基于FOO投票协议的无收据电子投票方案

罗芬芬[1,2] 林昌露[1,2] 张胜元[1,2] 刘忆宁[3]
(福建师范大学数学与计算机科学学院 福州 350117)[1]
(福建省网络安全与密码技术重点实验室(福建师范大学) 福州 350117)[2]
(桂林电子科技大学数学与计算科学学院 桂林 541004)[3]

摘 要 安全且实用的电子投票协议是信息安全领域的热点问题之一。引入了盲签名、投票编号、申诉标识等工具，提出了一种新的无收据的电子投票方案，该方案进一步完善了FOO投票协议，可保证选票的匿名性、可验证性和无收据性，并且允许投票者中途弃权。该方案不仅保持了原方案的各种优点，而且增强了系统的安全性和灵活性。因此，与其他类似方案相比较，该方案具有更好的通用性和实用性。

关键词 电子投票，FOO投票协议，盲签名，无收据
中图法分类号 TP309.2 **文献标识码** A **DOI** 10.11896/j.issn.1002-137X.2015.8.038

Receipt-freeness Electronic Voting Scheme Based on FOO Voting Protocol

LUO Fen-fen[1,2] LIN Chang-lu[1,2] ZHANG Sheng-yuan[1,2] LIU Yi-ning[3]
(School of Mathematics and Computer Science, Fujian Normal University, Fuzhou 350117, China)[1]
(Fujian Provincial Key Laboratory of Network Security and Cryptology (Fujian Normal University), Fuzhou 350117, China)[2]
(School of Mathematics and Computer Sciences, Guilin University of Electronic Technology, Guilin 541004, China)[3]

Abstract The secure and pratical electronic protocol is one of the hot research topics in the information security. A new receipt-freeness electronic voting scheme based on FOO voting protocol was proposed by using the tools of the blind signature, serial number and unique identity in this paper. The proposed scheme improves the FOO voting protocol and it holds the properities of the anonymity of the ballot, the verifiability and receipt-freeness. In addition, the voter can abstain from voting. Specially, the proposed scheme not only has all advantages of FOO voting protocol but also enhances the security and flexibility. Therefore, it is more universal and practical than the previous protocols.

Keywords Electronic voting, FOO voting protocol, Blind signature, Receipt-freeness

1 引言

电子投票系统是利用互联网技术和信息安全技术，使得投票者可以使用计算机在家或者在投票站通过网络来投票，并且投票后的计票、结果公布等其他工作都是由计算机自动完成的。该系统使得整个投票过程在活动的组织、选票的收集和结果的统计等方面都节省了大量的成本，而且进一步保证了投票的公正、公平、公开。

由美国密码学家Chaum[1]在1981年设计并提出的一种通过匿名信道传递选票的模型是历史上最早的电子选票方案，该模型采用了公钥密码体制并用数字假名投票来隐藏投票者的身份。在1985年，Cohen和Fisher[2]提出了基于同态加密技术的电子投票协议。随后，Benaloh[3]、Iverson[4]、Sako等[5]也分别提出了不同性质的电子投票协议。这些方案虽然都有各自的优点，但也存在一定的缺陷，比如Cohen和Fisher的投票协议要求必须同时进行所有的投票活动；Iverson的投票协议主要不能有效地防止作弊，这使得在整个投票过程中只有通过所有的投票者合作才能投票。2012年Essex和Hengartner提出的Hover投票协议[6]的安全性仍有待进一步检验。

近几年，基于网络的远程投票协议的研究受到了更多的关注，也取得了比较好的研究成果，包括：不需要投票站的无收据电子投票协议[7]、“端到端”可验证的互联网协议EVIV[8]、面向移动自组织网络的投票协议[9]、基于Hash函数的轻量级远程投票协议[10]，以及抗贿选攻击的互联网投票协议[11]，它们不断扩大了远程投票协议的应用范围。

