



文章编号:1001-9081(2018)04-1036-05

DOI:10.11772/j.issn.1001-9081.2017102400

## 基于同态门限密码体制的投票协议

代小康<sup>1,2</sup>, 陈长波<sup>2\*</sup>, 吴文渊<sup>2</sup>

(1. 重庆邮电大学 计算机科学与技术学院, 重庆 400000;  
2. 中国科学院重庆绿色智能技术研究院 自动推理与认知重庆市重点实验室, 重庆 400700)  
(\*通信作者电子邮箱 chenchangbo@cigit.ac.cn)

**摘要:**针对当前存在的投票协议普遍要求一个可信赖的管理机构的问题,提出一种新的投票协议。该协议综合运用同态加密、门限密码体制、盲签名、环签名、零知识证明等密码技术,在假设无人弃权或虽有人弃权但管理者不与其他投票人合谋作弊的情况下,消除了无可信第三方和健壮性共存的矛盾,同时满足了匿名性、合法性、健壮性、可验证性和无可信第三方等安全属性。

**关键词:**投票协议; 门限密码体制; 同态加密; 健壮性; 无可信第三方

**中图分类号:**TP309.2    **文献标志码:**A

### New voting protocol based on homomorphic threshold cryptography

DAI Xiaokang<sup>1,2</sup>, CHEN Changbo<sup>2\*</sup>, WU Wenyuan<sup>2</sup>

(1. College of Computer Science and Technology, Chongqing University of Posts and Telecommunications, Chongqing 400000, China;  
2. Chongqing Key Laboratory of Automated Reasoning & Cognition,  
Chongqing Institute of Green and Intelligent Technology, Chinese Academy of Sciences, Chongqing 400700, China)

**Abstract:** A new voting protocol was proposed to solve the problem that most of the existing voting protocols require a trusted management authority. This protocol comprehensively makes use of homomorphic encryption, threshold cryptography, blind signature, ring signature, zero knowledge proof, and so on, to resolves the coexistence problem between robustness and the absence of trusted third party under the assumption that no one abstains from voting or the authority does not cheat conspiracy with other voters when one voter abstains from voting, at the same time, anonymity, eligibility, robustness, verifiability and no trusted third party are also satisfied.

**Key words:** voting protocol; threshold cryptosystem; homomorphic encryption; robustness; no trusted third party

## 0 引言

自 1981 年美国密码学家 Chaum<sup>[1]</sup> 提出基于混合网传递选票模式的投票协议以来, 电子投票协议发展了 30 多年, 相应地, 对协议的属性要求也在不断变化。最早定义协议属性的是 1992 年日本的三位学者 Fujioka、Okamoto 和 Ohta<sup>[2]</sup>, 一个安全的协议必须满足以下属性:

- 1) 匿名性: 无法将某一张选票和投票者对应。
- 2) 合法性: 合法选票才能被计算在内。
- 3) 健壮性: 干扰、破坏投票流程的人将会被发现。
- 4) 可验证性: 每一个投票者均可验证自己的选票是否被计算在内。

但是随着投票协议的发展, 某些特定场景下, 比如强隐私环境中参与方互不信任, 协议还需要满足无可信第三方。

5) 无可信第三方: 无须假设投票的参与者(包括管理者、计票中心)诚实可信, 投票结果依然是可信的。

以上五个属性为安全投票协议的基本属性, 简称 FOO 安全属性。

1992 年日本的三位学者 Fujioka、Okamoto 和 Ohta<sup>[2]</sup> 提出并实现了第一个基于盲签名的投票协议, 该协议中投票人和

计票中心通过匿名信道交互, 保障了协议的匿名性。但是由于协议中采用盲签名技术来盲化选票, 因此在最后的计票阶段需要每个人出示自己的盲因子来解密选票, 如果某个投票人不出示自己的盲因子, 且投票人和计票中心是通过匿名信道交互的, 会无法找到该投票人, 致使投票活动失败, 因而该协议不具有健壮性。2007 年由 Antoniou 等<sup>[3]</sup> 提出的基于可信中心的投票方案中, 要求私钥保留者不会和管理者合谋, 否则投票人选票内容将会泄露, 不满足无可信第三方。同年, 由 Taghavi 等<sup>[4]</sup> 提出的基于秘密分享的投票方案中引入了第三方仲裁, 且加解密选票的公私钥是由某一方生成的, 同样不满足无可信第三方。2011 年由 Peng 等<sup>[5]</sup> 提出的基于同态加密的投票系统对选票进行有效的分组, 提高了加解密选票的效率, 同样采用门限密码体制生成加解密选票的公私钥对, 该方案满足无可信第三方和健壮性, 但是没有保障选票的匿名性。国内的投票协议中, 2004 年由曹刚等<sup>[6]</sup> 提出的基于盲签名的投票协议, 其要求计票中心是可信的, 否则, 所有人的选票将会被泄露, 不满足无可信第三方。2015 年罗芬芬等<sup>[7]</sup> 对 Fujioka、Okamoto 和 Ohta 的协议进行了改进, 新的方案中的唯一申诉标志是由管理中心生成的, 当投票者要求申诉并出示唯一申诉标志时, 管理中心知道对应的投票人, 协议的匿名性

收稿日期:2017-10-10;修回日期:2017-11-30。

基金项目:国家自然科学基金资助项目(11471307, 11671377, 11771421); 重庆市基础科学与前沿技术研究专项(cstc2015jcyjys40001)。

作者简介:代小康(1993—),男,湖北洪湖人,硕士研究生,主要研究方向:信息安全、隐私保护; 陈长波(1981—),男,山东济宁人,副研究员,博士,主要研究方向:符号计算、信息安全; 吴文渊(1976—),男,四川成都人,研究员,博士,主要研究方向:自动推理、信息安全。



