文章编号:0253-2328(2014)04-0336-03

基于盲签名的高效电子投票方案

李欣妍[1], 牟化建[2], 张韶华[1]
(1. 长江师范学院 数学与统计学院,重庆 408100; 2. 长江师范学院 计算机工程学院,重庆 408100)

摘 要:针对已有文献设计方案的不足,结合椭圆曲线密码体制和盲签名,提出了改进的电子投票方案,并对其安全性进行分析. 本方案采用椭圆曲线密码加密算法和盲签名等技术,防止抵赖、伪造、篡改,保护投票人的合法权益,具有更强的抗攻击性和实用性,满足理想的电子投票方案所具有的特征.

关键词:盲签名;椭圆曲线密码体制;电子投票;完整性;秘密性
分类号:(中图)TP309.7 文献标志码:A

电子投票是密码学的一个重要应用分支,它以密码学为理论基础,通过网络和计算机完成整个投票过程. 早在 1981 年 Chaum 提出了基于公钥密码算法的电子邮件定义,它同样也是电子选票的雏形[1];1994 年,Benaloh 提出了电子投票的无收据性(receipt-free)[2]. 1996 年 L. F. Cranor 等给出了电子投票需满足的 7 个性质[3],即:准确性(accuracy)、民主性(democracy)、秘密性(privacy)、可验证性(verifiablity)、方便性(convenience)、灵活性(flexibility)以及移动性(mobility). 随着网络技术以及密码技术的发展,越来越多的学者开始关注这个领域,随后苑浩等开始对电子投票系统研究,实现了电子投票的可验证性和预加密性,并对预加密方案存在的问题进行严格分析和验证[4];李凤银等实现了电子投票的无证书签名方案和无收据性[5];仲红、黄刘生、罗文龙在安全多方求和的基础上,研究出一个多选多的方案(简称仲-黄方案),他们认为这个方案保证了保密性、无收据性、健壮性、无争议性及高效性. 通过在此基础上的研究,孙培勇等发现该方案并不满足完全保密性,他们提出了基于多候选人的电子投票方案等[6]. 电子选举的不断发展不但体现在其需要满足的性质上,其形式也在不断变化,从起初的多选一到后来的多选多电子投票都有很多协议和草案. 陈晓洪提出了基于安全多方计算的电子投票系统应用研究[7],但由于电子投票处理的局限性,必须提出安全的电子投票协议,即如果计数之前投票被任意地修改,那么这个投票就是无效的. 由此可以看出电子投票一致协议的重要性.

虽然电子投票具有方便快捷的特点,但许多投票方式也存在技术缺陷,主要是在软件方面,这些缺陷有可能使得投票人反复投票、篡改. 针对这些问题,笔者参考诸多文献,并在文献[8—10]的基础上,结合椭圆曲线密码体制和盲签名,设计了防止重复投票、保护投票者信息和投票内容的方案.

1 椭圆曲线密码体制[1—2]

椭圆曲线密码体制既可以在有理数域、实数域和复数域上定义,还可以定义在有限域上,目前使用比较多的是定义在 p 为素数的有限域和特征为 2 的有限域 $F_{2^m}(m\geqslant 1)$ 上. 该种密码体制的加密原理源于有限域上椭圆曲线离散对数问题(ECDLP)的困难性. 下面以其特征域上的椭圆曲线为例,说明椭圆曲线密码算法的加密原理.

设 $GF(p)$ 为一个 $p\neq 2,3$ 的有限域,在 $GF(p)$ 上定义的椭圆曲线是满足 Eierstrass 方程的点,即

$$y^2+a_1xy+a_3y=x^3+a_2x^2+a_4x+a_6,$$
$$a,b\in GF(p),$$

及 $4a+27b\neq 0$ 的所有整数点 $(x,y)\in GF(p)*GF(p)$ 和无穷远点 0. 假设 P 为椭圆曲线上的任一点,则相应的离散对数问题如下:

给定 $P\in E_{(a,b)}(GF(p))$,求整数 x $(x\in GF(p))$,使得 $xP=Q$. 若这样的对数存在,就称为椭圆曲线离散对数问题,然而要从 Q 点和 P 点中求解出 x,是极其

收稿日期:2013-09-17
基金项目:重庆市教委科学技术研究项目(KJ121316);校级科研项目
作者简介:李欣妍(1981—),女,讲师,硕士,主要从事代数组合与密码学.

困难的.

