计算机科学 COMPUTER SCIENCE
http://www.jsjkx.com
DOI:10.11896/jsjkx.201000032

基于门限环签名的分级匿名表决方案

范家幸[1]　王志伟[1,2,3]
1 南京邮电大学计算机学院　南京 210023
2 江苏省大数据安全与智能处理重点实验室　南京 210023
3 江苏省计算机网络技术重点实验室　南京 210096
(jx_fan@126.com)

摘　要　表决是现代民主社会常用的一种方式,涉及政治、股份企业、法院判决等多个领域。表决是一种特殊的投票,它只有“同意”和“否决”两个候选对象,一方票数过半即得结果。区块链作为一种自带对账功能的数字记账技术,具有时间戳、公开性、不可篡改等特性,满足表决的透明性和可验证性。为实现表决的匿名性,文中采用环签名来隐藏表决内容与表决者的对应关系。文中提出的分级匿名表决方案,实现了表决的合法性、保密性、不可重复性、可更新性和可验证性。通过为表决者产生虚拟身份形成层级机制,可用于各表决者持票数不等的场景;分级匿名表决协议将门限环签名方案运用到表决场景,使得表决过程中一旦一方票数过半即可签名得到最终的表决结果,计票过程简单、高效。

关键词:匿名表决;区块链;分级;门限环签名;虚拟身份
中图法分类号　TP309

Hierarchical Anonymous Voting Scheme Based on Threshold Ring Signature

FAN Jia-xing[1] and WANG Zhi-wei[1,2,3]
1 School of Computer,Nanjing University of Posts and Telecommunications,Nanjing 210023,China
2 Jiangsu Key Laboratory of Big Data Security and Intelligent Processing,Nanjing 210023,China
3 Jiangsu Key Laboratory of Computer Networking Technology,Nanjing 210096,China

Abstract　Voting is a commonly used method in modern democratic society,involving many fields such as politics,stock companies,court decisions,etc. Voting is regarded as a specific form of balloting,with only two candidates in pro and con. Blockchain is a digital accounting technology with the characteristics of time stamp,openness and non-tamperability which satisfy the transparency and verifiability of voting. In order to realize the anonymity of voting,this paper uses ring signature to hide the correspondence between voting content and the voter. This paper puts forward a hierarchical anonymous voting scheme,which realizes the legitimacy,confidentiality,non-repeatability,updateability and verifiability of voting. By creating a hierarchy mechanism for the voting of virtual identities,it can be used in situations where the votes vary from vote to each voter,and this agreement applies the threshold ring signature scheme to the voting scene for the first time,making the voting process simple and efficient for the final voting results once one party has more than half of the votes cast.

Keywords　Anonymous voting,Blockchain,Hierarchical,Threshold ring signature,Virtual identity

1　引言

表决是现代民主社会常用的一种方式,涉及政治、股份企业、法院判决等多个领域。表决是一种特殊的投票,它只有“同意”和“否决”两个候选对象。由于网络的迅速发展以及现场组织投票的复杂性,电子投票逐渐成为人们研究的热点问题。电子投票需要满足合法性、保密性、可验证性、不可重投性、可更新性等安全要求,安全性问题一直是制约电子投票发展的瓶颈。如比利时大选由于电子投票机的漏洞,导致无法统计出正确票数、瑞士投票系统遭漏洞篡改等问题,一些国家已经停止使用电子投票。因此,研究电子投票的安全性,设计保护隐私的电子投票方案是非常必要的,许多研究者针对电子投票的安全性,利用各种密码学技术提出了许多安全性较高的电子投票方案。

1981 年,Chaum[1] 首先提出了电子投票的概念,与传统的纸质投票相比,电子投票在计票准确性、人力成本和实现范围等方面都有明显优势。一个完善的投票系统需要具备透明性、准确性、可验证性、保密性、可更新性[2-4] 等。基于密码学

到稿日期:2020-10-08　返修日期:2021-04-04
基金项目:国家自然科学基金(61672016)
This work was supported by the National Natural Science Foundation of China(61672016).
通信作者:王志伟(zhwwang@njupt.edu.cn)

的电子投票方案一般分为3种：基于盲签名技术[5]、基于同态加密算法[6-7]和基于混网方案[8-9]。Kumar等提出了使用基于身份的盲签名方案的安全匿名电子投票系统[10]，该方案基于随机预言机模型，在随机预言机模型下证明安全的方案在实际具体实现中未必是安全的。另外，盲签名的投票方案缺少通用的可验证性。基于同态加密方案最早由Cohen等[11]提出，常使用EIGamal[12]，Pailler[13]加密算法，同态加密方案的运行效率高、实现难度小，但计算成本较高。另外，纯粹的"可压缩"同态加密不适合处理写入选票。基于混网的投票方案最先由Chaum提出，由于其系统较为复杂，因此运行较效率低，尤其体现在大规模选举下计票速率缓慢。

环签名方案[14]允许群成员匿名地代表群组签名，群的组成是自发的，并且不存在群管理员来撤销签名者的身份。另外，无法判断两个签名是否是同一个群成员发布的。签名者与具体的签名方案相关联，其使用群成员的公钥共同产生签名，这些群成员可能完全不知道自己被参与进去了。自Rivest等于2001年正式提出环签名以来，出现了许多对环签名方案的改进，然而几乎所有的变化都依赖于随机oracle模型来进行安全性证明。Chow等[15]提出了一种基于双线性对的环签名方案，该方案被证明在不使用随机预言机模型的情况下对自适应选择消息攻击是安全的。环签名方案可以用于匿名举报[16]、电子投票[17-18]等，Tsang等[19]在上述提出的可链接环签名方案上构建了一个电子投票方案，可链接环签名允许任何人确定两个环签名是否为同一组成员签名。Bresson等[20]在环签名的基础上首次提出了d-out-of-n门限环签名，该签名在随机预言机模型下被证明是安全的，但在具体应用中的实现未必是安全的。与传统投票不同，表决的候选项只有两个，因此本文在表决方案中引入并扩展了门限环签名[21]，合理地设置门限值即可满足表决场景中一方得票数过半得到结果的特性，该方案是第一个在标准模型中被证明安全性的方案。

