Journal of Computer Applications
计算机应用, 2020, 40(9): 2639 - 2645
ISSN 1001-9081
CODEN JYIIDU
2020-09-10
http://www.joca.cn

文章编号:1001-9081(2020)09-2639-07
DOI:10.11772/j.issn.1001-9081.2020010096

基于安全多方的区块链可审计签名方案

王韫烨[1],程亚歌[1*],贾志娟[1],付俊俊[1],杨艳艳[1],何宇矗[1],马　威[2]
(1. 郑州师范学院 信息科学与技术学院,郑州 450044; 2. 华北水利水电大学 信息工程学院,郑州 450044)
(*通信作者电子邮箱13676951984@163.com)

摘　要:针对可信问题,提出了一种基于安全多方的区块链可审计签名方案。该方案引入了带有时间戳的信任向量,并构建由多维向量组构成的信任矩阵用以定期记录参与者的可信行为,从而为参与者建立一种可信的评估机制,最后将评估结果存储到区块链中作为查证的依据。在确保参与者可信的前提下,通过秘密共享技术构建了安全可信的签名方案。安全分析表明,该方案可以有效减少恶意参与者带来的破坏,可检测参与者的可信度,并可以抵抗移动攻击。性能分析表明,该方案具有较低的计算复杂度和较高的执行效率。

关键词:安全多方计算;区块链;可审计签名方案;信任机制;秘密共享
中图分类号:TP393.08　　**文献标志码:**A

Auditable signature scheme for blockchain based on secure multi-party

WANG Yunye[1], CHENG Yage[1*], JIA Zhijuan[1], FU Junjun[1], YANG Yanyan[1], HE Yuchu[1], MA Wei[2]
(1. *School of Information Science and Technology, Zhengzhou Normal University, Zhengzhou Henan* 450044, *China*;
2. *College of Information Engineering, North China University of Water Resources and Electric Power, Zhengzhou Henan* 450044, *China*)

Abstract: Aiming at the credibility problem, a secure multi-party blockchain auditable signature scheme was proposed. In the proposed scheme, the trust vector with timestamp was introduced, and a trust matrix composed of multi-dimensional vector groups was constructed for regularly recording the trustworthy behavior of participants, so that a credible evaluation mechanism for the participants was established. Finally, the evaluation results were stored in the blockchain as a basis for verification. On the premise of ensuring that the participants are trusted, a secure and trusted signature scheme was constructed through secret sharing technology. Security analysis shows that the proposed scheme can effectively reduce the damages brought by the malicious participants, detect the credibility of participants, and resist mobile attacks. Performance analysis shows that the proposed scheme has lower computational complexity and higher execution efficiency.

Key words: Secure Multi-party Computation (SMC); blockchain; auditable signature scheme; trust mechanism; secret sharing

0　引言

安全多方计算(Secure Multi-party Computation, SMC)是密码学中一个非常活跃的学术领域,具有很强的理论和实践意义。概括地说,所有的加密协议都是安全多方计算的特例。它在数据挖掘、统计分析、隐私保护和机密电子投票等方面起着重要作用。它由Yao[1]在1980年首次提出,是百万富翁问题的扩展。后经过Goldreich等[2]的广泛研究,安全多方计算已成为国际密码学的研究热点。

安全多方可以在没有可信第三方的条件下,解决一些由多人共同参与的棘手问题,具有很重要的现实意义。然而在实际执行中,安全多方协议的参与者存在诚实、半诚实和恶意三种类型的参与者。这对协议的执行带来了一定的困扰,为提高参与者的可信度,针对参与者的行为进行信任评估具有很重要的研究意义。

在基于信任机制的签名方案中,文献[3]中首先提出了"基于信任传递的虚拟身份认证"的概念模型,该模型提出了信任的建立、授权、存储和维护规则,以确保虚拟身份认证过程的安全性。文献[4]中提出了一种基于信誉机制的安全多方计算协议,该方案基于拉格朗日差值多项式,需要大量的多项式计算,其效率有待提高。文献[5]中提出了一种基于信任机制的安全路由决策方案,该方案引入了信任向量来实现证据链的收集。文献[6]中设计了分布式环境中的动态可信度评估模型,该方案将Shapley熵引入到可信度评估过程中,从而使方案的可信度评估结果能够更准确地反映节点的动态行为。基于基本的自动信任协商模型,文献[7]中结合安全多方计算理论提出了一种基于安全多方的自动信任协商协议来实现隐私保护。

文献[8]中提出了基于秘密共享的可动态更新签名方案,该方案通过交互信息来验证成员的可信性,但是不具有可追溯和可审计功能。文献[9]中提出了基于多项式的秘密共享

收稿日期:2020-02-28;**修回日期:**2020-04-20;**录用日期:**2020-04-28。
基金项目:国家自然科学基金资助项目(U1304614, U1204703);河南省教育厅高等学校重点科研项目(20A413008)。
作者简介:王韫烨(1980—),女,河南郑州人,讲师,硕士,主要研究方向:信息安全、人工智能; 程亚歌(1987—),女,河南登封人,助教,硕士,主要研究方向:安全多方计算、信息安全; 贾志娟(1973—),女,河南郑州人,教授,硕士,CCF会员,主要研究方向:软件工程; 付俊俊(1995—),女,河南驻马店人,助教,主要研究方向:软件工程、区块链; 杨艳艳(1986—),女,河南洛阳人,助教,硕士,主要研究方向:信息安全、可信计算; 何宇矗(1985—),男,河南汝州人,讲师,博士,主要研究方向:智能交通、机器学习; 马威(1980—),男,河南郑州人,讲师,博士,主要研究方向:物联网、可信计算。

的前摄性门限 RSA(Rivest, Shamir, Adleman)签名方案,计算效率有待提升。文献[10]中提出了适用于区块链的签名方案,该方案将节点的公钥存储在区块链上,实现动态更新之后仍可查看前期签名。文献[11]中提出了基于安全多方的公平秘密共享方案,该方案保护了参与者的秘密信息,但是参与者的可信性无法评估。文献[12]中通过同态加密实现了秘密出价选择计算出代理者,并通过秘密计算相似属性完成属性泛化的整体处理,但计算效率有待提高。文献[13]中提出了基于信任机制的安全多方签名方案,该方案通过评估参与者可信度确保参与者的可信性,但可信结果由参与者自己保存,存在被篡改的可能性。