无法得到保障。同年,杨婷婷等<sup>[8]</sup>提出基于多方排序协议的安全电子投票方案中,没有采用零知识证明来保证选票的有效性,且注册中心和候选人合谋即可知道每个人的选票内容,该协议不具有匿名性和健壮性。同年,刘高等<sup>[9]</sup>提出的一种可验证的多候选人电子投票方案中,假设投票人是半诚信的,即协议不满足无可信第三方要求。2016年,徐紫枫等<sup>[10]</sup>提出基于时间释放加密和数字签名的匿名电子投票方案,该方案中临时身份ID是由认证中心生成的,因此认证中心知道每张选票对应的投票人,该协议不具有匿名性。同年,董宇琦等<sup>[11]</sup>提出的基于隐私保护的电子选举投票系统,其加解密选票的公私钥是由第三方服务器生成的,且要求投票人不会发起主动攻击,该系统不满足无可信第三方和健壮性。2017年,黄仕杰等<sup>[12]</sup>提出基于同态实现多候选人的电子投票方案中,在计票阶段引入可信第三方来保证每张选票的有效性,该协议不满足无可信第三方要求。综上所述,目前存在的协议都没有同时满足匿名性、合法性、健壮性、可验证性和无可信第三方。

针对这一问题,本文引入门限密码体制,通过投票参与方相互监督,阻止了投票人、管理者的主动攻击,起到了取代可信第三方的作用,构造了同时满足匿名性、合法性、健壮性、可验证性、无可信第三方的投票协议。

## 1 预备知识

### 1.1 门限密码体制

一个系统中共有  $n$  个参与方,每个参与方持有一对公私钥  $(h_i, x_i)$ ,各参与方之间通过交互生成公钥  $h$ ,与  $h$  对应的私钥为  $x$ ,若至少需要  $k$  个参与者合作才能恢复  $x$ ,则该系统称为  $(k, n)$  门限密码系统<sup>[13]</sup>。

### 1.2 ELGamal 公钥密码体制<sup>[14]</sup>

**密钥生成:**系统随机选取一个大素数  $p$  ( $p$  必须满足存在  $q$ ,且  $q$  整除  $p - 1$ ),令  $\alpha$  为乘法群  $\mathbf{Z}_p^*$  的一个原根。随机生成一个整数  $x$  ( $1 \leq x \leq p - 1$ ),并计算  $y = \alpha^x \bmod p$ 。以  $(p, \alpha, y)$  作为用户公钥,  $x$  作为用户私钥。

**加密:**设用户想加密的明文为  $m$ ,且  $m < p$ ,随机选取整数  $k$  ( $1 \leq k \leq p - 1$ ),并计算  $a = \alpha^k \bmod p$ ,  $b = m \cdot y^k \bmod p$ 。密文为二元组  $(a, b)$ 。

**解密:**用户用私钥对密文解密: $m = b \cdot (a^x)^{-1} \bmod p$ 。

### 1.3 同态加密

对于一个加密算法有密文  $c_1, c_2$ ,如果该解密算法对于“\*”运算满足  $D(c_1) * D(c_2) = D(c_1 * c_2)$ ,那么称该加密算法对于“\*”运算是同态的。例如,ELgamal 公钥加密算法对于乘法运算是同态的。

### 1.4 匿名信道

匿名信道<sup>[1]</sup>,是指多个发送者将各自的消息同时发送给主机群,主机群对消息随机排序后发送给接收者,除了该消息的发送者,其他人均不知道随机排序后的消息和发送者的对应关系。例如:有  $n$  个主机,  $s$  个发送者,每个主机对应的公私钥为  $mix_{i(e)}, mix_{i(d)}$  ( $i = 1, 2, \dots, n$ ),每个发送者对应的消息和接收者的地址分别为  $M_j$  和  $A_j$  ( $j = 1, 2, \dots, s$ ),第  $j$  个发送者将消息  $M_j$  和  $A_j$  加密后得到  $Enc_{j,n}$ :

$$Enc_{j,n} = E_{mix_{1(e)}}(E_{mix_{2(e)}}(\dots(E_{mix_{n(e)}}(M_j, A_j))\dots))$$

然后将  $Enc_{j,n}$  发送给第一个主机,第一个主机对  $Enc_{j,n}$  解

密后得到  $Enc_{j,n-1} = E_{mix_{2(e)}}(\dots(E_{mix_{n(e)}}(M_j, A_j))\dots)$ 。

然后将  $Enc_{j,n-1}$  发送给第二个主机,每个主机重复该操作,则第  $n$  个主机解密得到  $M_j, A_j$ ,并将  $M_j$  发送给地址为  $A_j$  的接收者。

### 1.5 盲签名

盲签名是指签名者并不知道所签文件或消息的具体内容,而文件或消息的拥有者又可以得到签名者关于真实文件或消息的签名。设签名者  $B$  的公钥为  $e$ ,私钥为  $d$ ,模数为  $p$ ,用户  $A$  需要签名者  $B$  对消息  $M$  进行盲签名,基于 RSA(Rivest, Shamir 和 Adleman) 算法的盲签名如下:

1) 用户  $A$  随机选取一个整数  $k$ ,且  $1 \leq k \leq m$ ,对  $k$  作盲化处理: $t = M \cdot k^e \bmod p$ ,然后将  $t$  发送给签名者  $B$ ;

2) 签名者  $B$  对  $t$  进行签名后得到盲签名信息  $s = t^d = (M \cdot k^e)^d \bmod p = M^d k \bmod p$ ,然后将签名发送给用户  $A$ ;

