一种基于门限的电子投票方案

邹秀斌[1,2] 崔永泉[1] 付 才[1]
(华中科技大学计算机科学与技术学院信息安全实验室 武汉 430074)[1]
(江汉大学数计学院 武汉 430056)[2]

摘 要 在以往电子投票方案中,验票工作都是由一名验票员承担,该验票员若不诚实,可能不记录合法选票,却统计不合法选票。为了解决该问题,提出了一种基于门限的电子投票方案。在该方案中,验票工作需要 t 名验票员协作,从而使验票结果更可接受。而且,投票者公布的选票结果是选票真实内容的哈希值或者密文,没人能知道选票的真实内容,从而可以防止强迫投票者投票以及买卖投票等。

关键词 电子选票,门限,双线性映射
中图法分类号 TP309.7 **文献标识码** A

Threshold-based Electronic Voting Scheme

ZOU Xiu-bin[1,2] CUI Yong-quan[1] FU Cai[1]
(Laboratory of Information Security, College of Computer, Huazhong University of Science and Technology, Wuhan 430074, China)[1]
(College of Computer and Mathematics, Jianghan University, Wuhan 430056, China)[2]

Abstract A ballot checker is responsible for checking of ballot in the past electronic voting schemes. The ballot checker can not tally the legitimate ballot but count illegal ones if he is not honest. For solving the problem, the author presented an electronic voting scheme based on threshold. In this scheme, checking of ballot requires some ballot checkers's cooperation in the author's scheme. This makes the result of ballot checking acceptable. Voters publish Hash or ciphertext of the ballots content and nobody can know the authentic content of these ballots. It prevents someone from forcing voters to vote and voting trading, etc.

Keywords Electronic voting, Threshold, Bilinear map

1 引言

1981年,Chaum[1]最早提出了电子投票概念。而随着网络技术以及密码技术的发展,电子投票在现代生活中应用非常广泛,比如,各级单位、公司在民主选举或是集体决策时,电子投票方式更能提高员工的积极参与性,从而消除他们对选举活动的冷漠。另外,电子投票方式同传统投票方式相比,有很多优势,其中最主要的优势是减少人力、物力和财力等资源,同时,效率非常高。而且利用密码技术,电子投票的安全性得到了很大的提高。

1993年,Fujioka[2]提出了一种针对大型选举的实用秘密电子投票方案。在该电子投票方案中,参与方包括投票者(voter)、管理者(adminstrator)以及记票员(counter)。如果管理者和计票员合谋,该方案能够实现投票公平,而且,投票者和管理者的欺诈是可以禁止的。然而,该方案是在随机预言机模型下实现的。

投票者对自己的投票是否被统计,应该获得间接和直接的保证。2001年,Neff[3]提出了一种可验证的密钥混合技术,同时还把这种技术应用于通用的可验证电子投票。2006年,Adida[4]提出了一种选票协议。投票者投票后,这种选票协议可以部分判断其选票是否被统计。例如2007年,Chaum[5]等人详细地给出了一种选票方案,该方案亦允许投票者验证自己的投票是否被统计。

2008年,魏怀鉴[7]提出一个无可信中心的电子投票方案,在该方案中,在管理机构和计票机构都不可信的情况下仍能够保证投票的安全性。该方案能够始终保证投票者的匿名性,即使选票公开,任何人都不能确定投票者的身份;解决了选票碰撞的问题,即不同的投票人必定产生不同的选票。然而,在魏怀鉴所提方案中,由于记票机构知道投票者的投票情况,如果记票机构泄露投票者投票情况,则没有办法解决强迫投票者投票以及买卖投票等问题。2009年,郑丽[8]设计一个高效的电子投票方案。该方案满足可验证性和无收据性,同时还能保证选票内容的秘密性和投票者的合法性等。而郑丽利用的是同态ElGamal加密、门限ElGamal加密和零知识证明等技术。

总之,电子投票问题,已引起了学术界广泛关注。

到稿日期:2011-09-22 返修日期:2011-12-27 本文受国家自然科学基金(60903175,60703048),湖北省自然科学基金(2009CBD307,2008CDB352)资助。

邹秀斌(1974—),男,博士生,讲师,主要研究方向为公钥密码体制及其安全分析,E-mail:xbz1234@163.com;崔永泉(1976—),男,博士,讲师,主要研究方向为计算机病毒;付 才(1976—),男,博士,讲师,主要研究方向为无线网络安全、路由协议安全与软件脆弱性。

