。挑战者运行密钥产生算法,产生与S^*对应的密钥SK^*,并发送给敌手,这个过程可以进行多项式有界次问询。

c)挑战。敌手提交两个长度相等的消息m_0和m_1。此外,敌手选定一个想要挑战的访问结构p^*,其中敌手在阶段1中询问过的属性集合均不能满足此访问结构。挑战者选择随机数$b\in\{0,1\}$,并以p^*加密$\mathrm{m_b}$将密文$\mathrm{CT_{m\,b}}$给敌手。

d)阶段2。敌手发出对属性集合S^*的密钥产生询问,唯一的限制是这些S^*均不能满足挑战阶段的访问结构p^*。挑战者以阶段1中的方式进行回应,这个询问过程可进行多项式有界次。

e)猜测。敌手输出猜测$b'\in\{0,1\}$,如果$b'=b$,则敌手攻击成功。

4.2 安全分析

以下将证明在随机预言模型下,本文所提方案是安全的。

定理1 基于DBDH假设,如果本方案可以抵抗选择明文攻击(Chosen Plaintext Attack, CPA),则我们的方案是CPA安全的。

证明 假设一个概率多项式时间,敌手可以利用优势ϕ攻击。我们证明了以下DBDH游戏可以被敌手A以优势$\phi/2$攻击。e:$G_0\times G_0=G_1$是双线性映射,其中G是生成元为g阶为p的循环群。挑战者随机选择$a,b,c,z\in Z_p$,$u\in\{0,1\}$。如果$u=0$,$(g,A,B,C,Z)=(g,g^a,g^b,g^c,e(g,g)^{abc})$,如果$u=1$,$(g,A,B,C,Z)=(g,g^a,g^b,g^c,e(g,g)^z)$。

初始化:敌手至少控制两个授权权限,挑战者控制其余权限。敌

手确认了LSSS访问结构的挑战。挑战者随机选择$a=\xi, b=\psi, c=\zeta$，且随机数$\xi,\psi,\zeta\in Z_p$，并把$Y: e(A,B)=e(g,g)^{ab}$发给敌手

阶段1　敌手根据属性集要求提供许多他想要的私钥，但这些私钥不满足访问结构。在收到身份为RID的敌手的私钥请求时，挑战者随机选择$\beta_{RID}, k\in Z_p$并计算每个属性$k\in S$的私钥组件$d_j'=g^{\xi}\left(u_i'\prod_{k'=1}^{h'}u_{k'}a_{j,k'}\right)^{\xi_j}$，$D_j=g^{u_i}$。

阶段2　重复阶段1。

猜测：敌手提交V的猜想θ'，当$\theta=\theta'$时，如果$\theta=0$，代表挑战者的模拟器将输出：$\left(g,g^a,g^b,g^c,e(g,g)^{abc}\right)$，否则输出DBDH数组$\left(g,g^a,g^b,g^c,e(g,g)^z\right)$。如果$\theta=1$，敌手无法获得有用信息，他的优势$Pr=1/2$。当$\theta=0$，他的优势是$Pr=1/2+e$。所以在DBDH游戏中，敌手的概率多项式时间$\Pr(\theta=\theta')-1/2=1/2(1/2=\theta)+1/2.1/2-1/2=\vartheta/2$。如果游戏中的多项式时间是$\vartheta$，敌手不可忽视的优势是$\vartheta/2$。因此，基于DBDH假设，敌手在该安全游戏中没有优势，这表示本文的方案是安全的。

4.3　隐私保护分析

内容隐私　本文采用基于密文策略的属性基加密技术实现对交易信息的访问控制，相比对称密码技术，其更加安全。在交易密文生成之后，只有属性满足访问策略的用户才能解密交易数据，杜绝了区块链账本对所有节点公开所带来的一系列安全问题。在解密私钥生成的过程中，引入了用户标识符，限制解密密钥只能单一用户使用，因此，即使想串通，属性不满足访问结构的用户也不能解密交易信息。所以本方案对内容隐私的保护是合格且安全的。

身份隐私　本文使用新的签名算法来代替椭圆曲线签名生成钱包密钥对。用户的公钥不是真实身份，而是由随机值生成的随机化的身份散列。通过密钥生成算法，用户可以通过选择不同的随机值生成不同的密钥对。只有监管节点在得到属性密钥授权的情况下才可以得到用户的真实身份，如果用户非法才能揭露其身份。

4.4　方案比较

文献[14]提出了一种基于聚合签名的区块链签名方案，当事务有n个输入地址和m个输出地址时，签名的数量可以从n减少到1，接收方的身份隐私得到有效保护。但交易金额是公开的，同时没有监管功能。文献[15]中，使用环签名的匿名性来确保区块链应用中的数据安全和用户身份隐私。文献[16]提出使用属性基加密的方案，方案中把解密密钥分为两部分，一部分放到数据拥有者，一部分放到属性机构，这分散了属性机构的权力，防止了属性机构间的合谋但并没有设计监管功能。在文献[17]中，使用公钥密码实现可搜索关键字的区块链检索隐私保护机制，让数据拥有者在什么都不知道的情况下验证检索请求中的关键字授权。但方案[17]不涉及防合谋和不可连接。从表2可以看出，本文使用多属性机构的属性基加密方案实现了区块链数据的隐藏，同时防止了用户间合谋。修改后的签名算法能在有效保护用户身份隐私的同时实现用户可追踪，保证了链上交易安全。

