基于联盟链的身份环签密方案

俞惠芳* 吕芝蕊
(西安邮电大学网络空间安全学院 西安 710121)

摘 要：针对联盟链交易时存在的用户隐私泄露问题，该文提出基于联盟链的身份环签密(CB-IDRSC)方案。CB-IDRSC利用智能合约技术控制新交易加入，实现了公平可靠性；利用多个私钥生成器(PKGs)为用户生成私钥信息，满足联盟链部分去中心化要求和起到保护节点隐私的作用；并且具有机密性、不可伪造性和环签密者的无条件匿名性。性能分析中首先对CB-IDRSC中用到的智能合约进行部署；其次通过效率分析说明CB-IDRSC具有较高的计算效率；最后在忽略网络延时等因素影响的情况下，通过实验得出多私钥生成器的数量对系统参数生成和密钥生成阶段的效率影响不到3%。

关键词：身份环签密；联盟链；智能合约；多私钥生成中心
中图分类号：TN918; TP309 **文献标识码**：A **文章编号**：1009-5896(2023)03-0865-09
DOI: 10.11999/JEIT220284

Identity Ring SignCryption Based on Consortium Blockchain

YU Huifang LÜ Zhirui
(*School of Cyberspace, Xi'an University of Posts & Telecommunications, Xi'an* 710121, *China*)

Abstract: Focusing on the problem of user privacy leakage during consortium blockchain transactions, IDentity Ring SignCryption based on Consortium Blockchain (CB-IDRSC) is devised in this paper. CB-IDRSC uses the smart contract technology to control the addition of new transactions, and so realizes its fairness and reliability; It uses the multiple Private Key Generators (PKGs) to generate the private key information for users, and so satisfies the requirements of partial decentralization of consortium blockchain and can protect the node privacy; In addition, it has the confidentiality, unforgeability and unconditional anonymity of ring signcryptors. In performance analysis, the smart contract used in CB-IDRSC is firstly deployed, and high computation efficiency of CB-IDRSC is shown by efficiency analysis. By ignoring the influence of network delay and other factors, the experiments show the influence of the number of PKGs to efficiency of setup phase with key generation phase is less than 3%.

Key words: IDentity Ring SignCryption (IDRSC); Consortium blockchain; Smart contract; Multiple Private Key Generators (PKGs)

1 引言

中本聪研究团队提出的区块链技术[1]是具有公开透明性、不可篡改性、去中心化和共识确认等多种特性的分布式共享账本技术。按照应用范围区块链分为私有链、联盟链[2,3]和公有链。私有链基本属性有私密性和不可公开性；联盟链一般应用在成员权限各不相同的场景中[4]，比如支付、物流等场景。私有链、联盟链的节点数量和状态是可控的，数据读取与写入权限会受到限制。公有链向所有用户开放，没有权限的限定，所有人都可查看并使用公有链上的数据，具有完全公开透明的性质。联盟链是由多个用户共同参与管理交易记录的区块链，链中的数据只允许系统内的用户进行读写和发送，实现了去中心化。联盟链中节点用户产生的数据只有自己能看到，其他参与节点要获得交易数据必须得到数据拥有者授权的密钥，解决了区块链的数据隐私泄露等问题[5–7]。

智能合约[8]执行的各个环节中没有中间人角色，由计算机做监督和仲裁工作，共识机制判断合约是否需要按规定执行。这种无需第三方可信中心的形式，能有效确保交易的可追踪性与不可逆性，使联盟链上的交易不再依赖背书(链中验证并且声明交

收稿日期：2022-03-15；改回日期：2022-07-01；网络出版：2022-07-21
*通信作者： 俞惠芳 yuhuifang@xupt.edu.cn
基金项目：陕西省自然科学基础研究计划重点项目(2020JZ-54)
Foundation Item: The Key Project of Natural Science Basis Research Plan of Shannxi Province (2020JZ-54)

易是否合法的节点)。智能合约降低了用户在联盟链上的交易成本。联盟链与智能合约可以实现数据的去中心化共识存储、验证与计算[9]。

无可信中心环签名技术[10]不需要管理员和群成员的预定过程。环签名者随机获取多个成员组成一个用户集合，然后用环签名者私钥和环成员公钥得到环签名的结果，有效克服群签名中管理员权限过大的问题；接收者只知道消息由环中某成员签名，不确定真实签名者的身份，从而实现隐藏身份的作用[11,12]。融合环签名和加密可得到环签密[13–20]，环签密比起传统环签名后加密的方法减少了计算与通信成本。

为了增强用户在联盟链上进行交易和数据存储的安全性，本文提出基于联盟链的身份环签密(IDentity Ring SignCryption based on Consortium Blockchain, CB-IDRSC)，达到交易过程的隐私保护的目标。利用智能合约技术控制新交易节点的加入，无需可信中心。CB-IDRSC满足机密性、不可伪造性和环签密者的无条件匿名性。

2 基础知识

2.1 双线性映射

设q是一个大素数，G_1是具有q阶的加法循环群，G_2也是具有q阶乘法循环群，P是G_1的生成元，双线性映射e:$G_1\times G_1\to G_2$具有下列性质[21]：

(1) 双线性：对于任意的$a,b\in Z_q^*$和$P,Q\in G_1$，$e(aP,bP)=e(P,P)^{ab}$；

(2) 非退化性：存在$P,Q\in G_1$，使得$e(P,Q)\neq 1_{G2}$，其中1_{G2}代表G_2群的单位元；

(3) 可计算性：对于任意的$P,Q\in G_1$，存在一个有效的多项式时间算法计算$e(P,Q)$。

2.2 困难问题

双线性Diffie-Hellman(Bilinear Diffie-Hellman, BDH)问题：已知$(P,aP,bP,cP)\in G_1$，计算$e(P,P)^{abc}\in G_2$，其中$a,b,c\in Z_q^*$。

