基于椭圆曲线上的电子投票方案

吴鸿华　陈一宏
(北京理工大学理学院,北京 100081)
E-mail:wuhonghuadlx@sina.com

摘　要　本文基于数字签名和盲签名技术提出了一种新的电子投票方案。安全性建立在椭圆曲线离散对数(ECDLP)难题之上,方案满足电子投票的特点并且具有灵活性和通用性特点。

关键词　电子投票　椭圆曲线　椭圆曲线离散对数　数字签名　盲签名

A Electronic Voting System Based on Elliptic Curve

Wu Honghua　Chen Yihong
(Beijing Institute of Technology,Beijing 100081)

Abstract: This paper proposes a new electronic voting system based on the technology of digital signature and blind signature.The security of system relies on the problem of elliptic curve discrete logarithm(ECDLP).The system has trait of electronic voting and the characteristic of flexibility and accessibility.

Keywords: electronic voting,elliptic curve,elliptic curve discrete logorithm,digital signature,blind signature

1　概述

电子投票是人工投票的电子模拟,是现代密码学研究的重要领域。与人工投票相比,可以节省大量的人力物力,可以随时随地举行。这样选举委员会就免去了选择场地的困扰与选票的分发、收集的辛苦,选举者也免去了跑去特设投票点投票的麻烦。1981 年 chaun 基于公钥密码体制上建立起第一个真正意义上的电子投票方案,用户可以对自己的身份进行隐藏但是无法对用户的身份进行追踪。自此之后,人们对电子投票进行了大量的研究。Fujioka,Okatoma,Ohta 在 1992 年提出了一个简明实用的电子投票方案。但这种方案对用户的操作的步骤要求很严格,一旦破坏了操作的顺序,方案的安全性很难保证。Iverson 基于零知识建立电子投票方案,方案中几乎每一步都用到零知识验证,这使得方案运行的计算量增大,效率降低。最近,Sako 提出了两个可以防止监管委员会和选票收集者对选票进行改动且可以保证无记名性的电子投票方案,然而这两个方案均不保证公正性成立。也就是说,监管委员会和选票收集者可能会将投票的中间结果泄露给还未投票的人,从而使得各投票人不是在相互平等的位置上参与投票,投票的结果在一定程度受到影响。比较有代表性的还有 Sako,Kilian 基于零知识的多投票中心方案和 Niem,Renvall 多投票中心方案。前不久 Cranor 等人又设计并实现了一个适用于 Internet 投票 Sensus 协议。电子投票以各种密码技术为基础,对电子投票的研究同时促进了密码学领域的进展。

下面简要说明一下文章的内容,第一部分介绍了有代表性的电子投票以及存在的缺陷。第二部分介绍了电子投票知识。第三部分介绍基于椭圆曲线上的电子投票方案,方案主要利用数字签名和盲签名技术。第四部分主要是对所提出方案的分析。最后是文章的综述。

2　电子投票

电子投票作为人工投票的一种电子模拟,和人工投票一样应具有下面的特点:

(1)投票的完整性。所有的选票都能够被正确统计,放弃的投票者应及时公布。

(2)投票的可控性。投票是在监管委员会的控制下进行的,没有经过监管委员会的授权将没有资格参加投票。

(3)投票的不可重复性。为了保证每个合法投票人的利益,每个合法的用户仅且只能投一次票。即使用户进行二次投票,其投票结果也不能被统计。

(4)选票的保密性。选票内容对于选票收集者以外的人是保密的,他们无法进行复制、恢复、伪造合法用户的投票内容。同时选票的内容无法与选票者联系起来。

(5)选票的可验证性。任何合法的用户可以验证自己的选票是否被统计。

对于适用的电子投票方案还要求方案的灵活性,通用性(选票的形式没有要求),本文介绍的方案不仅具有上述的五个特点而且还具有很好的灵活性,通用性。方案经过修改后可适用于大型的 Internet 选举,也可以经过修改后适用于小的局域网选举,对于局域网的选举方案会更加快速高效。在方案中没有对选票性的独特要求,只要是建立一个选票内容与椭圆曲线上的对应或者是直接嵌入(比较容易时)。图 1 是本方案的流程图,具体方案描述请看下一部分内容。