在上述研究的基础上,本文设计了一种安全多方的区块链可审计签名方案。方案引入信任矩阵记录参与者的可信行为,并将其动态绑定到签名过程中。为确保可信评估值的可信性,利用区块链的公开透明和不可篡改性,将评估结果存储到区块链中作为后期审计的证据。

本文的主要贡献及创新为将安全多方和区块链结合,建立了一种可审计和追溯的可信机制,将参与者的可信度量化并形成可信矩阵,使参与者的可信度更加直观;并利用区块链不可篡改的特性将可信矩阵存储到区块链中作为审计的依据,使可信度更加真实可信。

1 预备知识

1.1 安全多方计算

安全多方计算[14]主要用于解决一组互相不信任的参与者之间的个人隐私保护问题。它是解决两个或多个参与者之间隐私计算问题的有效方法,能够确保多名互不信任的参与者之间共同完成计算任务而不会泄露各自的隐私信息。

设在分布式网络中,有一组彼此互不信任的参与者 $P_1, P_2, \cdots, P_n$。假设每个参与者都拥一份秘密数据 $x_1, x_2, \cdots, x_n$,他们秘密输入各自的秘密数据,并通过相互合作共同计算 $f:(x_1, x_2, \cdots, x_n) \rightarrow (y_1, y_2, \cdots, y_n)$。最后,每个参与者都可以得到各自的输出 y_i,在此过程中,每个参与者都无法获得其他参与者的任何信息。

在安全多方计算协议中,存在一些尝试破坏协议的人,这些人被称为攻击者。根据攻击者破坏的参与者类型,可以将攻击者分为两类[15]:

被动攻击者 如果攻击者破坏的是半诚实的参与者,即攻击者只能获取被破坏的半诚实参与者的输入、输出和中间结果,但既不能更改也不能停止协议的运行,参与者仍然能够严格执行协议内容,此类攻击者被称为被动攻击者。

主动攻击者 这类攻击者比被动攻击者攻击能力要强。该类攻击者不仅能够获取被破坏者的输入等信息,更可以更改及控制被破坏者的输入、输出,篡改中间结果,甚至可以中断协议的执行,此类攻击者被称为主动攻击者。

1.2 区块链

区块链[16]是一种按照时间顺序将数据区块以顺序相连的方式组合成的一种链式数据结构,并以密码学方式保证其不可篡改和不可伪造的分布式账本。区块链技术是利用链式数据结构来验证与存储数据、利用分布式节点共识算法来生成和更新数据、利用密码学的方式保证数据传输和访问的安全、利用由自动化脚本代码组成的智能合约来编程和操作数据的一种全新的分布式基础架构与计算方式。

作为电子货币交易的底层技术,区块链具有去中心化、匿名化、不可篡改、公开透明、可审计等良好特性,很好地解决了数据在传输过程中的可信性,在金融、医疗、能源互联网、物联网等领域发展迅速。

1.3 Asmuth-Bloom 秘密共享方案

1983 年 Asmuth 和 Bloom 提出了 Asmuth-Bloom 秘密共享方案[17],其详细方案步骤如下:

初始化 设秘密分发者为 Distribution Center(DC),P_i 是参与成员,t 为门限值,秘密为 s。秘密分发者 DC 选择大素数 $q(q > s)$,整数 A,以及严格递增正整数序列 $d = \{d_1, d_2, \cdots, d_n\}$,且 d 满足如下几个条件:

1) $0 \leqslant A \leqslant M/q - 1$;

2) $d_1 < d_2 < \cdots < d_n$;

3) $\gcd(d_i, d_j) = 1, i \neq j$;

4) $\gcd(d_i, q) = 1;\ i = 1, 2, \cdots, n$;

5) $M = \prod_{i=1}^{t} d_i > q \prod_{i=1}^{t-1} d_{n-t+1}$

秘密分发 秘密分发者 DC 计算:

$z = s + Aq$

$z_i = z \bmod d_i;\ i = 1, 2, \cdots, n$

并将 (z_i, d_i) 发送给 P_i,作为 P_i 的秘密份额。

秘密恢复 参与者可通过交换秘密份额恢复秘密 s。任意选取 t 个参与者 $P_i(i = 1, 2, \cdots, t)$ 恢复秘密。通过相互交换秘密后,P_i 建立同余方程组:

$$\begin{cases} z \equiv z_1 (\bmod d_1) \\ z \equiv z_2 (\bmod d_2) \\ \vdots \\ z \equiv z_t (\bmod d_t) \end{cases}$$

根据中国剩余定理可得唯一解:

$$z = \sum_{i=1}^{t} \frac{D}{d_i} e_i X_i \bmod D;\ i = 1, 2, \cdots, t$$

因此,可求出共享秘密 $s = z \bmod q$。

2 本文方案

本文通过引入带时间戳的信任矩阵来评估参与者的信誉值,将其动态地绑定到签名过程中,作为记录参与者行为的证据,并将评估结果存储到区块链中作为监督和审计的查证依据。其架构如图 1。

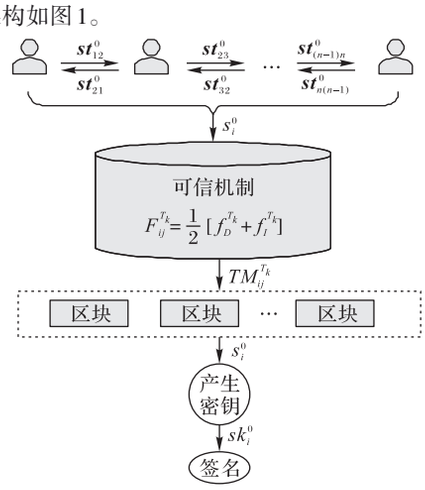

图 1 安全多方的区块链可审计签名架构

Fig. 1 Architecture of secure multi-party blockchain auditable signature scheme

如图 1 所示,参与者随机选取秘密标记信息 st_{ij}^0,并计算秘

密标记s_i^0。参与者通过秘密标记s_i^0验证信息来源的真实性,建立可信机制量化参与者的可信度,并将可信度量值存储到区块链上用于后期的追溯和审计。在参与者可信的情况下,参与者接收来自其他参与者的信息并产生自己的密钥用于签名。