判定双线性Diffie-Hellman (Decision-al Bilinearity Diffie-Hellman, DBDH)问题：已知$(P,aP,bP,cP)\in G_1$和$\phi\in G_2$，判定是否$e(P,P)^{abc}=\phi$，其中$a,b,c\in Z_q^*$。如果等式成立，谕言机$\mathcal{O}_{\mathrm{DBDH}}$返回1；否则，$\mathcal{O}_{\mathrm{DBDH}}$返回0。

计算性Diffie-Hellman(Computation-al bilinear Diffie-Hellman, CDH)问题：已知$(P,aP,bP)\in G_1$，计算$abP\in G_1$，其中$a,b\in Z_q^*$。

3 形式化定义

3.1 CB-IDRSC算法模型

(1) 交易节点认证。为了保证新加入交易的真实性，设计交易节点判定智能合约。智能合约要求新交易在加入联盟链之前，需要向已经通过智能合约认证的节点发送请求，超过一半节点认同，该交易才能写入智能合约。智能合约的运行机制请见图1所示。

(2) 分配节点。联盟链节点有真实签密者、签密环成员、PKG群成员3种角色。

(3) 环签密算法。参数建立算法：输入一个安全参数1^k，输出系统主密钥x和系统公共参数β。

生成密钥算法：输入β和用户身份ID_i，输出用户ID_i的私钥S_i。

环签密算法：输入环成员身份集合$\varpi=\{\mathrm{ID}_i|i=1,2,\cdots,n\}$、消息$M$、环签密者$\mathrm{ID}_\mathrm{s}\in\varpi$的私钥$S_\mathrm{s}$、接收者$\mathrm{ID}_\mathrm{r}$的公钥$Q_\mathrm{r}$，输出密文$\delta$给接收者$\mathrm{ID}_\mathrm{r}$。

解签密：输入ID_r的私钥S_r、密文δ、$\varpi=\{\mathrm{ID}_i|i=1,2,\cdots,n\}$、环签密者$\mathrm{ID}_\mathrm{s}\in\varpi$的公钥$Q_\mathrm{s}$，输出明文$M$或符号$\perp$。

3.2 CB-IDRSC安全模型

定义1 假设任意多项式时间敌手A赢得游戏G1的优势可忽略，则称CB-IDRSC满足不可区分性。

G1：挑战者Γ首先运行参数设置算法得到(x,β)，输出系统公开参数β给A，保密主控钥x。然后，A对Γ发起一系列适应性询问。

$$\mathcal{O}_\Gamma^{\text{Private key}}(\mathrm{ID}_i)\xrightarrow{S_i}\mathrm{A};$$

$$\mathcal{O}_\Gamma^{\text{Signcryption}}(M,\mathrm{ID}_\mathrm{s},\mathrm{ID}_\mathrm{r},\varpi)\xrightarrow{\delta}\mathrm{A};$$

$$\mathcal{O}_\Gamma^{\text{Unsigncryption}}(\delta,\mathrm{ID}_\mathrm{s},\mathrm{ID}_\mathrm{r},\varpi)\xrightarrow{M/\perp}\mathrm{A}。$$

接下来，A询问等长消息$\{M_0,M_1\}$, ID_r^*, $\mathrm{ID}_\mathrm{s}^*=\{\mathrm{ID}_i|i=1,2,\cdots,n\}$的挑战密文。挑战前，A不能询问$\mathrm{ID}_\mathrm{r}^*$的私钥，也不能替换$\mathrm{ID}_\mathrm{r}^*$的公钥。Γ选择任意的$\mu\in\{0,1\}$，最后返回消息$M_\mu$的挑战密文$\delta^*$给A。

A再次发出一系列适应性询问。A不能询问ID_r^*的私钥，也不能针对$(\mathrm{ID}_\mathrm{s}^*,\mathrm{ID}_\mathrm{r}^*,\delta^*)$询问解签密谕言机。

最后，A输出μ的一个猜测μ^*，如果A赢得G1，需要$\mu^*=\mu^*$。A的成功优势：$\mathrm{Adv}^{\mathrm{G1}}(\mathrm{A},k)=|\Pr[\mu^*=\mu]-1/2|$。

定义2 假设任意多项式时间伪造者F赢得游戏G2的优势是可忽略的，则称CB-IDRSC满足不可伪造性。

G2：Γ首先输出运行参数设置算法得到的(x,β)给F。然后，F对Γ发起与G1第1阶段完全相同的适应性询问。

最后，F输出伪造的密文δ^*给Γ。F不能查询

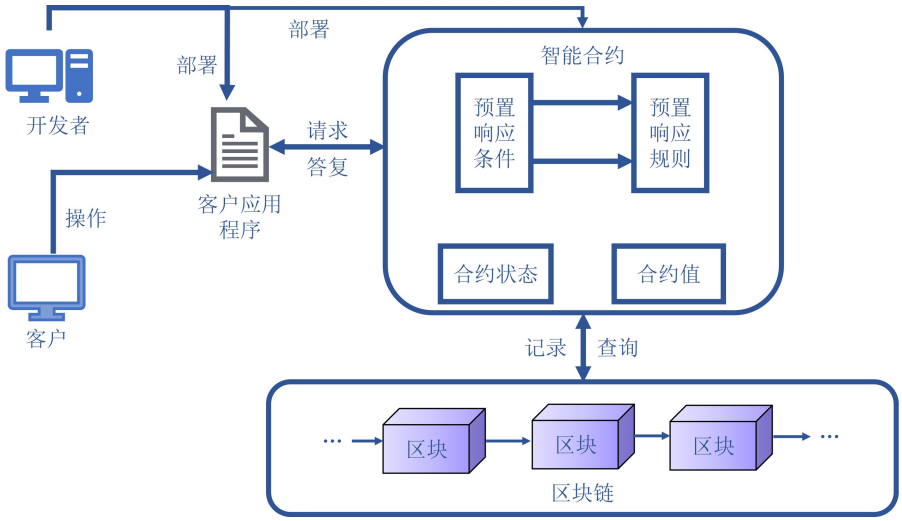

图 1 智能合约运行机制

ϖ中任何成员私钥，$\mathrm{ID}_s^* \in \varpi$的公钥不能替换，$\delta^*$不能是$(\mathrm{ID}_s^*, \mathrm{ID}_r^*, M^*)$的应答。

