第36卷 第13期 计 算 机 工 程 2010年7月
Vol.36 No.13 Computer Engineering July 2010
·安全技术· 文章编号：1000—3428(2010)13—0156—03 文献标识码：A 中图分类号：TP309

基于椭圆曲线盲数字签名的电子选举

丛清日，胡金初
(上海师范大学信息与机电工程学院，上海 200234)

摘 要： 椭圆曲线公钥密码体制具有安全性高、密钥量小、灵活性好的优点。基于椭圆曲线的数字签名在电子商务等领域为身份认证、数据完整性、不可否认性以及匿名性等提供了安全保障。提出一种基于有限域 $GF(p)$上非超奇异椭圆曲线上盲数字签名的方案，结合该方案设计一个在线电子投票协议。其安全性建立在椭圆曲线离散对数问题的难解性基础上，具有较好的实用价值。

关键词： 椭圆曲线；盲数字签名；在线电子投票

E-elections Based on Elliptic Curve Blind Digital Signature

CONG Qing-ri, HU Jin-chu
(College of Information and Mechanical & Electrical Engineering, Shanghai Normal University, Shanghai 200234)

【Abstract】 Elliptic curve cryptosystem is known as its unique advantages of high security, small amount of key and flexibility. Based on elliptic curve digital signature which provides security in many electronic commerce areas such as authentication, data integrity, non-repudiation and the anonymity, this paper proposes a blind digital signature based on the finite field $GF(p)$ on non-supersingular elliptic curve, and designs an online e-voting protocol which is in conjunction with this program. Its safety is dependent on the discrete logarithm of elliptic curve, and it is suitable for some practice.

【Key words】 elliptic curve; blind digital signature; online e-voting

1 概述

电子投票是传统投票的电子化形式。它在组织工作、投票收集与统计上节省了大量的人力和物力，效率高，为投票者提供了很多方便。但是，投票要保证投票者的利益，保证投票结果的公正。这是一个安全电子投票的目标。因此，要在一个目前并不安全的网络环境中满足这2条需求，最常用的就是密码技术。

2 椭圆曲线数字签名算法

椭圆曲线密码体制来源于对椭圆曲线的研究。椭圆曲线指的是由韦尔斯特拉斯(Weierstrass)方程 $y^2+axy+by=x^3+cx^2+dx+e$ 所确定的平面曲线。其中，系数 a, b, c, d, e 定义在某个域上，可以是有理数域、实数域、复数域，还可以是有限域 $GF(p)$，椭圆曲线密码体制中用到的椭圆曲线都定义在有限域上。椭圆曲线上所有的点加一个无穷远点的特殊点 O 构成的集合连同一个定义的加法运算构成一个 *Abel* 群。在等式 $kP=P+P+\cdots+P=Q$ 中，$Q, P\in E_p(a, b)$且 $k<p$，已知 k 和点 P 求点 Q 比较容易，反之，已知点 Q 和点 P 求 k 却相当困难，这个问题称为椭圆曲线上点群的离散对数问题。椭圆曲线密码体制正是利用这个难解的离散对数问题设计的。

域 F 上基于离散对数的数字签名方案大多是基于签名等式 $u=av+kw \mod(p-1)$的不同变形，利用 $h(m)$, r 和 s 的不同排列组合和各种变形可以衍生出上万种签名方案，其中，$h(m)$是安全的散列函数。

3 常用的基于椭圆曲线的盲数字签名算法

一个盲签名方案包含2个参与者的密码协议：签名者 A 和验证者 B。方案构造如下[1]：

(1)签名过程

1)系统初始化：选择一条安全的椭圆曲线 $E(Fp)$，且该曲线是非奇异化的，选择一个公开的基点 $G\in E(Fp)$，阶数为 n，m 为待签信息；2)信息的盲化：$e=h(m, da)$，da 为用户自己的私钥，将 e 发送。

(2)密钥的生成

1)假设签名者 A 要对信息 m 进行盲签名，选择 $d(d\in(1, p-1))$为自己的私钥，计算 $y=dG$ 为公钥并公布；2)A 选择一个随机值 $k(k\in(1, p-1))$，计算 $kG=(x, y)$, $R=x \mod p$；3)计算 $r=eR \mod p$；4)计算 $S=(ek+rd) \mod p$。