然而从验票工作来看，方案[2-8]都只有一名验票员，该验票员若不诚实，会引起验票结果错误。

1979年，Shamir[9]提出了(t,n)门限方案，即密钥分发者将主密钥分成若干个子密钥，然后把这些子密钥分配给n个成员，而只有至少t个成员才可以恢复密钥分发者的主密钥，这种方案主要用于密钥管理。

为了提高验证选票的安全性，本文作者结合Shamir的(t,n)门限思想以及Delerablée在文献[10]中的一些思想，利用双线性映射，提出了一种基于门限的电子投票方案(Threshold-Based Electronic Voting Scheme，以下简称为TBEVS方案)。在TBEVS方案中，参与方包括管理机构A(Administrator)、n位验票员(Ballot Checker)，以及若干名投票员(Voter)，该方案满足电子选票的要求。投票员投选票时，其身份是保密的；而在验证选票时，需要t名验票才能实现验票工作。以往方案大多数都是一名验票员承担验票工作，若其不诚实，他可能不记录合法选票，而统计不合法选票。在TBEVS方案中，由于在统计选票结果中，公布的是选票内容的哈希值，没人能知道选票的真实内容，从而可以防止强迫投票者投票以及买卖投票等。

2 相关知识

2.1 电子投票方案的安全要求

对于一般的电子投票方案，它应该具备以下一些性质：

(1)只有在有效投票者列表(其中的投票者具有合法投票资格)中的投票者，才能创建选票、参加投票。

(2)每一位合法投票者只能投一张选票。

(3)对一张选票而言，其所有者和内容都是机密的，如果没有投票者本人的默许，局外人是无法知道这张选票的内容和所有者的。

(4)投票者在投票之前，可以创建一张有效的选票并修改它。

(5)所有合法的选票都能够被正确统计记录。

(6)不诚实者不能够破坏电子投票方案。

(7)狭义的可验证性保证合法的选票被计入；广义的可验证性可以使任何感兴趣的第三方参与检验，同时不泄露投票者的隐私。

2.2 双线性映射

Boneh[11]引入双线性映射。从此以后，双线性映射大量应用于加密、签名等方面。

定义1 G_1、G_2、G_T都是阶为p的循环群，称一个有效可计算的映射$e:G_1\times G_2\to G_T$为双线性映射。该双线性映射满足下面一些性质：

(1)双线性：$u\in G_1$，$v\in Z_2$，$a,b\in Z$，$e(u^a,v^b)=e(u,v)^{ab}$。

(2)非退化性：存在生成元$u\in G_1$，生成元$v\in G_2$，满足$e(u,v)$是G_T的生成元。

(3)可计算性：对于$u,v\in G$，$e(u,v)$能够在有效时间内可计算。

2.3 *q-SDH* 假设(the Strong Diffie-Hellman 假设，简称为 *SDH* 假设)

Boneh[12]给出了*q-SDH*假设定义。令G_1、G_2、G_T都是阶为p的循环群，q是参数，则*q-SDH*问题定义如下：

给定元组$(g_1,g_1^x,g_1^{x^2},\cdots,g_1^{x^q},g_2,g_2^x)\in G_1^q\times G_2^2$，输出对$(c,g_1^{1/(x+c)})\in Z_p\times G_1$。

如果下面式子成立，算法A在双线性对群(G_1,G_2)中解决*q-SDH*问题具有优势ε。

$$SDHAdv_{q,A}=\Pr[A(g_1,g_1^x,\cdots,g_1^{x^q},g_2,g_2^x)=(c,g_1^{1/(x+c)})]\geqslant\varepsilon$$

定义2 如果无t时间算法在(G_1,G_2)中解决*q-SDH*问题具有优势ε，就说*q-SDH*假设成立。

3 TBEVS电子投票方案

TBEVS电子选票方案参与方包括：管理机构A(administrative organization)、n名验票员(ballot checker)、ℓ名投票者(Voter)。另外，本方案还需一公告板BB(bulletin board)。投票者将自己选票结果公布于公告板BB上，验票员对投票者所投选票进行验证，并将验票结果以及验票结果统计公布在公告板BB上。

设管理机构A的身份是ID_0，全体验票员为$T_1,T_2,\cdots,T_n$，其身份信息分别为$ID_1,ID_2,\cdots,ID_n$，令集合$T=\{T_1,T_2,\cdots,T_n\}$。令全体投票者为$V_1,V_2,\cdots,V_\ell$(其中ℓ是投票者的数目)，其身份分别为$I_1,I_2,\cdots,I_\ell$。该方案中用到的主要包括系统初始化setup、密钥生成和分发(join1和join2)、加密算法encrypt、解密算法decrypt等。

