一种适用于区块链钱包保护的无中心可验证门限签名方案*

张中霞，王明文†
(西南交通大学 数学学院，成都 611756)

摘 要: 区块链钱包存储的私钥是加密数字货币所有权的唯一标志，一旦丢失或被盗将带来无法挽回的损失。传统方案中无论是离线钱包、在线钱包，还是托管钱包保护方案，都将私钥集中储存在一个位置，容易导致单点故障等问题。基于门限思想提出了一种适用于区块链钱包保护的门限签名方案，通过参与者间的合作生成私钥并完成签名，避免单点攻击问题; 方案与椭圆曲线兼容，无须可信中心进行秘密分配，提升了可用性，且支持公开可验证功能，所有参与者可在不暴露秘密信息的情况下验证秘密份额的有效性，保障了参与者间的诚实问题。安全性分析表明，攻击难度等价于在有限域上求解离散对数问题，且能够抗成员欺骗攻击。

关键词: 区块链钱包; 门限签名方案; 私钥; 椭圆曲线; 可验证

0 引言

区块链是一个分布式的点对点网络[1]。区块链交易是用户通过地址转移价值的声明，由用户的私钥进行签名。交易由网络节点进行验证，交易的所有必要信息都存储在一个钱包里，区块链钱包交易只需要一个椭圆曲线签名即可授权完成[2]。钱包只能通过特定的私钥访问[3]，如果这把私钥被破解，加密数字货币就会被盗。与传统的银行交易不同，交易一旦实施，就不可逆转。即使已知这些货币被盗，也没有办法逆转违规交易。事实上，加密数字货币的生态系统一直被盗窃所困扰。近年来，发生了很多起盗窃金额超过 1 万比特币的事件[4]。卡巴斯基实验室(Kaspersky Labs)报告称，每月检测到大约 100 万个恶意软件感染，这些恶意软件旨在搜索和窃取比特币[5]。严重的盗窃事件导致用户对区块链钱包的信心下降，且阻止数字货币的发展。针对这一问题，目前已有许多研究人员提出了多种解决方案，如硬件钱包、软件钱包、托管钱包等。但这些方案都存在一个共同问题，其私钥都集中储存在一个位置，容易造成单点的安全风险。在保持匿名性和隐私性的要求下，解决区块链钱包安全问题的办法是对区块链钱包进行联合控制。在认为签名有效之前，多个参与者构造其签名来形成联合控制。联合控制非常有利于消除内部欺诈的风险，因为没有人能够单独获得签署的全部权限。因此，保护区块链钱包相当于保护可以授权交易的密钥，不应将密钥存储在单一位置，而应将密钥拆分，并由计算机的阈值集授权签名。破坏任意未达到阈值数量的机器都不允许攻击者窃取任何金钱或收集关于密钥的任何信息。所以，本文致力于研究一种基于门限思想的区块链钱包保护签名方案。

(t,n) 门限签名方案是密码学和分布式计算领域的重要研究内容，它支持在 n 个参与者之间进行分布式签名，使得大于或者等于 t 的任何子集都可以联合签名。门限签名方案要满足签名方案的标准属性，且必须具有与其他协议相似的安全性，以满足多方计算的需要，也就是说，没有一方可以破坏协议来提取另一方共享的密钥，并且少于 t 方的子集不能串谋生成签名。Shamir[6] 基于拉格朗日插值多项式的理论最先提出门限签名方案，但该方案需要可信的一方来分发私钥，且不能保证参与者的诚实问题。而文献[7,8]中提出的门限方案提供公开可验证的能力，任何人都可以验证秘密的正确性，解决了参与者不诚实的问题，但仍需要可信的第三方进行秘密的分发。如何设计一种无中心、可验证且能用于区块链钱包保护的门限签名方案是本文研究的重点。