1992年，日本学者Fujioka、Okamoto和Ohta[12]提出了第一个适用于大规模投票的协议，这是一种基于比特承诺和盲签名等密码技术的电子投票协议，简记为FOO投票协议。该协议具有较强的实用性，它的算法比较容易实现，能有效地保证投票的秘密性和公平性，被认为是一种可以安全组织大规模投票的协议，从而受到了极大的关注。许多大学和研究

到稿日期：2014-07-18 返修日期：2014-10-27 本文受国家自然科学基金项目(61103247,61363069)，福建师范大学“网络与信息安全关键理论和技术”校创新团队(IRTL1207)资助。

罗芬芬(1989－)，女，硕士生，主要研究方向为密码学及其应用；林昌露(1978－)，男，博士，副教授，主要研究方向为密码学及其应用，E-mail：cllin@fjnu.edu.cn(通信作者)；张胜元(1966－)，博士，教授，主要研究方向为编码与密码；刘忆宁(1973－)，博士，副教授，主要研究方向为信息安全。

机构都在FOO投票协议的基础上加以改进，开发出了具有实际意义的电子投票软件系统，如麻省理工学院的EVOX系统、华盛顿大学的Sensus系统等。FOO投票协议本身还存在着一些缺点，如：①投票效率较低；②选票碰撞问题；③不允许投票者弃权；④计票阶段的作弊问题。因此这些设计者们在开发电子投票系统软件的时候对FOO投票协议分别进行了相应改造的同时又产生了新的问题，比如华盛顿大学的Sensus改进的系统投票的中间结果就有可能泄漏；而在麻省理工学院改进的EVOX系统中，存在着一些管理机构可以舞弊的漏洞。

到目前为止，已经有多位学者就FOO协议中存在的问题提出了不同的解决方案。谢金宝等[13]的方案虽然加入了公证人群体，然而并没有解决选票碰撞的问题。陈晓峰等[14]提出了一种基于半信任模式的电子投票协议，是为了实现投票的无收据性，然而通信量较大等其他要求使得该协议难以投入实际应用。范安东等[15]提出了基于环签名的电子投票协议，该协议在一定程度上很好地实现了投票者的匿名性，但是在无收据方面仍然存在漏洞。夏静波等[16]提出的无收据的高效电子选举方案运用了圆锥曲线密码学理论、盲数字签名技术和抗干扰的智能卡技术，尽管该方案很好地结合了广义可验证性和无收据性，但是它的设计非常复杂。郭玲玲等[17]针对匿名性和无收据性的综合问题，提出了一种基于群盲签名的高效无收据的电子投票协议，但要求完全可信任的机构也是该方案本身的一个缺陷。陈晓洪[18]基于安全多方计算改进了电子投票协议，该方案无法满足匿名性、无收据性并且不允许弃权。叶炜等[19]基于原始的FOO投票协议提出了改进，但其方案不满足可验证性和无收据性。2012年，邹秀斌等[20]为了防止计票机构的不诚实而提出了一种基于门限的电子投票方案，该方案要求计票机构的数量大于或者等于 t 个，这样计票的结果才不容易造假，并且公告栏公布的投票结果是哈希值或者是经过加密的结果，这样也防止了选票买卖。大规模的电子投票的系统正处于摸索、实验、开发的阶段，电子投票协议研究的重难点就是电子投票方案的设计，FOO投票协议是目前电子投票方案中比较显著并且实用的电子投票协议。然而，FOO投票协议仍然有一些实际困难难以克服。

本文深入分析并总结了已有的改进FOO投票协议，引入了投票编号、申诉标识等技术，提出了新的改进方案，解决了FOO投票协议存在的几个关键问题：(1)选票碰撞问题；(2)不可弃权问题；(3)匿名性问题；(4)无收据性问题。该方案进一步完善了FOO投票协议，它可以保证选票的匿名性、可验证性和无收据性，并且允许投票者中途弃权。此外，该方案不仅保持了原方案的各种优点，而且增强了系统的安全性和灵活性，因此具有更好的通用性和实用性。