2.1　产生密钥

2.1.1　初始化

设$P_i(i=1,2,\cdots,n)$是n个参与者的集合,t为门限值,g为有限域$GF(p)$上的生成元,p和q是两个大素数,并满足$q/(p-1)$,$d_i(i=1,2,\cdots,n)$是一组严格单调递增的正整数序列,q和d满足Asmuth-Bloom方案,待签名消息为m,$D=\sum_{i=1}^{n}d_i$,公开n、t、g、p、q、d和D。

2.1.2　产生秘密标记信息

每个参与者P_i随机选取秘密标记信息$st_{i1}^0,st_{i2}^0,\cdots,st_{in}^0$满足Asmuth-Bloom方案,计算秘密标记$s_i^0=st_{i1}^0+st_{i2}^0+\cdots+st_{in}^0=\sum_{j=1}^{n}st_{ij}^0$,并将$st_{ij}^0$发送给$P_j(j=1,2,\cdots,n)$,同时$P_i$保留$st_{ii}^0$,广播$g^{st_{ii}^0}$和$g^{s_i^0}$。

此时,P_i保存了一份秘密标记信息组成的向量$\boldsymbol{ST}=(st_{1j}^0,st_{2j}^0,\cdots,st_{ii}^0,\cdots,st_{nj}^0)$和$s_i^0$。

2.1.3　产生身份标记信息

参与者P_i选择随机数a_i,计算$a=\sum_{i=1}^{n}a_i$,并广播g^{a_i}和g^a。这里,设$\mu_i=a+s_i^0$,$ID_i=\mu_i(\mathrm{mod}\,d_i)$,则它有唯一的解为:$ID=\sum_{i=1}^{n}\frac{D}{d_i}e_i\mu_i\,\mathrm{mod}\,D$,其中$e_i$满足$\frac{D}{d_i}e_i\equiv 1\,\mathrm{mod}\,d_i$。因此,参与者的身份验证信息为$(ID,\mu_i)$。

2.1.4　计算验证信息

设$\lambda_i^0=s_i^0+st_i^0$,$\delta_i^0=\mu_i+st_i^0$,$\omega_i^0=s_i^0q+a$,根据广播信息$g^{s_i^0}$,$g^{st_i^0}$和g^a,如果

$$\left(g^{(\delta_i^0-\lambda_i^0)}\,\mathrm{mod}\,p\right)\cdot\left(\left(g^{s_i^0}\right)^q\,\mathrm{mod}\,p\right)\mathrm{mod}\,p=\left(g^{(\omega_i^0)}\right)\mathrm{mod}\,p$$

则参与者$P_j\ (j\neq i)$接受参与者P_i发送的信息st_{ij}^0。

2.1.5　产生密钥

P_i收到其他参与者的秘密标记$st_{ij}^0(i=1,2,\cdots,n)$,生成个人私钥:

$$sk_i^0=(\sum_{j=1}^{n}st_{ij}^0+a_i)\,\mathrm{mod}\,d_i$$

则参与者公钥为:

$$pk_i^0=g^{sk_i^0}\mathrm{mod}\,p$$

组公钥为:

$$G_{pk}=\prod_{i=1}^{n}g^a\,\mathrm{mod}\,p$$

组私钥为:

$$G_{sk}=\sum_{i=1}^{n}a_i\ \mathrm{mod}\,p$$

2.2　可信机制的建立

为确保参与者的可信性,建立动态可信评估机制,动态更新参与者的秘密标记信息并生成带时间戳的信任向量,作为参加者可信的基础,并由信任向量构成信任矩阵(Trust Matrix,$\boldsymbol{TM}$)。其构建过程如图2。

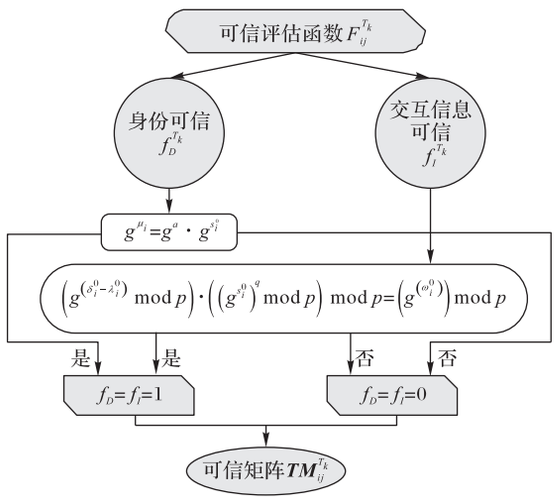

图2　可信机制

Fig. 2　Trust mechanism

如图2所示,可信评估函数主要包含两个方面,直接可信和间接可信。直接可信是指参与者的身份可信,间接可信是指参与者之间交互信息的可信性。其中身份的可信性通过等式$g^{\mu_i}=g^a\cdot g^{s_i^0}$判断,交互信息的可信性通过等式$\left(g^{(\delta_i^0-\lambda_i^0)}\,\mathrm{mod}\,p\right)\cdot\left(\left(g^{s_i^0}\right)^q\,\mathrm{mod}\,p\right)\mathrm{mod}\,p=\left(g^{(\omega_i^0)}\right)\mathrm{mod}\,p$判断。当等式成立时取值为1,否则为0。并将可信度量值组成可信矩阵用于审计和追溯。其具体执行过程如下。

可信评估函数为:$F_{ij}^{T_k}=\frac{1}{2}\left[f_D^{T_k}+f_I^{T_k}\right]$,这里$f(x)=[x]$为取整函数,$T$为更新周期。可信评估函数由参与者的直接信任和间接信任两部分构成。f_D为参与者P_i的在第k个周期的直接信任评估值,这里$ID_i=\mu_i(\mathrm{mod}\,d_i)$为参与者的身份信息。$f_I$为参与者$P_i$的在第$k$个周期的间接信任评估值。直接信任$f_D$和间接信任$f_I$的取值属于集合$A=\{0,1\}$,$F_{ij}^{T_k}$的取值范围为$B=\{0,1/2,1\}$。