椭圆曲线签名算法(ECDSA)是一种非常流行的签名方案，常用于区块链交易方案中。因为 ECDSA 签名和门限签名方案的突出优点，Goldfeder 等人[9]提出了一种无中心椭圆曲线门限签名算法，该方案采用椭圆曲线数字签名算法和门限签名协议实现对区块链钱包私钥的多方控制。但该方案中，每个玩家都应该有相同的权重不太现实，且不能防止成员之间欺骗的问题。Dikshit 等人[10]在此基础上提出的方案能够根据权值/优先级 w 为每个玩家分配一个或多个密钥，这使得该方案更加现实，但需要更多的空间来储存份额，且没有解决成员之间欺骗的问题。在文献[11]中，Dikshit 对文献[10]进行了改进，提出了一种所有参与方均为单一份额，并能满足权重概念要求的方案，但仍存在成员间欺骗的风险。

针对以上问题，本文提出的方案在兼容 ECDSA 的基础上，不需要可信的中心分发秘密，能在不泄露秘密和其他秘密份额的情况下向参与者提供份额，且支持公开可验证的能力，任何参与者都可以对所有份额进行验证，能够防止成员间的欺骗问题。该方案能够用于保护区块链钱包，与传统钱包将私钥储存在一个位置不同，方案将私钥进行门限分割保护，可以防止单点故障问题，是有效的钱包保护技术。本方案基于门限特性和有限域上求解对数问题的困难性，方案具备高安全性。

1 预备知识

1.1 Shamir 门限方案[6]

Z 为有限域，q 是有限域上的大素数，n 个参与者 $P_i(i=1,2,\cdots,n)$。随机选择 $t-1$ 次多项式方程为

$$f(x)=a_0+a_1x+a_2x^2+\cdots+a_{t-1}x^{t-1} \bmod q$$

其中: $a_i\in Z(q)(i=1,2,\cdots,t-1)$; 计算 $s_i=f(x_i)$，$i=1,2,\cdots,n$，把 s_i 作为秘密份额发送给参与者 P_i; 利用其中任意 t 个子密钥则可重构秘密，即

$$s=f(0)=\sum_{i=1}^{t}s_{i_l}\prod_{l=1,l\neq i}^{t}\frac{-x_l}{x_i-x_l} \bmod q$$

1.2 非交互的 DLEQ(g_1,h_1,g_2,h_2,α) 协议

非交互的 DLEQ 协议是指非交互的离散对数相等的零知识证明协议[12]，该协议中，要求 g_1、g_2 是 q 阶乘法群 G_q 的两个生成元且 g_1、g_2 是素数，非交互的 DLEQ 协议使证明者 P 能够在不泄露秘密 α 的情况下向验证者 V 证明他知道秘密 $\alpha(\alpha\in Z_q^*$ 且 $\alpha=\log_{g_1}h_2)$。具体如下:

a) P 选择 $l\in_R Z_q^*$，计算 $a_1=g_1^l$，$a_2=g_2^l$，$c=H(a_1,a_2)$ 和 $r=l=\alpha c(\bmod q)$，然后公开 (r,c) 作为知道秘密的证据。

b) V 验证等式 $c=H(g_1^rh_1^c\parallel g_2^rh_2^c)$ 是否成立，如果成立，则相信 P，否则，反之。

1.3 标准椭圆曲线数字签名算法

给定在 $Z_p(p$ 为素数) 上的椭圆曲线 E，给定 q 阶基点 G、私钥 d 和要签名的消息 m，签名产生过程如下[13]:

a) 计算 $e=\mathrm{SHA}-1(m)$，使用 ANSI X9.62 中的方法将 e 转换为整数。

b) 选择随机整数 k，$k\in[1,n-1]$。

c) 计算 $(x_1,y_1)=kG$。

d) 用 ANSI X9.62 将 x_1 转换为整数，再计算 $r=x_1 \bmod q$，若 $r=0$，则返回步骤 b)。

收稿日期: 2019-11-05; 修回日期: 2020-01-11 基金项目: 国家自然科学基金资助项目(61373009,11701478); 四川省科技计划资助项目(2020YFG0045,2020YFG0238)

作者简介: 张中霞(1994-)，女，四川金堂人，硕士研究生，主要研究方向为信息安全; 王明文(1973-)，男(通信作者)，四川自贡人，副教授，硕导，博士，主要研究方向为信息安全、人工智能等(wangmw@swjtu.edu.cn).