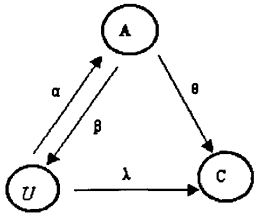

图 1

作者简介:吴鸿华,男,硕士研究生,研究方向:椭圆曲线数字签名及应用。陈一宏,北京理工大学理学院教授。

图 1 中 α 表示(ID_i,Q_1,Q_2),β 表示$(Q'_A,Q'',Q''',r,s's'')$,θ 表示 $h(ID_i)$,λ 表示(l,Q'_u,Q'',Q,r,s)。

3 方案描述

3.1 系统初始化

系统的公共参数:有限域 F_q,q 为素数,E(a,b)为定义在 F_q 上安全的椭圆曲线,|E(F_q)|=n,(|表示阶数)。设 G 为椭圆曲线上的一个基点且有|G|=p,p 要求满足 $p>2^{160}$。投票用户 U_i,(i=1,2…)的身份标识为 ID_i(i=1,2…)。h()为安全的哈希函数。()$_x$ 表示点的横坐标。

系统用户:监管委员会 A,选票收集者 C,投票用户 U_i,(i=1,2…)。

3.2 公私钥的生成

监管委员会 A 随机选择 $d_A\in[1,p-1]$作为私钥,计算 $Q_A=d_AG$ 作为公钥。

选票收集者C随机选择 $d_C\in[1,p-1]$作为私钥,计算 $Q_C=d_CG$ 作为公钥。

投票用户 U_i 随机选择 k∈[1,p-1], 计算 $Q'=kG$ 并发送给监管委员会 A。A 随机选择数 a∈[1,p-1] 计算 $Q''=Q'+aG=(x,y)$。r'=x mod n,$s''=a+r'd_A$。A 将(Q'',s'')发送给用户 U_i。U_i 计算 $d_i=s''+k$ 作为自己的私钥,U_i 的公钥为:$Q_i=d_iG=(s''+k)G=(a+k+r'd_AG)=Q''+(Q'')_x \bmod nQ_A$。用户 U_i 的公私钥的生成可以在投票前也可以在投票过程中生成。方案中将用户 U_i 的公私钥的生成放在投票过程中。

3.3 用户投票

(1)首先将选票内容 b 对应于椭圆曲线上的点 P_b(可以建立选票内容与椭圆曲线点的一个一一对应,当选票内容不多时也可以直接嵌入到椭圆曲线上,所以此步在方案运行时计算量可以忽略不计),用户 U_i 随机选择 $k_1,k_2,t\in[1,p-1]$,计算:$Q_1=k_1G$,$Q_1=tP_b+k_2G$,U_i 将(ID_i,Q_1,Q_2)发送给监管委员会 A。

(2)监管委员会首先通过 U_i 的身份标识 ID_i 审查用户 U_i 是否有资格投票。如果没有协议则终止。如果通过审查,将 ID_i 存入数据库,然后随机选择 $a,a'\in[1,p-1]$,计算:

$Q'_A=Q_2+a'Q_C=(x_1,y_1)$,$Q''=Q_1+aG=(x_2,y_2)$

$Q'''=d_AQ_C$,$r'=x_2 \bmod n$,$r=x_1 \bmod n$

$s''=a+r'd_A$ $s'=a'+rd_A$

将(Q'_A,Q'',Q''',r,s',s'')发送给用户 U_i。

与此同时,A 计算 $h(ID_i)$并发送给选票收集者 C。

(3)在 U_i 收到 A 的签名信息后首先验证 A 的公正性。U_i 计算 $Q'=(s'+k_1)Q_C-rQ'''$,验证 $Q'_A-Q'\overset{?}{=}tP_b$,如果等式不成立则说明监管委员会不诚实。如果成立 U_i 继续做计算:$d_i=s''+k_1$ 作为用户的私钥。

$s=t(s'+k_2)+rd_i$,$Q=(Q')_x^{-1} \pmod n P_b+tQ'$

$Q'_u=tQ_A$,$l=h(ID_i)$

用户 U_i 将(l,Q'_u,Q'',Q,r,s)发送给选票收集者 C。

(4)选票收集者 C 收到 $h(ID_i)$后,将其存入临时数据库,以备验证用户的投票合法性。在收到 U_i 的(l,Q'_u,Q'',Q,r,s)后,首先在临时数据库中搜索是否存在 l。如果没有,说明 U_i 没有被授权或者已经投过票,会话结束。在通过第一步验证后,选票收集者 C 继续做:$Q_0=sG-rQ'-r(Q''+(Q'')_x(\bmod n)Q_A)$