若等式$g^{\mu_i}=g^a\cdot g^{s_i^0}$成立,则直接信任$f_D=1$;否则为0。

若等式

$$\left(g^{(\delta_i^0-\lambda_i^0)}\,\mathrm{mod}\,p\right)\cdot\left(\left(g^{s_i^0}\right)^q\,\mathrm{mod}\,p\right)\mathrm{mod}\,p=\left(g^{(\omega_i^0)}\right)\mathrm{mod}\,p$$

成立,则间接信任$f_I=1$;否则为0。

此时,P_i将第k个周期的评估结果生成信任向量$\boldsymbol{TV}$:

$$\boldsymbol{TV}_i^{T_k}=\left[F_{i1}^{T_k}\quad F_{i2}^{T_k}\quad\cdots\quad F_{in}^{T_k}\right]$$

这里默认$F_{ii}^{T_k}=1$。

将第k周期所有参与者$P_i(i=1,2,\cdots,n)$的信任向量组成信任矩阵$\boldsymbol{TM}$,因此第k个周期所有参与者的评估结果为:

$$\boldsymbol{TM}_{ij}^{T_k}=\begin{bmatrix}F_{11}^{T_k}&F_{12}^{T_k}&\cdots&F_{1n}^{T_k}\\F_{21}^{T_k}&F_{22}^{T_k}&\cdots&F_{2n}^{T_k}\\\vdots&\vdots&&\vdots\\F_{n1}^{T_k}&F_{n2}^{T_k}&\cdots&F_{nn}^{T_k}\end{bmatrix}$$

因此,在第k周期时,参与者P_i对其他$n-1$个参与者的评估值为:

$$\boldsymbol{TM}_i^{T_k}=\begin{bmatrix}F_{i1}^1 & F_{i2}^1 & \cdots & F_{in}^1\\ F_{i1}^2 & F_{i2}^2 & \cdots & F_{in}^2\\ \vdots & \vdots & & \vdots\\ F_{i1}^{T_k} & F_{i2}^{T_k} & \cdots & F_{in}^{T_k}\end{bmatrix}$$

在第 $k+1$ 周期时，P_i 更新可信矩阵 $\boldsymbol{TM}_i^{T_k}$：

$$\boldsymbol{TM}_i^{T_k}=\begin{bmatrix}F_{i1}^1 & F_{i2}^1 & \cdots & F_{in}^1\\ F_{i1}^2 & F_{i2}^2 & \cdots & F_{in}^2\\ \vdots & \vdots & & \vdots\\ F_{i1}^{T_k} & F_{i2}^{T_k} & \cdots & F_{in}^{T_k}\end{bmatrix}\rightleftharpoons$$

$$\begin{bmatrix}F_{i1}^{T_{k+1}} & F_{i2}^{T_{k+1}} & \cdots & F_{in}^{T_{k+1}}\end{bmatrix}=\boldsymbol{TV}_{ij}^{T_{k+1}}$$

$$\downarrow$$

$$\boldsymbol{TM}_i^{T_{k+1}}=\begin{bmatrix}F_{i1}^1 & F_{i2}^1 & \cdots & F_{in}^1\\ F_{i1}^2 & F_{i2}^2 & \cdots & F_{in}^2\\ \vdots & \vdots & & \vdots\\ F_{i1}^{T_{k+1}} & F_{i2}^{T_{k+1}} & \cdots & F_{in}^{T_{k+1}}\end{bmatrix}$$

当参与者不可信时，则不能参与签名。

2.3 产生签名

1）$P_i(i=1,2,\cdots,t)$ 选择随机数 l_i，并计算 $\eta_i=g^{l_i\cdot\frac{\sum_{j=1}^{t}F_{ij}^{T_k}}{n}}\bmod p$，将 η_i 发送给 P_j 并广播。

2）当参与者 P_j 收到 η_i 时，$P_j(j=1,2,\cdots,t)$ 计算 $\eta=g^{\frac{1}{t}\sum_{i=1}^{t}\left(l_i\cdot\sum_{j=1}^{t}F_{ij}^{T_k}\right)}\bmod p=\prod_{i=1}^{t}g^{l_i\cdot\frac{\sum_{j=1}^{t}F_{ij}^{T_k}}{t}}\bmod p=\prod_{i=1}^{t}\eta_i\bmod p$。

3）$P_i(i=1,2,\cdots,t)$ 计算部分签名 $S_i^0=m\cdot\eta\cdot l_i+w_i^0\bmod D$，所以参与者的部分签名为 $\left(m,\eta,S_i^0\right)$，这里 $w_i^0=\frac{D}{d_i}e_isk_i^0\bmod D$。

4）P_i 计算签名 $S=\left(\sum_{i=1}^{t}S_i^0\bmod D\right)\bmod q$。所以，消息 m 的最终的签名为 $sig(m)=\left(m,\eta,S\right)$。

2.4 签名验证

P_i 用组公钥 G_{pk} 验证等式 $g^S\equiv u^{m\cdot\eta}\cdot G_{pk}\bmod p$。如果等式成立，则签名有效。

2.5 动态更新

由于存在移动攻击，攻击者可以通过长期稳定的攻击来获取参与者的专用密钥；然而，动态更新参与者的密钥可以有效地防止移动攻击并提高安全性。该解决方案可以使系统公钥在整个更新过程中保持不变，保留了使用系统公钥访问历史签名信息的功能。这里，将更新周期设置为 T。

每一个周期 T，参与者更新秘密标记信息 st_{ij}^0，并更新私钥 $sk_i^{T_k}$。

更新完成后，参与者还可以根据签名过程 1）~ 4）生成签名。

2.6 区块链可审计机制

如图3所示，参与者首先选择出代理者，由代理者将可信度量矩阵加密并存储到区块链中，当有申请者需要查验时，向代理者发起申请并从区块链中下载相应周期的可信矩阵，代理者将对应周期的组私钥发给该申请者，申请者通过解密即可得到原始可信矩阵并予以验证。