设从区间$[1,n-1]$任意地选取一整数d,计算$Q=dP$,那么密钥对为(d,Q),其中:d为其私钥;Q为其公钥.

2　高效的电子投票方案工作流程

本方案选择的安全椭圆曲线系统参数为(F_q,E,P,n),其中,包括以下参与者:

1)投票者(voter)U_j,作为群成员参加投票活动;

2)注册机构(registration authority)R,负责整个系统的初始化工作,将合法投票者吸收为群成员,并公布已注册投票者的公钥;

3)验票计票中心(ticket and counting center)C,检验选票的合法性,并用投票者发来的签名打开最终选票,统计计票结果;

4)验票员(ticket inspector),对投票者所投选票进行检验,统计验票结果并公布在公告板BB(bulletin board)上.

详细投票过程如下:

2.1　系统初始化

计票中心为C,投票者为U_j,$j=1,2,\cdots,m$,密钥分别为k_C,k_j,公钥分别为$K_C=k_C\cdot P \bmod n$,$K_j=k_j\cdot P \bmod n$. 注册机构R在布告牌BB上公布参数(F_q,E,P,n)及所有参与者的公钥$K_1,K_2\cdots,K_n$.

2.2　注册阶段

1)投票者U_j随机选取一个整数$f_j,f_j\in[1,n-1]$,计算$F_j=f_j\cdot P \bmod n$,并将(F_j,ID_j)传送给注册机构R,其中ID_j为投票者U_j的身份信息.

2)注册机构R收到F_j,随机选取一个整数b_j,将b_j传送给U_j.

3)投票者U_j收到b_j后,计算$u_j=f_j+b_j\cdot k_j \bmod n$,将$u_j$传送给注册机构$R$.

4)注册机构R收到u_j,计算等式$u_jP=F_j+b_jK_j$是否成立,并对照投票者的身份信息ID_j. 若上述等式成立,并且无重复身份信息,表明对方为合法投票者,则系统产生一个注册号,注册号为随机数x_j,并将x_j传给投票者U_j.

2.3　投票阶段

U_j收到注册号x_j后,计算$X_j=(K_Ck_j) \bmod n$及$M=(X_jm) \bmod n$,其中,m为自己的投票信息;其次,利用现有的参数b_j,f_j,K_j,计算$Y_j=(b_j\cdot K_j+f_j\cdot X_j) \bmod n$,在$[1,n-1]$内任意选取$k$,计算$V=k_j^{-1}(k-W) \bmod n$及$W=(f_jM-Y_j\cdot K_C) \bmod n$;最后,$U_j$将$((W,V,K),M)$和自己的身份及注册号$(x_j,ID_j)$传送给验票中心$C$.

2.4　验票阶段

验票中心C接收到$((W,V,K),M)$,根据(x_j,ID_j)计算出公钥. 若此公钥不存在于公告牌上,则此票无效,并向用户发出需要重复投票的反馈信息;若存在,则通过密钥交换协议,计算出解票因子

$$X_j=(K_C\cdot k_j) \bmod n=(k_C\cdot K_j) \bmod n,$$

并验证等式$K=VK_j+PW$是否成立. 若成立,则说明投票成功,用解票因子X_j计算出原投票消息

$$m=(X_j^{-1}\cdot M) \bmod n,$$

并将m和ID_j计入数据库中,此过程可随时公布选票结果;若等式$K=VK_j+PW$不成立,则说明此票为无效票. 验证过程如下:

$$\begin{aligned}VK_j+PW&=[k_j^{-1}(k-W)K_j+(f_jM-Y_j\cdot K_C)\cdot P] \bmod n=\\&[k_j^{-1}k_j(k-W)P+(f_jM-Y_j\cdot K_C)P] \bmod n=\\&(k-W+f_jM-Y_j\cdot K_C)P \bmod n=\\&(k-f_jM+Y_j\cdot K_C+f_jM-Y_j\cdot K_C)P \bmod n=\\&kP \bmod n=K.\end{aligned}$$

本步骤在传输过程中利用盲签名的特性,隐藏和保护投票者的个人隐私,同时在检验选票时起到了身份认证的作用,有效地防止投票者抵赖投票信息,并防止攻击者的信息伪造和篡改.

2.5　计数投票结果阶段

当验票中心C检查投票无误时,统计投票结果,并将投票结果公布于公告板BB.