e) 计算 $s = k^{-1}(e + dr) \bmod q$,若 $s = 0$,则返回步骤 b);否则,用密钥 d 对消息 m 的签名为 (r,s)。

1.4　改进的椭圆曲线数字签名算法

文献[14]将 ECDSA 签名算法进行了改进,能够避免有限域上的求逆运算,其安全性与 ECDSA 方案完全一样,但比 ECDSA 方案简单,实现速度也略快,更适用于门限方案。该方案具体推导过程如下:

设用户 A 的私钥为 P_{KA},由 $s = ke + dr$ 出发,用 e^{-1} 代替 e,得到 $s = e^{-1}k + dr$,化简 $se = k + der$,因为 $e = H(m)$ 是已知,则令 $s^* = se$,$s^* = k + der$,将 (s^*, r) 换成 (s,r),签名方程为 $s = k + der$。

签名算法:

a) 计算 $e = H(m)$。

b) 选择随机整数 $k, k \in [1, n-1]$,计算 $(x_1, y_1) = kG$。

c) 将 x_1 转换为整数,再计算 $r = x_1 \bmod q$,若 $r = 0$,则返回 b)。

d) 计算 $s = (k + der) \bmod q$,若 $s = 0$,则返回 b)。

e) 用密钥 d 对消息 m 的签名为 (r,s)。

验证算法:

a) 计算 $e = H(m)$。

b) 计算 $u = er \pmod q$。

c) $(x_1, y_1) = sG - uP_{KA}$,$r_1 = x_1 \bmod q$,若 $r = r_1$,则接受签名。

2　无中心可验证的 ECDSA 门限签名

本文提出的无中心可验证的 ECDSA 门限签名是采用文献[14]改进的签名方案,主要分为私钥共享阶段、门限签名阶段两大部分。在私钥共享阶段,本文采用了无中心可验证的门限方案[12,13]将私钥 d 分割,然后在门限签名阶段,计算出签名值。

2.1　私钥共享阶段

2.1.1　初始化

取 q(q 为素数)阶群 G_q 的两个生成元 g、h。p 表示大素数,且满足 $q \mid p-1$,G_q 为 Z_p^* 的唯一 q 阶子群。参与者 $P_i(i = 1,2,\cdots,n)$,各 P_i 的私钥表示为 Z_i,且 $Z_i \in Z_q$。对应的公钥表示为 $y_i = h^{Z_i} \pmod p$,秘密 $S = h^s$,$s \in {}_RZ_q^*$ H 表示一个密码 hash 函数,t 表示门限值,椭圆曲线参数组 $D = (E,G,q)$,消息 m。

2.1.2　无中心可验证密码分配

1) 密钥生成阶段

a) 参与者 $P_i(i = 1,2,\cdots,n)$ 选择多项式:

$$f_i(x) = \sum_{j=0}^{t-1} a_{ij} x^j \bmod q \quad a_{ij} \in {}_RZ_q^*$$

然后计算承诺:

$$C_{ik} = g^{a_{ik}} \bmod p \quad k = 0,1,\cdots,t-1$$

$$Y_{ij} = y_j^{f_i(j)} \bmod p \quad j = 0,1,\cdots,n$$

并公布 C_{ik}、Y_{ij}。

b) 参与者 P_i 使用非交互的 DLEQ 协议向其他成员证明他们收到的 Y_{ij} 是有效的,即满足

$$X_{ij} = g^{f_i(j)} \bmod p, Y_{ij} = y_j^{f_i(j)} \bmod p$$

P_i 随机选取 $w_{ij} \in {}_RZ_q^*$ $(j = 1,2,\cdots,n)$,计算

$$E_{1ij} = g^{w_{ij}} \bmod p, E_{2ij} = y_j^{w_{ij}} \bmod p \quad j = 1,2,\cdots,n$$

$$C_i = H(g \parallel h \parallel X_{i1} \parallel \cdots \parallel X_{in} \parallel Y_{i1} \parallel \cdots \parallel Y_{in} \parallel E_{1i1} \parallel \cdots \parallel E_{1in} \parallel E_{2i1} \parallel \cdots \parallel E_{2in}) \quad (1)$$

并计算:

$$R_i = (r_{i1} \cdots r_{in}) = (w_{i1} - c_i f_i(1) \pmod q, \cdots, w_{in} - c_i f_i(n) \pmod q)$$