区块链具有去中心化、数据防篡改、交易可追溯等特点，引入区块链技术可以为电子投票系统提供去中心可信第三方TTP服务，以保证投票过程的透明化与公平性，使用户具有更强的自主性，增强用户对协议的信任度。近年来，有许多学者提出了基于区块链的电子投票方案。Hjalmarsson等[22]将投票过程做成智能合约，构建了一个区块链上的投票系统，利用智能合约来确保选民隐私，审查了适合构建基于区块链的电子投票的现有区块链框架。Hardwick等[23]提出了一种基于区块链技术的电子投票方案，该方案提供了一定程度的权力下放，使得选民对票选有更多的控制权，同时讨论了支持电子投票方案的实施挑战和底层平台(区块链和智能合约)的局限性。仅依靠区块链技术来实现电子投票存在一定的安全隐患，因此，在本文方案中区块链技术仅作为一种实现表决公开性的平台，选民的隐私保护、可更新性、分级表决等特性都是依靠密码学技术来实现的。

本文的贡献如下：1)首先为基于门限环签名的分级匿名表决方案提出了系统模型和安全模型；2)通过扩展Yuen等[21]的门限环签名方案，构建了一个具体方案，实现了分级匿名表决的合法性、保密性、不可重复性、可更新性和可验证性；3)对门限环签名的不可伪造性和匿名性进行了证明，对提出的表决协议进行了安全分析。

本文第2节介绍了门限环签名的相关定义；第3节介绍了协议的参与方以及安全模型；第4节具体描述了协议的5个阶段以及实现细节；第5节对协议用到的门限环签名方案进行了安全性证明；第6节对表决协议进行了安全性分析；最后总结全文。

2 预备知识

2.1 配对

本协议用到的签名方案使用复合阶双线性群，令$n=pq$，参数如表1所列。

表1 符合和含义

Table 1 Symbols and meanings

符号	含义
G	n阶乘法循环群
G_p,G_q	G_p是G的p阶循环子群，G_q是G的q阶循环子群
g,h	g是G的生成元，h是G_q的生成元
G_T	G_T是n阶乘法群
$\hat{e}$	$\hat{e}$是双线性映射，$\hat{e}:G\times G\rightarrow G_T$
$G_{T,p},G_{T,q}$	$G_{T,p}$和$G_{T,q}$分别是G_T的p阶、q阶子群

其中，$\hat{e}$有以下性质：

(1)双线性。$u,v\in G$且$a,b\in Z$，有$\hat{e}(u^a,v^b)=\hat{e}(u,v)^{ab}$。

(2)非退化性。当$\langle g\rangle=G$，$\langle\hat{e}(g,g)\rangle=G_T$。

(3)可计算性。对于所有$u,v\in G$，$\hat{e}(u,v)$都是可计算的。

2.2 数学假设

对于协议中的所用密码方案，依赖于以下困难假设。

定义1(G_p中的计算性Diffie-Hellman假设) 已知元组(r,r^a,r^b)，其中$r\in_R G_p$且$a,b\in_R Z_p$，设多项式时间算法C至少以概率ε计算出r^{ab}。如果概率$Pr[C(r,r^a,r^b)=r^{ab}]\geqslant\varepsilon$，则称算法$C$具有优势$\varepsilon$。如果敌手不能在时间$t$内以不可忽略的概率解决CDH问题，则称在$G_p$中$(t,\varepsilon)$-CDH假设成立。

定义2(子群决策假设) w选自G和G_q的概率分别是1/2，判断w是否属于G_q。如果敌手不能判断出结果，则称子群决策问题假设成立。

通过估计敌手成功解决Diffie-Hellman问题和子群决策问题的概率来对假设进行形式化。按照以上公式，如果CDH问题在G_q中是难以解决的，那么在G中也是如此。Boneh[24]将子群决策问题难以解决的假设称为子群隐藏(SGH)假设。

2.3 门限环签名

这里引用Yuen等提出的门限环签名方案(TRS)[21]，由以下4种算法组成。

(1)$(sk_i,pk_i)\leftarrow KenGen(\lambda)$：输入安全参数$\lambda\in N$，输出一个公私钥对$(sk_i,pk_i)$。$SK$和$PK$分别是私钥和公钥的域。

(2)$param\leftarrow Setup(\lambda)$：输入安全参数$\lambda\in N$，输出一个包括$\lambda$在内的安全集param。

(3)$\sigma'=(n,d,y,\sigma)\leftarrow Sign(\hat{e},n,y,\chi,M)$：输入群规模$n$，门限$d\in\{1,\cdots,n\}$，$PK$中的$n$个公钥组成的集合$y$，$y$中公钥对应的私钥组成的集合$\chi$以及消息$M$，输出签名$\sigma$。

(4)$accecpt/reject\leftarrow Verify(n,d,y,M,\sigma)$：输入群规模$n$，门限$d\in\{1,\cdots,n\}$，$PK$中的$n$个公钥组成的集合$y$，消息签名对$(M,\sigma)$，返回接受或拒绝。若接受，则表明此消息签名对是合法的。

3 系统模型和安全模型

3.1 系统模型

系统模型如图1所示，包含3个主体，分别为表决者、公正人员和区块链。角色定义如下：

(1)表决者。表决者可能是公司董事，为通过某个议案进行表决；也可能是英美陪审团制度下的陪审团成员，需要对某一案件结果进行表决等，这些表决者大多时候需要隐藏自己的身份来防止自己的表决结果被泄露。

(2)公正人员。他们是可信方，分为两方分别接收同意票和反对票并对其进行统计，并发布最终的表决结果。记接收同意票的一方为 Teller$A$，接收否决票的一方为 Teller$B$。

(3)区块链。整个表决过程包括人员注册、审核、个人表决、票数统计以及发布结果都在区块链上进行。

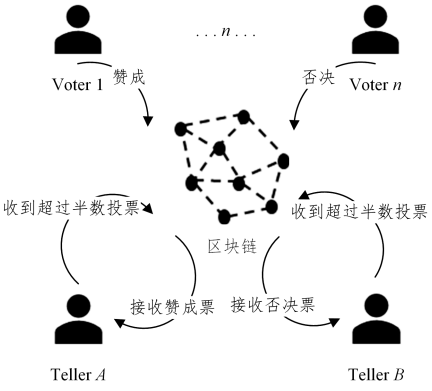

图1 系统模型

Fig. 1 System model

3.2 安全模型

在实际应用中，一个安全的表决系统应满足以下属性：

(1)合法性。只有符合要求的人员可以参与此次表决，使攻击者无法伪造合法表决。

(2)表决保密性。其他人无法知道表决者的表决结果。

(3)可验证性。可验证性分为个体可验证性和全局可验证性，个体可验证性指任何表决者都可以验证自己的表决被计入结果；全局可验证性指任何表决者都可以验证其他表决者表决的合法性。