如果解签密结果不是符号$\perp$，F赢得G2。F的优势是赢得G2的概率。

4　CB-IDRSC具体实例

4.1　交易节点认证

假设智能合约(Transaction Node Smart Contract, TNSC)中存在$2N$个交易节点，每次新交易加入联盟链的时候，至少需要TNSC中N个节点的验证通过，TNSC符号说明请见表1，具体交易节点认证请见流程1。

4.2　节点构成

在基于联盟链的身份签密(CB-IDRSC)方案中，参与环签密的联盟链节点有签密者、签密环成员、PKG群成员3种角色。节点交互过程请见图2。

(1) 签密者ID_s：CB-IDRSC中签密的节点用户，可向联盟链系统请求签密环成员和PKG群成员。

(2) 签密环：签密者ID_s从联盟链当中随机选出的多个节点用户。环成员用于辅助环签密者ID_s对消息进行签密操作，这些环成员不知道需要签密消息的具体内容。

(3) PKG群成员：PKG群成员是从联盟链中随机选出的多个节点，用于选择初始化参数，生成用户密钥，PKG群成员不知道签密消息的具体内容。

4.3　环签密方案

4.3.1　设置参数算法

给定一个安全参数k，$q \geq 2^k$是素数，G_1是q阶的加法循环群，G_2是q阶的乘法循环群，P是G_1的生成元，$e: G_1 \times G_2 \to G_2$是双线性映射。$H_1: \{0,1\}^* \to G_1$，$H_2: G_2 \to \{0,1\}^l$，$H_3: \{0,1\}^l \times G_1 \times G_1 \times G_2 \to {Z_q}^*$是安全的哈希函数，$l$表示消息长度，$\mathrm{ID}_i$是用户身份，消息空间为$\Omega=\{0,1\}^l$。PKG群中的节点独立选取私钥$x_j \in {}_R{Z_q}^*$，计算相应公钥$y_j=x_jP$(如果$y_j$重复，分别重新选取私钥$x_j$)，PKG群集合$U=\{\mathrm{PKG}_j | j=1,2,\cdots,m\}$。系统公钥$y=P\sum_{j=1}^{m} x_j$，对于第$j$个节点$\mathrm{PKG}_j$存在$U=\{\mathrm{PKG}_j|$

表 1　智能合约符号说明

符号	含义	符号	含义
NewN	新的交易节点	$\mathrm{ID}_{\mathrm{NewN}}$	新节点地址
OldN	旧的交易节点	O_NVer	旧节点验证新节点
M	通过验证的节点	$\mathrm{Tx}_{\mathrm{NewN}}$	新节点的交易
$\mathrm{Inf}_{\mathrm{NewN}}$	新节点信息	$\mathrm{Pri}_{\mathrm{NewN}}$	新节点的密钥

流程1　交易节点认证

输入：NewN, OldN, $2N$，M=0
输出：TNSC
打包新交易节点信息：
　$\mathrm{Data}_{\mathrm{NewN}}=(\mathrm{Inf}_{\mathrm{NewN}},\mathrm{ID}_{\mathrm{NewN}})$
新交易调用智能合约：
　$\mathrm{Tx}_{\mathrm{NewN}}=(H(\mathrm{Data}_{\mathrm{NewN}}),\mathrm{Pri}_{\mathrm{NewN}})$
旧节点对新节点进行验证：
　while $M<N$ do
　for(k=0; $k<N$; k++)
　if O_Nver=1
　M++
　end
　end
　end
　TNSC添加新节点信息：
　TNSC+=$(\mathrm{Inf}_{\mathrm{NewN}},\mathrm{ID}_{\mathrm{NewN}})$
　return TNSC

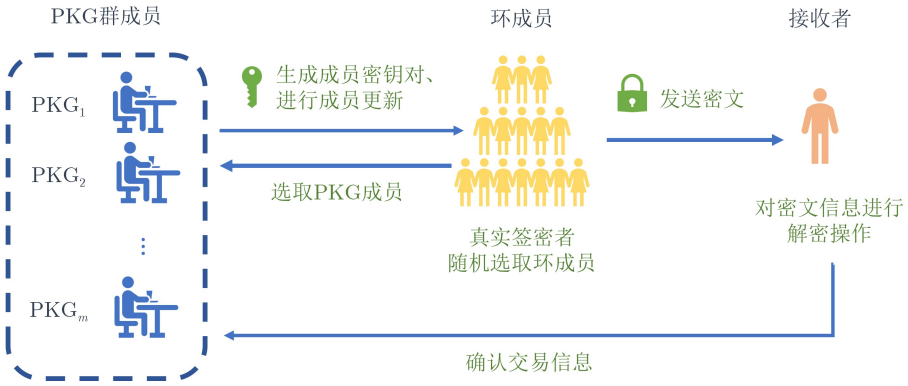

图 2 方案节点交互流程图

$j=1,2,\cdots,m\}$。系统公开全局参数β=$\{G_1$,G_2,q,P,e,y_j,H_1,H_2,$H_3\}$。

4.3.2 生成密钥算法

令$\varpi=\{\mathrm{ID}_i|i=1,2,\cdots,n\}$表示环成员身份的集合。生成密钥的算法为

(1) 用户计算公钥Q_i=$H(\mathrm{ID}_i)$；

(2) PKG_j计算$B_{ij}=Q_ix_j$，环成员ID_i的私钥$B_i=\sum_{j=1}^{m}B_{ij}$；环签密者ID_s通过x_j对私钥B_i发出上传请求。如果$B_iP=Q_i\sum_{j=1}^{m}x_jP=Q_iy$，保存$B_i$作为合约参数；否则，拒绝接收。