表2　现存隐私保护方案比较

Tab. 2　Comparison of existing privacy protection schemes

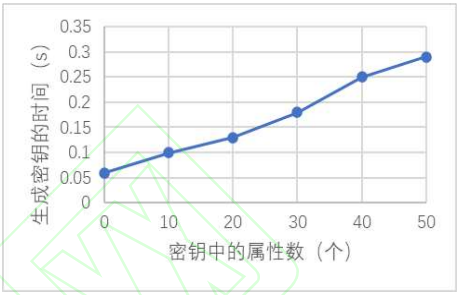
方案	加密技术	防合谋	不可链接	身份隐私	内容隐私	可追踪
文献[14]	聚合签名	—	√	部分	×	×
文献[15]	环签名	√	√	√	√	×
文献[16]	属性	√	×	部分	√	×
文献[17]	公钥	×	×	√	√	√
本方案	属性	√	√	√	√	√

5　实验验证

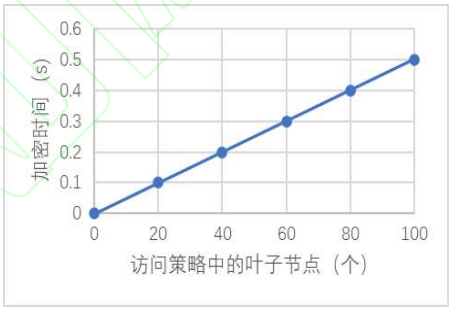
该实验在Ubuntu18.04系统中搭建了Hypeledger Fabric实验环境，在CPU为Intel Core i7-7500U@3.5 GHz的电脑上运行。

图3显示了运行密钥生成算法和加密所产生的密钥生成时间和加密时间的测量结果。该实现基于512位有限域上的超奇异椭圆曲线$y^2=x^3+x$的160位椭圆曲线组。在测试环境中，PBC库可以在大约5.5 ms内计算配对，G_0和G_1的求幂分别需要大约6.4 ms和0.6 ms。随机选择元素也是一项重要的操作，G_0需要16 ms，G_1需要1.6 ms。

正如预期的那样，运行密钥生成所需的时间与它所包含的密钥相关的属性数量几乎是线性的。加密链上数据的时间与访问策略中叶子节点的数量几乎是完全线性的。内部节点的运算相当于适度的乘法运算，不会显著增加运行时间。即使对于更大的问题实例，这两种方法仍然是可行的。



（a）密钥生成时间



（b）加密时间

图3　密钥生成和加密所需时间实验结果

Fig. 3　Time required for key generation and encryption Experiment results

现存的区块链隐私保护方案大多存在设计臃肿、开销大、实用性低等问题。为了验证该方案在区块链应用中的可行性，将本方案设计的加密和签名方案加入到本地搭建的私链中进行仿真实验很有必要。实验主要针对区块生成速度进行对比。因为区块生成过程包含交易生成、验证、数据上链等过程，所以链中块的生成速度是区块链隐私保护方案效率的一个直观体现。图4给出的是本方案与方案[15]、方案[17]在生成相同区块个数时所花费的时间对比。从图中给出的数据可以直观地看出，相比于方案[15]、方案[17]，本文提出的方案效率更高。由此证明该方案具有可行性。

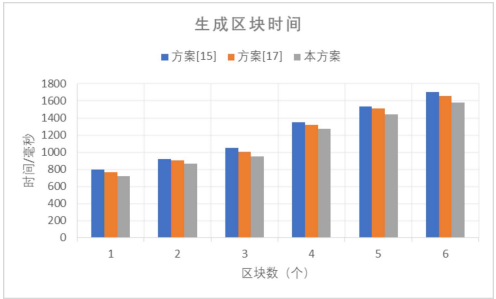


图4　区块生成时间对比

Fig. 4　Comparison of block generation time

6 结语

由于使用区块链技术存储交易信息的全球账本对加入区块链网络的任何节点开放,其带来的安全性问题阻挡了区块链的推广,所以区块链的隐私保护得到了许多学者的关注。随着区块链的应用越来越广泛,其复杂程度也在增加,所以区块链和属性基加密结合很有必要。本文利用MA-ABE实现对链上数据的访问控制,实现了交易隐私保护,利用修改后的IBS方案建立用户身份与钱包地址之间的连接,以此来实现对用户的监管。相比于方案[13],解除了单一属性机构必须完全可信的限制,并且防止了用户间合谋访问无权访问的数据。在隐私保护的同时,引入监管机制,在检测到非法交易时,把用户钱包地址拉入黑名单,这将大大降低非法交易的可能。最后经过安全分析和实验验证,证明了该方案的安全性和有效性。

参考文献(References)

[1] Nakamoto S. Bitcoin: A Peer-to-Peer Electronic Cash System[EB/OL]. (2008-11-01)[2021-07-21]. https://bitcoin.org/bitcoin.pdf

[2] 张奥, 白晓颖. 区块链隐私保护研究与实践综述[J]. 软件学报, 2020,31(5):1406-1434. (ZHANG A, BAI X Y. A review of blockchain privacy protection research and practice[J]. Journal of Software, 2020,31(5):1046-1434.)

