基于椭圆曲线的盲数字签名与电子投票协议

韩 然 周 梦
(北京航空航天大学 理学院,北京:100083)

摘 要:本文提出了一种基于椭圆曲线的盲数字签名方案,并设计了一个基于椭圆曲线的电子投票协议,对这些方案的性能进行了分析,其安全性是建立在椭圆曲线离散对数问题的难解性基础上的,从理论上讲是安全的,具有一定的实用价值。

关键词:椭圆曲线;盲数字签名;电子投票
中图分类号:TN918.1 文献标识码:A 文章编号:1672-464X(2004)04-0018-03

1 引言

数字签名是电子信息特殊的产物,是保证电子数据真实性的有效手段,而在实际应用中,有些情况却是需要签名者不能得知明文消息的内容,这就是盲数字签名(Blind digital signature),其在需要实现某些参加者的匿名性的密码协议中有着广泛而重要的应用,诸如在选举协议、安全的电子支付系统中等。盲数字签名方案是具有下列两个特性的一种数字签名方案:

⑴消息的内容对签名者来说是盲的;

⑵在签名被接受者泄露后,签名者不能追踪签名。

目前已有大量的文献讨论了盲数字签名方案的实现和应用问题,但主要是基于 RSA 体制和离散对数问题的盲数字签名方案[3][4][8]。本文利用了盲因子的特性,提出了一个基于椭圆曲线密码体制的盲数字签名方案,其安全性是基于椭圆曲线离散对数问题的难解性基础上的,由于椭圆曲线密码体制自身的短密钥、运算快的优点,此方案具有一定的实用价值。

作为数字签名与盲数字签名的一个重要应用是电子投票协议,它以各种密码学技术为理论基础,已被广泛应用于网络环境中。电子投票可以节省时间和人力资源,具有很高的效率和灵活性。一般的,作为公平选举,为防止欺骗,选举应该满足以下基本要求:

⑴合法性。只有合法选举人才能投票;

⑵合理性。不诚实的选举者不能扰乱选举;

⑶秘密性。所有选票必须保密,每一个人都不能知道他人的投票情况;

⑷不可重复性。每一个投票人只能够投票一次;

⑸可检验性。所有选举者都能检验他们的选票在最后的表中是否被统计上;

⑹安全性。任何人都不能修改他人的投票。

和其他密码协议一样,也存在多种电子投票协议,如基于 RSA 密码体制和离散对数问题的协议,它们或多或少地满足上述要求[5]-[8]。在这些协议中,它们有的使用了盲签名技术,有的未使用。而本文提出了一个基于椭圆曲线密码体制的电子投票协议,在其中使用了盲签名技术,并采用了一个变形的数字签名方案[9],使其运算速度更快,该协议满足上述的基本要求,具有较高的安全性和一定的实用价值。

本文在第 2 节设计了一种基于椭圆曲线的盲数字签名方案,并对其安全性进行了分析;第 3 节设计了一种基于椭圆曲线的电子投票协议。与之相关的椭圆曲线密码理论及椭圆曲线数字签名理论请参阅文献[1][2]。

2 基于椭圆曲线的盲签名方案

数字签名可以用秘密密钥密码体制实现,也可以用公开密钥密码体制实现。椭圆曲线数字签名算法(ECDSA)实际上是数字签名算法(DSA)的椭圆曲线模拟,一般的数字签名中,签名者总是首先要知道签名文件的内容,然后才对文件签名,但是有时候,要求认证者只能通过签名来认证签名者的身份是否合法而不能得知具体的明文消息,称这种签名为盲签名。一个盲签名方案包含两个参与者的密码协议:一个用户 A 和一个签名者 B。本方案如下:

⑴系统初始化:构造有限域 F_q 上的椭圆曲线 $E(F_q)$,该曲线是非奇异的,且满足安全条件,选择一个公开的基点 $G \in E(F_q)$,其阶为 n,被签名信息为 m。

收稿日期:2004-6-2

⑵密钥生成:用户 A 随机选取一个整数 d 作为密钥,公开点 $G_A=dG$ 作为公钥。

⑶签名生成:

签名者 B 的私钥设为 k_B,公钥 $G_B=k_BG$。

①用户 A 随机选取一个盲因子 $r\in\{1,2,\cdots,n-1\}$,计算 $m'=rm(\mathrm{mod}n)$,将 m'送给用户 B;

②签名者 B 随机选取整数 $k\in\{1,\cdots,n-1\}$,计算 $R=kG=(x,y)$,$a'=xm'\mathrm{mod}n$,$y'=k^{-1}(m'k_B-a')\mathrm{mod}n$,并将$(y',a',R)$传送给用户 A;

