新的盲签名方案在电子投票协议中的运用

周利娟[1] 王新庄[1] 梅万祺[2]

(1. 成都理工大学 信息管理学院, 四川 成都 610059; 2. 东北财经大学 研究生院, 辽宁 大连 116025)

〔摘要〕 电子投票的安全性至关重要. 文章创新性地将比特承诺技术运用于基于椭圆曲线的盲数字签名方案中, 该方案的安全性基于椭圆曲线离散对数困难问题, 有很强的安全性, 且在密钥长度和执行效率上具有显著优势. 并将该方案用于电子投票协议中, 对协议的安全性进行了分析, 有很强的实用价值.

〔关键词〕 椭圆曲线; 比特承诺; 盲数字签名; 电子投票

〔文章编号〕 1672-2027(2009)02-0075-03 〔中图分类号〕 TP309 〔文献标识码〕 A

0 引言

如今电子投票因其实用性而受到广泛关注. 而如何保证电子投票的公开、公平和公正, 则成为人们关心的焦点. 数字签名是保证电子数据真实性及确认签名者身份的有效手段[1~2]. 在电子投票协议中, 有时需要签名者不能得知所签署消息的具体内容, 这是盲签名所符合的. 它满足了参加投票者的匿名性.

本文将比特承诺技术运用于基于椭圆曲线的盲数字签名方案中, 该方案的安全性是建立在椭圆曲线离散对数的难解性基础上的. 由于椭圆曲线密码体制自身的短密钥, 运算快的特点, 及基于比特承诺的部分盲签名方案允许了签名者在签名中加入用户的身份信息, 这防止了用户滥用签名方法和保证了签名者不能侵犯用户的身份隐私[3~4]. 该方案的优点使得其在电子投票协议中的运用具有很高的安全性.

作为公平选举的电子投票, 为防止欺骗, 它应该满足以下的这些特性:

1) 合法性: 只有经过许可的合格的投票人才能投票.

2) 健壮性: 不诚实的投票者不能扰乱和破坏整个投票过程.

3) 匿名性: 所有选票的内容都是秘密的, 任何人都不知道他人的投票结果.

4) 不可重复性: 所有的投票者只能投一次票, 不可重复投票.

5) 完全性: 所有的合法选票应被正确统计和认证.

6) 公正性: 任何其他人都不能修改他人的投票, 影响投票结果.

7) 可验证性: 投票者可验证自己的投票是否被统计上.

本协议主要用到了基于椭圆曲线和比特承诺技术的部分盲签名方案. 下面我们先介绍该盲签名方案, 再介绍它在电子投票协议中的运用.

1 基于椭圆曲线和比特承诺的盲签名方案

1.1 基于椭圆曲线的盲签名

盲签名是由 D. Chaum 于 1983 年首次提出. 盲数字签名技术具有以下两种特性: 1)签名消息的内容对签名者是不可见的. 2)签名消息的内容被泄露后, 签名者不能追踪签名. 这些特性满足了电子投票的保密要求: 在认证的同时不泄露内容[5].

本方案的安全性是基于椭圆曲线离散对数问题的难解性基础上的, 有很强的安全性. 方案包含用户 P 和签名者 S, 如下:

* 收稿日期: 2009-01-08

作者简介: 周利娟(1984-), 女, 湖北仙桃人, 成都理工大学信息管理学院在读硕士研究生, 主要从事信息安全、密码学研究.

1) 系统初始化:构造有限域 F_q 上的椭圆曲线. 该曲线 $E(F_q)$非超奇异, $G\in E(F_q)$是公开的基点. $n=ord(G)$是公开基点的阶.

2) 密钥生成: 用户 P 随机选取整数 d 作为密钥, $G_p=dG$ 为公钥.

3) 签名生成: 签名者 S 的私钥设为 k_s, 公钥 $G_s=k_sG$.

ⅰ)用户 P 随机选取整数 $r\in[1, 2, \cdots, n-1]$ 作盲因子, 盲化消息 m, 计算 $m'=rm(\mathrm{mod}n)$, 并将 m' 发送给 S.

ⅱ)签名者 S 随机选取整数 $k\in\{1, 2, \cdots, n-1\}$. 计算 $R=kG=(x, y)$. $b'=xm'\mathrm{mod}n$, $y'=k^{-1}(m'k_B-b')\mathrm{mod}n$, 将$(y', b', R)$发送给 P.

ⅲ)用户 P 去掉盲因子, 计算 $y=r^{-1}y'\mathrm{mod}n$, $b=r^{-1}b'\mathrm{mod}n$, 得到签名(y, b, R).