公布证据 (C_i, R_i)。

c) 其他参与者根据 C_{ik} 来计算:

$$X_{ij} = \prod_{k=0}^{t-1} C_{ik}^{j^k} \bmod p \quad j = 1,2,\cdots,n$$

再利用已经知道的 $(C_i, r_{ij}, g, h, X_{ij}, Y_{ij})$ $(j = 1,2,\cdots,n)$,计算 E_{1ij},E_{2ij}:

$$E_{1ij} = g^{r_{ij}} X_{ij}^{c_i} \bmod p, E_{2ij} = y_j^{r_{ij}} Y_{ij}^{c_i} \bmod p \quad j = 1,2,\cdots,n$$

再验证式(1)是否成立。若成立,则表明成员 P_i 分发的份额是正确的;否则,指控 P_i。

d) 当所有参与者共享 Y_{ij},P_j 计算出加密的秘密份额: $Y_j^{Z_j^{-1}} = h^{\sum_{i=1}^{n} f_i(j)} = S_j$,其中 $Y_j = \prod_{i=1}^{n} Y_{ij}$,得到 S_j。

2) 秘密恢复阶段

任意 t 个参与者 $P_j(j = 1,2,\cdots,t)$ 参与秘密重构,并提供他们得到 S_j,使用非交互的 DLEQ 协议证明 S_j 确实是 Y_j 中得到的,即选取 $w_i \in {}_RZ_q^*$,计算 $b_{1j} = h^{w_j} \bmod p$,$b_{2j} = S_j^{w_j} \bmod p$,$r_j = w_j - c_j z_j \pmod q$,$c_j = H(b_{1j} \parallel b_{2j})$,公布 (r_j, c_j) 作为他们知道 S_j 的证据,其他参与者验证:

$$c_j = H(h^{r_j} y_j^{c_j} \parallel s_j^{r_j} Y_j^{c_j}) \quad (2)$$

是否成立。若成立,则可证明。参与者根据

$$S = \prod_{j=1}^{t} S_j^{\lambda_j} \quad (3)$$

$$\lambda_j = \prod_{l \neq j, l=1}^{t} \frac{j}{l-j}$$

恢复秘密。

2.2　ECDSA 门限签名阶段

利用 2.1 节中无中心可验证密码分配的方法,将签名私钥 d 在 n 个参与者 P_i 之间共享,签名公钥 $y = dG$。

1) 签名阶段

a) 计算 $e = H(m)$。

b) 任意 t 个参与者 $P_i(i = 1,2,\cdots,t)$,随机选取 $k_i \in {}_RZ_q^*$,计算 $k_i G$,并发送给 $P_j(j = 1,2,\cdots,t, j \neq i)$,参与者 P_i 使用非交互的 DLEQ 协议证明其他成员相信他们收到的 $k_i G$ 是有效的,即计算 $a_{1i} = g^{k_i} \bmod p$,$a_{2i} = h^{k_i} \bmod p$,$r_i = k_i - c_i k_i G \pmod q$,$C_i = H(a_{1i} \parallel a_{2i})$,公布 (r_i, c_i)。

其他参与者可验证下式是否成立:

$$C_i = H(g^{r_i} g^{k_i^G c_i} \parallel h^{r_i} h^{k_i G c_i})$$

c) P_i 计算 $\sum_{i=1}^{t} k_i G = kG = (x_1, y_1)$,$\sum_{i=1}^{t} k_i = k$。将 x_1 转换为整数,再计算 $r = x_1 \bmod q$,若 $r = 0$,则返回步骤 b)。

d) 参与者 $P_i(i = 1,2,\cdots,t)$ 利用第 2 章中的无中心可验证密码分配的方法,获得签名私钥 $d = \prod_{i=1}^{t} S_i^{\lambda_i}$,$\lambda_j = \prod_{l \neq j, l=1}^{t} \frac{j}{l-j}$,则任意 t 个参与者 $P_i(i = 1,2,\cdots,t)$ 可计算出 s:

$$s = \left(\sum_{i=1}^{t} k_i + er \prod_{i=1}^{t} S_j^{\lambda_j}\right) \bmod q, \lambda_j = \prod_{l \neq j, l=1}^{t} \frac{j}{l-j}$$