(3)验证过程

1)验证者 B 接收到(r, S)后，从签名中心获得 A 的公钥 y 计算 $Y=y \mod p$；2)计算 $w=e^{-1}$；3)计算 $x'=w(SG-rY)=(x, y)$，若 $x'=0$，则盲群验证失败，否则，计算 $x \mod p$ 是否等于 r，若相等，则接受签名，否则，拒绝签名。

4 改进的基于椭圆曲线的盲数字签名算法

上述算法需要进行模逆操作，但对大整数求逆是一种比较耗时的运算，因此，e 的大小很容易制约整体的运算速度，这在带宽、计算能力或存储能力等受限的一些特殊应用场合将会是瓶颈。因此，本文设计了一个改进的避免大整数求逆的盲签名算法。

(1)签名过程

1)生成密钥：①假设签名者 A 要对信息 m 进行盲签名，选择 $d(d\in(1, p-1))$为自己的私钥，计算 $y=dG$ 为公钥并公布；②A 选择一个随机值 $k(k\in(1, p-1))$，计算 $kG=(x, y)$, $R_x=x \mod p$；③计算 $R=e R_x \mod p$；④计算 $S=(k+Rd) \mod p$。

基金项目： 上海市教委基金资助项目(06DZ003)

作者简介： 丛清日(1983－)，男，硕士研究生，主研方向：数字签名；胡金初，教授

收稿日期： 2009-11-28 **E-mail：** ri--ri@163.com

2)输出签名(R, S, e)。

(2)验证过程

1)验证者 B 接收到(R, S, e)后，从签名中心获得 A 的公钥 y，计算 $Y=y \bmod p$；

2)计算 $R'=e(SG-RY)$；

3)验证，若 $R'=0$，则盲验证失败，否则，计算 $R'\bmod p$ 是否等于 R，若相等，则接受签名，否则，不接受签名。

5 性能分析评估

根据文献[2]，G 是椭圆曲线上的一个基点，E 是定义在域(Fp)上的椭圆曲线且要求 $q\approx 2^{160}$。给定 dG，d 是一个随机的 160 位整数。因此，时间复杂度换算关系按如下关系式运算：

$T_{EC\text{-}MUL}\approx 29T_{mul}$

$T_{EC\text{-}ADD}\approx 0.12T_{mul}$

$T_{INV}\approx 0.4T_{EC\text{-}MUL}\approx 11.6T_{mul}$

为了便于比较签名方案的计算时间效率，设 T_{mul} 为在模意义下 2 个整数相乘的计算时间，T_{INV} 为在模意义下计算逆元素所需时间，$T_{EC\text{-}MUL}$ 为椭圆曲线模意义下数乘的计算时间，$T_{EC\text{-}ADD}$ 为椭圆曲线模意义下模加的计算时间。比较而言，模意义下的加运算的计算时间均远远小于相应的乘运算时间，可以忽略不计。对比数据如表 1 所示。

表 1 时间复杂度比较

方案	签名时间复杂度	签名时间粗略估计	验证时间复杂度	验证时间粗略估计
原方案	$T_{EC\text{-}MUL}+3T_{mul}$	$32T_{mul}$	$T_{EC\text{-}MUL}+2T_{mul}$	$31T_{mul}$
改进方案	$T_{INV}+3T_{EC\text{-}MUL}$	$98.72T_{mul}$	$3T_{EC\text{-}MUL}+T_{EC\text{-}ADD}$	$87.12T_{mul}+T_{EC\text{-}ADD}$

6 盲数字签名算法在电子选举中的应用

从第 1 个电子投票协议的提出到现在约 30 年时间里，许多学者和研究人员在这一领域进行了深入的研究和探讨，提出了相当多的电子投票方案或改进了已有的方案。在安全性和效率上都取得了很大的改进，理论上取得了一定的可喜成果，但是在实际应用中总会或多或少有令人不太满意的情况出现。文献[3]基于公开密钥、数字签名、盲签名、位保证等多种密码学技术提出了一个较为成功的电子投票方案，记为 FOO。该方案保证了投票的合法性和投票人身份的保密性，同时其算法易于实现、网络通信量较小，适合进行大规模投票。FOO 方案称得上是电子投票发展史上一个革命性的进步，它使电子投票得到了前所未有的发展。但 FOO 方案并不是完美的，仍然存在一些缺陷，例如：不允许投票人弃权，投票碰撞，无法区分不诚实的计票机构和不诚实的投票人。