(4)不可重复性。每名表决者只有一票被计入最终表决结果。

(5)可更新性。表决截止时间前，表决者可修改自己的表决意见。

基于以上的安全目标，协议采用门限环签名来签署表决意见。对于一些具有重要身份的表决者，可以根据实际情况来增加他们表决结果的比重。例如，股份有限公司的表决权是按照股东所持股份来计算的，而不是按照股东人数。在第4节提出的匿名表决协议中，我们将表决人员分成三级，一级人员拥有一票，二级人员拥有两票，三级人员拥有三票。其中用到了以下3个预言机，它们共同模拟了敌手破坏方案安全性的能力。

(1)$pk_i \leftarrow \mathcal{JO}(\perp)$：添加新用户到系统中并返回其公钥 pk_i。

(2)$sk_i \leftarrow \mathcal{CO}(pk_i)$：输入查询 $\mathcal{JO}$ 后得到的公钥 $pk_i \in PK$，并返回对应的私钥 $sk_i \in SK$。

(3)$\sigma \leftarrow \mathcal{SO}(n, d, y, v, M)$：输入群规模 n，门限值 $d \in \{1, \cdots, n\}$，n 个公钥的集合 y，参与签名的 d 个用户公钥集 v 以及消息 M，返回一个合法签名 σ'。

下面给出两个安全定义。

(1)不可伪造性

本方案中的不可伪造性在模拟器 $\mathcal{S}$ 和敌手 $\mathcal{A}$ 之间的游戏中进行了定义，其中敌手 $\mathcal{A}$ 有对预言机 $\mathcal{JO}$，$\mathcal{CO}$ 和 $\mathcal{SO}$ 的访问权限：

1)$\mathcal{S}$ 产生系统参数 param 给敌手 $\mathcal{A}$。

2)敌手 $\mathcal{A}$ 根据任何自适应策略查询预言机。

3)敌手 $\mathcal{A}$ 将群大小 $n \in N$，门限 $d \in (1, \cdots, n)$，PK 中的 n 个公钥集合 y，消息 $M \in \mathcal{M}$ 和签名 $\sigma \in \Sigma$ 提供给模拟器 $\mathcal{S}$。

若满足以下条件 $\mathcal{A}$，则赢得游戏：

1)$Verify(\cdot) = accept$。

2)y 中所有公钥都是 $\mathcal{JO}$ 的查询输出。

3)y 中最多输出 $(d-1)$ 个公钥到 $\mathcal{CO}$ 中。

4)(M, y) 不是 $\mathcal{SO}$ 的查询输入。

本文定义 $\mathrm{Adv}_{\mathcal{A}}^{unf}(\lambda) = \Pr[\mathcal{A} \text{ wins the game}]$。

定义 3(不可伪造性) 若对于所有的概率多项式时间的敌手 $\mathcal{A}$，$Adv_{\mathcal{A}}^{unf}(\lambda)$ 是可以忽略的，则称门限环签名方案是不可伪造的。

(2)匿名性

本方案中的匿名性在模拟器 $\mathcal{S}$ 和敌手 $\mathcal{A}$ 之间的游戏中进行了定义，其中敌手 $\mathcal{A}$ 有对预言机 $\mathcal{JO}$，$\mathcal{CO}$ 和 $\mathcal{SO}$ 的访问权限：

1)$\mathcal{S}$ 产生系统参数 param 给敌手 $\mathcal{A}$。

2)敌手 $\mathcal{A}$ 根据任何自适应策略查询预言机，假设 $\mathcal{A}$ 对 $\mathcal{CO}$ 共进行了 v 次查询，则有如下限制：$v < n - d$。

3)敌手 $\mathcal{A}$ 将群大小 $n \in N$，门限 $d \in (1, \cdots, n)$，消息 M，n 个来自 $\mathcal{JO}$ 的查询输出的公钥集合 y 提供给模拟器 $\mathcal{S}$。$\mathcal{S}$ 随机选择 y 的子集 v，其中 $|v| = d$，且 v 中不包含任何对 $\mathcal{CO}$ 和 $\mathcal{SO}$ 的查询。令 χ 是私钥集合，$|\chi| = d$ 且私钥对应的公钥都包含在 v 中。$\mathcal{S}$ 计算 $\sigma' = Sign(n, d, y, v, \chi, M)$。

4)$\mathcal{A}$ 自适应地查询预言机。假设 $\mathcal{A}$ 共对 $\mathcal{CO}$ 进行了 v' 次查询，限制 $v' < n - d - v$。若任何对 $\mathcal{SO}$ 或 $\mathcal{CO}$ 的查询包含公钥 pk，则使得 $pk \in y$，则 $\mathcal{S}$ 停止。

5)$\mathcal{A}$ 输出下标 $\hat{\pi}$。

本文定义 $Adv_{\mathcal{A}}^{Anon}(\lambda) = \Pr[\hat{\pi} \in y] - \dfrac{d}{n-(v+v')}$。

定义 4(匿名性) 若对于所有概率多项式时间敌手 $\mathcal{A}$，$Adv_{\mathcal{A}}^{Anon}(\lambda)$ 是可以忽略的，则称该方案是匿名的。

综上所述有：

定义 5(门限环签名方案的安全性) 如果一个门限环签名方案是不可伪造且匿名的，则这个方案是安全的。

4 基于门限环签名的分级匿名表决协议

根据上述的系统模型和安全模型，下面给出具体的分级匿名表决协议。该协议描述了各个表决阶段的执行细节：

准备阶段、注册阶段、表决过程、票数统计以及发布结果。

4.1 准备阶段

公正方产生区块链的初始块，并将待表决内容、表决规范（M_a表示同意，M_d表示否决）、各个阶段时间节点、公共参数以及公正方的签名验证密钥放在初始块上。一条简单的区块链如图2所示，初始块包含公开信息并关联特定的表决事件，每个Token对应一条投票记录。