2 预备知识

定义1 对任意的 $u_i, v_i, x_j, y_j \in R$ 且 $i=1,2,3,\cdots; j=1,2,3,\cdots$，运算"$\otimes$"定义为：

$$(x^*, y^*) \stackrel{\triangle}{=} (u_i, v_i) \otimes (x_j, y_j) = (u_i x_j, v_i y_j)$$

2.1 比特承诺

比特承诺又叫做位承诺，是指承诺者 A 向接收者 B 承诺一个或几个消息，但不泄露消息值。在承诺完毕后，承诺者 A 不能改变其承诺的值，并在未来给出这个承诺值的消息。

2.2 安全电子投票的基本要求

一个电子投票协议在安全性上应该满足以下9个方面的基本要求[14,19]。

(1)匿名性：除了投票人以外，其他任何人都不知道投票的内容，也不可能通过投票和选票来确定投票人。

(2)完整性：所有合法有效的投票都应该被正确地统计。

(3)合法性：只有被授权的合法投票人才有投票资格。

(4)准确性：所有投票必须是合法的选票才能被计入选票。

(5)公正性：投票的最终结果不能被任何事情影响。

(6)唯一性：任何投票人有且只有一次合法的投票机会。

(7)可验证性：任何投票者都可以检验自己的投票是否已经被正确计入。

(8)无收据性：任何投票者既不能得到又不能去构造一个证明自己选票的收据，无法向任何人证明自己的选票内容。

(9)弃权性：允许具有投票资格的投票者中途弃权，并且保证投票正常进行。

3 FOO投票协议及其分析

3.1 FOO投票协议

FOO投票协议[8]是一个能较好地实现安全选举的电子投票协议，是目前比较简明实用的电子投票协议。该协议所涉及的核心密码技术主要有比特承诺、数字签名和盲签名技术。该协议所使用的符号和相关信息如表1所列。

表1 FOO协议中相关的符号说明

参与实体	投票者 V_i	管理者 A	计票者 C
公开信息	身份标识 ID_i	公钥(e,n)	公钥(e_c,n)
私有信息	位承诺随机数 k_i，盲化因子 r_i	私钥 d	私钥 d_c

该协议的具体信息流程如图1所示。

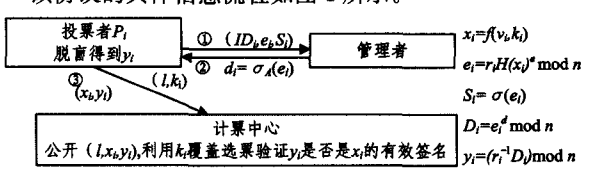

图1 FOO投票协议示意图

(1)投票者准备阶段

(i)投票者 V_i 选择并填写一张选票，选择一个随机数 k_i 作为比特承诺的密钥，并用位承诺方案 f 加密 v_i，即计算 $x_i = f(v_i, k_i)$；

(ii)V_i 再随机选择一个盲化因子 r_i 用来盲化 x_i，即计算 $e_i = r_i H(x_i)^e \bmod n$；

(iii)V_i 对 e_i 进行签名：$S_i = \sigma_i(e_i)$，并且将 (ID_i, e_i, S_i) 发送给投票管理者 A(如图1中的过程①)。

(2)管理者授权证书阶段

(i)如果 V_i 是首次申请证书，则管理者 A 检查 S_i 是否是 V_i 对 e_i 的合法签名，如果是合法签名，则管理者 A 对 e_i 签名：$D_i = e_i^d \bmod n$，并将 D_i 作为投票授权证书颁发给 V_i(如图1中的过程②)。

(3)投票者投票阶段

(i)投票者 V_i 对 D_i 进行脱盲，得到关于 x_i 的签名 y_i：$y_i = (r_i^{-1} D_i) \bmod n$；

(ii)如果签名合法，则投票者 V_i 匿名地将 (x_i, y_i) 发给计

票者 C(如图 1 中的过程③)。

3.2 FOO 投票协议分析

虽然 FOO 投票协议在一定程度上满足了电子投票协议的安全要求,但是深入分析其安全性后发现该协议仍存在如下一些问题。

(1)"选票碰撞"问题[19]