本文针对这些缺陷提出改进，并给出一个在线电子投票方案[4]。FOO 方案能够伪造投票是因为其存在一个不完善的签名机构。为了避免签名机构的作弊问题，下面提出一种新型的选举协议，它满足以下 3 个特性：

⑴必须包含被计票机构验证合法性的信息；

(2)不能被其他人(相对于选举人)伪造；

(3)必须保持匿名性。

系统的参与者及其功能如下：

(1)群管理员

为投票系统选择合适的椭圆参数，为申请投票的人提供公钥和私钥，使合法投票人获得某种匿名的电子存在，从而可以独立匿名地进行投票和签名。

(2)投票人(选举活动的主体)

投票人通过注册获得秘密的指令，并利用该指令进行匿名选举。

(3)可信中心

主要是在投票前为投票人进行注册。

(4)投票发放中心

为合法的投票人发放空白投票，当投票人提交填写好的投票时负责验证投票的合法性，最终为计票机构发送合法有效的投票。

(5)计票机构

计算并公布最终的选举结果。

在线电子投票协议的流程如图 1 所示。

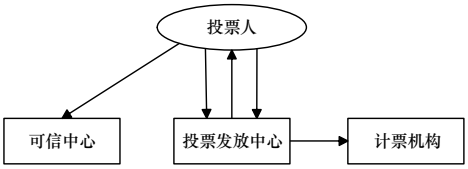

图 1 电子投票方案

(1)系统初始化

群管理员构造有限域 F_q 上的一条椭圆曲线 $E(F_q)$，该曲线是非奇异且满足安全条件的，选择一个公开的基点 $G\in E(F_q)$，其阶为 n，为计票机构提供密钥 X_J，公钥为 $Y_J=X_JG$。

(2)投票人注册

在注册有效阶段时间内，可信中心 T 与选举人 V_i 面对面地交互。面对面交互是因为通过网络获取选举人的身份信息不能完全保证真实，而且同一个选举人可能同时以不同的身份进行登记。可信中心将所有合法投票人的身份证明 ID_i 登记在一张秘密表 $List1$ 中，当验证通过后，合法的投票人向群管理员申请一对私钥 k_{i1} 和 k_{i2}，对应的公钥分别为 $Y_{i1}=k_{i1}G$ 和 $Y_{i2}=k_{i2}G$，投票人在获得私钥后在另一秘密表 $List2$ 中的随机位置写入一对口令 $S_{i1}(ID_i)$和 $S_{i2}(ID_i)$及公钥 Y_{i1}，以便投票验收阶段排除非法投票。其中，$S_{i1}(ID_i)$和 $S_{i2}(ID_i)$分别是投票人 V_i 用自己的双私钥加密的一对口令，与 Y_{i1} 对应。注册有效时间内可信中心无法得到 $List2$，注册结束后可信中心也无法从得到的 $List2$ 和已有的 $List1$ 的内容中找到对应关系。

(3)申请投票

注册阶段结束后，V_i 向投票发放中心提交 $S_{i1}(ID_i)$申请一张合法投票，投票发放中心根据从可信中心获得的 $List2$ 中有无 $S_{i1}(ID_i)$判断是否为一个合法的投票人，若有，则承认其为一合法投票者并发放一张空白投票$\{S_{i1}(ID_i)\| S_x(S_{i1}(ID_i))\}$，否则，认为申请者为非法投票者，拒绝为其发放投票。其中，$S_x(S_{i1}(ID_i))$是投票发放中心根据上文设计的基于椭圆曲线的数字签名算法对其进行的签名；$\|$是附加号；$A\|B$ 表示把 B 串附在 A 串后面。此阶段合法投票人完成匿名申请投票。