其详细实施过程如下。

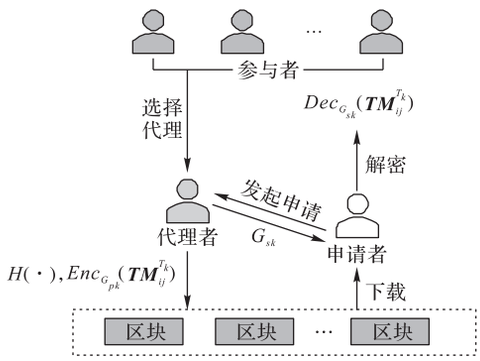

图3 区块链审计流程

Fig. 3 Flowchart of blockchain audit

2.6.1 半可信代理的选择

参与者通过竞标出价选择出半可信代理者。每个参与者秘密出价得到一个标准数据 $H=(h_1,h_2,\cdots,h_n)$，n 个参与者合作保密计算获得各自的出价 h_i 排序，最后由出价最高者作为代理。

首先，参与者 $P_i(i=1,2,\cdots,n)$，商定一个全集 $A=[1,N]$，满足 $H\subseteq A$，每个参与者在全集 A 中构造一个 N 维向量 $\boldsymbol{B}_i=(b_{i1},b_{i2},\cdots,b_{ij},\cdots,b_{iN})$，其中对于每一个 $j\in A$，定义 $b_{ij}=\begin{cases}1, j=h_i\\ 0, j\neq h_i\end{cases}$。

其次，P_i 用系统公钥加密 $\boldsymbol{B}_i$ 得到：

$$E(\boldsymbol{B}_i)=\boldsymbol{B}_i^*=(b_{i1}^*,b_{i2}^*,\cdots,b_{iN}^*)$$

并将 $\boldsymbol{B}_i^*$ 发给 P_{i+1}。P_{i+1} 收到 P_i 发送来的 $\boldsymbol{B}_i^*$ 后，进行如下计算：P_{i+1} 根据 $\boldsymbol{B}_{i+1}=\left(b_{(i+1)1},b_{(i+1)2},\cdots,b_{(i+1)N}\right)$ 得到 $\boldsymbol{B}_{i+1}^*$，其中对于任意 $j\in A$，有 $b_{(i+1)j}^*=\begin{cases}b_{(i+1)j}, & b_{(i+1)j}=1\\ b_{ij}^*, & b_{(i+1)j}=0\end{cases}$，故得到，$E(\boldsymbol{B}_{i+1})=\boldsymbol{B}_{i+1}^*=\left(b_{(i+1)1}^*,b_{(i+1)2}^*,\cdots,b_{(i+1)N}^*\right)$，然后，$P_{i+1}$ 将 $\boldsymbol{B}_{i+1}^*$ 发送给 P_{i+2}。依此类推，最终 P_n 得到 $\boldsymbol{B}_n^*=(b_{n1}^*,b_{n2}^*,\cdots,b_{nN}^*)$ 并公布。

最后，参与者 $P_i(i=1,2,\cdots,n)$ 计算公式：

$$R_i=\sum_{j=1}^{h_i}b_{nj}^* \tag{1}$$

得到最终的出价排序，由出价最高者作为代理，假设出价最高者为 P_r。

2.6.2 区块链审计

P_r 作为代理，将第 $T_k(k=1,2,\cdots,n)$ 周期的可信评估矩阵 $\boldsymbol{TM}_{ij}^{T_k}$ 用系统公钥加密得到密文 $Enc_{G_{pk}}\left(\boldsymbol{TM}_{ij}^{T_k}\right)$，并对密文进行哈希处理得到 $H\left(Enc_{G_{pk}}\left(\boldsymbol{TM}_{ij}^{T_k}\right)\right)$，将最后得到的哈希值存放到区块链中。

当有需求时，参与者 P_k 或其他参与者向代理者发起请求，代理 P_r 将组私钥发送给申请者 P_k，P_k 从区块链上下载数据并用私钥解密得到可信评估矩阵 $\boldsymbol{TM}_{ij}^{T_k}$。

3　方案分析

3.1　正确性分析

定理1　参与者共同计算出的签名有效。

证明　$sk_i^{T_k}=\left(\sum_{j=1}^{n}st_{ij}^{T_k}+a_i\right)\bmod d_i$

令

$$\beta=\sum_{j=1}^{n}st_{ij}^{T_k}q+a_i \tag{2}$$

所以,有

$sk_i^{T_k}=\beta \bmod d_i$

根据中国剩余定理,可得到同余方程组:

$$\begin{cases}sk_1^{T_k}\equiv\beta \bmod d_1\\ sk_2^{T_k}\equiv\beta \bmod d_2\\ \vdots\\ sk_t^{T_k}\equiv\beta \bmod d_t\end{cases}$$

得到唯一的解:$\beta=\sum_{i=1}^{t}\frac{D}{d_i}e_isk_i^{T_k} \bmod D$

因为 $w_i^{T_k}=\frac{D}{d_i}e_isk_i^{T_k}$

故

$$\beta=\sum_{i=1}^{t}w_i^{T_k} \bmod D \tag{3}$$

当$t>2$时,根据文献[18],有

$m\cdot\eta\cdot\sum_{i=1}^{t}l_i+\beta<D$

所以有

$$S=\left(\sum_{i=1}^{t}S_i^{T_k} \bmod D\right)\bmod q=\left[\sum_{i=1}^{t}\left(m\cdot\eta\cdot l_i+w_i^0 \bmod D\right)\right]\bmod q=\left(m\cdot\eta\cdot\sum_{i=1}^{t}l_i+\sum_{i=1}^{t}w_i^0 \bmod D\right)\bmod q$$

由式(2)、(3),可得到

$$s=\left(m\cdot\eta\cdot\sum_{i=1}^{t}l_i+\sum_{i=1}^{t}\left(\sum_{j=1}^{n}st_{ij}^{T_k}q+a_i\right)\right)\bmod q=\left(m\cdot\eta\cdot\sum_{i=1}^{t}l_i+\sum_{i=1}^{t}a_i\right)\bmod q$$

所以有

$$g^s\equiv g^{m\cdot\eta\cdot\sum_{i=1}^{t}l_i+\sum_{i=1}^{t}a_i} \bmod p\equiv g^{m\cdot\eta\cdot\sum_{i=1}^{t}l_i}\cdot g^{\sum_{i=1}^{t}a_i} \bmod p\equiv\eta^{m\cdot\eta}\cdot G_{pk} \bmod p$$