3) 用户  $A$  收到盲签名信息  $s$  后,通过解盲计算得到  $B$  对消息  $M$  的签名信息  $S$ :

$$S = sk^{-1} \bmod p = M^d k k^{-1} \bmod p = M^d \bmod p$$

### 1.6 环签名

签名者用其他环内成员的公钥产生一个带断口的环,再利用自己的私钥将断口连接起来形成一个完整的环,任何验证人利用环成员的公钥都可以验证一个环签名是否由环内的某个成员生成。假设环中成员为  $n$  个,每个成员都有自己的 ElGamal 加密和签名系统(由于生成环签名的过程较为复杂,具体参考 2001 年 Rivest 等<sup>[15]</sup>提出的算法,这里只作抽象表达),则第  $i$  个成员生成环签名的流程:

输入参数:  $p_{i(d)}, p_{1(e)}, p_{2(e)}, \dots, p_{n(e)}$  和  $m$ ,其中:  $p_{i(e)}$ 、 $p_{i(d)}$  分别为环内第  $i$  个成员的公私钥,  $m$  为待签名信息。

输出签名:  $S_{(p_{i(d)}) \parallel (p_{1(e)}) \parallel (p_{2(e)}) \parallel \dots \parallel (p_{n(e)})}(m)$ 。

## 2 新的投票协议

本协议包括投票人、管理者、计票中心三方参与者,其中计票中心可以用公告栏代替,投票人和管理者有自己的 ElGamal 加密和签名系统。本协议一共分为四步,分别为生成加密选票的公私钥,管理者对选票进行签名,投票人对选票进行环签名并投票、计票。

协议中涉及的符号如表 1 所示。

表 1 协议中的符号含义

Tab. 1 Meanings of notations in the protocol

符号	含义
$p, q$	$p, q$ 为大素数,且 $q$ 整除 $p - 1$
$\mathbf{Z}_p, \mathbf{Z}_q$	阶分别为 $p, q$ 的有限域
$p_i$	第 $i$ 个投票者
$ID_i$	第 $i$ 个成员的身份标识
$A$	管理者
CA	计票中心
$p_{i(e)}, p_{i(d)}$	分别为 $p_i$ 的公钥和私钥
$A_{(e)}, A_{(d)}$	分别为 $A$ 的公钥和私钥
$h_i$	$p_i$ 加密选票的公钥份额
$s_i$	$p_i$ 解密选票的私钥份额
$x$	解密选票的私钥
$h$	加密选票的公钥
$S$	签名操作
$E$	加密操作
$D$	解密操作



## 2.1 生成加解密选票的公私钥

该阶段运用ELGamal门限密码体制<sup>[13]</sup>的思想,通过所有投票人合作,生成加解密选票的公私钥对。流程如下:

1)  $p_i$  随机选取  $x_i \in \mathbb{Z}_q^*$  计算  $h_i = g^{x_i} \bmod p$  将  $h_i$  签名并附上自己的 ID 后广播出去:

$p_i$  广播:  $(S_{p_i(d)}(h_i) \parallel ID_i)$

2)  $n$  个投票人都收到其他  $n - 1$  个投票者的广播后, 每个投票人计算  $h = \prod_{i=1}^n h_i$ , 则加密选票的公钥为  $h$ 。

3)  $p_i$  随机选取关于  $z$  的  $k - 1$  ( $k < n$ ) 次多项式  $f_i(z) \in \mathbb{Z}_q^*(z)$ ,  $f_i(z) = f_{i0} + f_{i1}z + \cdots + f_{i,k-1}z^{k-1}$ , 其中:  $f_{i0} = x_i$ , 且  $f_{i1}, f_{i2}, \dots, f_{i,k-1}$  均不为 0。

4)  $p_i$  计算  $F_{it} = g^{f_{it}} \bmod p$  ( $t = 0, \dots, k - 1$ ) 然后签名  $F_{it}$  并附上自己的 ID 后广播出去:

$p_i$  广播:  $(S_{p_i(d)}(F_{i0}, F_{i1}, \dots, F_{i,k-1}) \parallel ID_i)$

当  $n$  个投票人均广播  $(S_{p_i(d)}(F_{i0}, F_{i1}, \dots, F_{i,k-1}) \parallel ID_i)$  后, 令  $s_{ij} = f_i(j)$  其中:  $j = 1, 2, \dots, n$ ,  $p_i$  对  $s_{ij}$  签名并发送给  $p_j$ :

$p_i \rightarrow p_j: E_{p_j(e)}(S_{p_i(d)}(s_{ij}) \parallel ID_i)$

5)  $p_j$  可以验证式(1)来判断其他人发送给自己的  $s_{ij}$  是否正确:

$$g^{s_{ij}} \bmod p = \prod_{t=0}^{k-1} F_{it}^t \quad (1)$$

同时  $p_j$  通过其他  $n - 1$  个投票人发送过来的  $s_{ij}$  计算  $s_j = \sum_{i=1}^n s_{ij} \circ$

当所有的投票人计算出自己的  $s_i$  且验证式(1)成立后, 此时协议第一步结束。第一步结束后每个投票人掌握的  $s_i$  即为解密选票的私钥份额。令  $f(z) = f_1(z) + \cdots + f_n(z)$ , 则  $f(i) = s_i$  且  $f(0) = \sum_{i=1}^n x_i = x$ , 即  $f(0)$  为解密选票的私钥。由于方程含有  $k$  个未知数, 则至少需要  $k$  个投票人合作才能得到私钥, 由于解密选票的私钥不掌握在某一个人手中, 且不用假定某一方是可信赖的, 此时保障了协议的无可信第三方。