在 FOO 投票协议中,仅仅通过比特承诺密码的算法来区分不同选票者的选票。如果两个投票者的承诺密钥以及选票内容恰好相同,则出现两张完全相同的选票,而计票中心只会记录一张合法的选票,丢弃其中一张。因为比特承诺的密钥选择没有其他要求,所以出现选票碰撞的可能性不可忽略。

(2)弃权问题

在 FOO 投票协议中是不允许投票者弃权的,因为一旦有人弃权,管理者就可以冒充合法的投票者进行投票。该协议是由管理者单独负责投票者的身份验证,计票者只负责计票工作,从而使得有效的选票完全依赖于管理者的签名,如果投票过程中有人弃权,管理者必然知道,就有可能冒充投票者进行非法投票。协议中要求弃权者提交一张空白选票,但是一个投票者如果已经选择了弃权,肯定也不愿意花时间去投空白选票,从而该协议的弃权不容忽视。

(3)匿名性问题

在 FOO 投票协议中,如果公告板公布的投票人数和实际投票人数不相等,这时就需要投票者出示自己的盲化因子以及管理者的盲签名来证明自己的选票是合法的,从而破坏了投票者的匿名性。

(4)可验证性问题

每个投票者都可以根据公告板上公布的信息验证自己的投票是否被正确计入,但是这个可验证性必须是在没有人弃权的情况下才能满足,因此 FOO 投票协议不适合实际应用。

(5)无收据性问题

在 FOO 投票协议中,投票者只要提供自己的盲化因子以及管理者的盲签名就可以表明自己的投票内容,那么投票者就可以向别人提供自己的投票内容,从而导致选票买卖的行为,因此该协议的无收据性所导致的问题不能忽略。

基于对以上问题的分析和讨论,在电子投票的选票碰撞性、匿名性和无收据性上仍然还有很大的改进空间。本文主要是针对电子投票协议的选票碰撞性、投票者的匿名性和投票的无收据性提出相应的改进。

4 改进的 FOO 投票协议

该改进方案共由投票者、管理者及计票者三方共同完成,具体过程共分为 4 个阶段,分别为初始化阶段、注册阶段、投票阶段及计票阶段。

4.1 初始化阶段

A:管理中心;

p_i:第 i 投票者,其中 $i=1,2,\cdots,n$;

T:计票中心;

ID_i:给具有投票资格的第 i 个投票者的投票编号;

IDC_i:唯一的申诉标识,无法通过 ID_i 猜测 IDC_i,投票者的选票没有被正确计入时可提出的申诉标识;

k_i:计票中心用来给第 i 个投票者填写选票的随机数,计票中心随机发送可以避免重复;

$Sig(IDC_i,k_i)$:对 IDC_i 和 k_i 签名,防止在传送过程中被第三方造假,接收方可以用来验证是否由计票中心传送。

管理中心 A 生成 RSA 签名方案,并公布公钥 (e,N),其中 $N=p\times q$,其中 p,q 均为素数。

4.2 注册阶段

该阶段完成投票者的注册登记工作,注册登记由投票人提出申请,由管理中心 A 和计票中心 T 共同完成。具体的信息流程如图 2 所示。

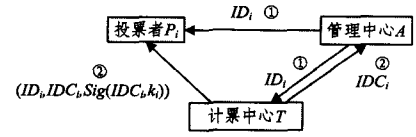

图 2 注册阶段信息流程

(1)管理中心验证申请投票人是否具有投票资格,给具有投票资格的投票人发送 ID_i,并且将 ID_i 发送给计票中心(如图 2 中的过程①)。

(2)计票中心 T 接收 ID_i,发放$(ID_i,IDC_i,Sig(IDC_i,k_i))$给投票者,同时将 IDC_i 发送给管理中心 A,其中 IDC_i 是唯一的申诉标识。