定理2　可信评估函数可以正确有效地判断参与者的可信性。

证明　根据可信评估函数:

$F_{ij}^{T_k}=\frac{1}{2}\left[f_D^{T_k}+f_I^{T_k}\right]$

直接信任$f_D^{T_k}$通过验证等式

$g^{\mu_i}=g^a\cdot g^{s_i^0}$

来验证参与者身份的可信性。由于

$\mu_i=a+s_i^0$

因此,很容易验证得到$g^{\mu_i}=g^{a+s_i^0}=g^a\cdot g^{s_i^0}$。

间接信任评估函数$f_I^{T_k}$通过验证等式:

$$\left(g^{\left(\delta_i^0-\lambda_i^0\right)} \bmod p\right)\cdot\left(\left(g^{s_i^0}\right)^q \bmod p\right)\bmod p=\left(g^{\omega_i^0}\right)\bmod p$$

来验证参与者的行为可信性,由于

$\lambda_i^0=s_i^0+st_i^0,\delta_i^0=\mu_i+st_i^0$

$\omega_i^0=s_i^0q+a,\mu_i=a+s_i^0$

所以有

$$\left(g^{\left(\delta_i^0-\lambda_i^0\right)} \bmod p\right)\cdot\left(\left(g^{s_i^0}\right)^q \bmod p\right)\bmod p=\left(g^{\left(a+s_i^0+st_i^0-s_i^0-st_i^0\right)} \bmod p\right)\cdot\left(\left(g^{s_i^0}\right)^q \bmod p\right)\bmod p=\left(g^a \bmod p\right)\cdot\left(\left(g^{s_i^0}\right)^q \bmod p\right)\bmod p=\left(g^a\cdot g^{s_i^0\cdot q}\right)\bmod p=\left(g^{a+s_i^0\cdot q}\right)\bmod p=g^{\omega_i^0} \bmod p$$

因此,可信评估函数$F_{ij}^{T_k}=\frac{1}{2}\left[f_D^{T_k}+f_I^{T_k}\right]$可信有效。

定理3　通过秘密比较数组$H=(h_1,h_2,\cdots,h_n)$的大小可以正确有效地选择出代理者。

根据向量$\boldsymbol{B}_i=(b_{i1},b_{i2},\cdots,b_{ij},\cdots,b_{iN})$的构成方式可知,对于任意的$j\in A$,若$j=h_i$,则有$b_{ij}=1$;若$j\neq h_i$,则有$b_{ij}=0$。依此类推得到$\boldsymbol{B}_n^*=(b_{n1}^*,b_{n2}^*,\cdots,b_{nN}^*)$,参与者根据式(1)$R_i=\sum_{j=1}^{h_i}b_{nj}^*$可计算得到最终的排序结果,出价最高者则被选为代理。

3.2　安全性分析

3.2.1　签名算法安全性分析

本方案基于中国剩余定理求解,至少需要t个同余方程组才能求解,少于t个方程则无法求解。因此,恶意攻击者必须在同一周期T_k内同时获得t个或多于t个的参与者方可求解出签名信息。

在密钥生成阶段,若有恶意攻击者试图通过窃取参与者的私钥参与签名,根据私钥计算公式,$sk_i^0=\left(\sum_{j=1}^{n}st_{ij}^0+a_i\right)\bmod d_i$,攻击者需同时获得$n$个参与者的秘密标记$st_{ij}^0$和$P_i$的个人身份标记信息$a_i$。这里$\sum_{i=1}^{n}st_{ij}^0$由$n$个参与者秘密选取计算获得,而$a_i$为参与者的身份标记信息,同样也由参与者秘密选取。攻击者需在同一个周期内同时获得n个参与者的秘密标记信息st_{ij}^0和参与者P_i的个人身份标记信息a_i,才能计算得到sk_i^0,这对攻击者来讲是不可能的。攻击者可能通过截取公开信息$g^{st_{ij}^0}$、$g^{s_i^0}$和g^{a_i}获得st_{ij}^0和a_i,然而,通过$g^{st_{ij}^0}$、$g^{s_i^0}$和g^{a_i}求解st_{ij}^0和a_i是离散对数难题,攻击者不可能通过计算得到。因此,攻击者无法通过计算$g^{st_{ij}^0}$、$g^{s_i^0}$和g^{a_i}获得私钥。

系统公钥$G_{pk}=\prod_{i=1}^{n}g^a \bmod p$和系统私钥$G_{sk}=\sum_{i=1}^{n}a_i \bmod p$由参与者的身份信息生成。组公钥$G_{pk}$属于公开信息,攻击者可能通过获得系统公钥计算系统私钥,然而由$G_{pk}=\prod_{i=1}^{n}g^a \bmod p$求解$a$同样也是离散对数难题,故攻击者无法获得。

在签名阶段,攻击者可能通过拦截广播信息η_i计算l_i和$F_{ij}^{T_k}$,而$\eta_i=g^{l_i\cdot\frac{\sum_{i=1}^{t}F_{ij}^{T_k}}{n}} \bmod p$,通过计算$\eta_i$求$l_i$和$F_{ij}^{T_k}$依然是求解离散对数难题,攻击者无法获得。

3.2.2　不可伪造性分析

不可伪造性简单来讲就是指一些恶意攻击者不能通过篡

改或者伪造来改变合法的签名。

如果攻击者想要伪造签名，首先要获得参与者的私钥信息 sk_i^0，由于 $sk_i^0 = \left(\sum_{j=1}^{n} st_{ij}^0 + a_i\right) \bmod d_i$，根据参与者的身份验证等可知，必然有 $s_i^{T_k'} \neq s_i^{T_k}$，$a_i' \neq a_i$，$\mu_i' \neq \mu_i$，故有 $ID_i' \neq ID_i$，即参与者身份验证信息不可信。根据可信评估机制可以很容易判断出该参与者行为不可信，所以攻击者无法伪造参与者私钥。