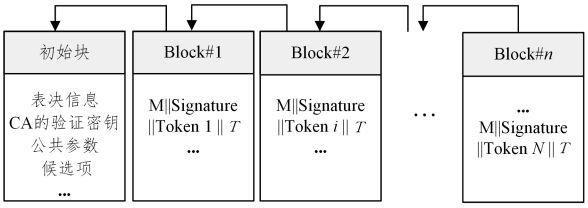

图2 投票区块链

Fig. 2 Voting blocks

公共参数的产生：双线性组发生器产生系统参数$(N=pq, G, G_T, \hat{e}) \leftarrow g(1^\lambda)$。发生器$g$同时给出生成元$g_1, B_0, u, u_1, \cdots, u_k \in G, h_1 \in G_q$和$\alpha \in Z_N$。设$g_2 = g_1^\alpha, h_2 = h_1^\alpha$。令$H: N \times G^* \times \{0,1\}^* \rightarrow \{0,1\}^k$，$H_0: \{0,1\}^* \rightarrow G$为密码学上的哈希函数。公共参数如下：$(N, G, G_T, \hat{e}, g_1, g_2, B_0, h_1, h_2, u, u_1, \cdots, u_k, H, H_0)$。

4.2 注册阶段

每个用户选择$s_i \in_R Z_N$用户的公钥为$g_1^{s_i}$，私钥为$g_2^{s_i}$，公钥唯一标识了用户身份。想要参与表决的用户在注册截止时间前对自己的身份信息签名后发送给CA（可由Teller$A$或者Teller$B$担任），由CA审核用户身份，当CA收到n个合法用户的签名后，开启群验证，验证ID和签名者是否匹配。验证通过后向用户发放表决Token，使其成为合法表决者。具体过程如下：

(1)用户i对身份信息m_i签名$\sigma_i = H_0(m_i)^{s_i} \cdot sk_i$，并将$(m_i, \sigma_i)$发送给CA，CA收到后首先查看其公钥是否在表决者名单中，若不在则直接丢弃此条记录。若发现重复的身份信息m_i，则验证$\hat{e}(\sigma_i, g_1) = \hat{e}(H_0(m_i) \cdot g_2, pk_i)$，并剔除不合法的信息签名对。假设在规定时间内共收到$n(n$为奇数$)$个合法用户的签名，开启群验证来减少验证次数。计算$\sigma = \sigma_1, \cdots, \sigma_n$，验证$\hat{e}(\sigma, g_1) = \hat{e}(H_0(m_1) \cdot g_2, pk_1), \cdots, \hat{e}(H_0(m_n) \cdot g_2, pk_n)$，为了减少计票员在统计票数时存储公钥的空间，下面使用公钥聚合后的群验证：

$$\begin{cases} apk = \prod_{i=1}^{n} pk_i^{H_1(pk_i, \{pk_1, \cdots, pk_n\})} \\ \sigma_i = (H_0(m_i)^{s_i} \cdot sk_i)^{a_i}, a_i = pk_i^{H_1(pk_i, \{pk_1, \cdots, pk_n\})} \\ \sigma = \prod_{i=1}^{n} \sigma_i, M = \prod_{i=1}^{n} H_0(m_i) \\ 验证: \hat{e}(\sigma, g_1) = \hat{e}(M \cdot g_2, apk) \end{cases}$$

通过验证后，CA根据用户V_i的身份将其分为3个等级，一级用户拥有一票表决权，二级用户拥有两票表决权，三级用户拥有三票表决权；并产生相应人数的$Token: et_i = Sign_{CA}(V_{ipub})$，两个随机数$a, b$，设一级用户的下标为$i$，二级用户下标为$j$，三级用户的下标为$z$，其中$pk_j^a \neq pk_i \neq pk_z \neq pk_z^b$，$pk_z^a \neq pk_z^b \neq pk_i \neq pk_j$，且$a, b$是公开的，$pk_j^a$，$pk_z^b$作为虚拟合法表决者。表决者的分级信息如表2所列。

表2 表决者的分级信息

Table 2 Hierarchical information of voters

等级	虚拟身份	持有票数
一级	无	1
二级	pk_j^a	2
三级	pk_z^a and pk_z^b	3

为了避免CA通过Token将用户身份与选票对应，将Token随机发放给每个表决者，这里的“随机”可以由智能合约实现，并由CA调用合约接口，表决者只需要接收Token，智能合约的功能就是将所有Token随机分配给每个合法用户。当然，实现“随机”的方法可以根据不同的系统实现灵活选择，本文只是提出一种方案，因此不再阐述实现细节。表决者可以通过验证CA的签名来判断Token的真伪。Token可看作是表决者收到的选票。在表决者收到各自对应的Token后，二级表决者V_j可通过计算sk_j^a获得公钥为pk_j^a的虚拟身份对应的私钥。类似地，三级表决者可获得公钥为pk_z^a和pk_z^b的虚拟身份对应的私钥。

(2) CA将合法表决者的公钥以及高级表决者产生的虚拟身份的公钥公布在区块链上，即形成门限环签名的公钥环。合法表决者的公钥都包含在其中，表决者只有使用环中的公钥和自己的私钥才能完成签名，进而进行表决。

4.3 表决阶段

每名表决者在表决时选择M_a（同意）或者M_d（否决）签名并对Token打上时间戳，然后将Token与签名一同发给对应的公正方。设所有表决者（包括虚拟表决者）的公钥构成公钥环$_y = \{pk_1, \cdots, pk_n\}$。

(1)选择同意的表决者计算$(m_1, \cdots m_k) = H(d, _y, M_a)$，并随机选择$r_i \in Z_N$。

1)普通表决者V_i计算：

$S_{1,i} = g_2^{s_i}(u\sum_{j=1}^{k} u_j^{m_j})^{r_i}$，$S_{2,i} = g_1^{r_i}$并yoken加上时间戳$T$，向Teller A的地址发起交易，将$(S_{1,i}, S_{2,i}, et_i \parallel T)$发送给Teller A。

2)二级表决者V_i计算：

$$S_{1,i} \cdot S_{1,i+1} = g_2^{s_i + a * s_i}(u\sum_{j=1}^{k} u_j^{m_j})^{r_i + r_{i+1}}$$

$$S_{2,i} \cdot S_{2,i+1} = g_1^{r_i + r_{i+1}}$$

将Token加上时间戳，向Teller A的地址发起交易，将签名$(S_{1,i} \cdot S_{1,i+1}, S_{2,i} \cdot S_{2,i+1}, et_i \parallel T)$发送给Teller A。