(3) PKG_j计算$B_{rj}=Q_rx_j$，接收者ID_r的私钥$B_r=\sum_{j=1}^{m}B_{rj}$。

4.3.3 环签密算法

环签密者ID_s生成密文的算法为

(1) 选取$d\in_RZ_q^*$，计算：

$$R=d\cdot P,\ R_m=e(y,Q_r)^d$$

(2) 计算$C=M\oplus H_2(R_m)$。

(3) 选取$u_i\in_RG_1$，$i\in\{1,2,\cdots,n\}(i\neq s)$，计算$h_i=H_3(M\parallel\mathrm{ID}_i\parallel u_i\parallel R_m)$；$i$=$s$时，计算：

$$u_s=Q_s\cdot d-\sum_{i=1,i\neq s}^{n}(u_i+h_i\cdot Q_i)$$

$$h_s=H_3(M\parallel\mathrm{ID}_s\parallel u_s\parallel R_m)$$

(4) 计算$V=(h_s+d)\sum_{j=1}^{m}B_{sj}$。

(5) 输出密文$\delta=(C,V,\cup_{i=1}^{n}\{u_i\},R)$。

(6) 环签密者ID_s请求将密文δ上传到TNSC的账号上。

4.3.4 解签密算法

接收者ID_r依据δ，进行如下操作

(1) 计算$R_m=e\left(R,\sum_{j=1}^{m}B_{rj}\right)$。

(2) 计算$M=C\oplus H_2(R_m)$。

(3) 计算$h_i=H_3(M\parallel\mathrm{ID}_i\parallel u_i\parallel R_m)$。

(4) 如果

$$e(P,V)=e\left(y,\sum_{i=1}^{n}(u_i+h_iQ_i)\right)$$

接收者ID_r接受明文M，TNSC公布交易，将交易信息并入新的区块；否则，认为密文δ无效，TNSC拒绝公布该交易。

4.3.5 更新系统参数

系统需要更新参数的时候，PKG群中的节点重新独立选取$x'_j\in_RZ_q^*$，计算公钥y'_j=x'_jP，新的系统公钥$y'=P\sum_{j=1}^{m}x'_j$，新的PKG群集合$U'=\{\mathrm{PKG}'_j|j=1,2,\cdots,m\}$，则对于第$j$个节点$\mathrm{PKG}'_j$存在

$$\mathrm{PKG}'_j=\{(y'_j,x'_j)\,|j=1,2,\cdots,m\}$$

然后PKG'_j调用密钥生成算法，为用户更新密钥对信息并保留使用过的系统参数。

4.4 正确性分析

从下面推导过程可以看出，本文提出的CB-IDRSC是正确的。

$$\begin{aligned}R'_m=&e\left(R,\sum_{j=1}^{m}B_{rj}\right)=e\left(d\cdot P,Q_r\cdot\sum_{j=1}^{m}x_j\right)\\=&e\left(P\cdot\sum_{j=1}^{m}x_j,Q_r\right)^d=e(y,Q_r)^d=R_m\end{aligned}$$

$$\begin{aligned}e(P,V)=&e\left(P,(d+h_s)\sum_{j=1}^{m}B_{sj}\right)\\=&e\left(P,(d+h_s)Q_s\sum_{j=1}^{m}x_j\right)\\=&e\left(y,\sum_{i=1,i\neq s}^{m}(u_i+h_i\cdot Q_i)+u_s+h_sQ_s\right)\\=&e\left(y,\sum_{i=1}^{n}(u_i+h_i\cdot Q_i)\right)\end{aligned}$$

5　CB-IDRSC安全性证明

5.1 保密性

定理1　随机谕言模型下敌手A经过q_i次H_i谕言机(i=1,2,3)询问、q_{F}次私钥谕言机询问、q_{s}次签密谕言机询问、q_{u}次解签密谕言机询问后，能证明底层身份环签密具有机密性，则说明CB-IDRSC同样具有机密性。令A区分CB-IDRSC密文的优势为ε，则Γ解决DBDH问题的优势$\varepsilon'\geq\varepsilon/eq_2q_{\mathrm{F}}$。

证明　Γ收到DBDH问题随机实例$(P,aP,bP,cP,\phi\in G_2)$,目标在于计算$\phi=e(P,P)^{abc}$。G1中A扮演挑战者Γ的子程序。q_1表示A询问H_1谕言机的次数，询问任何谕言机前A首先发出针对ID_i的H_1询问。整数$\alpha\in\{1,2,\cdots,q_1\}$，$\phi$是$\mathrm{ID}_i=\mathrm{ID}_\alpha$的概率，$\mathrm{ID}_\alpha$表示挑战的目标身份，Γ不能泄露$\alpha$的值给A。

游戏开始时，Γ运行参数设置算法得到系统参数$\beta(y=aP)$，输出β给A。然后，A对Γ发起多项式有界次适应性询问。

H_1询问：A询问ID_i的哈希值。如果起初为空的列表L_1中存在询问内容，Γ输出Q_i给A；否则，Γ应答如下：

如果$\mathrm{ID}_i=\mathrm{ID}_\alpha$，Γ输出$Q_i\leftarrow bP$，添加$(\mathrm{ID}_i,Q_i,-)$到$L_1$。否则，Γ随机选取$l_i\in Z_q^*$，输出$Q_i\leftarrow l_iP$，添加$(\mathrm{ID}_i,Q_i,l_i)$到$L_1$中。