3　安全性分析

1)本方案的整体安全性取决于算法的复杂度. RSA算法的安全性[1−2]由大素数和椭圆曲线两部分构成. 其中:大素数分解的复杂度与离散对数问题相当;椭圆曲线的复杂度,取决于在其曲线上选择的点的个数. 这两者的组合叠加,又使得解决这个问题的难度系数加大. 现阶段的研究表明,其在性能上是值得信赖的,比大数分解及素数上的离散对数体制的难度系数更大. 一般认为,其复杂度处于全指数规模. 在域$GF(2^{160})$上设计的椭圆曲线密码体制,其安全性能完全可以达到1 024位模数的RSA体制的安全标准.

2)在本方案中,由于投票内容m在签名的同时进行了加密,攻击方式无法接触到投票内容. 加密算法的安全性能与投票方的密钥、方案所选择的大整数及签名概率等,都有密切的联系.

3)对于截获性攻击方式的攻击,可以从以下的方面加以分析.截获过程根据以下两式:

$F_j = f_j \cdot P \bmod n$, $K = k \cdot P \bmod n$,

求出 f_j 和 k,再根据 f_j 和 k 来伪造票据.这两个参数的求解,也就是对椭圆曲线体制的求解过程,因而其安全性规模与体制是一致的.

4)对于伪造方式的攻击,若其伪造的选票为 $((W_0,V_0),M)$,此选票在验票中心将无法获得通过,会得到要求重新投票的提示,直到通过为止.因此,本方案对于伪造攻击是足够安全的.

5)由于 (x_j,ID_j) 对每个选举者是唯一的,验票中心将对收到的选票检验所含注册号是否已经投票,若已存在此注册号,则选票无效.因此,本方案可以有效防止重复投票的行为.

6)验票中心对众多公开参数的攻击,如 b_j, f_j, K_j 等,也具有足够的安全性.例如 b_j, f_j 为由投票者随机产生的大整数,而这些攻击对于验证中心来说是无效的,同时也意味着穷举法对体制是无效的.

7)就投票因子来说,本方案也是安全的.由 $X_j = (K_C \cdot k_j) \bmod n = (k_C \cdot K_j) \bmod n$ 可以看出,只有投票者本人和验票中心才有自己的密钥和对方的公钥,而其他人是不能使用此投票因子的.

4 投票方案的性质

1)秘密性.对于投票选举来说,选票的内容具有很高的秘密性.在本方案中,$M = (X_j \cdot m) \bmod n$,其中:$m$ 为选举的内容;M 为将选举的内容进行加密的数据.由此式可知,在投票的过程中,选票内容是秘密而不被别人所知的.

2)匿名性.投票选举一般为无记名投票.此特征在本方案中可以得到足够的保证.在选票 $((W,V),M)$ 中,所有投票站的信息都会被清除.因此,选票在投出后,就不再与选举者有任何关系,这也就保证了选举过程的匿名性.

3)唯一性.选举过程中,每个合法的选举人,只能提交一张选票.因此,一人多投在方案中得到防止.在验票中心,每个投票者在公告牌上的公钥信息是唯一的.对于 (x_jID_j),仅有公告牌上有公钥的投票者与自己的密钥进行交换,才可以得到解票因子.非法的投票者无法得到正确的解票因子.此方法保证了投票的唯一性.

4)完整性.在本方案中,凡是合法的选票,通过验票中心,都会被正确装入选举数据库中,保证了所有选票的完整性.

5)稳定性.本方案对各种恶意攻击,及各种投票过程中的不诚信行为,具有很强的防御能力,可以稳定运行,确保得到正确的选举结果.

6)可验证性.对于选举得到的结果,可以在以后任意时间,被重新检验.这也确保了选举结果不会被伪造.

对参考文献[8—10]中的方案及本方案进行各种性能测试和对比分析(表1).由表1可以看出,本方案是一个合理的电子投票方案.

表1 文献[8—10]中的方案和本文方案的性能测试与比较

文献	匿名性	可验证	防止重复票	是否具有算法	可恢复性
文献[8]	是	是	否	否	是
文献[9]	是	是	是	否	否
文献[10]	是	是	是	是	否
本方案	是	是	是	是	是

5 结语

本文利用椭圆曲线密码体制的密钥短、所占空间小、加解密速度快等优点,以盲签名为理论基础,比较和研究了众多文献后提出改进的电子投票方案.此电子投票系统对外界和验证中心来说具有身份认证、加密效果、可验证、防止重复票、可恢复性等性能.电子投票是电子商务的一个重要应用,虽然许多研究者对加密技术、身份认证技术及签名技术进行研究以确保投票系统满足所有性质,但将合理的方案实现于软件还待进一步研究.