3)三级表决者V_i计算：

$$S_{1,i} \cdot S_{1,i+1} \cdot S_{1,i+2} = g_2^{s_i + a * s_i + b * s_i}(u\sum_{j=1}^{k} u_j^{m_j})^{r_i + r_{i+1} + r_{i+2}}$$

$$S_{2,i} \cdot S_{2,i+1} \cdot S_{2,i+2} = g_1^{r_i + r_{i+1} + r_{i+2}}$$

将Token加上时间戳，向Teller A的地址发起交易，将签名$(S_{1,i} \cdot S_{1,i+1} \cdot S_{1,i+2}, S_{2,i} \cdot S_{2,i+1} \cdot S_{2,i+2}, et_i \parallel T)$发送给Teller A。

(2)同样地，选择否决的表决者计算$(m_1, \cdots m_k) = H(d, _y, M_d)$，并随机选择$r_i \in Z_N$，其他计算以及发送内容与选择同意的表决过程一致，不同的是这里不再发送给Teller A，而是发送给公正方Teller B，具体的过程将不再赘述。

(3)改票。在投票截止时间前，若表决者想要改票，可以

更新 Token 上的时间重新发送结果，公正方只保留每名表决者最新的投票结果。由于表决只有同意和否决两个选择，且为了减轻 CA 统计消耗的资源，每个表决者只有一次改票机会。因此在收到两次相同的 Token 后，CA 可将这个 Token 标记为无效，以后不再接收。

4.4 计票阶段

(1)投票截止后，公正双方开始统计自己收到的选票，主要做两方面的验证。第一，验证 Token 是否有效，即验证 Token 上是否含 CA 的有效签名，并丢弃无效票；第二，对带有重复 Token 的表决票，只保留最新时间的结果。由于每个人的表决结果在区块链上都是可见的，因此，所有人都可以检查自己的表决结果是否被记录，也可以统计票数来验证公正方的结果。

(2)设$\{1,2,\cdots,d\}$是表决同意者的下标，$\{d+1,\cdots,n\}$是否决者的下标。

对于 Teller A，定义$f_i=\begin{cases}1, & i=1,\cdots,d\\ 0, & i=d+1,\cdots,n\end{cases}$

对于 Teller B，定义$f_i=\begin{cases}0, & i=1,\cdots,d\\ 1, & i=d+1,\cdots,n\end{cases}$

对于 $i=1,\cdots,n$，公正方选择$x_i\in_R Z_N$，并设：

$$C_i=\left(\frac{g_1^{s_i}}{B_0}\right)^{f_i}h_1^{x_i},\pi_i=\left(\left(\frac{g_1^{s_i}}{B_0}\right)^{2f_i-1}h_1^{x_i}\right)^{x_i}$$

令 $C=\prod_{i=1}^{n}C_i$，有$B_0^dC=h_1^x\prod_{i=1}^{d}g_1^{s_i}$，其中 $x=\sum_{i=1}^{n}x_i$。

4.5 验证及发布结果

(1)当 $d\geqslant\left\lceil\frac{n}{2}\right\rceil$，即 Teller A 收到超过半数的表决票时，计算：

$$S_1=h_2^x\prod_{i=1}^{d}S_{1,i},S_2=\prod_{i=1}^{d}S_{2,i}$$

并进行验证。首先验证：

$$\hat{e}(C_i,C_i)=\hat{e}(h_i,\pi_i)\cdot\hat{e}\left(C_i,\frac{g_1^{s_i}}{B_0}\right)$$

若上式成立，则验证：

$$\hat{e}(S_1,g_1)=\hat{e}(S_2,u\prod_{j=1}^{k}u_j^{m_j})\cdot\hat{e}(g_2,B_0^dC)$$

若验证通过，则 Teller A 在区块链上发布表决通过的结果并附上签名$(S_1,S_2,\{C_i,\pi_i\}_{i=1}^n)$。

(2)当 $n-d\geqslant\left\lceil\frac{n}{2}\right\rceil$，即 Teller B 收到超过半数的表决票时，计算：

$$S_1=h_2^x\prod_{i=d+1}^{n}S_{1,i},S_2=\prod_{i=d+1}^{n}S_{2,i}$$

并进行验证。首先验证：

$$\hat{e}(C_i,C_i)=\hat{e}(h_i,\pi_i)\cdot\hat{e}\left(C_i,\frac{g_1^{s_i}}{B_0}\right)$$

若上式成立，则验证：

$$\hat{e}(S_1,g_1)=\hat{e}(S_2,u\prod_{j=1}^{k}u_j^{m_j})\cdot\hat{e}(g_2,B_0^{n-d}C)$$

若通过以上验证，则 Teller B 在区块链上发布表决被否的结果并附上签名$(S_1,S_2,\{C_i,\pi_i\}_{i=1}^n)$。

5 安全性证明

本协议中二级用户和三级用户的虚拟身份是公布在区块链上的，并且也作为环中的一员，他们的公钥和用户真正的公钥相关联，也就是说虚拟身份的暴露会带来真实身份的暴露，因此以一级用户为例进行说明。

(1)若 CDH 假设在G_p中成立，则基于门限环签名的分级匿名表决方案是不可伪造的。

证明：setup：模拟器 $\mathcal{B}$ 生成双线性群生成元$(N=pg,G,G_T,\hat{e})\leftarrow\mathcal{G}(1^\lambda)$。给定 CDH 问题$(g,g^a,g^b)\in G_p^3$，要求 $\mathcal{B}$ 输出 g^{ab}。$\mathcal{B}$ 设置以下参数：设整数$\mu=4q_e$，在 0 到 k 之间随机选择整数 κ，在 0 到 $\mu-1$ 中均匀随机地选择$x',x_1,\cdots,x_k$，随机数$\gamma\in Z_N$，并设$z_1=g^{\frac{p\gamma}{q}}$，由于 $g\in G_q$，因此$z_1\in G_q$，故能根据g^b计算出z_1^b。然后随机选择生成元$h_1\in G_q,y',y_1,\cdots,y_k,\alpha,\beta\in Z_N$，并设：

$$g_1=g^{z_1},g_2=g^az_1^q,\mu=g_2^{N-\kappa\mu+x'}$$

$$\mu_1=g_2^{x_1}g^{y_1},\cdots,\mu_k=g_2^{x_k}g^{y_k},h_2=h_1^q,B_0=h_1^\beta$$

最后，$\mathcal{B}$ 选择一个哈希函数 $H:N\times G^*\times\{0,1\}^*\rightarrow\{0,1\}^k$。

敌手 $\mathcal{A}$ 将获得 $\mathcal{B}$ 提供的公共参数：$(N,G,G_T,\hat{e},g_1,g_2,B_0,h_1,h_2,\mu_1,\cdots,\mu_k,H)$。对于消息 $m=\{m_1,\cdots,m_k\}$，定义$F(m)=(N-\mu\kappa)+x'+\sum_{i=1}^{k}x_im_i,J(m)=y'+\sum_{i=1}^{k}y_im_i$。