4)签名验证:只需验证 $yR+bG=mG_B$ 是否成立即可. 若成立, 则签名正确; 否则, 签名不正确.

1.2 比特承诺技术在部分盲签名方案中的运用

将比特承诺技术运用于部分盲签名方案中, 让签名者在签名中加入了用户的身份信息, 这一有效特征防止了用户滥用签名方法及保证签名者不能侵犯用户的身份隐私[6, 7].

设 $H:\{0, 1\}^*\rightarrow\{0, 1\}^{2|N|}$ 代表一个多形式时间内可计算的单向 hash 函数. 签名者 S 随机选取私钥 $e\in_R Z_q^*$, 公钥 $BC(e)$公开. 素数 p, q 满足 $p-1=2q$, 则用户 P 获得关于信息 m 的部分盲签名协议如下:

1)S 选择 $u\in_R Z_q^*$, 计算 $\beta=BC(u)$, 并发送 β 给 P.

2)P 选择 $k, r\in_R Z_q^*$, 计算 $\alpha=BC(u)BC(e))^kBC(r)\mathrm{mod}p$, 由比特承诺方案的性质, $\alpha=BC(u+ke+r)$.

3)P 计算 $\varepsilon=H(m, \alpha)+k\mathrm{mod}q$, 然后将 ε 发送给 S.

4)S 计算 $R=u+\varepsilon e\mathrm{mod}p$, 并将 R 发送给 P. 这里 S 可以把 ε 存储在数据库中作为用户 P 的身份标志信息, 以备将来用户 P 滥用签名时辨别其身份.

5)P 验证是否 $BC(R)=\alpha(BC(e))^{\varepsilon}\mathrm{mod}p$, P 再计算出 $\rho=R+r\mathrm{mod}q$ 及 $T=BC(\rho)$, 从而获得信息 m 的签名$\{m, \alpha, T\}$.

2 新方案在电子投票协议中的运用

基于椭圆曲线的盲签名的使用, 不仅满足了电子投票协议的各种安全性能的要求, 而且由于比特承诺技术的使用, 使得投票管理机构在签名中加入投票者的身份信息, 这一新特征有效保护了投票者的隐私权和投票内容. 因而, 这种新的盲签名方案在电子投票协议中的运用有很重要的意义[8~10]. 本协议中, 有三个参与方:投票者 V_i, 投票管理机构 A, 计票员 C. 协议如下:

1)系统初始化:构造有限域 F_q 上的椭圆曲线 $E(F_q)$. 该曲线非超奇异, 且满足安全条件. 公开基点 $G\in E(F_q)$, 阶为 n, V_i 的密钥 k_i, 公钥 $G_i=k_iG$; A 的密钥为 k_A, 公钥 $G_A=k_AG$, A 与 C 有公共密钥 k_{AC}, v_i 为投票选择.

2)用比特承诺将合格 V_i 的身份标志信息嵌入并得到投票者编号 R_i. A 随机选择 u_i, 计算并发送 $\beta_i=BC(u_i)$给 V_i. V_i 随机选择 l_i, r_i, 并由比特承诺的性质, 计算 $\alpha_i=BC(u_i+l_ie_i+r_i)$. V_i 计算 $\varepsilon_i=H(m, \alpha_i)+l_i\mathrm{mod}n$. 然后将 ε_i 发送给 A. 这里, ε_i 是投票者 V_i 的身份标志信息. $H:\{0, 1\}^*\rightarrow\{0, 1\}^{2|N|}$ 为单向 hash 函数. A 计算 $R_i=u_i+\varepsilon_ik_i\mathrm{mod}n$, 并将 R_i 发送给 V_i. 这里, A 可以把 ε_i 存储在数据库中作为投票者 V_i 的身份标志信息, 以备将来 V_i 滥用签名时辨别其身份.

3)V_i 填写选票 v_i, 随机选取盲因子 r_i, 盲化选票得 $v'=r_iv_i$, 对 v' 进行签名:随机选取一个整数 $m\in\{1, \cdots, n-1\}$, 计算 $mG=(x, y)$, $t=x\mathrm{mod}n$, $s=k+v'k_i(\mathrm{mod}n)$, 将(R_i, s, t, v')发送给 A. R_i 为合格的投票者 V_i 的编号.

4)A 根据 R_i 对 V_i 进行签名认证. $sG=(x_1, y_i)+v'G_i$. 若 $x_i\mathrm{mod}n=t$, 则接受 V_i 签名. 随机选取整数 $c\in\{1, \cdots, n-1\}$, $cG(x_A, y_A)$, $t_A=x_A\mathrm{mod}n$, $y=c^{-1}(v'+k_At_A)(\mathrm{mod}n)$, $PA'_i=k_{AC}^{-1}v'G$, 并将(y, t_A, PA_i)发送给 V_i.