3.1 系统初始化

setup(λ)。该算法实现系统初始化功能。首先，给定安全参数λ，p是大素数，且p满足$|p|=\lambda$。设G_1、G_2、G_T都是阶为p的循环群。令$e:G_1\times G_2\to G_T$为双线性映射。其次，选择随机生成元$g\in G_1$，$h\in G_2$；随机选择$\gamma,\varphi\in Z_p$，主密钥$MK=(g,h,\gamma,\varphi)$，系统公开选票加密密钥$EK=(h,w,\rho)$，其中$w=g^\gamma$，$\rho=e(g,h)$

3.2 密钥生成和分发

Join1(MK,ID_i)。该算法作用是管理机构A为验票员T_i产生解密选票的子密钥DK_i。管理机构A将验票工作交给t名验票员，设s是管理机构A的临时私钥，管理机构A需要向验票员T_i分发子密钥s_i，由于考虑到管理机构A授权给不同组进行验票工作，那么管理机构A至少要选择C_n^t个$t-1$多项式。当n很大且t大小适中时，C_n^t是个很大的数。所以，为了减少开销，新方案中的管理机构A选择一个关于x,y的多项式，这样管理机构A工作起来很轻松。设一个关于x,y的多项式如下所示：

$$F(x,y)=(a_0+y)+(a_1+y)x+\cdots+(a_{t-1}+y)x^{t-1}$$

式中，$a_0,a_1,\cdots,a_{t-1}\in Z_p$。

随机选择$\xi\in Z_p$，令$f(x)=F(x,\xi)$。当$i=1,\cdots,n$时，计算$s_i=f(ID_i)$，$A_i=g^{\frac{f(ID_i)}{\gamma+f(0)}}$，$B_i=h^{\frac{1}{\gamma+f(0)}}$，$D=g^{\frac{1}{\gamma+f(0)}}$，需要注意的是$s_0=s=a_0+\xi$。令生成元$g\in G_1$，$h\in G_2$，计算$\rho_0=e(g^s,h)$；当$j=1,\cdots,n$时，计算$\rho_j=e(g^{a_j+\xi},h)$；然后管理机构A广播$\rho_0,\rho_1,\cdots,\rho_n,D$。将$s_i$发送给验票员$T_i$。验票员$T_i$可以验证下面的等式

$$e(g^{s_i},h)=\prod_{j=0}^{t-1}\rho_j^{ID_i^j} \tag{1}$$

是否成立。若成立，则验票员T_i可以接受管理机构A发送给他的s_i。否则，验票员T_i广播元组$\langle ID_0,ID_i,invalid\rangle$，指明身份为$ID_0$的管理机构A发给验票员$T_i$的$s_i$是无效的。

身份为 ID_i 的验票员 T_i 要求管理机构 A 重新发一个 s_i。由于

$$\begin{aligned}e(g^{s_i},h)&=e(g,h)^{f(ID_i)}\\&=e(g,h)^{(a_0+\xi)+(a_1+\xi)ID_i+(a_2+\xi)ID_i^2+\cdots+(a_{t-1}+\xi)ID_i^{t-1}}\\&=e(g,h)^{(a_0+\xi)}e(g,h)^{(a_1+\xi)ID_i}\cdots e(g,h)^{(a_{t-1}+\xi)ID_i^{t-1}}\\&=e(g^{(a_0+\xi)},h)e(g^{(a_1+\xi)},h)^{ID_i}\cdots e(g^{(a_{t-1}+\xi)},h)^{ID_i^{t-1}}\\&=\prod_{j=0}^{t-1}\rho_j^{ID_i^j}\end{aligned}$$

因此，只要管理机构 A 发给验票员 T_i 的 s_i 是正确的，等式(1)肯定成立。之后，当验票员 T_i 成功接收 s_i 后，判断下面等式

$$D^{s_i}=A_i \tag{2}$$

是否成立。如果成立，则验票员 T_i 接收 A_i，并把(ID_i, A_i, B_i)作为自己验票时的子密钥 DK_i，否则要求重发 A_i。

Join2(MK, I_i)。该算法为投票者 V_i 产生密钥(该密钥用于产生选票的关键字)。当管理机构 A 认为身份为 I_i 的投票者 V_i 是合格的投票者时，他随机选择 $x_i\in\mathbb{Z}_p$，且要求 x_1, x_2, …, x_ℓ 都互不相等。将 x_i 秘密发送给 V_i。令 $\eta_{1,i}=g^{x_i}$，管理机构 A 广播 $\eta_{1,i}$。投票者 V_i 验证下面等式