## 2.2 管理者对选票进行签名

第二步的主要流程是投票人对选票明文采用ELGamal公钥密码体制加密, 然后将加密后的选票进行盲化, 然后将盲化后选票发送给管理者请求签名。

### 2.2.1 投票人加密并盲化选票

假设选票空间一共有  $m$  种选择, 可以从素数表选取从小到大的  $m$  个素数对应这  $m$  种选择, 即明文空间的集合表示为  $Q = \{Q_1, Q_2, \dots, Q_m\}$ 。

该步涉及的符号表示如表 2 所示。

表 2 加密和盲化阶段由  $p_i$  生成的符号的含义

Tab. 2 Meanings of notations generated by  $p_i$  in encryption and blinding stages

符号	含义	符号	含义
$v_i$	$p_i$ 加密后的选票	$r_i$	$p_i$ 盲化后的随机串
$u_i$	$p_i$ 盲化后的选票	$\Phi_i$	$p_i$ 的选票明文
$t_i$	$p_i$ 的随机串	$k_i$	$p_i$ 的盲化因子

第二步的流程如下:

1)  $p_i$  对选票进行加密  $a_i = g^{e_i} \bmod p, b_i = \Phi_i \cdot h^{e_i} \bmod p$ , 其中  $e_i$  为随机数,  $\Phi_i \in \{Q_1, Q_2, \dots, Q_m\}$ ,  $v_i = (a_i, b_i)$ 。

2)  $p_i$  对  $v_i$  进行盲化  $u_i = \text{blind}(v_i, k_i)$ 。

3)  $p_i$  对  $u_i$  签名后和自己身份的  $ID_i$  一起发送给管理者:

$p_i \rightarrow A: S_{p_i(d)}(u_i) \parallel ID_i$

### 2.2.2 管理者验证权限并签名

管理者接收到  $p_i$  发送过来的  $S_{p_i(d)}(u_i) \parallel ID_i$  后, 根据  $ID_i$  采用对应的  $P_{i(e)}$  来验证签名的有效性, 并检验  $p_i$  是否是第一次申请签名。如果  $p_i$  已经申请过签名或者签名验证不通过, 则放弃该消息, 该张选票作废; 否则管理者用自己的私钥对  $u_i$  签名, 并用  $P_{i(e)}$  加密后发送给  $p_i$ , 即

$A \rightarrow p_i: E_{p_i(e)}(S_{A(d)}(u_i))$

当所有投票人均收到管理者发送过来的  $E_{p_i(e)}(S_{A(d)}(u_i))$  后该步结束, 因为选票是盲化的, 即管理者无法将脱盲后的选票和投票人对应起来。

## 2.3 投票阶段

该步的主要流程是  $p_i$  将已经获得管理员签名的选票脱盲, 然后对脱盲后的选票进行环签名, 并同时生成选票的零知识证明。

### 2.3.1 选票脱盲

$p_i$  接收到管理者发送过来的  $E_{p_i(e)}(S_{A(d)}(u_i))$  后, 用自己的私钥解密得到  $S_{A(d)}(u_i)$ , 并验证签名的有效性, 如果签名验证不通过, 则放弃该消息; 否则  $p_i$  对  $S_{A(d)}(u_i)$  脱盲得到带有管理者签名的选票  $S_{A(d)}(v_i)$ 。

### 2.3.2 对选票进行环签名

$p_i$  以自己的私钥和其他投票人的公钥作为输入得到关于选票  $S_{A(d)}(v_i)$  的环签名:  $S_{(p_i(d) \parallel p_1(e) \parallel p_2(e) \parallel \dots \parallel p_n(e))}(S_{A(d)}(v_i))$ , 以下用  $Sign_i$  表示  $S_{(p_i(d) \parallel p_1(e) \parallel p_2(e) \parallel \dots \parallel p_n(e))}(S_{A(d)}(v_i))$ 。

### 2.3.3 生成选票的零知识证明

不失一般性设  $\Phi_i = Q_k$  ( $Q_k \in \{Q_1, Q_2, \dots, Q_m\}$ ),  $p_i$  计算:

$$\alpha_t = g^{\omega_t} a_i^{e_t} \bmod p$$

$$\beta_t = h^{\omega_t} (b_i / \Phi_i)^{e_t} \bmod p$$

$$\alpha_k = g^s \bmod p$$

$$\beta_k = h^s \bmod p$$

其中:  $t = 1, 2, \dots, m$  且  $t \neq k$ ;  $s \in \mathbb{Z}_q; c_t \in \mathbb{Z}_q; \omega_t \in \mathbb{Z}_q \circ (\alpha_1, \beta_1), (\alpha_2, \beta_2), \dots, (\alpha_m, \beta_m)$  即为选票的零知识证明, 以下用  $ZK_i$  表示  $(\alpha_1, \beta_1), (\alpha_2, \beta_2), \dots, (\alpha_m, \beta_m)$ ,  $p_i$  将  $Sign_i, v_i, ZK_i$  通过匿名信道发送到计票板, 此时计票板显示:

$Sign_1, v_1, ZK_1$

$Sign_2, v_2, ZK_2$

$\vdots$

$Sign_n, v_n, ZK_n$

任意投票人  $p_{j(j \neq i)}$  或者管理者均可验证签名  $Sign_i$  来验证选票是否来自投票人群体。任意投票人  $p_j$  或者管理者对选票  $v_i$  的有效性存在质疑的均可发送随机数  $c_{pj} \in \mathbb{Z}_q$  追加在  $v_i$  后面要求  $p_i$  给出证明, 此时  $p_i$  给出  $(c_1, c_2, \dots, c_m, \omega_1, \omega_2, \dots, \omega_m)$  作为应答, 以下用  $Ans_i$  表示  $(c_1, c_2, \dots, c_m, \omega_1, \omega_2, \dots, \omega_m)$ 。其中:  $\omega_k = s - c_k e_i \bmod q, c_k = c_{pj} - (c_1 + \dots + c_{k-1} + c_{k+1} + \dots + c_m) \bmod q$ 。