5)V_i 收到后, 对 PA'_i 进行脱盲, 得到 $PA'_i=r_i^{-1}PA'_i$, 然后将(y, t_A, v', PA_i)送给计票员 C.

6)C 收到(y, t_A, v', PA_i)后, 对 A 进行签名认证. $rG+t_AG_A=y(x'_A, y'_A)$若 $x'_A\mathrm{mod}n=t_A$, 则接受本选

票, 并记下本选票结果 $P_i = k_{AC} PA_i = vG$. 最后进行统计并公布选票结果.

7) V_i 通过检查(R_i, P_i)看自己的票是否被计入.

3　性能分析

1) 通过第 2 步, 嵌入投票者的身份标志信息得到合格的投票者 V_i 的编号 R_i, 以免 V_i 滥用签名. 实现了协议的合法性, 健壮性与不可重复性.

2) 第 3, 4 步通过选取盲因子盲化投票内容, 使得 A 对 V_i 的票无法知晓, 从而满足了匿名性要求.

3) 第 6, 7 步中通过计票和检验可以实现协议的完全性和可验证性条件.

4) 在每个投票过程中, A 只知道 V_i 的编号而不知道选票内容, 而 C 只知选票内容, 却不知道 V_i 的编号和身份标志信息, 因而他们要伪造选票也是不可能的. 因此, 极好地达到了协议的公平性要求.

4　结束语

本协议满足了通过网络来进行电子投票的需求. 文中的盲签名方案和电子投票协议都是建立在椭圆曲线离散对数难解性基础上的, 因此从理论上讲是安全的. 本协议的创新点在于将比特承诺技术运用到使用盲签名的电子投票中, 不仅防止了投票者滥用签名方法, 而且保证投票选举机构不能侵犯投票者的身份隐私和修改选票, 因而在防止投票中心伪造选票这一方面, 具有很高的安全性和实用性[11]. 希望在实际的投票系统环境中能加以运用, 进一步验证该协议的效果, 并不断改善其效率, 得到最终完善.

参考文献:

[1] ELGamal T. A public key cryptosystem and signature scheme based on discrete logarithm[J]. IEEE Trans, 1985, IT-31(4): 469-472

[2] Ham L. New digital signature scheme based on discrete logarithm[J]. Electronics Letter, 1994, 30(5): 396-398

[3] 冯登国, 裴定一. 密码学导引[M]. 北京: 科学出版社, 2001

[4] 张先红. 数字签名原理及技术[M]. 北京: 机械工业出版社, 2003

[5] 史有辉, 李伟生. 盲签名研究综述[J]. 计算机工程与科学, 2005, 27(7): 83-85

[6] 钟　鸣, 杨义先. 一种基于比持承诺的部分盲签名方案[J]. 通信学报, 2001, 22(9): 1-6

[7] 祁　明, 史国庆. 强盲签名技术的研究与应用[J]. 计算应用研究, 2001(3): 34-37

[8] 陈　英, 马洪涛. 一种基于椭圆曲线密码体制的电子投票方案[J]. 图书与情报, 2007(3): 107-111

[9] 韩　然, 周　梦. 基于椭圆曲线的盲数字签名与电子投票协议[J]. 北京电子科技学院学报, 2004(12): 18-20

[10] 王泽成, 苏晓萍, 汪精明. 一个基于椭圆曲线的代理签名和代理盲签名方案[J]. 青海大学学报, 2002, 20(3): 36-39

[11] 陈晓峰, 王育明. 基于匿名通讯信道的安全电子投票方案[J]. 电子学报, 2003, 31(3): 390-393

A New Blind Signature Scheme Used to the Electronic Voting Agreement

Zhou Lijuan[1]　**Wang Xinzhuang**[1]　**Mei Wanqi**[2]

(1. Department of IM, Chengdu University of Technology, Chengdu 610059;
2. Grade School of Dongbei University of Finance and Economics, Dalian 116025, China)

〔**Abstract**〕 The security of E-voting is essential. The bit commitment is innovatively used to the blind digital signature scheme which based on elliptic curve. The scheme, whose security is based on the elliptic curve separate logarithm difficult problem, has the very strong security. And in the key length and efficiency of carried out, it has the remarkable superiority. At last, it is applied to a protocol of electronic voting. The performance analysis to the scheme shows that it is theoretically secure and suitable in practical applications.

〔**Key words**〕 elliptic curve; bit commitment; blind digital signature; electronic voting

【责任编辑: 王映苗】