$$\eta_{1,i}=g^{x_i} \tag{3}$$

是否成立，如果成立，则投票者 V_i 接收管理机构 A 发送给自己的 x_i。如果不成立，则要求管理机构 A 秘密发送 x_i。这样，管理机构 A 随机选择 $x_1, x_2, \cdots, x_\ell\in\mathbb{Z}_p$，$\eta_{1,1}=g^{x_1}$，$\eta_{1,2}=g^{x_2}$，…，$\eta_{1,\ell}=g^{x_\ell}$。分别将 $x_1, x_2, \cdots, x_\ell$ 秘密发送给投票者 $V_1, V_2, \cdots, V_\ell$，并广播 $\eta_{1,1}, \eta_{1,2}, \cdots, \eta_{1,\ell}$，令 B 是集合$\{\eta_{1,1}, \eta_{1,2}, \cdots, \eta_{1,\ell}\}$。类似地，管理机构 A 随机选择 $z_1, z_2, \cdots, z_n\in\mathbb{Z}_p$，计算 $\eta_{2,1}=g^{z_1}, \cdots, \eta_{2,n}=g^{z_n}$ 并广播 $\eta_{2,1}, \eta_{2,2}, \cdots, \eta_{2,n}$。随后，将 $z_1, \cdots, z_n$ 分别秘密发送给验票员 $T_1, T_2, \cdots, T_n$。

3.3 加密算法

encrypt(EK, m_i)。设选票内容 $m_i\in G_T$，投票者 V_i(其中$i=1,\cdots,\ell$)。随机选择 k_i，计算 $F_{i,1}=w^{k_i}$，$F_{i,2}=h^{k_i}$，$K_i=\rho^{k_i}$ 计算 m_i 的密文 $C_i=m_iK_i$。

3.4 解密算法

decrypt($F_{i,1}$, $F_{i,2}$, C_i)。$T_1, T_2, \cdots, T_n$ 是能够参与验票工作的成员集合。从中选取 t 个成员负责验票工作。不失一般性，设负责验票工作的验票成员集合为 $T_1, T_2, \cdots, T_t$。其相应的身份信息为 $ID_1, ID_2, \cdots, ID_t$。针对公告板 BB 上投票者 V_i 提供的元组($\theta_{i,1}$, $\theta_{i,2}$, $F_{i,1}$, $F_{i,2}$, C_i)，解密 C_i。

$$\chi_j=\sum_{k=1,k\neq j}^{t}\frac{-ID_k}{ID_j-ID_k}$$

$$\begin{aligned}&e(F_{i,1},\prod_{j=1}^{t}B_j)\cdot e(F_{i,2},\prod_{j=1}^{t}(A_j)^{\chi_j})\\&=e(w^{k_i},h^{\sum_{i=1}^{t}\frac{1}{\gamma+f(ID_i)}})\cdot e(h^{k_i},g^{\sum_{i=1}^{t}\frac{\chi_i f(ID_i)}{\gamma+f(0)}})\\&=e(g^{k_i\gamma},h^{\frac{1}{(\gamma+f(0))}})\cdot e(h^{k_i},g^{\frac{f(0)}{\gamma+f(0)}})\\&=e(g,h)^{\frac{k_i\gamma}{(\gamma+f(0))}}\cdot e(g,h)^{\frac{k_i f(0)}{(\gamma+f(0))}}=e(g,h)^{k_i}\end{aligned}$$

于是得到 $K_i=e(g,h)^{k_i}$。从而得到明文 $m_i=C_i/K_i$。

4 TBEVS 电子投票方案工作过程

TBEVS 电子投票方案工作流程(见图 1)如下：

(1)系统初始化　管理机构 A 运行 setup(λ)算法，得到主密钥 $MK=(g,h,\gamma)$，设 $H(x)$ 是哈希函数，系统公开 g, h, 选票加密密钥 $EK=(h,w,\rho)$以及 $H(x)$函数，其中 $w=g^\gamma$，$\rho=e(g,h)$。

(2)验票员密钥生成　管理机构 A 将验票工作授权给验票员 $T_1, T_2, \cdots, T_n$，但只有至少 t 名验票员才能进行验票，否则无法知道投票者的投票内容。管理机构 A 运行 Join1(MK, ID_i)算法，给验票员 T_i(其中 $i=1,\cdots,n$)发送子密钥 s_i, A_i，其中 $s_i=f(ID_i)$，$A_i=g^{\frac{f(ID_i)}{\gamma+f(0)}}$。