假设有恶意参与者试图伪造可信评估值 $F_{ij}^{T_k}$，由于可信评估值 $F_{ij}^{T_k} = \frac{1}{2}\left[f_D^{T_k} + f_I^{T_k}\right]$，由 f_D 和 f_I 两部分组成，直接信任 f_D 通过 $g^{\mu_i} = g^a \cdot g^{s_i^0}$ 判断得到，间接信任通过 $\left(g^{\left(\delta_i^0 - \lambda_i^0\right)} \bmod p\right) \cdot \left(\left(g^{s_i^0}\right)^q \bmod p\right) \bmod p = \left(g^{\left(\omega_i^0\right)}\right) \bmod p$ 而得到，若攻击者单纯地篡改结果，很容易发现通过等式验证不成立。另外，将可信评估值存储到区块链中，保证了可信值的公开透明性和可溯源性，具有可审计查证功能，因此，即使有恶意攻击者篡改了可信评估值，通过区块链存证系统查询验证，很容易发现可信评估的异常情况。

3.2.3 可以抵抗移动攻击

移动攻击意味着，只要有攻击者成功地入侵并控制其中的一个参与者，攻击者便可将攻击目标成功地转移到系统中的其他参与者。当然移动攻击者可能在短时间内无法完全成功入侵并控制其他参与者，但是如果有足够的时间持续攻击，则攻击者可能通过攻击获得 t 个以上的参与者的信息，从而成功破坏系统的安全性。

为了防止移动攻击的发生，方案动态更新参与者秘密标记和私钥，随者周期 T_i 的增加定期更新，攻击者只有在有限的同一个周期时间段内同时成功入侵并控制 t 个以上参与者的个人秘密信息才能攻破系统的安全性，这对攻击者来讲是困难的。

3.3 性能分析

3.3.1 效率分析

本文方案与其他方案相比，能够动态评估参与者的可信行为，并具有可审计的特性。表 1 是本文方案与其他方案的对比结果，其中：1 表示方案有此项功能，0 表示方案没有此项功能。

表 1 签名方案对比

Tab. 1 Comparison of signature schemes

方案	可信评估	可审计	前向安全	动态更新
本文方案	1	1	1	1
文献[4]方案	1	0	0	0
文献[8]方案	0	0	1	1
文献[9]方案	0	0	0	1
文献[10]方案	0	0	1	1
文献[11]方案	0	0	0	0

文献[4]基于信誉的安全多方秘密共享方案，该方案具有信誉机制，但没有审计和动态更新设计，也没有前向安全性。文献[8-10]都具有前向安全行和可动态更新功能，但是都不能动态评估参与者的可信性，也不具有可审计特点。文献[11]基于安全多方的秘密共享方案不具有可信、可审计的特性，也没有动态更新和前向安全性。

另外，本文方案采用秘密共享技术，主要涉及有模乘、模加、模幂以及一次模逆计算，很大程度上降低了计算复杂度，节省了时间成本，与基于拉格朗日插值多项式、双线性对的签名方案相比，效率有所提升。

为理解方便，定义了表 2 符号。

表 2 符号定义

Tab. 2 Symbol definition

运算算法	符号	计算复杂度
模乘	m	$O((lbn)^k)$
模逆	u	$O((lbn)^{-1})$
哈希	h	$O(h(x))$

表 3 是本文和文献[9]的计算复杂度对比结果，文献[9]是基于拉格朗日插值多项式的 RSA 签名方案，需要较为繁琐的多项式计算。其对比结果如下。

表 3 计算复杂度对比

Tab. 3 Comparison of computational complexity

方案	签名过程	签名验证
本文方案	$t\left[O((lbn)^k) + 3O(lbn)\right]$	$O((lbn)^k) + O(lbn)$
文献[9]方案	$(4t+1)O(lbn)^k + 3O(h(x))$	$3tO(lbn)^k + 2tO\left((lbn)^{-1}\right) + O(h(x))$

3.3.2 仿真实验

本文仿真实验环境是 64 位 Window 10 操作系统，MyEclipse2015 系统，CPU 为英特尔酷睿 i5-8300H 处理器，主频 2.3 GHz，内存为 8 GB，其实验结果如图 4。

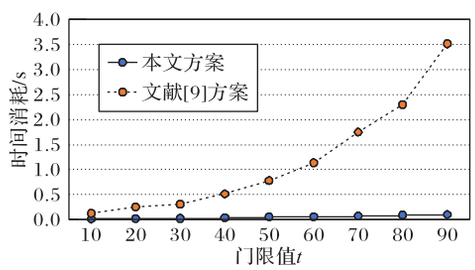

图 4 门限值与时间消耗

Fig. 4 Threshold and time consumption

图 4 为参与者数量固定不变、门限值变化的情况下本文方案和文献[9]方案的时间消耗对比。由图 4 可知，本文方案和文献[9]方案的时间消耗均随着门限值 t 的增加而增加，这是因为签名过程中参与者的数量 n 与时间成正相关关系。从图 4 可以看出，文献[9]方案比本文方案耗时更多，这是因为文献[9]方案是基于朗格朗日插值多项式，需要大量的多项式计算，而本文方案基于中国剩余定理，因此相率相对较高。

图 5 为门限值 t 固定、参与者数量 n 增加的情况下本文方案和文献[9]方案的时间消耗对比。由图 5 可知，本文方案和文献[9]方案的时间消耗均随着参与者数量 n 的增加而增加，同理，这是因为签名过程中参与者的数量 n 与时间消耗成正相关关系。可以看出，本文方案时间消耗要低于文献[9]方案。

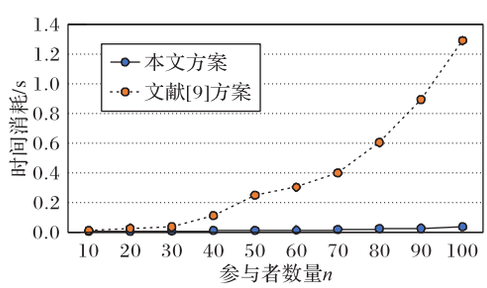

图 5 参与者数量与时间消耗

Fig. 5 Participant number and time consumption

4　结语

本文设计的基于安全多方的区块链可审计签名方案,将安全多方和区块链相结合,建立了一种可信评估机制将参与者的可信度量化,更加客观地评估参与者的可信度。利用区块链不可篡改、公开透明的特性,将可信评估矩阵存放到区块链上作为查证的依据,实现了可审计、可追溯的功能。采用秘密共享技术设计了一种安全多方的签名方案,方案基于中国剩余定理与其他方案相比具有计算量小的优点。

参考文献 (References)

[1] YAO A C. Protocols for secure computations[C]// Proceedings of the 23rd Annual IEEE Symposium on Foundations of Computer Science. Piscataway: IEEE, 1982:160-164.