e) 若 $s = 0$,则跳至步骤 b);否则,返回 (r,s)。

2) 验证阶段

a) 计算 $e = H(m)$。

b) 计算 $u = er \pmod q$。

c) 将已得到的 (r,s) 代入下面计算:

$$(x_1, y_1) = sG - uy \quad (4)$$

$r_1 = x_1 \bmod q$,若 $r = r_1$,则接受签名。

3　安全性与正确性分析

3.1　正确性分析

定理 1　非交互零知识证明保障了分发秘密的正确性。

证明　在密钥分发阶段,任意成员 P_i 可以根据 $(C_i, r_{ij}, g, h, X_{ij}, Y_{ij})$ $(j = 1,2,\cdots,n)$,计算 E_{1ij} 和 E_{2ij}:

$$g^{r_{ij}} X_{ij}^{c_{ij}} \bmod p = g^{w_{ij} - c_i f_i(j)} X_{ij}^{c_{ij}} \bmod p = g^{w_{ij} - c_i f_i(j)} g^{f_i(j) c_i} \bmod p = g^{w_{ij}} = E_{1ij}$$

$$y_j^{r_{ij}} Y_{ij}^{c_{ij}} \bmod p = y_j^{w_{ij} - c_i f_i(j)} Y_{ij}^{c_{ij}} \bmod p = y_j^{w_{ij} - c_i f_i(j)} y_j^{c_i f_i(j)} \bmod p = y_j^{w_{ij}} = E_{2ij}$$

再将 E_{1ij}、E_{2ij} 代入式(1)可得到 C_i 是否与公布的相等,若相等则表明成员 P_i 分发的份额是正确的。在密钥重构阶段,每个成员通过自己的私钥解密 S_j,非交互零知识证明保障了 S_j 确实是从私钥 Z_j 中解密的,这是因为根据 (r_j, c_j) 有:

$$h^{r_j} y_j^{c_j} \bmod p = h^{w_j - c_j Z_j} y_j^{c_j} \bmod p = h^{w_j - c_j Z_j} h^{c_j Z_j} \bmod p = h^{w_j} \bmod p = b_{1j} \bmod p$$

$$S_j^{r_j} Y_j^{c_j} \bmod p = S_j^{w_j - c_j Z_j} Y_j^{c_j} \bmod p = S_j^{w_j - c_j Z_j} S_j^{c_j Z_j} \bmod p = S_j^{w_j} \bmod p = b_{2,j} \bmod p$$

将 b_{1j}、b_{2j} 代入式(2),判断 c_j 是否与公布的一致,若一致,则分发秘密正确。

定理 2　秘密的正确性。任何 t 个诚实的参与者都可以合作重构出正确的秘密。

证明　假设 t 个股东持有的秘密是 $S_1, S_2, \cdots, S_t$,下面的方程成立:

$$\prod_{j=1}^{t} S_j^{\lambda_j} = \prod_{j=1}^{t} (Y_j^{Z_j^{-1}})^{\lambda_j} = \prod_{j=1}^{t} \left(\prod_{i=1}^{t} Y_{ij}\right)^{Z_j^{-1}\lambda_j} = \prod_{j=1}^{t} \left(y_j^{\sum_{i=1}^{t} f_i(j)}\right)^{Z_j^{-1}\lambda_j} =$$

$\prod_{j=1}^{t}\left(h^{\sum_{i=1}^{t}f(j)}\right)^{Z_j^{-1}\lambda_j}=h^{\sum_{j=1}^{t}\sum_{i=1}^{t}f(j)\lambda_j}=h^{\sum_{i=1}^{t}\sum_{j=1}^{t}f(j)_{i\neq j}\prod_{i\neq j}\frac{-x_j}{x_i-x_j}}-h^{s}=S$

所以,定理成立。

定理 3 如果式(4)成立,则门限签名有效。

证明 因为 $\prod_{j=1}^{t}S_j^{\lambda_j}=s=d$,则 $sG-uy=\left(\sum_{i=1}^{t}k_i+er\prod_{i=1}^{t}S_j^{\lambda_j}\right)G-uy=(k+erd)G-erdG=kG=(x_1,y_1)$。