H_2询问：A发出H_2询问，Γ输出$r\in_R\{0,1\}^l$，添加(R,R_m,r)到初始为空的列表L_2中。

H_3询问：A发出H_3询问，Γ输出任意的$h_i\in Z_q^*$，添加$(M||\mathrm{ID}_i||u_i||R_m,h_i)$到初始为空的列表$L_3$中。

私钥询问：Γ收到ID_i的私钥询问。若$\mathrm{ID}_i=\mathrm{ID}_\alpha$，Γ终止游戏；否则，查询$L_1$得到$(\mathrm{ID}_i,Q_i,l_i)$，Γ计算$S_i\leftarrow l_iaP$，添加$(\mathrm{ID}_i,u_i,B_i)$到初始为空的列表$L_k$中。

环签密询问：Γ收到$(M,\varpi,\mathrm{ID}_{\mathrm{s}},\mathrm{ID}_{\mathrm{r}})$的环签密询问。如果$\mathrm{ID}_{\mathrm{s}}\neq\mathrm{ID}_\alpha$，Γ正常调环签密算法，输出得到的密文；否则，Γ响应如下：

(1) 随机选取$d\in Z_q^*$，计算：

$$R=d\cdot P-b\cdot P,\ R_m=e(R,B_{\mathrm{r}})$$

(2) 计算$C=M\oplus H_2(R_m)$。

(3) 选取$u_i\in_R G_1$，$i\in\{1,2,\cdots,n\}(i\neq s)$，计算$h_i=H_3(M\parallel\mathrm{ID}_i\parallel u_i\parallel R_m)$。

(4) 计算$V=daP$。

(5) $i=s$时，随机选取$h_s\in Z_q^*$，计算：

$$u_s=d\cdot P-h_{\mathrm{s}}Q_{\mathrm{s}}-\sum_{i=1,i\neq s}^{n}(u_i+h_i\cdot Q_i)$$

$$h_{\mathrm{s}}=H_3(M\parallel\mathrm{ID}_s\parallel u_s\parallel R_m)$$

(6) 存储$(M||\mathrm{ID}_{\mathrm{s}}||u_s||R_m,h_s)$到列表$L_3$。

(7) 输出密文$\delta=(C,V,\cup_{i=1}^n\{u_i\},R)$。

A通过下列等式验证密文δ的有效性：

$$\begin{aligned}&e\left(y,\sum_{i=1}^{n}(u_i+h_iQ_i)\right)\\&=e\left(aP,\sum_{i=1,i\neq s}^{n}(u_i+h_iQ_i)+u_{\mathrm{s}}+h_{\mathrm{s}}Q_{\mathrm{s}}\right)\\&=e(aP,dP)\\&=e(P,V)\end{aligned}$$

解签密询问：A对密文δ做解签密询问。如果$\mathrm{ID}_{\mathrm{r}}\neq\mathrm{ID}_\alpha$，Γ正常运行解签密算法输出运行结果；否则，Γ回应如下：

(1) 检索L_1得到$Q_{\mathrm{r}}\leftarrow bP$。

(2) 检索L_2得到不同R_m值使A在询问(R,y,Q_{r},R_m)时，$\mathcal{O}_{\mathrm{DBDH}}$返回1。如果有这种情况，计算$M=C\oplus H_2(R_m)$。

(3) 调用H_1,H_3谕言机得到Q_i,u_i,h_i，若$e(P,V)=e\left(y,\sum_{i=1}^{n}(u_i+h_iQ_i)\right)$，Γ输出$M$给A；否则，Γ输出⊥给A。

接下来，A发出对$(\{M_0,M_1\},\varpi,\mathrm{ID}_{\mathrm{s}}^*,\mathrm{ID}_{\mathrm{r}}^*)$的挑战询问，$\{M_0,M_1\}$长度相等。限制在于阶段1中A不能询问$\mathrm{ID}_r^*$的私钥。如果$\mathrm{ID}_{\mathrm{r}}^*\neq\mathrm{ID}_\alpha$，Γ停止游戏；否则，Γ随机选择$\mu\in\{0,1\}$，$\phi\in G_2$，设置$R^*\leftarrow cP$，从$L_1$得到$Q_{\mathrm{r}}^*\leftarrow bP$，然后继续回应如下：

(1) 选取$u_i^*\in_R G_1$，$i\in\{1,2,\cdots,n\}(i\neq s)$，计算$h_i=H_3(M_\mu\parallel\mathrm{ID}_i\parallel u_i\parallel\phi)$。

(2) 计算$C^*=M\oplus H_2(\phi)$;

(3) 计算：

$$u_s^*=l_s^*\cdot R^*-\sum_{i=1,i\neq s}^{n}(u_i^*+h_i^*\cdot l_i^*P)$$

$$h_{\mathrm{s}}^*=H_3\left(M_\mu\parallel\mathrm{ID}_{\mathrm{s}}^*\parallel u_{\mathrm{s}}^*\parallel\phi\right)$$

(4) 计算$V=h_{\mathrm{s}}^*\sum_{j=1}^{m}B_{sj}^*+\sum_{j=1}^{m}x_j^*l_s^*R^*$;

(5) 输出$\delta^*=(C^*,V^*,\cup_{i=1}^n\{u_i\},R^*)$。

A再次发出像第1阶段那样的适应性询问。A不能询问$\mathrm{ID}_{\mathrm{r}}^*$的私钥，A也不能针对挑战密文$\delta^*$询问解签密谕言机。最后，Γ输出DBDH问题的解答实例：

$\phi=e(y,Q_{\mathrm{r}}^*)^d=e(aP,bP)^c=e(P,P)^{abc}$

概率评估：Γ挑战不失败的情况下才能解决DBDH问题。Γ在阶段1或2中不失败概率是$\varphi^{q_{\mathrm{F}}}$，挑战中不失败的概率是$1-\varphi$。则Γ在游戏中不失败的