(3)投票者验证 $Sig(IDC_i,k_i)$是否为计票中心的签名,若不是,则可以向仲裁机构提出申诉。

(4)投票者 p_i 选择并填写一张选票,并且利用计票中心发送的 k_i 作为比特承诺的密钥,并用位承诺方案 f 加密 v_i,即计算 $x_i=f(v_i,k_i)$。

(5)p_i 再随机选择一个盲化因子 r_i 来盲化 x_i,即计算$e_i=r_iH(x_i)^e \bmod n$。

(6)p_i 对 e_i 进行签名:$S_i=\sigma_i(e_i)$,并且将(IDC_i,e_i,S_i)发送给投票管理中心 A。

(7)管理中心 A 接收(IDC_i,e_i,S_i),检验以下条件是否满足:

(i)p_i 是合法的投票人;

(ii)p_i 是第一次申请投票证书;

(iii)对 e_i 的签名 S_i 是有效的。

若以上 3 个条件都满足,则管理中心 A 对 e_i 签名:$d_i=\sigma_A(e_i)$,将 d_i 作为管理者颁发给投票者 p_i 的投票验证签名。

(8)注册阶段结束以后,A 宣布已获得签名的投票者的总数,并公布(IDC_i,e_i,S_i)列表。

该部分具体的信息流程如图 3 所示。

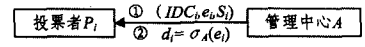

图 3 注册阶段信息流程

4.3 投票阶段

投票者 p_i 接收到计票中心发送的消息$(ID_i,IDC_i,Sig(IDC_i,k_i))$,$d_i=\sigma_A(e_i)$,进行如下操作:

(1)投票人 p_i 进行盲逆变换:$y_i=\dfrac{d_i}{r_i} \bmod n$。

(2)p_i 检查 y_i 是否是 A 对 x_i 的合法签名,如果不是,则 p_i 向 A 证明(x_i,y_i)的不合法性并重新投票。

(3)p_i 通过匿名信道将$(ID_i,IDC_i,Sig(IDC_i,k_i),x_i,y_i)$发送给计票机构。

(4)计票机构检查 y_i 是否是 A 对 x_i 的合法签名,若验证成功,则计票机构将(ID_i,x_i^*,y_i^*)加入到列表中,$(x_i^*,y_i^*)=$

$(u,v)\otimes(x_i,y_i)$，同时将(u,v)发送给投票者。

该阶段具体的信息流程如图4所示。

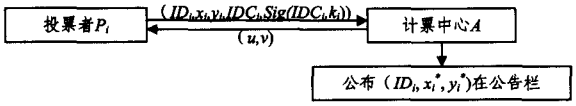

图4 投票阶段信息流程

4.4 计票阶段

(1)投票者p_i检查投票者的数量是否等于选票的数量。

(2)投票者检查自己的选票是否在列表中。若不存在，则公开$(IDC_i,Sig(IDC_i,k_i))$，即有效的唯一申诉标识和签名，要求将相应的选票内容加入到列表中。

(3)计票中心用k_i打开x_i获得v_i，将v_i添加到列表中检查其是否是合法选票。

(4)计票中心将收到的$(ID_i,IDC_i,Sig(IDC_i,k_i),x_i,y_i)$与之前保留的消息$(ID_i,IDC_i,Sig(IDC_i,k_i))$进行比对，将未收到的$(ID_i,IDC_i,Sig(IDC_i,k_i))$视为弃权票。

(5)计票机构统计选票并宣布投票结果。

5 安全性分析

电子投票协议需要满足完整性、合法性、唯一性、公平性、准确性、匿名性、弃权性、可验证性、无收据性等基本要求。本协议采用了盲签名、投票编号等技术，目的就是要保证该协议能够较好地满足这些要求。下面就这几个方面对本协议的安全性进行详细分析。