此时计票板显示:

$$Sign_1, v_1, ZK_1, c_{p_j}, c_{p_k}, c_{p_l}, \dots, Ans_{p_j}, Ans_{p_k}, Ans_{p_l} \dots$$

$$Sign_2, v_2, ZK_2, c_{p_j}, c_{p_k}, c_{p_l}, \dots, Ans_{p_j}, Ans_{p_k}, Ans_{p_l} \dots$$

⋮

$$Sign_n, v_n, ZK_n, c_{p_j}, c_{p_k}, c_{p_l}, \dots, Ans_{p_j}, Ans_{p_k}, Ans_{p_l} \dots$$

任意投票人  $p_i$  ( $i = 1, 2, \dots, m$ ) 或者管理者均可验证式

(2) ~ (4) 是否成立:

$$\alpha_i = g^{\omega_i} a^{c_i} \bmod p \quad (2)$$

$$\beta_i = h^{\omega_i} (b/Q_i)^{c_i} \bmod p \quad (3)$$

$$c = \sum_{i=1}^m c_i \bmod q \quad (4)$$

如果成立则说明  $p_i$  的选票明文  $\Phi_i \in \{Q_1, Q_2, \dots, Q_m\}$ , 否则该选票无效。

当所有选票验证通过,且签名有效时,该步结束。该步中环签名是为了防止在有人弃权的情况下管理者冒充该投票人进行投票;选票的零知识证明是为了防止投票人存在恶意投票的行为。这两者保证了协议的合法性。

## 2.4 计票阶段

当投票阶段结束后公告栏上均是有效选票,假设有  $k$  张选票是合法的,显示如下:

$$Sign_1, v_1, ZK_1, c_{p_j}, c_{p_k}, c_{p_l}, \dots, Ans_{p_j}, Ans_{p_k}, Ans_{p_l} \dots$$

$$Sign_2, v_2, ZK_2, c_{p_j}, c_{p_k}, c_{p_l}, \dots, Ans_{p_j}, Ans_{p_k}, Ans_{p_l} \dots$$

⋮

$$Sign_k, v_k, ZK_k, c_{p_j}, c_{p_k}, c_{p_l}, \dots, Ans_{p_j}, Ans_{p_k}, Ans_{p_l} \dots$$

由  $v_1, v_2, \dots, v_k$  和 ELGamal 乘法同态得到选票的和为  $S$ :

$$S = (b_1 b_2 \cdots b_k) / (a_1 a_2 \cdots a_k)^*$$

其中: $x$  为解密选票的私钥,任意  $k$  个人合作均可得到  $x$ 。解开  $S$  的素因子分解  $S = Q_1^{\theta_1} Q_2^{\theta_2} \cdots Q_m^{\theta_m}$ , 得到选票  $Q_i$  的个数为  $\theta_i$  ( $i = 1, 2, \dots, m$ ), 至此,投票活动结束。

## 3 安全性分析

本章假设当某一投票人弃权的情况下,管理者不会和另外的投票人合谋伪造选票。在此假设下,本文协议具有以下几个方面的属性:健壮性、匿名性、合法性、可验证性、无可信第三方。现就这几个方面展开分析。

### 3.1 健壮性

投票人发起的主动攻击存在以下三种情况:破坏公私钥对的生成、重复投票和投不合法的选票。由管理者发起的主动攻击只可能是伪造选票,其中能使投票流程被迫终止的行为只有两种:破坏公私钥对的生成、投不合法的选票。由于重复投票、投不合法的选票和伪造选票的行为属于协议的合法性保障的范围,所以将这些行为纳入对合法性的讨论。非投票人和管理者发起的攻击也纳入合法性的讨论。下面只需证明破坏生成公私钥对的人将会暴露自己的身份,那么协议的健壮性得证。

**定理 1** 投票流程是健壮的。

**证明** 对生成公私钥对的攻击存在以下两种:

1)  $p_i$  在 2.1 节中的第 1) 步中给出  $y \neq h_i$ 。

2)  $p_i$  在 2.1 节中的第 4) 步中发送给  $p_j$  的  $s_{ij} \neq f_i(j)$ 。

在第一种攻击中,如果  $p_i$  给出  $y = h_i + a$ , 其中  $a \neq 0$ , 且不被人发现,那么生成的加密和解密选票的公私钥不一致,最

后无法解密选票,则  $p_i$  达到自己的目的。此时  $p_i$  必须令  $F_{i0} = h_i + a$ , 若  $F_{i0} \neq h_i + a$ , 则可以立即发现  $p_i$  是攻击者,在 2.1 节的第 4) 步前,  $p_i$  都是安全的,在第 5) 步中  $p_i$  给  $p_j$  发送  $s_{ij}$  后,  $p_j$  验证式(1):

$$g^{x_i+j \cdot f_{i1}+\cdots+j^{k-1} \cdot f_{i,k-1}} b \bmod p = F_{i0} \cdot F_{i1}^j \cdots \cdots$$

$$F_{i,k-1}^{j^{k-1}} b \bmod p$$

化简后得:

$$a \cdot g^{j \cdot f_{i1}+\cdots+j^{k-1} \cdot f_{i,k-1}} \bmod p = 0$$

因为  $a \neq 0$ , 则必有  $a \cdot g^{j \cdot f_{i1}+\cdots+j^{k-1} \cdot f_{i,k-1}} = b \cdot p$  ( $b$  为非零整数), 对任意的  $j \in \{1, 2, \dots, n\}$  且  $j \neq i$  等式  $g^{j \cdot f_{i1}+\cdots+j^{k-1} \cdot f_{i,k-1}} = (b \cdot p)/a$  恒成立, 必有:  $bp = a; f_{i1}, f_{i2}, \dots, f_{i,k-1} = 0$ 。此时  $f_{i1}, f_{i2}, \dots, f_{i,k-1} \notin \mathbb{Z}_q^*$ , 则  $F_{i1}, F_{i2}, \dots, F_{i,k-1}$  不是模  $p$  上的离散对数运算, 对  $F_{i1}, F_{i2}, \dots, F_{i,k-1}$  求对数得  $f_{i1}, f_{i2}, \dots, f_{i,k-1} = 0$ , 此时可以确定  $p_i$  为攻击者。需要注意的是: 此时可能存在  $p_j$  和  $p_i$  合谋, 伪装验证式(1) 通过, 但是只要对于任意的  $p_j$  ( $j \in \{1, 2, \dots, n\}$  且  $j \neq i$ ) 验证式(1) 不通过, 则可判定  $p_i$  为攻击者。

在第二种攻击中,  $p_i$  和  $p_j$  合谋, 此时虽然  $p_i$  发送错误的  $s_{ij}$  给  $p_j$  (不同于上面的情况, 此时  $y = h_i$ , 只是  $p_i$  发送给  $p_j$  的  $s_{ij} \neq f_i(j)$ ) 而且  $p_j$  伪装验证(1) 通过, 但到了计票阶段,  $p_j$  拿出自己的  $s_j$  企图干扰恢复  $x$  时, 任意  $p_{i(i \neq j)}$  均可验证式(5) 是否成立, 若不成立, 则可以确定  $p_j$  为攻击者。

$$g^{s_j} \bmod p = \prod_{i=1}^n (h_i \prod_{t=1}^{k-1} F_{it}^y) \quad (5)$$

综上, 定理 1 得证, 协议具有健壮性。

### 3.2 可验证性

假设选票在匿名信道上传输时不会发生丢失, 则所有有效选票均会出现在计票板上, 此时任意  $p_i$  可以根据  $v_1, v_2, \dots, v_k$  自己来计算选票的和  $S$ , 确保自己的选票被计算在内。

### 3.3 匿名性

匿名信道和盲签名保障了投票人的匿名性。盲签名的安全性基于 RSA, 匿名信道的安全性可参考文献[1]。

### 3.4 合法性

**定理 2** 合法的选票才会被计算在内。

**证明** 产生不合法的选票有三种方式: 投票人重复投票、投票人投不合法票、管理者或其他人伪装成投票人投票。

**投票人重复投票:**  $p_i$  可能存在重复投票的行为, 但  $p_i$  知道每一张合法的选票必须要有  $A$  的签名, 如果  $p_i$  第二次向  $A$  申请签名, 那么第二次  $A$  必然会发现, 此时可以确定  $p_i$  为攻击者。

**投票人投不合法票:** 因为在整个投票流程中不会解密单张选票,  $p_i$  的选票明文可能不合法, 即  $\Phi_i \notin \{Q_1, Q_2, \dots, Q_m\}$ , 但任意的  $p_{j(j \neq i)}$  可以提出挑战  $c_{pj} \in \mathbb{Z}_q$  要求  $p_i$  给出对应的  $Ans_{pj}$ , 此时  $p_j$  根据  $Ans_{pj}$  验证式(2) ~ (4), 如果成立, 则说明  $p_i$  的选票是合法的; 否则  $p_i$  为攻击者。

**管理者伪装成投票人投票:** 因为管理者可以很方便地生成管理者签名, 所以他可能想伪装成投票人进行投票(注意: 此时必须是在有人弃权的情况下, 否则选票的总数会大于投票人的总数, 可以立即断定管理者是攻击者), 但是管理者没有投票人的私钥, 无法生成环签名, 所以管理者不能伪造选票。

**其他人伪装成投票人投票:** 因为其他人没有投票人的私钥, 所以无法生成投票人的签名, 继而也无法得到管理者的签



名。所以其他人无法伪装成投票人投票。

综上,定理 2 得证。

### 3.5 无可信第三方

本协议没有假设参与方中的任何一方是可信赖的,所以该协议满足无可信第三方。

## 4 效率分析与比较

由于幂运算在加解密和签名中支配其他运算,所以以幂运算的次数为单位来计算协议的复杂度,在生成加解密选票的公私钥阶段(初始化),每个投票人进行  $O(k + n)$  次幂运算,  $n$  个投票人则是  $O(kn + n^2)$  次幂运算。在管理者对选票进行签名阶段(签名),每个投票人进行两次幂运算,  $n$  个投票人则是  $O(n)$  次幂运算,管理者进行  $O(n)$  次幂运算。在投票阶段,每个投票人进行  $O(m)$  次幂运算,  $n$  个投票人则是  $O(mn)$  次幂运算。在计票阶段,计票板进行一次幂运算。本协议各阶段各参与方计算复杂度如表 3,与文献[16~18]协议比较结果如表 4,属性比较如表 5 所示。

表 3 本文协议各阶段的计算复杂度

Tab. 3 Computational complexity of each phase of proposed protocol

阶段	参与方		
	投票人	管理者	计票板
初始化	$O(kn + n^2)$	—	—
签名	$O(n)$	$O(n)$	—
投票	$O(mn)$	—	—
计票	—	—	$O(1)$