概率是$\varphi^{q_F}(1-\varphi)$，其值在φ=1–(1/(1+q_F))时达到最大。Γ在游戏中不失败的概率至少是$1/eq_F$，即

$$\varphi^{q_F}(1-\varphi)=\left(1-\frac{1}{1+q_F}\right)^{(1+q_F)}\frac{1}{q_F}\geq\frac{1}{eq_F}$$

Γ均匀随机选择ϕ的概率至少是$1/q_2$。因此，Γ得到DBDH问题实例解答的概率至少为ε/eq_2q_F。对充分大的q_2,q_F，Γ在游戏中取得成功的概率可忽略。 证毕

5.2 不可伪造性

定理2 在随机谕言模型下能证明底层的身份环签密具有不可伪造性，则说明CB-IDRSC同样具有不可伪造性。如果伪造者F能以优势ε攻破CB-IDRSC的密文，则Γ解决CDH问题的优势$\varepsilon'\geq\varepsilon/eq_F$。

证明 Γ收到CDH问题的随机实例$(aP,bP)\in G_1$，目标在于计算$abP\in G_1$。G2中Γ扮演子程序F的挑战者。

游戏开始时，Γ运行设置算法得到系统参数$\beta(y=aP)$，发送β给F。然后，F对Γ发出跟**定理1**中第1阶段相同的询问。

最后，F给挑战者Γ输出伪造密文$\delta^*=(C^*,V^*,\cup_{i=1}^n\{u_i^*\},R^*)$。F不能查询$\mathrm{ID}_s^*$的私钥。如果$\mathrm{ID}_s^*\neq\mathrm{ID}_\alpha$，Γ放弃游戏；否则，Γ在多项式时间内得到CDH问题实例解答$abP=V^*/(d+h_s^*)$。如果Γ利用F取得成功，必然成立公式

$$\begin{aligned}e\left(P,V^*\right)&=e\left(P,(d+h_s^*)Q_s^*\sum_{j=1}^m x_j^*\right)\\&=e\left(y,(d+h_s^*)\,bP\right)\\&=e\left(P,(d+h_s^*)\,abP\right)\end{aligned}$$

概率评估：Γ挑战不失败的情况下才能解决CDH问题。依据**定理1**的概率评估可得，Γ在G_2中不失败的概率至少是$1/eq_F$。故Γ得到CDH问题实例解答的概率至少是ε/eq_F。对充分大的q_F，Γ取得胜利的概率是可忽略的。 证毕

5.3 无条件匿名性

定理3 CB-IDRSC满足环签密者的无条件匿名性。

证明 d是从Z_q^*随机选择的，$R=dP$也是随机的；C是消息M和Hash的异或运算得到的，所以C是等概率分布的。$u_i\in G_2$是随机选择的，h_i是哈希函数，因此，u_s,V是等概率分布的。综上所述，密文$\delta=(C,V,\cup_{i=1}^n\{u_i\},R)$的各部分都是等概率分布的，因此，能够准确确定真实签密者的概率不会超过$1/n$。因此，CB-IDRSC满足环签密者的无条件匿名性。 证毕

6 性能分析

仿真实验所使用计算机主要性能参数为：Windows 10 操作系统，CPU 1.80 GHz，内存16 GB。智能合约部署选择以太坊官网提供的合约编译器：Browser-solidity，关键参数请见表2，合约的地址为：0x5B38Da6a701c568545dCfcB03FcB875f56beddC4，签密者地址0xf8e81D47203A594245E36C48e151709F0C19fBe8。

本节依据计算时间成本比较CB-IDRSC和文献[19,20,22,23]中的方案。每个方案特征比较请见表3。

通过Visual C++编译软件通过调用PBC库，得到主要密码操作运行1次所需的计算时间请见表4。

每个对比方案在环签密和解签密时的计算时间比较情况请见表5。

为了更加方便直观对运行效率进行对比，采用Origin软件针对比较方案的计算时间进行相关的仿真实验，实验中n表示环成员的个数，m表示在系统设置时选择的PKG个数。从图3和图4可以看出，随着环成员个数的增加，对比方案的环签密和

表 2 智能合约部署的关键参数

名称	参数
chainid	0xd05
gaslimit	160000000
timestamp	1638087433
block.number	7

表 3 各方案的特征比较

方案	不可伪造性	机密性	生成密钥方式	是否适合联盟链
方案1[19]	√	√	密钥生成中心	×
方案2[20]	√	√	密钥生成中心	×
方案3[22]	√	√	密钥生成中心	×
方案4[23]	√	√	密钥生成中心	×
CB-IDRSC	√	√	多私钥生成中心	√

表 4 各密码操作的计算时间(ms)

符号	执行操作	所需时间
T_{H}	1次哈希运算	11.71
T_{mul}	1次标量乘法运算	0.03
T_{ec}	1次指数运算	5.00
T_{bp}	1次双线性对运算	15.23
T_{I}	1次逆运算	1.52

表 5　环签密与解签密的时间比较(ms)

方案	环签密的计算时间	解签密的计算时间
方案1[19]	$(2n+4)T_H+T_{bp}+T_{ec}+(n+9)T_{mul}$	$(n+3)T_H++T_{bp}+T_{ec}+3T_{mul}$
方案2[20]	$(n+4)T_H+T_{bp}+2nT_{mul}$	$(n+2)T_H+3T_{bp}+nT_{mul}+T_I$
方案3[22]	$(n+1)T_H+T_{bp}+2nT_{ec}+2nT_{mul}$	$(n+2)T_H+5T_{bp}+2nT_{mul}$
方案4[23]	$(2n+2)T_H+T_{bp}+(3n+1)T_{mul}$	$(2n+1)T_H+4T_{bp}+2nT_{mul}$
CB-IDRSC	$(n+1)T_H+T_{bp}+nT_{mul}$	$(n+1)T_H+3T_{bp}$