[3] BUNZ B, AGRAWAL S, ZAMANI M, et al. Zether: Towards privacy in a smart contract world[C]//Proceedings of the 2020 International Conference on Financial Cryptography and Data Security. Berlin: Springer, 2020: 423-443.

[4] ZHOU J, CAO Z F, QIN Z, et al. LPPA: Lightweight privacy-preserving authentication from efficient multi-key secure outsourced computation for location-based services in VANETs[J]. IEEE Transactions on Information Forensics and Security, 2019, 15: 420-434.

[5] CAO Z F, WANG H B, ZHAO Y L. AP-PRE: Autonomous path proxy re-encryption and its applications[J]. IEEE Transactions on Dependable and Secure Computing, 2017, 16(5): 833-842.

[6] GENTRY C, SAHAI A, WATERS B. Homomorphic encryption from learning with errors: Conceptually-simpler, asymptotically-faster, attribute-based[C]// Proceedings of the 2013 Annual Cryptology Confererence. Berlin: Springer, 2013: 75-92.

[7] 朱岩, 宋晓旭, 薛显斌, 等. 基于安全多方计算的区块链智能合约执行系统[J]. 密码学报, 2018, 6(2): 246-257. (ZHU Y, SONG X X, XUE X B, et al. Blockchain smart contract execution system based on secure multi-party computing[J]. Journal of Cryptologic Research, 2018, 6(2): 246-257.)

[8] DE FILIPPI P. Bitcoin: A Regulatory Nightmare to a Libertarian Dream[J]. Social Science Electronic Publishing, 2014, 3(2): 289-296.

[9] YUAN C, XU M X, SI X M, et al. Blockchain with accountable CP-ABE: How to effectively protect the electronic documents[C]// IEEE International Conference on Parallel and Distributed Systems. Piscataway: IEEE, 2017:800-803.

[10] XUE Z Y, WANG M, ZHANG Q Y, et al. A Regulatable Blockchain Transaction Model with Privacy Protection[J] International Journal of Computational Intelligence Systems, 2021, 14(1):1642-1652.

[11] 赵晓琦, 李勇. 可审计且可追踪的区块链匿名交易方案[J]应用科学学报, 2021, 39(1):29-41. (ZHAO X Q, LI Y. Auditable and traceable blockchain anonymous transaction scheme[J]. Journal of Applied Sciences, 2021, 39(1): 29-41.)

[12] HILL A. BlockTorrent: A Blockchain Enabled Privacy-Preserving Data Availability Protocol for Multi-stakeholder Scenarios[C]// 2021 IEEE International Conference on Blockchain (Blockchain). Piscataway: IEEE, 2021:103-112.

[13] FENG T, PEI HM, MA R, et al. Blockchain data privacy access control based on searchable attribute encryption[J]. Computers, Materials& Continua, 2021, 66(1):871-890.

[14] QIAO K, TANG HB, YOU W. Blockchain Privacy Protection Scheme Based on Aggregate Signature[C]// 2019 IEEE 4th International Conference on Cloud Computing and Big Data Analysis (ICCCBDA). Piscataway: IEEE, 2019: 492-497.

[15] MEI Y R, GONG J, XIANG F, et al. A Blockchain Privacy Protection Scheme Based on Ring Signature.[J]. IEEE Access, 2020, 8:76765-76772.

[16] 汪金苗,谢永恒,王国威,等. 基于属性基加密的区块链隐私保护与访问控制方法[J]. 信息网络安全,2020, 20(9):47-51. (WANG J M, XIE Y H, WANG G W, et al. Blockchain privacy protection and access control method based on attribute-based encryption[J]. Information network security, 2020, 20(9): 47-51.)

[17] GUO F C, JIANG P, LIANG K T, et al. Searchain: Blockchain-based private keyword search in decentralized storage[J]. Future Generation Computer Systems, 2020, 107(2):781-792.

This work is partially supported by the state grid project (SGHAXTOOWWJS2200033).

MA Haifeng, born in 1977, Ph. D., associate professor. His research interests include Cloud computing security and blockchain security.

LI Yuxia, born in 1996, M. S. candidate. Her research interests include Blockchain and privacy protection.

XU Qingshui, born in 1971, Ph. D., professor. His research interests include Cyberspace security.

YANG Jiahai, born in 1966, Ph. D., professor. His research interests include internet management, network measurement and security.

GAO Yongfu, born in 1998, M. S. candidate. His research interests include Blockchain and privacy protection.