则 $P_b=(Q_0)_x(Q-d_AQ_0)$,$P_b\to b$

选票收集者C将选票结果 b 和 $h(ID_i)$存入数据库,并将 $h(ID_i)$从临时数据库中删除。在投票一定时间内,选票收集者 C 公布临时数据库中的数据,即公布选举放弃者或者选票没有者。用户可以通过对照公布的数据与个人身份标识的哈希函数值来确认投票是否成功。

3.4 方案的正确性

$$\begin{aligned}d_CQ_0&=d_C[sG-rQ'-r(Q''+(Q'')_x(\bmod n)Q_A)]\\&=d_C[(t(a'+k_2+rd_A)+rd_i)G-tQ_A-r(Q''+(Q'')_x(\bmod n)Q_A)]\\&=d_C[t(a'+k_2)G]\\&=(a'+k_2)Q_C\end{aligned}$$

则 $Q-d_CQ_0=P_b\to b$ 恢复用户的选票。

4 方案分析

(1)本方案基于椭圆曲线离散对数难题,鉴于椭圆曲线低密钥高安全性特点,本方案具有很强的实用性。

(2)对于用户的公钥,签名验证者通过用户的签名信息 Q'' 和监管委员会的公钥 Q_A 恢复。这样使得本方案具有很强的灵活性,解决了椭圆曲线签名方案应用过程中的公钥分存难题。

(3)在用户 A 和监管委员会间的通信中,利用盲因子 t 实现对选举内容的盲化,使得监管委员以及密码分析者无法获得用户的选票内容。同样在用户 A 和选票收集者间的通信中,我们加入了$(Q')_x^{-1} \pmod n$盲因子,因为此因子只有当用户向选票收集者发送签名以后选票收集者才可以通过自己的私钥恢复,所以对其他人是盲的。否则密码分析者很容易伪造选票:密码分析者可以获得选票内容与椭圆曲线的对应表,分析者首先假设用户的选票内容为 P'_b,选择要修改的选票内容 P_c 计算 $P=Q+P_c-P'_b$,发送(l,Q'_u,Q'',P,r,s)给选票收集者,如果有 $P_b=P'_b$ 成立,则(l,Q'_u,Q'',P,r,s)可以通过验证并被统计。显然攻击者成功的可能性为$\frac{1}{m}$,m 为选票的个数。在加入盲因子 $(Q')_x^{-1}$ (mod n)后有效避免了这种伪造。

(4)密码分析者可以获得消息(l,Q',Q_u'',Q,r,s,s''),试图通过这些信息计算用户的私钥。由于他没有随机数 k,要想获得数 k,就要通过 kG 来求解,这是求解 ECDLP 问题,在选择安全的椭圆曲线参数条件下是不可能的。另一方面,在 $s=t(s'+k_2)+rd_i$ 中有三个未知数,所以也无法获得用户的私钥。分析者通过(Q'',Q'_u,Q,Q_A,r,s),可以得到:

$$\begin{aligned}Q_0&=sG-rQ'-r(Q''+(Q'')_x(\bmod n)Q_A)\\&=(t(a'+k_2+rd_A)+rd_i)G-tQ_A-r(Q''+(Q'')_x(\bmod n)Q_A)\\&=t(a'+k_2)G\end{aligned}$$

要想获得选票内容必须有选票收集者的私钥,获得选票收集者的私钥也是求解 ECDLP 问题。

(5)在本方案中,用户私钥的生成过程也是监管委员会对用户的授权过程。选票收集者通过冗余消息的验证和用户身份的哈希函数值可以判断用户的合法性(已通过监管委员会的授权)。

(6)对于同一个用户第二次向监管委员会申请资格投票,由于监管委员会已经保存用户的资料,所以用户的二次申请将不会成功。用户试图进行二次投票,因为只有在用户被授权以后才可以通过选票收集者的第一步验证。如果用户已经投过票则在临时数据库中没有这个用户的身份标示的哈希函数值,使

(下转 195 页)

IC卡发卡子系统。

以上内容概要介绍了智能大厦中信息系统的实现问题。

4 信息化在智能大厦中的应用前景分析

随着房地产业的发展，作为房地产业的重要组成部分——智能化大厦与IT行业的融合越来越深入，领跑房地产业的一些企业已与IT业进行了有效整合。

展望房地产信息化未来的发展前景，以下几种趋势值得关注，当然这也很大程度上影响到了未来智能化大厦的信息化发展走向：

(1)网络时代人们对智能大厦和智能小区的要求是高度信息化。大厦和小区的信息化功能将被列为评价楼盘综合性能的不可缺少的一个重要指标。大厦内信息化社区的提供与外界进行数据交换的软硬件设施和服务是智能大厦功能向外拓展的必要条件。