注:“—”表示无该阶段或该阶段计算复杂度为 0。

表 4 不同协议的计算复杂度比较

Tab. 4 Computational complexity comparison of different protocols

阶段	文献[16] 协议	文献[17] 协议	文献[18] 协议	本文 协议
初始化	$O(n)$	$O(n^2)$	$O(n)$	$O(kn + n^2)$
签名	—	—	$O(n)$	$O(n)$
投票	$O(n^2)$	$O(n^3 + n^2)$	$O(n^2)$	$O(mn)$
计票	$O(n)$	$O(n)$	$O(n)$	$O(1)$
合计	$O(n^2)$	$O(n^3 + n^2)$	$O(n^2)$	$O(kn + mn + n^2)$

注:“—”表示无该阶段或该阶段计算复杂度为 0。

从表 4 可知,当选票空间  $m$  与投票人总数  $n$  相差不大时本文协议与文献[16,18]协议有相同的复杂度,优于文献[17]协议的复杂度。从表 5 可知,文献[16~18]协议都没有同时满足匿名性、合法性、健壮性、可验证性、无可信第三方等属性。

表 5 不同协议属性的比较

Tab. 5 Attribute comparison of different protocols

属性	文献[16] 协议	文献[17] 协议	文献[18] 协议	本文 协议
匿名性	是	是	是	是
合法性	是	是	是	是
健壮性	否	是	是	是
可验证性	否	否	是	是
无可信第三方	否	否	否	是

## 5 结语

本文采用同态门限密码体制、环签名机制、盲签名等技术

提出了一个新的投票协议,该协议满足了 FOO 安全属性(无收据性除外),实现了投票协议真正意义上的公正性。但是本协议不足的一点是:当存在投票人弃权的情况下,此时管理者和某一个投票人可以合谋伪造选票。

### 参考文献(References)

- [1] CHAUM D L. Untraceable electronic mail, return addresses, and digital pseudonyms[J]. Communications of the ACM, 1981, 24(2): 84~90.
- [2] FUJIOKA A, OKAMOTO T, OHTA K. A practical secret voting scheme for large scale elections[C]// AUSCRYPT 1992: Proceedings of the 1992 Workshop on the Theory and Application of Cryptographic Techniques, LNCS 718. Berlin: Springer, 1993: 244~251.
- [3] ANTONIOU A, KORAKAS C, MANOLOPOULOS C, et al. A trust-centered approach for building e-voting systems[C]// EGOV 2007: Proceedings of the 2007 International Conference on Electronic Government. Berlin: Springer, 2007: 366~377.
- [4] TAGHAVI T, KAHANI M, BAFGHI A G. A verifiable multi-authority e-voting scheme for real world environment[M]// ELLEITHY K. Advances and Innovations in Systems, Computing Sciences and Software Engineering. Berlin: Springer, 2007: 421~426.
- [5] PENG K, BAO F. Efficient multiplicative homomorphic e-voting [C]// ISC 2010: Proceedings of the 2010 International Conference on Information Security. Berlin: Springer, 2010: 381~393.
- [6] 曹刚,施荣华.一种 Internet 上的匿名电子投票协议的研究与设计[J].计算机工程与应用,2004,40(12): 156~157.(CAO G, SHI R H. The research and design of an anonymous vote protocol of Internet [J]. Journal of Computer Engineering and Applications, 2004, 40(12): 156~157.)
- [7] 罗芬芬,林昌露,张胜元,等.基于 FOO 投票协议的无收据电子投票方案[J].计算机科学,2015,42(8): 180~184.(LUO F F, LIN C L, ZHANG S Y, et al. Electronic voting protocol with receipt-freeness based on the FOO voting protocol[J]. Computer Science, 2015, 42(8): 180~184.)
- [8] 杨婷婷,林昌露,刘忆宁,等.基于多方排序协议的安全电子投票方案[J].计算机系统应用,2015,24(8): 25~32.(YANG T T, LIN C L, LIU Y N, et al. Secure electronic voting scheme based on multi-party ranking[J]. Computer Systems and Applications, 2015, 24(8): 25~32.)
- [9] 刘高,刘忆宁,王东.一种可验证的多候选人电子投票方案[J].计算机工程与科学,2015,37(9): 1667~1670.(LIU G, LIU Y N, WANG D. A verifiable e-voting scheme with multi-candidates[J]. Computer Engineering and Science, 2015, 37(9): 1667~1670.)
- [10] 徐紫枫,曾康,周福才.基于时间释放加密和数字签名的匿名电子投票方案[J].计算机应用与软件,2016,33(12): 325~328.(XU Z F, ZENG K, ZHOU F C. Anonymous electronic voting scheme based on time-released encryption and digital signature[J]. Computer Applications and Software, 2016, 33(12): 325~328)
- [11] 董宇琦,翟健宏,孙彤,等.基于隐私保护的电子选举投票系统[J].计算机应用,2016,36(增刊2): 73~76.(DONG Y Q, ZHAI J H, SUN T, et al. Electronic voting system based on privacy protection [J]. Journal of Computer Applications, 2016, 36(S2): 73~76.)