$\mathcal{B}$ 假定 τ 为挑战签名者，并随机选取$s_i\in Z_N,i=1,\cdots,n$，设$pk_i=\begin{cases}g_1^{s_i}, & i\neq\tau\\ g^bz_1^b, & i=\tau\end{cases}$

预言机模拟：

$\mathcal{HO}$：询问用户 i，返回pk_i。

$\mathcal{CO}(pk_i)$：若 $i=\tau$，$\mathcal{B}$ 失败并退出，否则 $\mathcal{B}$ 返回$g_2^{s_i}$。

$\sigma\leftarrow SO(n,d,y,v,M)$：输入消息 M，公钥集 $y=\{pk_i'\}_{i=1}^n$，d 个签名用户的公钥集 v，$\mathcal{B}$ 计算(C_i,π_i)，得到$B_0^dC=h_1^x\prod_{i=1}^{d}g_1^{s_i}$。定义 $m=H(d,y,m)$，令 $m=\{m_1,\cdots,m_k\}$。若$x'+\sum_{i=1}^{k}x_im_i\equiv0\bmod\mu$，$\mathcal{B}$ 终止。对于所有$pk_i\in v$且$i\neq\tau$，$\mathcal{B}$ 计算$(S_{1,i},S_{2,i})$。若$pk_\tau\in v$，$\mathcal{B}$ 选择随机数$r_\tau\in Z_N$并计算：

$$S_{1,\tau}=(g^b)^{\frac{-J(m)}{F(m)}}(u\sum_{j=1}^{k}u_j^{m_j})^{r_\tau}$$

$$S_{2,\tau}=(g^bz_1^b)^{\frac{-1}{F(m)}}(gz_1)^{r_\tau}$$

令$\bar{r}=r_\tau-\frac{b}{F(m)}$，则有$S_{1,\tau}=g_2^b(u\prod_{j=1}^{k}u_j^{m_j})^{\bar{r}}$。

输出：$\mathcal{A}$ 返回$(n^*,d^*,y^*,M^*,\sigma^*)$。定义$m^*=(m_1^*,\cdots,m_k^*)=H(d^*,y^*,M^*)$。且对这$d^*$个用户的私钥询问和签名询问次数之和不能超过$d^*-1$次。若$pk_\tau\notin v$或$x'+\sum_{i=1}^{k}x_im_i^*\neq\mu\kappa$，则 $\mathcal{B}$ 终止。否则，假设pk_τ就是 τ 位置的签名者，那么 σ^* 就是合法签名，则有：

$$\hat{e}(C_i^*,C_i^*)=\hat{e}(h_i,\pi_i^*)\cdot\hat{e}(C_i^*,\frac{g_1^{s_i}}{B_0})$$

$$\frac{\hat{e}(C_i^*,C_i^*)}{\hat{e}(C_i^*,\frac{g_1^{s_i}}{B_0})}=\hat{e}(C_i^*,\frac{C_i^*B_0}{pk_i})=\hat{e}(h_i,\pi_i^*)$$

由于$\hat{e}(h_i,\pi_i^*)$在G_T中的阶数为 q，因此$C_i^*,\frac{C_i^*B_0}{pk_i}$中必有一个为 q 阶。若$(C_i^*)^q=0$，则C_i^*为 q 阶，然后 $\mathcal{B}$ 设$f_i=0$，即pk_i不是签名者，此时 $\mathcal{B}$ 终止。若$\frac{C_i^*B_0}{pk_i}=0$，则$\frac{C_i^*B_0}{pk_i}$为 q 阶，$\mathcal{B}$ 设$f_i=1$。

令 $\delta\in Z_N$ 且 $\delta=0 \bmod q$，$\delta=1 \bmod p$。由等式 $\hat{e}(S_1^*,g_1)=\hat{e}(S_2^*,u\prod_{j=1}^{k}u_j^{m_j^*})\cdot\hat{e}(g_2,B_0^{d^*}C_i^*)$ 得 $\hat{e}(S_1^*,g_1)^\delta=\hat{e}(S_2^*,u\prod_{j=1}^{k}u_j^{m_j^*})^\delta\cdot\hat{e}(g_2,B_0^{d^*}C_i^*)^\delta$ 可化简成 $\hat{e}(S_1^*,g)^\delta=\hat{e}(S_2^*,g^{J(m^*)})^\delta\cdot\hat{e}(g^a,B_0^{d^*}\sum_{i|i\in y^*}\left(\frac{pk_i}{B_0}\right)^{f_i})^\delta$，进一步有 $\hat{e}(S_1^*,g)^\delta=\hat{e}(S_2^*,g^{J(m^*)})^\delta\cdot\hat{e}(g^a,\sum_{i|i\in y^*,i\neq\tau}(g^{s_i})^{f_i}\cdot g^b)^\delta$，因此 $S_1^{*\delta}=(S_2^{*J(m^*)}\cdot(\prod_{i|i\in y^*,i\neq\tau}g^{s_if_i}\cdot g^b)^a)^\delta$。

由此解决 CDH 问题：

$$g^{ab}=(S_1^*(S_2^*)^{-J(m^*)}\prod_{i|i\in y^*,i\neq\tau}(g^a)^{-s_if_i})^\delta$$

综上，若假设 CDH 在 G_p 中成立，则攻击者无法伪造超过半数的表决票。

(2)若假设 SGH 在 G_p 中成立，则基于门限环签名的分级匿名表决方案是匿名的。

证明：setup：给定子群决策问题，要求模拟器 $\mathcal{B}$ 判断 $h\in G$ 或 $h\in G_q$。$\mathcal{B}$ 给出以下参数：随机选择生成元 $u,u_1,\cdots,u_k$，$B_0\in G,\alpha\in Z_N$，并设 $g_1=g,g_2=g_1^\alpha,h_1=h,h_1=h^\alpha$。最后给出哈希函数 $H:N\times G^*\times\{0,1\}^*\rightarrow\{0,1\}^k$，敌手 $\mathcal{A}$ 获得以上公共参数：$(N,G,G_T,\hat{e},g_1,g_2,B_0,h_1,h_2,u,u_1,\cdots,u_k,H)$。然后 $\mathcal{B}$ 选取随机数 $s_i\in Z_N,i=1,\cdots,n$，并设 $pk_i=g_1^{s_i},sk_i=g_2^{s_i}$。