③用户 A 计算 $y=r^{-1}y'\mathrm{mod}n$,$a=r^{-1}a'\mathrm{mod}n$,输出签名(y,a,R);

⑷签名验证:只需验证 $yR+aG=mG_B$ 是否成立即可,若成立,则签名正确,否则不正确。这是因为:$yk\equiv r^{-1}m'k_B-r^{-1}a'\equiv r^{-1}rmk_B-r^{-1}ra\equiv mk_B-a(\mathrm{mod}n)$,所以 $yR+aG=mG_B$。

⑸性能分析:

①由盲数字签名的特性,明文消息 m 对签名者 B 来说应该是盲的,因为 B 不知道盲因子 r,所以不能由盲消息恢复出原消息,正确猜出 r 的概率为 $1/n$;

②攻击者若截取 R,试图通过 R 来求解 k,这是求解椭圆曲线离散对数问题;

③攻击者若截取 y',试图伪造 y',但是不知道 B 的密钥,也是徒劳的,因此,本方案满足盲数字签名的要求。

3 基于椭圆曲线的电子投票协议

投票选举是现实生活中的一种常见的活动,电子投票是一种重要的密码协议,已被广泛地应用于网络环境中,一般的,电子投票协议需要两个机构:选举管理机构和选举记票机构,首先选举者盲化一张选票送给选举管理机构,选举管理机构对其身份进行认证,并对选票进行签名,然后由选举者对选票进行托盲,由选举记票机构进行选票统计。

本协议是一种基于椭圆曲线密码体制的电子投票协议,其安全性是建立在椭圆曲线离散对数问题的难解性基础上的,具有较高的安全性和灵活性,并满足电子投票协议的基本要求。由于椭圆曲线中的逆运算是最费时间的,所以我们在对盲化选票进行签名时采用了一个椭圆曲线数字签名的变形方案[9],避免了逆运算,使其运算速度更快。方案如下:

⑴系统初始化:构造有限域 F_q 上的椭圆曲线 $E(F_q)$,该曲线是非奇异的,且满足安全条件,选择一个公开的基点 $G\in E(F_q)$,其阶为 n,选举成员为 V_i,其密钥 k_i,公钥 $G_i=k_iG$;选举管理机构为 A,其密钥为 k_A,公钥为 $G_A=k_AG$;选举主持人为 C,A 与 C 之间有一公共密钥 k_{AC},v_i 代表相应的投票选择。

⑵选举者 V_i 选择并填写一张选票 v_i,并随机选择一个盲因子 r_i,且 $r_ir_i^{-1}=1$,计算 $v'=r_iv_i$,然后对 v'进行一般的椭圆曲线数字签名:随机选择一个整数 $k\in\{1,\mathrm{L},n-1\}$,计算 $kG=(x,y)$,$t=x\mathrm{mod}n$,$s=k-v'k_i(\mathrm{mod}n)$,将(ID_i,s,v',t)送给 A,其中 ID_i 为 V_i 的身份标志。

⑶选举管理机构 A 首先检查选举者 V_i 有无权利选举,如果 V_i 无权利参加选举,则 A 拒绝给 V_i 签名;否则,A 记录 V_i 的身份标志 ID_i,检查 V_i 在此之前是否投过选票,若是,则拒绝;否则 A 对 V_i 进行签名认证,做如下计算:$sG+v'G_i=(x_0,y_i)$,若 $x_i\mathrm{mod}n=t$,则接受 V_i 的签名,随后 A 对 v'进行签名:随机选择一个整数 $b\in\{1,\mathrm{L},n-1\}$,计算 $bG=(x_A,y_A)$,$t_A=x_A\mathrm{mod}n$,$y=b^{-1}(v'+k_At_A)(\mathrm{mod}n)$,$P_{Ai}=k_{AC}^{-1}v'G$,然后将$(y,t_A,P_{Ai})$送给 V_i,在投票结束时,A 公布所有的(ID_i,P_{Ai})。

⑷V_i 收到(y,t_A,P_{Ai})后对 P_{Ai}进行脱盲,计算 $P_{Ai}'=r_i^{-1}P_{Ai}$,然后将(y,t_A,v',P_{Ai}')送给主持人 C。