(3)投票者密钥生成　管理机构 A 运行算法 Join2(MK, I_i)算法，将 x_i(其中 $i=1,\cdots,\ell$)发送给投票者 V_i。投票者 V_i 在投票过程中要用到 x_i。

(4)投票者投票　投票者 V_i(其中 $i=1,\cdots,\ell$)运行算法 encrypt(EK, m_i)，随机选择 k_i，计算 $F_{i,1}=w^{k_i}$，$F_{i,2}=h^{k_i}$，$K_i=\rho^{k_i}$，计算 m_i 的密文 $C_i=m_iK_i$。投票者 V_i 随机选择 $r_i\in\mathbb{Z}_p$，计算 $\theta_{i,1}=g^{r_ix_i}$，$\theta_{i,2}=h^{r_i}$。投票者 V_i 生成投票元组($\theta_{i,1}$, $\theta_{i,2}$, $F_{i,1}$, $F_{i,2}$, C_i)，并将该元组放到公告板 BB 上，他自己保留 r_i。由于选票 m_i 已加密，因此无人知道该元组是投票者 V_i 产生的；由于无人(包括管理机构 A)知道 r_i。因此没人能知道公布于公告板 BB 的选票是谁投票的。

(5)验票员验票　管理机构 A 从验票员 $T_1, T_2, \cdots, T_n$ 中选出 t 名验票员来参加选票工作，并对外公布其身份。对于公告板上的投票元组($\theta_{i,1}$, $\theta_{i,2}$, $F_{i,1}$, $F_{i,2}$, C_i)，首先，t 名验票员检查是否存在$\beta\in B$，且 β 满足下面等式

$$e(\beta,\theta_{i,2})=e(h,\theta_{i,1}) \tag{4}$$

如果式(4)满足，说明投票元组($\theta_{i,1}$, $\theta_{i,2}$, $F_{i,1}$, $F_{i,2}$, C_i)是合法投票者的投票。若元组($\theta_{i,1}$, $\theta_{i,2}$, $F_{i,1}$, $F_{i,2}$, C_i)是合法选票，t 名验票员协作运行 decrypt($F_{i,1}$, $F_{i,2}$, C_i)算法，得到 K_i，明文 $m_i=C_i/K_i$。计算 $M_i=H(m_i,\beta,\theta_{i,2},\omega_{i,1},\cdots,\omega_{i,t})$。从而得到验票结果元组($\omega_{i,1}$, …, $\omega_{i,t}$, M_i)，且 $\omega_{i,j}=(ID_j, g^{y_jz_j}, h^{z_j})$(其中 $j=1,\cdots,t$)。验票员们在公告板 BB 上公布验票结果元组($\omega_{i,1}$, …, $\omega_{i,t}$, M_i)，并把它归类到相应的投票情况分类表中。

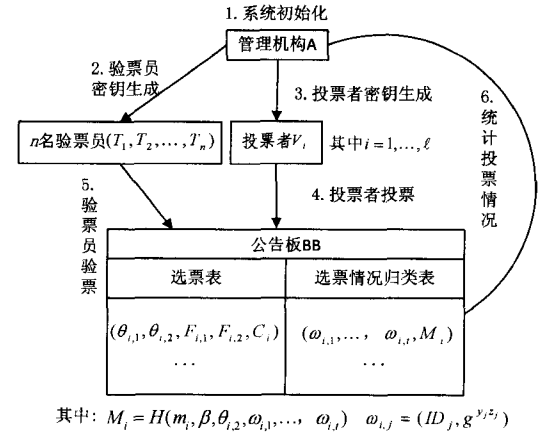

图 1　TBEVS 电子投票方案工作流程

需要注意的是：如果还存在选票($\bar{\theta}_{i,1}$, $\bar{\theta}_{i,2}$, $\bar{F}_{i,1}$, $\bar{F}_{i,2}$, $\bar{C}_i$)和 $\beta\in B$ 且满足式(4)，说明选票($\theta_{i,1}$, $\theta_{i,2}$, $F_{i,1}$, $F_{i,2}$, C_i)和($\bar{\theta}_{i,1}$, $\bar{\theta}_{i,2}$, $\bar{F}_{i,1}$, $\bar{F}_{i,2}$, $\bar{C}_i$)是同一人所投的选票。应忽略掉选票($\bar{\theta}_{i,1}$, $\bar{\theta}_{i,2}$, $\bar{F}_{i,1}$, $\bar{F}_{i,2}$, $\bar{C}_i$)。