预言机模拟：

$\mathcal{HO}$：询问用户 i，返回 pk_i。

$\mathcal{CO}(pk_i)$：$\mathcal{B}$ 返回 $g_2^{s_i}$。

$\sigma\leftarrow\mathcal{HO}(n,d,y,v,M)$：输入用户规模 n，门限 d，消息 M，公钥集 $y=\{pk_i'\}_{i=1}^n$，d 个签名用户的公钥集 v，$\mathcal{B}$ 按签名算法返回一个签名。

挑战：$\mathcal{A}$ 提供消息 M^*，门限 d^* 和 n 个查询 $\mathcal{HO}$ 输出的公钥的集合 y^*。$\mathcal{B}$ 选择 y^* 的子集 v^* 且 $|v^*|=d^*$，v^* 中不能包含 $\mathcal{CO}$ 查询过的元素，然后 $\mathcal{B}$ 使用以上输入并运行签名算法产生一个环签名 σ^*。

输出：要求 $\mathcal{A}$ 输出一个签名者的下标 $\hat{\pi}$，若 $\hat{\pi}$ 是真正的签名者，则 $\mathcal{B}$ 输出 $h\in G_q$，否则输出 $h\in G$。

分析：假设挑战签名为 $(S_1^*,S_2^*,\{C_i^*,\pi_i^*\}_{i=1}^{n^*})$，$y^*=\{pk_1^*,\cdots,pk_n^*\}$。若 $h_1\in G$，则存在 $x_i,\bar{x}_i\in Z_N$，使得 $C_i^*=\left(\frac{pk_i^*}{B_0}\right)h_1^{x_i}=h_1^{\bar{x}_i}$。令 $x_i,\bar{x}_i$ 分别对应 $f_i^*=1$ 和 $f_i^*=0$ 的场景，可以得出 π_i^* 是相同的值：

$$\pi_i^*=\left(\left(\frac{g_1^{s_i}}{B_0}\right)^{2f_i-1}h_1^{x_i}\right)^{x_i}=\begin{cases}\left(\left(\frac{pk_i^*}{B_0}\right)h_1^{x_i}\right)^{x_i}=(h_1^{\bar{x}_i})^{x_i}, & f_i=1\\ \left(\left(\frac{pk_i^*}{B_0}\right)^{-1}h_1^{\bar{x}_i}\right)^{\bar{x}_i}=(h_1^{x_i})^{\bar{x}_i}, & f_i=0\end{cases}$$

因此，敌手无法通过 $\{C_i^*,\pi_i^*\}_{i=1}^{n^*}$ 来判断真正的签名者。另外，S_1^* 需要经过等式验证，S_2^* 的计算用到了一组随机数，因此都没有泄露关于真实签名者的信息。若 $h\in G$，则 $\mathcal{A}$ 挑战失败；若 $h\in G_q$，则 $\mathcal{A}$ 挑战成功。

综上，$\mathcal{B}$ 可以通过 $\mathcal{A}$ 猜测真实签名者下标是否成功来决定 $h\in G$ 还是 $h\in G_q$。

6 协议分析

6.1 合法性

用户的公钥唯一、公开地代表了用户的真实身份，参与表决的用户首先提交 (m_i,σ_i) 给 CA，CA 收到后首先检查身份信息，并将没有表决权的用户签名丢弃，然后核实用户身份。当公正方收到的申请中包含相同的身份信息 m_i 时，应先对其进行单独验证：$\hat{e}(\sigma_i,g_1)=\hat{e}(H_0(m_i)\cdot g_2,pk_i)$。在保证所有用户身份信息唯一后 $(m_1\neq\cdots\neq m_n)$，再进行群验证。这样做可有效抵御恶意公钥攻击。进行群验证时，用户的公钥为 $g_1^{s_i}$，私钥为 $g_2^{s_i}$，用户 i 对身份信息 m_i 签名 $\sigma_i=H_0(m_i)^{s_i}\cdot sk_i$。若攻击者想要冒充合法用户 Bob 的身份(即 m_i 相同)来通过群验证，则攻击者首先要注册一个恶意公钥 $pk_2=g_1^\alpha\cdot(pk_1)^{-1}$，其中 pk_1 是 Bob 的公钥，然后选择随机数 $\alpha\in Z_N$。接着攻击者发送自己和 Bob 的聚合签名 $\sigma=H_0(m)^\alpha\cdot g_2^\alpha$，这个签名将会通过验证，因为 $\hat{e}(\sigma,g_1)=\hat{e}(H_0(m)^\alpha\cdot g_2^\alpha,g_1)=\hat{e}(H_0(m)\cdot g_2,g_1^\alpha)=\hat{e}(H_0(m)\cdot g_2,pk_1\cdot pk_2)$ 满足了验证等式。

通过验证的用户获得唯一 Token 并成为合法表决者。同时，$\text{Token}=Sign_{\text{CA}}(V_{\text{ipub}})$，即认证中心对表决者身份的签名。用户可以通过验证 Token 上公正方的签名来验证 CA 的真实性，这是一个双向验证的过程。

6.2 保密性

本文提出的表决方案使用环签名来隐藏签名者的真实身份，使得表决内容与签名者无法对应。传统投票方法使用盲签名来隐藏投票的内容，但在最终计票时依然需要去盲以统计投票内容，不能做到完全保密。本协议使用的环签名使得真正的签名者隐藏在所有合法表决者中，而表决内容是始终公开的。表决者通过选取随机数 r_i 来计算 $S_{1,i}=g_2^{s_i}(u\sum_{j=1}^{k}u_j^{m_j})^{r_i}$，$S_{2,i}=g_1^{r_i}$，以形成个人签名 $(S_{1,i},S_{2,i})$，环签名的最终形成需要依次经过以下等式的验证：

$$\hat{e}(C_i,C_i)=\hat{e}(h_i,\pi_i)\cdot\hat{e}\left(C_i,\frac{g_1^{s_i}}{B_0}\right)$$

$$\hat{e}(S_1,g_1)=\hat{e}(S_2,u\prod_{j=1}^{k}u_j^{m_j})\cdot\hat{e}(g_2,B_0^dC)$$