(下转第 1063 页)



- [EB/OL]. [2017-05-10]. <https://www.tu-braunschweig.de/Medien-DB/sec/pubs/2014-ndss.pdf>.
- [6] 罗世奇,田生伟,孙华,等.深度信念网络的恶意代码分类策略研究[J].小型微型计算机系统,2017,38(11):2465-2470.(LUO S Q, TIAN S W, SUN H, et al. Research strategy of classify malicious code into families on the method of deep belief networks [J]. Journal of Chinese Computer Systems, 2017, 38(11): 2465 - 2470.)
- [7] 罗世奇,田生伟,孙华,等.栈式自编码的恶意代码分类算法研究[J].计算机应用研究,2018,35(1):261-265.(LUO S Q, TIAN S W, SUN H, et al. Research on malicious code classification algorithm of stacked auto encoder[J]. Application Research of Computers, 2018, 35(1): 261 - 265.)
- [8] SESHAGIRI P, VAZHAYIL A, SRIRAM P. AMA: static code analysis of Web page for the detection of malicious scripts [J]. Procedia Computer Science, 2016, 93: 768 - 773.
- [9] SHIBAHARA T, YAGI T, AKIYAMA M, et al. Efficient dynamic malware analysis based on network behavior using deep learning [C]// Proceedings of the 2016 IEEE Global Communications Conference. Piscataway, NJ: IEEE, 2017: 1 - 7.
- [10] MOSER A, KRUEGEL C, KIRDA E. Limits of static analysis for malware detection[C]// Proceedings of the Twenty-Third Annual Computer Security Applications Conference. Piscataway, NJ: IEEE, 2007: 421 - 430.
- [11] CAO S, YANG N, LIU Z. Online news recommender based on stacked auto-encoder[C]// Proceedings of the 2017 IEEE/ACIS 16th International Conference on Computer and Information Science. Piscataway, NJ: IEEE, 2017: 721 - 726.
- [12] NATARAJ L, KARTHIKEYAN S, JACOB G, et al. Malware images: visualization and automatic classification[C]// VizSec 2011. Proceedings of the 8th International Symposium on Visualization for Cyber Security. New York: ACM, 2011: Article No. 4.
- [13] SHAID S Z M, MAAROF M A. Malware behavior image for malware variant identification[C]// Proceedings of the 2014 International Symposium on Biometrics and Security Technologies. Piscataway, NJ: IEEE, 2014: 1 - 6.
- [14] KANCHERLA K, MUKKAMALA S. Image visualization based malware detection[C]// Proceedings of the 2013 IEEE Symposium on Computational Intelligence in Cyber Security. Piscataway, NJ: IEEE, 2013: 40 - 44.
- [15] 韩晓光,曲武,姚宣霞,等.基于纹理指纹的恶意代码变种检测方法研究[J].通信学报,2014,35(8):125-136.(HAN X G, QU W, YAO X X, et al. Research on malicious code variants detection based on texture fingerprint[J]. Journal on Communications, 2014, 35(8): 125 - 136.)
- [16] 韩晓光,姚宣霞,曲武,等.基于图像纹理聚类的恶意代码家族标注方法[J].解放军理工大学学报(自然科学版),2014(5):440-449.(HAN X G, YAO X X, QU W, et al. Malicious code family tagging based on image texture clustering technology [J]. Journal of PLA University of Science and Technology (Natural Science Edition), 2014(5): 440 - 449.)

This work is partially supported by the Scientific Research Innovation Project of Education Innovation Plan for Graduate Students in Xinjiang Uygur Autonomous Region (XJGRI2017007), the Science and Technology Talent Training Project of Xinjiang Uygur Autonomous Region (QN2016YX0051), the Cernet Next Generation Internet Technology Innovation Project (NGII20170420).

**LUO Shiqi**, born in 1993. M. S. candidate. His research interests include information security, image processing.

**TIAN Shengwei**, born in 1973. Ph. D., professor. His research interests include intelligence computing.

**YU Long**, born in 1974. M. S., professor. Her research interests include computer intelligence.

**YU Jiong**, born in 1964. Ph. D., professor. His research interests include network security, grid computing.

**SUN Hua**, born in 1974. Ph. D., associate professor. Her research interests include information security.

(上接第1040页)

- [12] 黄仕杰,洪璇.基于同态实现多候选人的电子投票方案[J].计算机应用与软件,2017,34(3):284-288.(HUANG S J, HONG X. An electronic voting scheme realizing multi candidates based on homomorphism[J]. Computer Applications and Software, 2017, 34(3): 284 - 288.)
- [13] DESMEDT Y. Threshold cryptosystems[C]// AUSCRYPT 1992: Proceedings of the 1992 Workshop on the Theory and Application of Cryptographic Techniques, LNCS 718. Berlin: Springer, 1993: 1 - 14.
- [14] ELGAMAL T. A public key cryptosystem and a signature scheme based on discrete logarithms[J]. IEEE Transactions on Information Theory, 1985, 31(4): 469 - 472.
- [15] RIVEST R L, SHAMIR A, TAUMAN Y. How to leak a secret [C]// ASIACRYPT 2001: Proceedings of the 7th International Conference on the Theory and Application of Cryptology and Information Security, LNCS 2248. Berlin: Springer, 2001: 552 - 565.
- [16] IFTENE S. General secret sharing based on the Chinese remainder theorem with applications in e-voting[J]. Electronic Notes in Theoretical Computer Science, 2007, 186: 67 - 84.

- [17] LI H, SUI Y, PENG W, et al. A viewable e-voting scheme for environments with conflict of interest[C]// CNS 2013: Proceedings of the 2013 International Conference on Communications and Network Security. Piscataway, NJ: IEEE, 2013: 251 - 259.

- [18] YUAN L, LI M, GUO C, et al. A verifiable e-voting scheme with secret sharing[C]// ICCT 2015: Proceedings of the 2015 International Conference on Communication Technology. Ghaziabad: IEEE, 2015: 304 - 308.

This work is partially supported by the National Natural Science Foundation of China (11471307, 11671377, 11771421), the Chongqing Research Program of Basic Research and Frontier Technology (cstc2015jcyjys40001).

**DAI Xiaokang**, born in 1993, M. S. candidate. His research interests include information security, privacy preservation.

**CHEN Changbo**, born in 1981, Ph. D., associate research fellow. His research interests include symbolic computation, information security.

**WU Wenyuan**, born in 1976, Ph. D., research fellow. His research interests include automatic reasoning, information security.