(6)统计投票结果　当公告板 BB 上的投票情况表没有错误时，t 名验票员统计投票结果，并将投票结果公布于公告

板 BB 上。

5 TBEVS 方案安全分析

定理 1 合格投票者 $V_i(i=1,\cdots,\ell)$能够提供唯一合法选票。

定理 2 只有在有效投票者列表(其中的投票者具有合法投票资格)中的投票者,才能创建选票、参加投票。

证明:由于管理机构 A 产生了集合 $B=\{\eta_{1,1},\eta_{1,2},\cdots,\eta_{1,\ell}\}$。投票者 V_i 在公告板 BB 上的选票表中公布了元组 $(\theta_{i,1},\theta_{i,2},F_{i,1},F_{i,2},C_i)$。$t$ 名验票员检查是否存在 $\beta\in B$,且有等式 $e(\beta,\theta_{i,2})=e(h,\theta_{i,1})$ 成立,如果不存在 β,说明$(\theta_{i,1},\theta_{i,2},F_{i,1},F_{i,2},C_i)$是非法投票者产生的;如果存在 β,说明$(\theta_{i,1},\theta_{i,2},F_{i,1},F_{i,2},C_i)$是由投票者 V_i 产生的。

如果有人怀疑元组$(\theta_{i,1},\theta_{i,2},F_{i,1},F_{i,2},C_i)$是否由投票者 V_i 本人产生的,投票者 V_i 能公示 r_i,说明元组$(\theta_{i,1},\theta_{i,2},F_{i,1},F_{i,2},C_i)$是他的投票元组。如果 t 名验票员发现以前检验过投票元组$(\theta_{i,1},\theta_{i,2},F_{i,1},F_{i,2},C_i)$,$t$ 名验票员可以不重复统计投票者 V_i 的选票。

定理 3 在 TBEVS 方案中,如果没有投票者本人的默许,局外人无法知道投票者的选票的内容。

证明:对于合格投票者 $V_i(i=1,\cdots,\ell)$而言,投票者 V_i 在公告板 BB 上的选票表中公布了投票元组$(\theta_{i,1},\theta_{i,2},F_{i,1},F_{i,2},C_i)$。其选票内容已加密成 C_i,局外人无法知道投票者 V_i 的选票内容;而且在验票过程中,t 名验票员仅仅知道投票元组$(\theta_{i,1},\theta_{i,2},F_{i,1},F_{i,2},C_i)$相应的选票内容,只知道该元组是由合法投票者产生的,但不知道由谁产生的元组。

定理 4 投票者 $V_i(i=1,\cdots,\ell)$认为自己的选票没有正确地归类到公告板 BB 上的选票归类表中,可以要求重新验证自己的选票。

投票者 V_i 秘密保存了 x_i,r_i,而 $\omega_{i,1},\cdots,\omega_{i,t}$信息已公开,所以他可以计算 $\overline{M}_i=H(m_i,g^{x_i},h^{r_i},\omega_{i,1},\cdots,\omega_{i,t})$。若在相应的投票情况分类表中没有发现$(\omega_{i,1},\cdots,\omega_{i,t},\overline{M}_i)$,投票者 V_i 觉得自己的选票没有被验票员合理统计,他可以向管理机构 A 提出从新检验自己的投票的要求。管理机构 A 做出检验后,决定投票者 V_i 和验票员 $T_1,T_2,\cdots,T_t$ 中,谁在欺诈,并追究其责任。

首先,投票者 V_i 公布自己的 r_i,而管理机构 A 公布 x_i,若 $h^{x_i}=\theta_{i,2}$,说明投票者 V_i 是合格投票者。判断下面等式是否成立

$$\theta_{i,1}=g^{r_ix_i} \tag{5}$$

如果不成立,说明$(\theta_{i,1},\theta_{i,2},F_{i,1},F_{i,2},C_i)$不是由投票者 V_i 产生的元组。如果成立,说明该投票元组是投票者 V_i 的投票元组,管理机构 A 运行解密算法 decrypt$(F_{i,1},F_{i,2},C_i)$,重新得到选票的内容 $\widetilde{m}_i$,计算 $\widetilde{M}_i=H(\widetilde{m}_i,g^{x_i},h^{r_i},\omega_{i,1},\cdots,\omega_{i,t})$,如果 $\overline{M}_i\neq\widetilde{M}_i$,说明验票员 $T_1,T_2,\cdots,T_t$ 验票错误,管理机构 A 追究其责任。否则,说明投票者 V_i 的说法是错误的。