⑸C 收到(y,t_A,v',P_{Ai}')后,先对 A 进行签名认证,计算 $y^{-1}v'G+y^{-1}t_AG_A=(x_A',y_A')$,若 $x_A'\mathrm{mod}n=t_A$,则接受这张选票,随后计算 $P_i=k_{AC}P_{Ai}'=v_iG$,因为 v_i的取值很小,因此 C 可以预先计算出作为选票结果的 P_i,然后根据 P_i的值就可以得到本张选票的选举结果,记录该选票,在所有的选举者投完票后,C 公开所有的 P_{Ai}' 及其对应的选举结果。

性能分析:

⑴作为选举协议很重要的一点是匿名性,依据本协议的盲签名的特性,选取一盲因子 r_i 对所投的票直接进行盲化,由于 A 不知道盲因子 r_i,使得 A 对投票人的票无法知晓,然后 A 对盲化的票进行签名,随后选举人将其中的盲因子去掉,则主持人得到的仅是 A 签过名的一张票,而不知道是谁投的,从而达到匿名性。

⑵在上述第⑵步中的 A 对 V_i 的签名认证验证为:由 $s=k-v'k_i(\mathrm{mod}n)$,得 $s+v'k_i=k(\mathrm{mod}n)$,所以有 $sG+v'G_i=kG$;上述第⑸步 C对 A 的签名验证为:由 $y=b^{-1}(v'+k_At_A)(\mathrm{mod}n)$,得 $b=y^{-1}(v'+k_At_A)(\mathrm{mod}n)$,两边同乘 G,便得证。

⑶若攻击者(s,v',t)截取,由 v'得到选票 V_i 相当于解离散对数问题,要伪造签名,由于不知道 V_i 的私钥,也是无能为力的,正确猜测 r_i 的概率为 $1/n$,因此 A 要伪造选票也是不可能的。若攻击者截取(y,t_A,P_{Ai}),假冒选举管理机构 A,试图要伪造和更改选票,但由于不知道 k_{AC},也是徒劳的。因此,本方案中是认为 A 和 C 都是诚实的。

⑷当投票完成时,选举主持人C统计完选票后公布所有的P_{Ai}'及其对应的选举结果,此时选举者可以根据自己发送给C的P_{Ai}'查询投票是否被公开,以判断自己的选票是否被统计,若P_{Ai}'被公开,查询相对应的投票结果是否是自己的投票,从而完成对自己选票的查询。

4 结束语

本文中的盲签名方案和电子投票协议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,而椭圆曲线离散对数问题在安全、运算时间、密钥长度、便于计算机实现等方面都优于有限域上的离散对数、整数分解等问题,所以椭圆曲线密码体制越来越得到人们的重视,椭圆曲线上的密码方案也将得到广泛的应用。

参考文献:

[1] Neal Koblitz, Elliptic curve cryptosystems, Math.Comp.,vol.48,pp.203-209,1987.
[2] Silverman .J. H., The arithmetic of elliptic curves. GTM106, Springer-Verlag.New York.1986.
[3] T ElGamal. A public key cryptosystem and signature scheme based on discrete logarithm. IEEE Trans. 1985,IT-31(4):469-472.
[4] L Ham. New digital signature scheme based on discrete logarithm. Electronics Letters,1994,30(5):396-398.
[5] Nurmi H. Salomaa. Santean L. Secrete Ballot Elections in Computer Networks, Computer & Security,V.10,1991,553-560.
[6] Iversen K. R. A Cryptographic Scheme for Computerized General Elections, Advances in Cryptology-Crypto' 91,Springer-Verlag, 1992,405-419.
[7] Fujioka A, Okamoto T, Ohta K. A Practical Secret Voting Scheme for Large Scale Elections. Advances in Cryptology-Ausocrpt' 92, Springer Verlag,1993.
[8] 冯登国,裴定一. 密码学导引[M].北京:科学出版社,2001.
[9] 杨君辉,戴宗择,杨栋毅,刘宏伟.一种椭圆曲线签名方案与基于身份的签名协议[J].软件学报,2000.11(10):1303-1306.

作者简介:
韩 然,男,山东人,1976年生,北京航空航天大学理学院硕士研究生。主要研究方向:椭圆曲线密码学。

A Protocol of Electronic Voting and Blind Digital Signature Based on Elliptic Curve

Han Ran Zhou Meng
(Institution of Science, Beijing University of Aeronautics and Astronautics, Beijing: 100083)

Abstract: In this paper, a blind digital signature scheme is proposed, and a protocol of electronic voting based on the elliptic curve cryptosystem is designed. The performance analysis to these schemes shows that they are theoretically secure and suitable for some practical applications. The reason lies in that the elliptic curve discrete logarithm problem is difficult to be solved.
Key words: elliptic curve; blind digital signature; electronic voting