(1)完整性

通过设置唯一的投票编号，每个人都可以在计票机构的公告板上跟踪自己的选票是否已经被计票机构正确统计，而且通过双向验证，确保了所有的选票都可以得到正确的统计，选举的结果是真实、可靠的。

(2)合法性

与原始FOO投票协议类似，新协议充分利用了数字签名防伪造的特性，任何非法人员都无法冒充合法投票人来获得授权中心的授权。因此协议满足合法性的要求。

(3)唯一性

在新协议中，投票者在投票之前，首先要通过管理中心资格审查，获得一个唯一的身份标识ID_i和一个唯一的申诉标识IDC_i，计票中心一旦发现投票者的ID_i和IDC_i重复，则将其视为弃票。

(4)公正性

本协议将投票阶段和统计阶段分开进行，并且管理中心和计票中心的相互牵制，有效防止了投票结果的提前泄露。因此，本协议满足投票的公正性。

(5)准确性

因为在原始FOO投票协议中，随机数r_i是由投票者自己产生并且发送给计票中心的，可能会产生选票碰撞。在改进的协议中，r_i由计票中心产生，这使得位承诺的密钥由计票中心发送，就不会造成重复，可以避免选票碰撞。

(6)匿名性

在原始FOO投票协议中，当投票者的票没有被正确计入时，投票者需要出示盲化因子r_i，会造成投票者身份的暴露。而本协议中，只需要出示IDC_i(唯一的申诉标识)，IDC_i和ID_i没有必然的关系，不会暴露投票者的身份。

(7)弃权性

本协议允许投票人弃权，计票中心将收到的$(ID_i,IDC_i,Sig(IDC_i,k_i))$与计票中心保留的信息比对，发现有些$(ID_i,IDC_i,Sig(IDC_i,k_i))$没有返回，则将$ID_i$投的票视为弃权票，并且会公布出来。因为返回的信息中有$Sig(IDC_i,k_i)$，签名具有不可伪造性，所以能将弃权的票正确统计出来。

(8)可验证性

在本协议中，每个投票人都可以跟踪自己的选票是否已被统计。计票中心会发送可验证的有序数对(u,v)给投票人，公告栏上将公布信息(ID_i,x_i^*,y_i^*)，当$(x_i^*,y_i^*)=(u,v)\otimes(x_i,y_i)$成立时，则投票人的票被正确计入；否则，投票人可以公布自己的$(IDC_i,Sig(IDC_i,k_i))$，要求计票中心将自己投的票正确计入。

(9)无收据性

根据定义1的运算，记$(x^*,y^*)=(u_i,v_i)\otimes(x_j,y_j)=(u_ix_j,v_iy_j)$，则根据投票协议的结构容易得到如下两个方程：

$$(x^*,y^*)=(u_1,v_1)\otimes(x_1,y_1)=(u_1x_1,v_1y_1)$$

$$(x^*,y^*)=(u_2,v_2)\otimes(x_2,y_2)=(u_2x_2,v_2y_2)$$

即有$(u_1x_1,v_1y_1)=(u_2x_2,v_2y_2)$。

当投票人想要买卖选票时，提供ID_i和(u,v)给买票人验证所需的信息，虽然$(x^*,y^*)=(u_1,v_1)(x_1,y_1)$符合买票人的要求，但大家都知道，$(u_1,v_1)$可以造假成$(u_2,v_2)$，$(x^*,y^*)=(u_2,v_2)(x_2,y_2)$也成立，即另一组有序数对$(u_2,v_2)$对同一个候选人也成立，买票人无法相信投票人，则无法达成买卖，所以符合无收据性。

6 性能分析和量化分析

6.1 性能分析

通过与原始的FOO投票协议[12]、陈晓洪的基于安全多方计算的投票方案[18]、叶炜和吕锋的改进FOO投票协议的方案[19]、郭玲玲和李忠献的基于群盲签名的无收据投票方案[17]进行比较(见表2)，表明本协议基本解决了电子选举存在的安全性问题。