[2] GOLDREICH O, MICALI S, WIGDERSON A. How to play ANY mental game[C]// Proceedings of the 19th Annual ACM Conference on Theory of Computing. New York: ACM, 1987:218-229.

[3] 王亮. 基于信任传递的移动商务虚拟身份认证机制研究[D]. 北京:北京交通大学, 2015: 44-47. (WANG L. Research on mobile business virtual identity authentication mechanism based on trust transfer [D]. Beijing: Beijing Jiaotong University, 2015: 44-47.)

[4] 郑炜. 多种机制下基于秘密共享的理性安全多方计算协议的研究[D]. 北京:北京工业大学, 2018: 34-38. (ZHENG W. Research on rational security multi-party computing protocol based on secret sharing under various mechanisms[D]. Beijing: Beijing University of Technology, 2018:34-38.)

[5] 李峰,司亚利,陈真,等. 基于信任机制的机会网络安全路由决策方法[J]. 软件学报, 2018, 29(9):2829-2843. (LI F, SI Y L, CHEN Z, et al. Trust-based security routing decision method for opportunistic networks[J]. Journal of Software, 2018, 29(9): 2829-2843.)

[6] 朱友文. 分布式环境下的隐私保护技术及其应用研究[D]. 合肥:中国科学技术大学, 2012:77-81. (ZHU Y W. Research on privacy-preserving technologies in distributed environment and their applications[D]. Hefei: University of Science and Technology of China, 2012:77-81.)

[7] 王煜. 基于安全多方计算的自动信任协商协议研究[D]. 长沙:湖南大学, 2012:26-27. (WANG Y. Research on automatic trust negotiation protocol based on secure multi-party computing[D]. Changsha: Hunan University, 2012:26-27.)

[8] 程亚歌,胡明生,公备,等. 具有强前向安全性的动态门限签名方案[J]. 计算机工程与应用, 2020, 56(5):125-134. (CHENG Y G, HU M S, GONG B, et al. Dynamic threshold signature scheme with strong forward security[J]. Computer Engineering and Applications, 2020, 56(5):125-134.)

[9] 徐甫. 基于多项式秘密共享的前摄性门限RSA签名方案[J]. 电子与信息学报, 2016, 38(9): 2280-2286. (XU F. Proactive threshold RSA signature scheme based on polynomial secret sharing [J]. Journal of Electronics and Information Technology, 2016, 38(9):2280-2286.)

[10] 程亚歌,贾志娟,胡明生,等. 适用于区块链电子投票场景的门限签名方案[J]. 计算机应用, 2019, 39(9): 2629-2635. (CHENG Y G, JIA Z J, HU M S, et al. Threshold signature scheme suitable for blockchain electronic voting scenarios[J]. Journal of Computer Applications, 2019, 39(9):2629-2635.)

[11] 傅泽源,张永华,徐建国. 基于安全多方的公平秘密共享方案[J]. 数学建模及其应用, 2018, 7(2):30-35. (FU Z Y, ZHANG Y H, XU J G. Fair secret sharing scheme based on secure multi-party[J]. Mathematical Modeling and Its Applications, 2018, 7(2):30-35.)

[12] 王斌,张磊,张国印. 基于多方安全计算的属性泛化mix-zone[J]. 通信学报, 2019, 40(4): 83-94. (WANG B, ZHANG L, ZHANG G Y. Attribute generalization mix-zone based on multiple secure computation[J]. Journal on Communications, 2019, 40(4):83-94.)

[13] CHENG Y, HU M, WANG L, et al. A secure multi-party signature scheme based on trust mechanism[C]// Proceedings of the 13th Chinese Conference on Trusted Computing and Information Security, CCIS 1149. Singapore: Springer, 2019: 119-132.

[14] 李顺东,杜润萌,杨颜璟,等. 安全多方多数据排序[J/OL]. 计算机学报[2020-01-16]. http://kns. cnki. net/kcms/detail/11. 1826. tp. 20190917. 1500. 007. html. (LI S D, DU R M, YANG Y J, et al. Secure multi-party multi-data sorting[J/OL]. Chinese Journal of Computers [2020-01-16]. http://kns. cnki. net/kcms/detail/11. 1826. tp. 20190917. 1500. 007. html.)

[15] 李强. 安全多方计算协议的研究与应用[D]. 上海:上海交通大学, 2003:6-7. (LI Q. Research and application of secure multi-party computing protocol [D]. Shanghai: Shanghai Jiao Tong University, 2003:6-7.)

[16] 杨保华,陈昌. 区块链原理、设计与应用[M]. 北京:机械工业出版社 2017: 9-19. (YANG B H, CHEN C. Blockchain Principle, Design and Application[M]. Beijing: China Mechine Press, 2017:9-19.)

[17] ASMUTH C, BLOOM J. A modular approach to key safeguarding [J]. IEEE Transactions on Information Theory, 1983, 29(2): 208-210.

[18] HOU Z, TAN M. A CRT-basted (t, n) threshold signature scheme without a dealer[J]. Journal of Computational Information Systems, 2015, 11(3):975-986.

This work is partially supported by the National Natural Science Foundation of China (U1304614, U1204703), the Key Scientific Research Project of Universities of Henan Education Department (20A413008).

WANG Yunye, born in 1980, M. S., lecturer. Her research interests include information security, artificial intelligence.

CHENG Yage, born in 1987, M. S., teaching assistant. Her research interests include secure multi-party computation, information security.

JIA Zhijuan, born in 1973, M. S., professor. Her research interests include software engineering.

FU Junjun, born in 1995, teaching assistant. Her research interests include software engineering, blockchain.

YANG Yanyan, born in 1986, M. S., teaching assistant. Her research interests include information security, trusted computing.

HE Yuchu, born in 1984, Ph. D., lecturer. His research interests include smart transportation, machine learning.

MA Wei, born in 1980, Ph. D., lecturer. His research interests include internet of things, trusted computing.