(4)投票人选举

投票人 V_i 填写完投票信息 m_i，$m_i=\{S_{i1}(ID_i)\|S_x(S_{i1}(ID_i))\|(C_1, C_2)\|(R, S)\|S_{i2}(ID_i)\| Y_{i1}\}$，其中，$(C_1, C_2)$是投票人将填写好的选票内容编码到 $E(F_q)$上的一点 M，然后产生一个随机整数 r，$C_1=M+rY_J$，$C_2=rG$，$S_{i2}(ID_i)$是投票人在投票表单上填写的第 2 个口令，(R, S)是投票人用私钥 k_{i1} 对整张投票的签名，填写完毕后投票人将 m_i 发送回投票发放中心。

(5)投票发放中心验证转发投票

投票发放中心在收到投票信息后，发回“收到报文的收据”给投票人，以解决投票发放中心事后可能会因某种原因而否认接收到选票的问题。投票发放中心主要做 3 个方面的

工作：验证投票人的真假，验证投票单的真假，将筛选的合法有效的投票单发送给计票中心。投票发放中心获得 m_i 后，取出 $S_{i1}(ID_i)$验证是不是合法投票表(*List*2)中的一员，若是，则继续取出 $S_{i2}(ID_i)$，根据 *List*2 查看是否与之前取出的 $S_{i1}(ID_i)$ 对应，若都满足，则承认其是合法的投票人，在 *List*2 中为 $S_{i1}(ID_i)$项做一标记，这用来检验是否为二次投票；否则，认为是非法的投票人，投票信息无用。投票发放中心将经过筛选的合法投票集中投送到计票机构。投票发放中心另一个重要的作用就是隐藏选票信息包的实际起源等敏感信息，从而增强匿名投票的效果。

(6)统计投票结果并公布

计票机构收到从投票发放中心发来的投票，用自己的计票私钥 X_J 计算 $C_1\text{-}X_JC_2=M+rY\text{-}X_J(rG)=M+rY\text{-}r(X_JG)=M$，结果就是点 M，再对点 M 进行解码就可以得到投票的明文，最后将投票明文、投票人的 $S_{i1}(ID_i)$, $S_{i2}(ID_i)$, (R, S), Y_{i1} 公布在电子公告板上，(R, S)和 Y_{i1} 可方便检查投票信息是否被篡改。

该方案的安全性表现如下：(1)合法性。$S_x(S_{i1}(ID_i))$可以确保投票表单的唯一性及投票表单的合法性，$S_x(S_{i1}(ID_i))$由投票发放中心颁发和签名，别人无法获得投票发放中心的私钥，签名无法伪造。(2)秘密性。投票人的投票信息保密，投票信息由计票机构的公钥加密，只有计票机构的私钥可以解开，别人中途无法得知某一投票的详细信息。计票机构也仅能获得投票信息而无法得知具体的投票人信息。最后的电子版上只有投票人的 $S_{i1}(ID_i)$和对应的投票信息，投票人的私人信息只有投票人自己能对应上。(3)抗否认性。投票信息是由投票人自己签名的，一方面可以有效抵抗投票人否认投票信息，另一方面也可用作投票人对电子版公布的自己的投票信息验证真伪。(4)不可伪造性。不诚实的投票者即使通过某一手段获得了一张有效的投票单，但是因为他没有真正投票者的私钥对，所以无法获得正确的 $S_{i2}(ID_i)$，这样不诚实的投票就会被筛选掉而不会对正常的投票造成干扰。即使投票发放中心或计票机构作假想修改投票，也会因为没有 V_i 的私钥而失败。所用到的签名、加密其难度都建立在椭圆曲线离散对数难解性基础上，因此，这是安全的。

本方案不仅满足电子选举的基本特性，而且还解决了 FOO 方案的一些不足：(1)无论投票人是否弃权，计票机构和可信中心均不可伪造投票，因为投票是由投票人的私钥签名的，不再由计票机构和可信中心签名，所以它们不可伪造投票，即使这 2 个部门相互勾结也无法伪造投票。(2)用 $S_x(S_{i1}(ID_i))$区别不同的投票解决了“投票碰撞”问题。这样不会出现 FOO 方案中的“合法选民的合法选票由于该选票的位保证与别人重复，而可能不被记入选票结果”[5]。(3)不诚实的投票人无论是偷取别人的合法投票，还是自己伪造假的投票都无法对正常的投票造成干扰，都会被合法的投票者举报或被投票发放中心筛选掉。

7 结束语

本文提出的基于椭圆曲线的盲数字签名相对基于其他数学难题的盲数字签名方案而言，具有密钥短、软硬件实现方便、速度快的优点。因此，本文的电子投票从理论上讲是安全、高效的、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必将得到广泛的应用。

参考文献

[1] 龚晓萍, 刘志朋, 黄继红. 基于椭圆曲线盲签名的安全数字时间戳方案[J]. 计算机工程, 2008, 34(13): 147-149.