解签密操作所消耗的时间均呈现线性增长，CB-IDRSC的增长的趋势相对平缓一些。从图5可以看出，CB-IDRSC具有更小的计算开销。

CB-IDRSC是多PKG方案，会影响到系统参数设置阶段与密钥生成阶段的执行效率。为了确认多PKG方案针对CB-IDRSC计算成本的影响是可忽略的，在实验中假定环签密成员数为10。从图6的实验结果看，PKG个数m从30增加到70的时候，多PKG方案对系统参数设置阶段和密钥生成阶段的效率影响不超过3%。

7　结束语

联盟链凭借交易成本低、节点连接稳定、受特定群体控制等特性为物联网、银行、金融、医疗等行业提供重要的技术支撑，但其部分去中心化结构也带来用户隐私泄露的隐患。在这个工作中，提出基于联盟链的身份环签密方案，通过将真实签密者隐藏在多个环成员中的方法，使得用户身份信息和联盟链账号地址之间的关联性降低，从而达到保护用户隐私的目的。

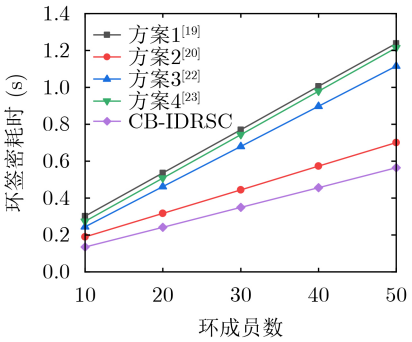

图 3 环签密耗时比较图

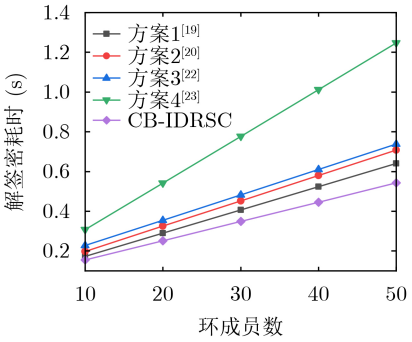

图 4 解签密耗时比较

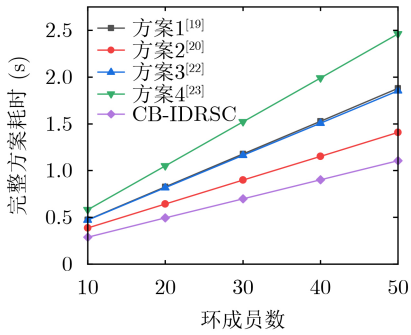

图 5 完整方案耗时比较

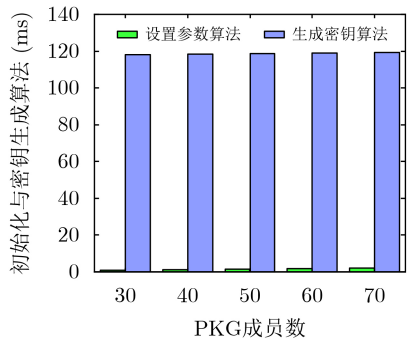

图 6 初始化与密钥生成阶段的执行时间

参 考 文 献

[1] 姚前, 张大伟. 区块链系统中身份管理技术研究综述[J]. 软件学报, 2021, 32(7): 2260–2286. doi: 10.13328/j.cnki.jos.006309.
YAO Qian and ZHANG Dawei. Survey on identity management in blockchain[J]. *Journal of Software*, 2021, 32(7): 2260–2286. doi: 10.13328/j.cnki.jos.006309.

[2] 张慧茹, 汪美荃, 李光顺. 区块链安全与隐私保护前沿技术发展现状[J]. 信息技术与网络安全, 2021, 40(5): 7–12. doi: 10.19358/j.issn.2096-5133.2021.05.002.
ZHANG Huiru, WANG Meiquan, and LI Guangshun. The development status of frontier technology of blockchain

security and privacy protection[J]. *Information Technology and Network Security*, 2021, 40(5): 7-12. doi: 10.19358/j.issn.2096-5133.2021.05.002.

[3] 姚英英, 常晓林, 甄平. 基于区块链的去中心化身份认证及密钥管理方案[J]. 网络空间安全, 2019, 10(6): 33–39. doi: 10.3969/j.issn.1674-9456.2019.06.007.

YAO Yingying, CHANG Xiaolin, and ZHEN Ping. Decentralized identity authentication and key management scheme based on blockchain[J]. *Cyberspace Security*, 2019, 10(6): 33–39. doi: 10.3969/j.issn.1674-9456.2019.06.007.

[4] 李佩丽, 徐海霞, 马添军. 区块链隐私保护与监管技术研究进展[J]. 信息安全学报, 2021, 6(3): 159–168. doi: 10.19363/J.cnki.cn10-1380/tn.2021.05.10.

LI Peili, XU Haixia, and MA Tianjun. Research progress of blockchain privacy protection and supervision technology[J]. *Journal of Cyber Security*, 2021, 6(3): 159–168. doi: 10.19363/J.cnki.cn10-1380/tn.2021.05.10.

[5] 孟小峰, 刘立新. 基于区块链的数据透明化: 问题与挑战[J]. 计算机研究与发展, 2021, 58(2): 237–252. doi: 10.7544/issn1000-1239.2021.20200017.

MENG Xiaofeng and LIU Lixin. Blockchain-based data transparency: Issues and challenges[J]. *Journal of Computer Research and Development*, 2021, 58(2): 237–252. doi: 10.7544/issn1000-1239.2021.20200017.