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] BENALOH J, TUINSTRA D. Receipt-Free ballot elections[C]//Proceedings of the 26th Annual ACM Symposium on Theroy of Computing (STOC'94), Montreal ACM, 1994: 544-553.

[3] CRANOR L F, CYTRON R K. Design and implementation of a practical security-conscious electronic polling system [R]. Washington: Washington University, 1996.

[4] 苑浩,杨宝霖.一种改进的预加密可验证电子投票方案[J].计算机应用研究,2012,29(8):3048-3052.

[5] 李凤银,刘培玉,朱振方.高效的无证书签名方案[J].计算机工程与应用,2011,47(10):23-26

(下转第351页)

molecule library of 3rd generation multidrug resistance modulators[J]. Bioorganic & Medicinal Chemistry, 2009,17(6):2524-2535.

[6] 纪彩虹. 一类抗疟化合物的定量构效关系研究[J]. 甘肃联合大学学报:自然科学版,2010,24(4):47-49.

[7] 赵春燕. QSAR 研究在生命分析化学和环境化学中的应用[D]. 兰州:兰州大学,2006.

[8] LUAN Feng, XU Xuan, LIU Huitao, et al. QSAR Studies of PTP1B Inhibitors: 1, 2-Naphthoquinone Derivatives[J]. Letters in Drug Design & Discovery, 2012,9(10):915-925.

[9] LÜ Weijuan, CHEN Yonglei, CHEN Hongli, et al. Optimization of the micellar electrokinetic capillary chromatographic determination of dauricine and daurisoline in *Rhizoma Menispermi* and its herbal medicine using experimental design and radial basis function neural network [J]. Journal of Analytical Chemistry,2013,68(6):525-531.

[10] LUAN Feng, XU Xuan, LIU Huitao, et al. QSAR modeling for the antimalarial activity of 1, 4-naphthoquinonyl derivatives as potential antimalarial agents[J]. Current Computer-Aided Drug Design, 2013,9(1):95-107.

Research on Quantitative Structure-activity Relationship (QSAR) of XR Multi-resistant Modifier

Ji Caihong[1], *Zhan Huiying*[2]

(1. Department of Journal, Lanzhou University of Arts and Science, Lanzhou 730010, China;
2. School of Chemistry Engineering, Lanzhou University of Arts and science, Lanzhou 730000, China)

Abstract: 40 XR type compounds structure and active linear models in calcein AM analysis were built through heuristic method. The predicted model coefficient of determination is $R^2=0.882\ 7$. The nonlinear model was built through the method of radial basis function neural network (RBFNN), and the predicted model coefficient of determination is $R^2=0.927\ 6$. Comparing these two methods, the predicted outcome of RBFNN model is more precise and more suitable for building the Quantitative structure-activity relationship research model.

Key words: multi-resistant modifier; HM; RBFNN; QSAR

(责任编辑、校对　高继红)

(上接第 338 页)

[6] 孙培勇,刘忆宁,延吉红,等. 一种安全的多候选人电子投票方案[J]. 计算机工程与应用,2012,48(25):217-228.

[7] 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.

[8] 黄宏升,仲红,燕飞飞,等. 一种抗强制的电子投票方案[J]. 计算机应用,2009,29(6):1725-1727.

[9] 丛清日,胡金初. 基于椭圆曲线盲数字前面的电子选举[J]. 计算机工程,2010,36(13):156-158.

[10] 宋程远,张串绒,曹帅. 一种盲签名方案及其在电子投票协议中的应用[J]. 计算机工程,2012,30(6):139-144.

Effective Electronic Voting Based on Blind Signature

Li Xinyan[1], *Mou Huajian*[2], *Zhang Shaohua*[3]

(1. College of mathematics and statistics, Yangtze Normal University, Chongqing 408100, China;
2. College of Computer Engineering, Yangtze Normal University, Chongqing 408100, China)

Abstract: In the light of the part problems in literatures, an improved electronic voting scheme is put forward in the paper by combining elliptic curve crypto system and blind signature, and its security is analyzed. The results show that the program can prevent repudiation, forgery, tamper, and protect the legitimate rights and interests of the voters. It also has stronger robustness and practicality, which can meet the characteristics of an ideal electronic voting scheme.

Key words: blind signature; elliptic curve cryptosystem; electronic voting; integrity; confidentiality

(责任编辑、校对　张　刚)