定理 5 当验票员的人数小于 t 时,他们是无法进行验票工作的。

6 同其它方案比较

在电子投票系统中,选票加密、解密算法的运算复杂度以及电子投票的特性要求是我们重点考虑的问题。表 1 列出各方案的比较情况。

表 1 各方案比较表

项目 \ 方案名称	文献[2]方案	文献[7]方案	文献[8]方案	TBEVS 方案
选票加密运算量	O(1)次盲化运算,O(1)次签名	O(1)次哈希运算。和 O(1)次模乘法运算	O(L)模幂运算,O(1)次签名处理,L 是候选人人数	O(1)次模幂运算,O(1)次模乘法运算
选票解密运算量	O(1)次签名检查运算	O(1)次哈希运算。和 O(1)次模乘法运算	O(L) 模幂运算和模乘法运算。L 是候选人人数。	O(t)次模乘法运算,O(1)次双线性对运算,O(1)次模除法运算
验票员数量	1	1	1	t
投票后是否可验证	是	是	是	是
选票匿名性	是	是	是	是
投票的唯一性	是	是	是	是
防止强迫投票者投票以及买卖投票	是	否	是	是

文献[2]方案给出了一个大规模的电子选票系统,但该系统中,选票加密、解密都没有用到具体的算法。根据表 1,其加密解密时间复杂度要根据实践中所用选票加密算法、解密算法而确定。文献[7]方案选票加密解密时间复杂度主要与其所使用的哈希函数有关。文献[8]方案考虑到候选人的数目,选票加密解密时间复杂度是 O(L)。而 TBEVS 方案是在标准模型下实现的。同文献[2,7,8]方案相比,TBEVS 选票加密解密时间复杂度相对优化。从验票员数量来看,只有 TBEVS 方案有 t 名,这样,TBEVS 方案的验票工作更加可信可靠。另外文献[2,8]方案及 TBEVS 方案均满足电子选票的一般特性:投票后可以验证,具有投票匿名性、投票的唯一性,可防止强迫投票者投票或买卖投票。在文献[7]方案中,虽然验票员不知道投票情况,但验票员知道投票者的身份,他还可以计算出投票元组的各个分量。所以,从表 1 可以发现文献[7]方案除了不满足防止强迫投票者投票或买卖投票外,其它电子投票的一般特性都满足。

结束语 本文提出了一种基于门限的电子投票方案,在该方案中,验票工作需要 t 名验票员协作,从而使验票结果更可接受。同时,作者提出的电子选票方案满足一般电子选票方案的要求。

参 考 文 献

[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[M]. Springer, 1993

[3] Neff C A. A verifiable secret shuffle and its application to e-voting[Z]. ACM, 2001

[4] Adida B, Neff C A. Ballot casting assurance[Z]. USENIX Association, 2006

[5] Chaum D, et al. Science, Secret ballot elections with unconditional integrity[Z]. Citeseer, 2007

[6] Cui Guo-hua, W Y, Su Li. A Secure Elect ronic Vot ing Scheme Based on List Signature Schemes[J]. Computer Engineering & Science, 2008, 30(1007-130X): 4

[7] 魏怀鉴，鲍皖苏，隗云，等. 无可信中心的电子投票方案[J]. 计算机应用研究，2008，25(7)：2159-2160

[8] 郑丽，王箭. 一种新的无收据的电子投票方案[J]. 小型微型计算机系统，2009，30(2)：380-384

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

[10] Delerablée C, Paillier P, Pointcheval D. Fully collusion secure dynamic broadcast encryption with constant-size ciphertexts or decryption keys [C] // Pairing-Based Cryptography - CPairing 2007. 2010: 39-59

[11] Boneh D, Franklin M. Identity-based encryption from the Weil pairing[C]//CRYPTO 2001. Springer, 2001

[12] Boneh D, Boyen X. Short signatures without random oracles and the SDH assumption in bilinear groups[J]. Journal of Cryptology, 2008, 21(2): 149-177

(上接第 28 页)

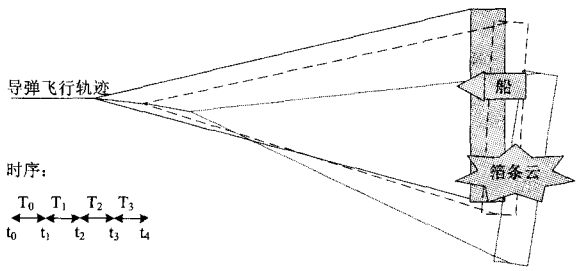

图 6 单舰反导仿真过程想定

3.5 仿真应用中的推理

(1) T_0: Missile(A) ∧ Ship(B)