[6] KOSBA A, MILLER A, SHI E, *et al*. Hawk: The blockchain model of cryptography and privacy-preserving smart contracts[C]. 2016 IEEE Symposium on Security and Privacy (SP), San Jose, USA, 2016: 839–858. doi: 10.1109/SP.2016.55.

[7] 田国华, 胡云瀚, 陈晓峰. 区块链系统攻击与防御技术研究进展[J]. 软件学报, 2021, 32(5): 1495–1525. doi: 10.13328/j.cnki.jos.006213.

TIAN Guohua, HU Yunhan, and CHEN Xiaofeng. Research progress on attack and defense techniques in block-chain system[J]. *Journal of Software*, 2021, 32(5): 1495–1525. doi: 10.13328/j.cnki.jos.006213.

[8] 欧阳丽炜, 王帅, 袁勇, 等. 智能合约: 架构及进展[J]. 自动化学报, 2019, 45(3): 445–457. doi: 10.16383/j.aas.c180586.

OUYANG Liwei, WANG Shuai, YUAN Yong, *et al*. Smart contracts: Architecture and research Progresses[J]. *Acta Automatica Sinica*, 2019, 45(3): 445–457. doi: 10.16383/j.aas.c180586.

[9] 陈思吉, 翟社平, 汪一景. 一种基于环签名的区块链隐私保护算法[J]. 西安电子科技大学学报, 2020, 47(5): 86–93. doi: 10.19665/j.issn1001-2400.2020.05.012.

CHEN Siji, ZHAI Sheping, and WANG Yijing. Blockchain privacy protection algorithm based on ring signature[J]. *Journal of Xidian University*, 2020, 47(5): 86–93. doi: 10.19665/j.issn1001-2400.2020.05.012.

[10] SINGH S, SATISH D, and LAKSHMI S R. Ring signature and improved multi-transaction mode consortium blockchain-based private information retrieval for privacy-preserving smart parking system[J]. *International Journal of Communication Systems*, 2021, 34(14): e4911. doi: 10.1002/dac.4911.

[11] ZHAO Kaixin, SUN Dong, REN Gang, *et al*. Public auditing scheme with identity privacy preserving based on certificateless ring signature for wireless body area networks[J]. *IEEE Access*, 2020, 8: 41975–41984. doi: 10.1109/ACCESS.2020.2977048.

[12] WANG Lingling, LIN Xiaodong, QU Lijun, *et al*. Ring selection for ring signature-based privacy protection in VANETs[C]. ICC 2020–2020 IEEE International Conference on Communications (ICC), Dublin, Ireland, 2020: 1–6. doi: 10.1109/ICC40277.2020.9149247.

[13] YU Huifang, LIU Junze, WANG Zhicang, *et al*. Certificateless ring signcryption for multi-source network coding[J]. *Computer Standards & Interfaces*, 2022, 81: 103602. doi: 10.1016/j.csi.2021.103602.

[14] GUPTA P and KUMAR M. A verifiable ring signature scheme of anonymous signcryption using ECC[J]. *International Journal of Mathematical Sciences and Computing*, 2021, 7(2): 24–30. doi: 10.5815/ijmsc.2021.02.03.

[15] YU Huifang, WANG Weike, and ZHANG Qi. Certificateless anti-quantum ring signcryption for network coding[J]. *Knowledge-Based Systems*, 2022, 235: 107655. doi: 10.1016/j.knosys.2021.107655.

[16] ZHANG Shaomin, ZHENG Tengfei, and WANG Baoyi. A privacy protection scheme for smart meter that can verify terminal's trustworthiness[J]. *International Journal of Electrical Power & Energy Systems*, 2019, 108: 117–124. doi: 10.1016/j.ijepes.2019.01.010.

[17] YU Huifang, BAI Lu, HAO Ming, *et al*. Certificateless signcryption scheme from lattice[J]. *IEEE Systems Journal*, 2021, 15(2): 2687–2695. doi: 10.1109/JSYST.2020.3007519.

[18] GUO Hui and DENG Lunzhi. Certificateless ring signcryption scheme from pairings[J]. *International Journal of Network Security*, 2020, 22(1): 102–111.

[19] ZHANG Shaomin, RONG Jieqi, and WANG Baoyi. A privacy protection scheme of smart meter for decentralized smart home environment based on consortium blockchain[J]. *International Journal of Electrical Power &*

Energy Systems, 2020, 121: 106140. doi: 10.1016/j.ijepes.2020.106140.

[20] CAI Ying, ZHANG Hao, and FANG Yuguang. A conditional privacy protection scheme based on ring signcryption for vehicular *Ad Hoc* networks[J]. *IEEE Internet of Things Journal*, 2021, 8(1): 647–656. doi: 10.1109/JIOT.2020.3037252.

[21] ZHOU Caixue, GAO Guangyong, CUI Zongmin, *et al*. Certificate-based generalized ring signcryption scheme[J]. *International Journal of Foundations of Computer Science*, 2018, 29(6): 1063–1088. doi: 10.1142/S0129054118500211.

[22] FENF Tao and LIU Ningning. A sensitive information protection scheme in named data networking using attribute-based ring-signcryption[C]. 2017 IEEE Second International Conference on Data Science in Cyberspace (DSC), Shenzhen, China, 2017: 187–194. doi: 10.1109/DSC.2017.67.

[23] 赵楠, 章国安. VANET中基于无证书环签密的可认证隐私保护方案[J]. 计算机科学, 2020, 47(3): 312–319. doi: 10.11896/jsjkx.19010115.

ZHAO Nan and ZHANG Guoan. Authenticated privacy protection scheme based on certificateless ring signcryption in VANET[J]. *Computer Science*, 2020, 47(3): 312–319. doi: 10.11896/jsjkx.19010115.

俞惠芳：女，博士，教授，研究方向为密码理论与信息安全.

吕芝蕊：女，硕士生，研究方向为区块链密码理论和格密码理论.

责任编辑：马秀强