表2 性能分析

	FOO协议	文献[18]	文献[19]	文献[17]	新方案
完整性	√	√	√	√	√
匿名性	×	×	√	√	√
准确性	√	√	√	√	√
唯一性	√	√	√	√	√
合法性	√	√	√	√	√
公正性	√	√	√	√	√
可验证性	√	√	×	×	√
无收据性	×	×	×	√	√
弃权性	×	×	√	×	√

从上述性能分析表可知，文献[12,17-19]中的每个方案都不能同时满足一个安全的电子投票的9个基本要求：原始的FOO投票协议[12]不能满足匿名性、无收据性并且不允许弃权；陈晓洪的基于安全多方计算的电子投票方案[18]不满足匿名性、无收据性和弃权性；叶炜等人的FOO投票协议及其改进方案[19]满足弃权性，但不满足可验证性和无收据性；郭玲玲等人的基于群盲签名的无收据电子投票方案[17]满足无收据性，但却不满足可验证性和弃权性。本协议能够弥补其他协议的不足，同时满足2.2节中所提的所有基本要求。

6.2 新协议的量化分析

本节将新协议的运算量与FOO协议以及其他3个相关协议的运算量进行比较。表3的运算次数是指各代理机构处理一个投票者的相关信息的运算量。

表3 量化分析(单位:次)

协议 \ 运算	投票者RSA加密	投票者RSA签名	注册机构RSA签名	签证机构RSA盲签名	投票者盲化计算	投票者散列计算	计票中心RSA签名
FOO协议	3	1	0	1	1	1	0
文献[17]	3	1	1	1	1	0	0
文献[18]	3	1	2	1	1	1	0
文献[19]	3	1	1	1	1	3	0
新方案	3	1	0	1	1	1	1

从表3中可看出,与原始的FOO电子投票协议比较,文献[17]没有投票者的散列计算,减轻了投票者的工作量,增加了1次注册机构的签名;文献[18]使注册机构的签名次数增加到2次;文献[19]增加了2次投票者的散列计算,这个计算对投票者很容易,而增加1次注册机构的签名增加了投票者的等候时间。以上这些协议都没有达到很好的安全性。为了满足预期的安全性,新协议的运算量稍有增加。增加的运算量只是1次计票中心的签名,对于投票者来说,只是增加计票中心的RSA签名,并不需要投票者增加任何操作,只需增加一点投票者的等待时间。通过比较,新方案所增加的总计算量并不大,且能满足投票协议的安全性。

结束语 本文分析了FOO投票协议存在的问题及漏洞,提出了一种新的无收据性的电子投票方案,保留了原有的FOO投票协议的基本框架,引入了投票编号和申诉标识等工具,建立了一个可以避免选票碰撞且满足匿名性、弃权性和无收据性等的电子投票方案。此外,本方案满足无收据性,即能有效地预防选票的买卖。但方案仅满足个人可验证,无法满足普遍可验证性,并且在信息的传输过程中,信息量太大。因此,设计安全的普遍可验证且高效的改进FOO投票协议将是一个有意义的研究内容。

参 考 文 献

[1] Chaum D. Untraceable electronic mail, return addresses, and digital pseudonyms[J]. Communications of the ACM, 1981, 24(2): 84-88

[2] Cohen J, Fisher M. A robust and verifiable cryptographically security election scheme[C]// Proceedings of the 26th ACM Symposium on Foundations of Computer Science. 1985: 372-382

[3] Benaloh J, Tuinstra D. Receipt-free secret-ballot elections (extended abstract)[C]// Proceedings of the 26th ACM Symposium on Theory of Computing. 1994: 544-553

[4] Iversen K R. A cryptographic scheme for computerized general elections[M]// Advances in Cryptology-CRYPTO'91. Spinger, 1992: 405-419

[5] Sako K, Kilian J. Secure voting using patially compatiable homomorphisms[M]// Advances in Cryptology-CRYPTO'94. Springer, 1994: 405-419