证毕。

3.2 安全性分析

a) 计算安全性。该方案是基于求解有限域上椭圆曲线离散对数问题的困难性和门限方案的安全性实现的,所以在计算上是安全的,若非参与者想从签名公钥 $y=dG$ 中得到签名私钥,则需解决椭圆曲线离散对数问题,所以是不行的。

b) 鲁棒性。当参与者的数量 $n\geqslant 2t-1$ 时,即使有 $t-1$ 个不诚实的参与者,该方案也能重构出秘密,不影响签名。这是因为参与者在密钥产生阶段,验证者能够通过公布的 (C_i,R_i) 计算出 E_{1ij}、E_{2ij},再将 E_{1ij}、E_{2ij}、X_{ij}、Y_{ij}、g、h 代入式(1)中,看得到的 C_{ij} 是否与公布的相等。若相等,参与者可以根据自己的私钥获得 $Y_j^{Z_j^{-1}}=S_j$,因为 $n\geqslant 2t-1$,即使存在 $t-1$ 个不诚实者,也有 t 个参与者是诚实的,也能根据式(2)求出正确的秘密,不会影响到整体签名。

c) 抗成员欺骗攻击。方案通过非交互零知识证明来防止成员之间的欺骗行为。每个成员都可通过公布的参数来验证其他成员发布的秘密份额是否有效,即验证 $c_j=H(h^r y_j^{c_j}\parallel d_j^r Y_j^{c_j})$ 是否成立,若不成立,则指控该成员,并拒绝接受他的秘密份额。因此,该方案能够防止成员之间的欺骗,但这种欺骗对文献[11]中所描述的方案却是有效的,成员无法检测出其获得的子秘密的真伪,最终导致恢复的秘密错误。

d) 门限特性。任意少于 t 个签名者合作都无法重构秘密。拥有秘密的 $t-1$ 次多项式上的 $t-1$ 个点,不足以确定该多项式。这是因为 $t-1$ 个线性方程组里面约束的数目少于未知数的数目,所以方程有无数解,而不是唯一一组解。因此任意 $t-1$ 或少于 $t-1$ 个签名者合作无法获得其他签名者的秘密密钥。

e) 攻击者无法从公布的 Y_{ij}、S_i 中获得关于成员私钥 Z_j 的任何信息。假设攻击者获得了 Z_j,即 $Y_j^{Z_j^{-1}}=S_j$,$Y_j=\prod_{i=1}^{n}Y_{ij}$,则攻击者具有在有限域上求解离散对数的问题能力,而事实在计算上是不可行的,所以假设不成立。

4 性能分析

下面是本文方案与各方案间的比较。门限方案中,文献[8]的方案虽然能公开验证份额,但不能同时对多个秘密进行共享,且需要可信中心。文献[16]的方案能对份额进行验证,但不支持公开验证份额。文献[17,18]的方案能一次对任意多个秘密进行共享,但不具有可(公开)验证能力,也需要可信中心的参与。文献[19]的方案能一次对多个秘密进行共享,但不具有公开验证的能力,且需要可信中心的参与。

基于门限思想的椭圆曲线签名方案中,文献[9,11]虽能验证份额,也不需要可信中心,但不具备公开验证功能。文献[9]中要求每个玩家都应该有相同的权重,不太现实,且不能防止成员之间的欺骗问题。文献[10]在文献[9]的基础上进行改进,使该方案更加现实,但需要更多的空间来储存份额,且没有解决成员之间欺骗的问题。文献[11]对文献[10]进行了改进,但仍存在成员间欺骗的风险。本文提出的方案不仅能公开验证份额,而且不需要可信中心,能抗成员欺骗攻击,可用于保护区块链钱包。表 1 给出了几种方案在相关方面的比较。

表 1 相关工作比较

方案	是否能验证份额	是否具有公开可验证属性	是否不需要可信中心
文献[8]	是	是	否
文献[9,11]	是	否	否
文献[16]	是	否	否
文献[17,18]	否	否	否
文献[19]	是	否	否
本文方案	是	是	是