[2] Jurisic A, Menezes A. Elliptic Curves and Cryptography[EB/OL]. (2003-09-12). http://www.certicom.corn/whitepapers.

[3] Fujiok A, Okatoma T, Ohta K. A Practical Secret Voting Scheme for Large Scale Elections[C]//Proc. of AUSCRYPT'92. Berlin, Germany: Springer-Verlag, 1993: 244-251.

[4] 袁时金. 普通数字签名算法的研究与改进[D]. 杭州: 浙江工业大学, 2002.

[5] 蔡庆华. 数字签名及其在电子选举中的应用研究[D]. 合肥: 合肥工业大学, 2005.

编辑　张正兴

（上接第 155 页）

的用户列表 *list* 中，则返回“没有该用户信息”，并终止连接；若 $ID \in list$，服务器 S 则生成一个随机数 R_i，并用服务器的私钥 d 对 r_i 进行签名得到 r_i^d，同时用 U 的公钥 e_1 计算 $(R_i \| r_i^d)^{e_1}$ 发送给用户 U。4)用户 U 用自己的私钥 d_1 解密 $(R_i \| r_i^d)^{e_1}$，并用 S 的公钥 (n, e) 解密 r_i^d 得到 r_i，看是否与 U 发送给 S 的随机数 r_i 相同，若不相同则断开与服务器的连接。若相同，则成功验证服务器的身份，生成另一个随机数 r_i'，并计算 $(g(\xi_i), MAC, C, r_i')^e$ 发送给服务器 S。5)服务器 S 解密 $(g(\xi_i), MAC, C, r_i')^e$ 得到 $g(\xi_i)$，检验是否有 $g(\xi_i) \in \boldsymbol{Y}_{i\text{-}1}$，若 $g(\xi_i) \in \boldsymbol{Y}_{i\text{-}1}$ 成立，则认为身份非法，否则，将 $g(\xi_i)$ 记录入登记表 $\boldsymbol{Y}_i = \boldsymbol{Y}_{i\text{-}1} \cup \{g(\xi_i)\}$ 中并进行下一步；S 用私钥 d 解密 $g(\xi_i)$ 得到 ξ_i，然后计算 $\boldsymbol{A}\xi_i$，若 $\boldsymbol{A}\xi_i = \boldsymbol{b}$，则认为身份得到认证并转入下一步，否则，认为身份非法。6)比较 *MAC*，S 先用 $\boldsymbol{b}$ 计算 (ID, C) 的消息认证码 MAC'，若 $MAC' = MAC$，则解密 C 得到 M，否则拒绝。

本方案的形式化描述如下：

$U \to S$： $\{(ID, r_i)^e\}$

$U \leftarrow S$： $\{(R_i \| r_i^d)^{e_1}\}$

$U \to S$： $\{g(\xi_i), MAC, C, r_i'\}^e$

4 结束语

由于文献[1-3]中设计的用户认证协议是一次性的单向认证协议，应用范围也只限于固定终端登录的网络应用系统中，因此本文在 RSA 算法的基础上设计了一种实用有效的一次性口令的双向身份认证协议。客户端和服务器端通过种子密钥鉴别，在防止窃听、重放、假冒、猜测等常用攻击手段的基础上，进一步有效防止了伪服务器攻击，明显增强应用系统的安全性。

参考文献

[1] 刘　丽, 蔡红柳, 王丽丽. 基于非齐次线性方程组的认证协议的研究[J]. 装甲兵工程学院学报, 2005, 19(2): 89-90.

[2] 包小敏, 王晓峰. 两个认证协议的安全缺陷[J]. 装甲兵工程学院学报, 2006, 20(6): 60-62.

[3] 黄宏凝, 王晓峰, 包小敏. 基于非齐次线性方程组的认证协议的改进[J]. 通信技术, 2008, 41(2): 176-178.

编辑　张正兴