[6] Essex A, Hengartner U. Hover: Trustworthy elections with hash-only verification[J]. IEEE Security & Privacy, 2012, 10(5): 18-24

[7] Chen X, Wu Q, Zhang F. New receipt-free voting scheme using double-trapdoor commitment[J]. Information Sciences, 2011, 181(8): 1493-1502

[8] Rui J, Paulo F, Carlos R. EVIV: An end-to-end verifiable internet voting system[J]. Computers & Security, 2013, 32(2): 170-191

[9] Li C, Hwang M, Liu C. An electronic voting protocol with deniable authentication for mobile ad hoc networks[J]. Computer Communications, 2008, 31(10): 2534-2540

[10] Francesc S, Josep M M, Jordi P, et al. Simple and efficient hash-based verifiable mixing for remote electronic voting[J]. Computer Communications, 2010, 33(6): 667-675

[11] Chung Y, Wu Z. Casting ballots over internet connection against bribery and coercion[J]. Computer Journal, 2012, 55(10): 1169-1179

[12] Fujioka A, Okamoto T, Ohta K. A practical secret voting scheme for large scale elections[M]// Advances in Cryptology-AUSCRYPT'92. Springer, 1993: 615-619

[13] 谢金宝,刘晖波. 电子选举系统的基本框架与信息流程[J]. 计算机工程,2000(S1):97-102
Xie Jin-bao, Liu Hui-bo. A Basic Frame and Information Flow of Electronic Vole Model[J]. Computer Enginering, 2000(S1): 97-102

[14] 陈晓峰,王继林,王育民. 基于半信任模型的无收据的电子投票[J]. 计算机学报,2003,26(5):557-662
Chen Xiao-feng, Wang Ji-lin, Wang Yu-min. Receipt-Free Electronic Voting Based on Semi-Trusted Model[J]. Journal of Computers, 2003, 26(5): 557-662

[15] 范安东,孙琦,张杨松. 基于环签名的匿名电子投票方案[J]. 四川大学学报(工程科学版),2008,40(1):113-117
Fan An-dong, Sun Qi, Zhang Yang-song. The Scheme and Implementation of Anonymous Electronic Voting Based on Ring Signature[J]. Journal of Sichuan University (Engineering Science Edition), 2008, 40(1): 113-117

[16] 夏静波,张四兰,陈建华. 一个无收据的高效电子选举方案[J]. 武汉大学学报(理学版),2006,52(3):340-344
Xia Jing-bo, Zhang Si-lan, Chen Jian-hua. A Receipt Free Electronic Voting Scheme[J]. Journal of Wuhan University (Natural Science Edition), 2006, 52(3): 340-344

[17] 郭玲玲,谷利泽,李忠献. 基于群盲签名的无收据电子投票方案[C]//2009年中国高校通信类院系学术研讨会论文集. 2009
Guo Ling-ling, Gu Li-ze, Li Zhong-xian. The Scheme of non-receipt Electronic Voting Based on Group and Blind Signature[C]// Proceedings of Academic Conference on Communications in China Colleges and Universities. 2009

[18] 陈晓洪. 基于安全多方计算的电子投票系统应用研究[D]. 南京:南京理工大学,2010
Chen Xiao-hong. The Stability of A New Lü Chaotic System with A Sort of Parameters[D]. Nanjing: Nanjing University of Science and Technology, 2010

[19] 叶炜,吕锋. FOO协议及其在电子投票系统中的改进[D]. 武汉:武汉理工大学,2009
Ye Wei, Lv Feng. The Improvement of the FOO Protocol and Its Application in Electronic Voting System[D]. Wuhan: Wuhan University of Technology, 2009

[20] 邹秀斌,崔永泉,付才. 一种基于门限的电子投票方案[J]. 计算机科学,2012,39(7):39-43
Zou Xiu-bin, Cui Yong-quan, Fu Cai. Threshold-based Electronic Voting Scheme[J]. Computer Science, 2012, 39(7): 39-43