5 结束语

传统的区块链钱包保护方案中,都将私钥存储在一个位置,会面临单点故障的问题,本文基于门限思想,提出了一种适用于区块链钱包保护的椭圆曲线门限签名方案,将私钥分割,并在参与者间共享,有效抵抗了单点攻击,攻击难度等价于求解有限域上的离散对数问题。此外,本方案不依赖可信的分发中心共享秘密,提升了钱包保护方案的可用性。使用非交互零知识证明协议保证了参与者能够在不泄露各自秘密的情况下恢复秘密,保障了秘密的安全性,同时还能防止参与者间的欺骗行为,任何参与者都可以验证秘密份额的正确性。最后,本文还证明了方案的正确性和安全性。安全性分析表明,本文的门限方案能够有效抵抗成员间的欺骗行为,且具有良好的鲁棒性。

参考文献:

[1] Bitstar coin. Transaction [EB/OL]. (2014) [2020-01-23]. https://en.bitcoin.it/wiki/Transactions.

[2] Nakamoto S. Bitcoin: a peer-to-peer electronic cash system [EB/OL]. (2018) [2020-01-23]. https://bitcoin.org/bitcoin.pdf.

[3] Antonopoulos A M. 精通比特币 [M]. 薄荷凉幼,陈萌琦,陈姝吉,等译. 1 版. 南京: 东南大学出版社,2016: 50-64.

[4] Benoit O, Peyrin T. Side-channel analysis of six SHA-3 candidates [M]. Berlin: Springer, 2010: 140-157.

[5] Piret G, Roche T, Carlet C. PICARO: a block cipher allowing efficient higher order side-channel resistance [M]. Berlin: Springer, 2012: 311-328.

[6] Shamir A. How to share a secret [J]. Communications of the ACM, 1979, 22(11): 612-613.

[7] Stadler M. Publicly verifiable secret sharing [C]//Proc of International Conference on the Theory and Applications of Cryptographic Techniques. Berlin: Springer, 1996: 190-199.

[8] Schoenmakers B. A simple publicly verifiable secret sharing scheme and its application to electronic voting [C]//Proc of Annual International Cryptology Conference. Berlin: Springer, 1999: 148-164.

[9] Goldfeder S, Gennaro R, Kalodner H, *et al*. Securing Bitcoin wallets via a new DSA/ECDSA threshold signature scheme [EB/OL]. (2015) [2020-01-23]. https://www.cs.princeton.edu/ stevenag/thresholdsigs.pdf.

[10] Dikshit P, Singh K. Weighted threshold ECDSA for securing Bitcoin wallet [J]. Accentas Trans on Information Security, 2016(2): 43-51.

[11] Dikshit P, Singh K. Efficient weighted threshold ECDSA for securing Bitcoin wallet [C]//Proc of ISEA Asia Security and Privacy. Piscataway, NJ: IEEE Press, 2017: 1-9.

[12] Yu Jia, Kong Fanyu, Hao Rong. Publicly verifiable secret sharing with enrollment ability [C]//Proc of the 8th ACIS International Conference on Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing. Piscataway, NJ: IEEE Press, 2007: 194-199.

[13] Bitstar coin. Elliptic curve digital signature algorithm [EB/OL]. (2014) [2020-01-23]. https://en.bitcoin.it/wiki/Elliptic_Curve_Digital_Signature_Algorithm.

[14] 杨君辉,戴宗铎,杨栋毅,等. 一种椭圆曲线签名方案与基于身份的签名协议 [J]. 软件学报,2000,11(10): 1303-1306.

[15] 于佳,陈养奎,郝蓉,等. 无可信中心的可公开验证多秘密共享 [J]. 计算机学报, 2014, 37(5): 1030-1038.

[16] Feldman P. A practical scheme for non-interactive verifiable secret sharing [C]//Proc of the 28th IEEE Symposium on the Foundations of Computer Science. Piscataway, NJ: IEEE Press, 1987: 427-437.

[17] He J, Dawson E. Multistage secret-sharing scheme based on one-way function [J]. Electronics Letters, 1994, 30(19): 1591-1592.

[18] Yang C C, Chang T Y, Hwang M S. A (t,n) multi-secret sharing scheme [J]. Applied Mathematics and Computations, 2004, 151(2): 483-490.

[19] Dehkordi M H, Mashhadi S. New efficient and practical verifiable multi-secret sharing scheme [J]. Information Sciences, 2008, 178(9): 2262-2274.