(2)电子商务将大有可为。随着信息化建设的推进，电子商务的市场在全球范围内急剧扩大，各发达国家都把发展电子商务作为拓展全球市场的有效手段，积极地参与、协商与合作。在这良好的外部环境下，房地产电子商务将会成为21世纪整个产业发展的一大亮点和推动产业发展的巨大动力。迎接挑战，房地产电子商务在目前可从企业与企业间的电子商务方式、企业对客户的服务方式、网上信息发布、建立虚拟企业以及信息化的物业管理等方面展开。

(3)房地产业务和管理将会实现高度信息化。与未来网络社会相适应，不论是普通的消费者还是专业的房地产企业，都要求房地产业务和管理的高度信息化。同样在企业与企业合作当中，也只有运用了网络信息技术，才能保证有更多的市场机会和服务品质。

毋庸置疑，在信息化社会中，任何产业都不可能脱离IT行业的影响而存在，信息技术的应用促进了房地产业的变革，提高了开发效率、服务质量和管理水平。

参考文献

1.IBM/Lotus技术红皮书.IBM公司，2002

2.[美]Tamura R A等著.王建华等译.Lotus Notes和Domino Server 4.6技术大全[M].北京：机械工业出版社，1998

3.中科软大厦信息系统培训资料

4.http://www.soufun.com

(上接139页)

在服务器的帮助下，把IC卡当成用户A，把服务器当成用户B，则可利用椭圆曲线方案通过Massey-Onmura系统或ElGamal系统实现认证与签名。其中，运算$k(k_BP)$和$d(cP_m)$都采用上述协议所提供的方法。

参考文献

1.Volker Müller.Fast Multiplication on Elliptic Curves over Small Fields of Characteristic Two[J].Journal of Cryptology,1998-11

2.Willi Meier,Othymar Staffelbach.Efficient Multiplication on Certain Nonsupersingular Elliptic Curves.Advances in Cryptology—CRYPTO'92

3.Alfred J Menezes.Elliptic Curves Public Key Cryptosystem[M].Klumber Academic Publishers,1993

4.Neal Kobilits.Elliptic Curves Cryptosystem[J].Mathematics of Computation,1987;48(177):203~209

5.Pfitrzmann B,Waidner M.Attacking on Protocols for Server-aided RSA Computation.Advances in Cryptology—Eurocrypt'92

6.Anderson R J.Attacking on Server-assisted Authentication Protocols [J].Electronic Letters,1992:1473

(上接152页)

得用户第二次投票也不能成功。

(7)在方案中，对于消息的嵌入可以将选票内容直接嵌入到椭圆曲线上，也可以直接建立一个选票内容的一一对应，在方案运行前进行预运算使得在方案的运行中此过程可以不占用运行时间。而且这种一一对应可以任意组合，使得方案具有很强的灵活性。

5 综述

方案的安全性基于椭圆曲线离散对数难题，在选择安全参数条件下是安全的。而且方案可以防止监管委员会的欺诈。但是方案对于选票收集者的诚实性不能保证。如何防止选票收集者的欺诈也是一个值得研究的论题。

参考文献

1.Sako K Electronic.Voting System with Objection to the Center[S].SCIS92213C,1992:27~31

2.Sako K Electronic.Voting Scheme Allowing Open Objection to the Tally[J].IEICE Trans Fund,1994;E7724(1):24~30

3.Chen L,BurmesterM.A Practical Secret Voting Scheme Which Allows Voters to Abstain[C].见：1994年中国密码会议论文集.北京：科学出版社，1994:100~107

4.A Fujioka,T Okatoma,K Ohta.A Practical Secret Voting Scheme for Large Scale Elections[C].In:Proceedings of Auscrypt 92,1992:2442251

5.K R Iverson.A Cryptographic Scheme for Computerized General Elections[C].In:Proceedings of Crypto 91,1991:4052419

6.K Sako,J Kilian.Secure Voting Using Partially Compatible Homomorphisms[C].In:Proceedings of Crypto 94,1994:4112424

7.Shiang-Feng Tzeng,Min-Shiang Hwang.Digital Signature with Message Recovery and its Variants Based on Elliptic Curve Discrete Logarithm Problem.Computer Stardands & Interfaces,2004;(26):61~71