(2) t_1: Happens(Missile. State(track) ∧ (In(A,B), t_1)

(3) T_1: Tracking(A,B) Rule 1and Rule 5

(4) t_2: Happens(Chaff_cloud(C) (In(A,C), t_2)

(5) T_2: Jamming(A,B) Rule 1and Rule 6

(6) t_3: Happens(∧ In(A,B), t_3)

(7) T_3: Jammed(A,B) Rule 1and Rule 7

(8) t_4: Happens(→Missile(A), t_4) Simulation ended.

白方实体在 t_3 时刻观察到干扰成功，在 t_4 时刻观察到仿真结束，与期望的结果相同。

基于 EWOnto，可以从现实世界的环境、系统和任务中获得知识，形成知识库。然后，试验和训练的规划者定义行动的对象和约束，提出部分或全部的实体、属性和关系。分析人员利用 EW 过程内特定的推理规则以及知识库中获得的事实，确定提出的规划是否满足特定的互操作需求。本体论的长期目标是基于一致认识的知识库，实现对 EW 装备及其模型的分析/综合功能。

结束语 本文在分析电子战系统和电子战交战过程的基础上，概括了电子战仿真系统中的实体、状态、属性、关系等要素，提出了电子战系统的本体论，并采用形式化的方式将该本体论应用到单舰反导的实例中。虽然该本体论本身可能不是非常完备，但是我们将在下一步工作中基于对电子战的认识对其进行改进，并希望其能够在电子战系统的信息化、建模与仿真、试验和训练中发挥基础性作用。

参 考 文 献

[1] Miller J A, Baramidze G T, Sheth A P, et al. Investigating Ontologies for Simulation Modeling [C]// Annual Simulation Symposium 2004. 2004: 55-63

[2] Kokar M M, Matheus C J, Baclawski K. Ontology-based situation awareness[J]. Information Fusion, 2009, 10: 83-98

[3] Smith B. Ontology [C]// Floridi L, ed. Blackwell Guide to the Philosophy of Computing and Information. Oxford: Blackwell, 2003: 155-166

[4] Sindico A, Tortora S, Chiarini P A, et al. An electronic warfare meta-model for network centric systems [C]// 2010 2nd International Workshop on Cognitive Information Processing. June 2010: 23-28

[5] Kars S, Oğuztüzün H. An Ontology for a Naval Wargame Conceptual Model [C]// Metadata and Semantic Research Communications in Computer and Information Science. 2011, 240, Part 1: 1-11

[6] Ford R, Martin D, Elenius D, et al. Ontologies and tools for analysing and composing simulation confederations for the training and testing domains [J]. Journal of Simulation, 2011(8): 230-245

[7] 施毅，汪新林，陆廷金. 基于顶层本体的电子对抗领域本体构建方法[J]. 计算机工程，2008(22)

[8] Alberts D S, Garstka J J, Stein F P. Network-Centric Warfare: Developing and Leveraging Information Superiority [M]. Center for Advanced Concepts and Technology, July 2002

[9] 王国玉，等. 无边界靶场[M]. 北京：国防工业出版社，2007：45-47

[10] Arnold J T. The Shoreline: Where Cyber and Electronic Warfare Operations Coexist [R]. A Research Report Submitted to the Faculty In Partial Fulfillment of the Graduation Requirements, February 2009

[11] Steinman J, Lammers C, Valinski M. A Unified Technical Framework for Net-centric Systems of Systems, Test and Evaluation, Training, Modeling and Simulation, and Beyond…[C]// Proceedings of the Fall 2008 Simulation Interoperability Workshop. 08F-SIW-041. 2008

[12] Obrst L. Ontologies for Semantically Interoperable Systems[C]// CIKM 2003. 2003: 366-369

[13] Wallace, Jeffrey, Hannibal B. Software and Hardware System Integration and Intelligent Automation using Ontology-based Knowledge Representation Technology[C]// the Proceedings of the 2008 International Conference on Artificial Intelligence. World Academy of Sciences, Las Vegas, NV, July 2008: 14-16

[14] DoD. FM 3-36 Electronic Warfare in Operations[Z]. February 2009

[15] Nicollin X, Sifakis J. An Overview and Synthesis on Timed Process Algebras [C]// REX Workshop 1991. 1991: 526-548