整个投票过程不会泄露任何签名信息。本协议的安全性基于安全的传输通道才能实现，不考虑用户在发送表决信息时被敌手截获的情况。

6.3 不可重复表决和可更新性

本协议利用 Token 加时间戳的方法来保证投票的不可重复性和可更新性。每个表决者收到的 Token：$et_i=Sign_{\text{CA}}(V_{\text{ipub}})$ 是唯一的，它是认证中心对每个合法表决者公钥的签名，相当于每个表决者只有一张登记过自己身份的选票；此外，表决者还可在规定的时间内利用自己的 Token 表决多次，但是计票时只保留带有最新时间戳的表决，为了减少计票资源的消耗，可根据情况调整最大改票次数。

6.4 可验证性

本协议实现了个体可验证性和全局可验证性。由于区块链上数据的公开性和不可篡改性，每名表决者都可以查看自己的表决结果是否被记录，也可以看到其他人的表决结果，并可通过验证签名来判断其他人投票的合法性。另外，通过简单的计算可以检验最终表决结果的正确性。

结束语 本文在 Yuen 等提出的门限环签名方案的基础上提出了一种基于门限环签名的分级匿名表决协议,该协议实现了表决的合法性、匿名性、不可重复性、可更新性和可验证性。该协议的安全性是基于安全的传输通道实现的,不考虑用户在发送表决信息时被敌手截获的情况;同时也是在 CA 可信的前提下保证整个投票过程的安全;此外,区块链上也存在 51%的攻击,因此需要进一步对可能存在的安全漏洞进行分析和解决。

参 考 文 献

[1] CHAUM D L. Untraceable electronic mail return addresses, and digital pseudonyms[J]. Commun ACM (USA), 1981, 24(2): 84-88.

[2] WANG K H, MONDAL S K, CHAN K, et al. A review of contemporary e-voting: Requirements, technology, systems and usability[J]. Data Science and Pattern Recognition, 2017, 1(1): 31-47.

[3] GRITZALIS D A. Principles and requirements for a secure evoting system[J]. Computers & Security, 2002, 21(6): 539-556.

[4] ANANE R, FREELAND R, THEODOROPOULOS G. E-voting requirements and implementation[C]// The 9th IEEE International Conference on E-Commerce Technology and The 4th IEEE International Conference on Enterprise Computing. E-Commerce and E-Services, 2007: 382-392.

[5] RIBARSKI P, ANTOVSKI L. Comparison of ID-based blind signatures from pairings for e-voting protocols[C]// International Convention on Information and Communication Technology. Electronics and Microelectronics, 2014: 1394-1399.

[6] ÀNGELS CERVERÓ M, VÍCTOR M, MIRET J M, et al. An Efficient Homomorphic E-Voting System over Elliptic Curves [C]// International Conference on Electronic Government and the Information Systems Perspective. 2014: 41-53.

[7] PENG K, BAO F. Efficient Multiplicative Homomorphic E-Voting[C]// International Conference on Information Security. Springer-Verlag, 2010: 381-393.

[8] LEE B, BOYD C, DAWSON E, et al. Providing receipt-freeness in mixnet-based voting protocols[C]// International Conference on Information Security and Cryptology. 2004: 245-258.

[9] ZHONG S, BONEH D, JAKOBSSON M, et al. Optimistic mixing for exit-polls[C]// International Conference on the Theory and Application of Cryptology and Information Security. 2002: 451-465.

[10] KUMAR M, KATTI C P, SAXENA P C. A Secure Anonymous E-Voting System Using Identity-Based Blind Signature Scheme [C]// International Conference on Information Systems Security. 2017: 29-49.

[11] COHEN J D, FISCHER M J. A robust and verifiable cryptographically secure election scheme[C]// Symposium on Foundations of Computer Science. IEEE, 1985: 372-382.

[12] CRAMER R, GENNARO R, SCHOENMAKERS B. A secure and optimally efficient multi-authority election scheme [J]. Transactions on Emerging Telecommunications Technologies, 2012, 8(5): 481-490.

[13] BAUDRON O, FOUQUE P A, POINTCHEVAL D, et al. Practical multi-candidate election system[C]// Twentieth Acm Symposium on Principles of Distributed Computing. 2001: 274-283.

[14] LIU J K. Ring Signature [C]// Advances in Cyber Security: Principles, Techniques, and Applications. 2019: 93-114.

[15] CHOW S S M, WEI V K, LIU J K, et al. Ring signatures without random oracles[C]// Proceedings of the 2006 ACM Symposium on Information, Computer and Communications Security. 2006: 297-302.

[16] WANG H, HE D, LIU Z, et al. Blockchain-Based Anonymous Reporting Scheme With Anonymous Rewarding [J]. IEEE Transactions on Engineering Management, 2019, 6(2): 3676-3687.

[17] KURBATOV O, KRAVCHENKO P, POLUYANENKO N, et al. Using Ring Signatures For An Anonymous E-Voting System[C]// 2019 IEEE International Conference on Advanced Trends in Information Theory (ATIT). 2019: 187-190.

[18] TORNOS J L, SALAZAR J L, PILES J J. Optimizing ring signature keys for e-voting[C]// 2015 International Wireless Communications and Mobile Computing Conference. 2015: 817-821.

[19] TSANG P P, WEI V K. Short linkable ring signatures for e-voting, e-cash and attestation[C]// International Conference on Information Security Practice and Experience. 2005: 48-60.

[20] BRESSON E, STERN J, SZYDLO M. Threshold Ring Signatures and Applications to Ad-hoc Groups[C]// Annual International Cryptology Conference. 2002: 465-480.

[21] YUEN T H, LIU J K, AU M H A, et al. Threshold ring signature without random oracles[C]// Acm Symposium on Information. 2011: 261-267.

[22] HJALMARSSON F P, HREIOARSSON G K, HAMDAQA M, et al. Blockchain-Based E-Voting System[C]// 2018 IEEE 11th International Conference on Cloud Computing. 2018: 983-986.

[23] HARDWICK F S, AKRAM R N, MARKANTONAKIS K. E-Voting with Blockchain: An E-Voting Protocol with Decentralisation and Voter Privacy[C]// in Proc. iThings & GreenCom & CPSCom & SmartData. 2018: 1561-1567.

[24] BONEH D. Evaluating 2-DNF Formulas on Ciphertexts [C]// Springer-Verlag. 2005: 325-341.

FAN Jia-xing, born in 1996, postgraduate, Her main research interests include public key cryptography and cryptography applications.

WANG Zhi-wei, born in 1976, Ph. D, professor. His main research interests include applied cryptography, public key cryptography, etc.

(责任编辑:喻藜)