第 22 卷 第 1 期 电 子 科 学 学 刊 Vol.22 No.1
2000 年 1 月 JOURNAL OF ELECTRONICS Jan. 2000

基于椭圆曲线密码体制的投票协议 [1]

刘胜利 杨 波 王育民

(西安电子科技大学 ISN 国家重点实验室 西安 710071)

摘 要 本文设计了一种基于椭圆曲线密码体制的投票协议. 该协议的特点是能够使投票者在计算机网络上进行无记名投票, 并可以有效地抵制各种欺骗行为, 从而使安全选举成为可能.

关键词 椭圆曲线密码体制, 投票协议, 安全选举

中图号 TN918.1

1 引 言

随着科学技术的日新月异, 计算机已普及到了各个单位乃至家庭和个人. Internet 网的迅猛发展, 使得 "不出家门而知天下事" 不再是一个梦想, "不出家门而参于天下事" 也已不再是奢望. 一个理想的计算机网络上的投票协议就是要使公民坐在自己家中, 行使自己的民主权力, 投出自己神圣的一票. 理想的协议 [1] 应既能防止欺骗又能保护个人隐私, 它至少应具有如下五个特性: (1) 只有经许可的投票者才能投票; (2) 每个人投票不得超过一次; (3) 任何人都不能确定别人投了谁的票; (4) 没有人能修改其他任何人的选票内容而不被发现; (5) 所有投票者都能确信他们的选票在最后被统计上了.

椭圆曲线密码体制 (ECC) 因其安全性高、密钥量小, 灵活性好等优点, 目前在密码领域有着广阔的应用前景. 本文设计了一个基于 ECC 的投票协议, 使网上选举具有更好的安全性能. 其内容安排如下: 第 2 节介绍投票协议中所用到的一些基本原理; 第 3 节描述投票协议的具体设计; 在第 4 节对所设计的投票协议进行分析; 第 5 节对所有的内容进行总结.

2 基本原理介绍

2.1 一种基于椭圆曲线密码体制的多层加解密的方法

本文基于文献 [2] 中的 Menezes-Vanstone 椭圆曲线密码体制的加解密原理, 提出了一个多层加解密方法.

假设有 n 个实体 $\mathrm{Mix}_i(i=1,2,\cdots,n)$, 每个实体都有定义在 Z_{P_i} ($P_i>3$, 素数) 上的一条椭圆曲线 E_i, E_i 包含有一个循环子群 H_i, 并且在 H_i 上的离散对数问题是难解的. 秘密钥为 d_i, 公开信息有 α_i,β_i,P_i, 其中 $\beta_i=d_i\cdot\alpha_i$ 为公开钥, α_i 为 H_i 的生成元. 明文信息为 $m_j=(m_{j1},m_{j2})$, 是明文空间 $M=Z_p^*\times Z_p^*$ 中的一个点. 设加密者 V_j 要利用 n 个实体 Mix_i 的公开钥进行层层加密, n 个实体 Mix_i 利用自己的秘密钥进行层层解密恢复明文信息. 令 $P\Leftarrow\min_{i=1}^{n}P_i$, 为一素数, 则

(1) 加密过程: 加密者 V_j 生成随机数 k_{jn}, $k_{jn}(\mathrm{mod}P)\neq 0$, 利用 Mix_n 的公开信息 (α_n,β_n,P_n) 加密. 计算 $c_n=k_{jn}\cdot\alpha_n$, $c_n\in E_n$ (用 E_n 代表椭圆曲线上的所有的点构成的集合); $k_{jn}\cdot\beta_n=(w_{n1},w_{n2})$; $c'_n\equiv w_{n1}\cdot m_{j1}(\mathrm{mod}P_n)$; $c''_n\equiv w_{n2}\cdot m_{j2}(\mathrm{mod}P_n)$ 得到密文 $Z_n(m_{j1},m_{j2})=\mathrm{Encrypt}_n((m_{j1},m_{j2})=(c_n,(c'_n,c''_n))$.

[1] 1998-05-12 收到, 1999-01-04 定稿
陕西省自然科学基金资助课题

类似地，加密者 V_j 生成一个随机数 k_{ji}， $k_{ji}(\mathrm{mod}P)\neq 0(i=n-1,n-2,\cdots,1)$，利用 Mix_i 的公开信息 (α_i,β_i,P_i) 加密，得

$$Z_i(m_{j1},m_{j2})=\mathrm{Encrypt}_i(c_{i+1},c_{i+2},\cdots,c_n,(c'_{i+1},c''_{i+1}))=(c_i,c_{i+1},c_{i+2},\cdots,c_n,(c'_i,c''_i)),$$

其中 $c_i=k_{ji}\cdot\alpha_i$； $k_{ji}\cdot\beta_i=(w_{i1},w_{i2})$； $c'_i\equiv w_{i1}\cdot c'_{i+1}(\mathrm{mod}P_i)$； $c''_i\equiv w_{i2}\cdot c''_{i+1}(\mathrm{mod}P_i)$。最后得到 n 重加密信息 $Z_1(m_{j1},m_{j2})=(c_1,c_2,\cdots,c_{n-1},c_n,(c'_1,c''_1))$。

(2) 解密过程：$\mathrm{Mix}_i(i=1,2,\cdots,n)$ 利用自己的秘密钥 d_i 对 $Z_i(m_{j1},m_{j2})=(c_i,c_{i+1},\cdots,c_n,(c'_i,c''_i))$ 进行解密，得

$$Z_{i+1}(m_{j1},m_{j2})=\mathrm{Decrypt}_i(c_i,c_{i+1},\cdots,c_n,(c'_i,c''_i))=(c_{i+1},c_{i+2},\cdots,c_n,(c'_{i+1},c''_{i+1})),$$

其中 $d_i\cdot c_i=(w_{i1},w_{i2})$； $c'_{i+1}\equiv w_{i1}^{-1}c'_i(\mathrm{mod}P_i)$； $c''_{i+1}\equiv w_{i2}^{-1}c''_i(\mathrm{mod}P_i)$。最后从 $Z_n(m_{j1},m_{j2})=(c_n,(c'_n,c''_n))$ 中解得 $\mathrm{Decrypt}_n(c_n,(c'_n,c''_n))=(m_{j1},m_{j2})$。

用此种加密方法，明文空间的每个明文都可以嵌入到椭圆曲线中去。其缺点是有一倍的信息扩展。对于 n 重加密则有 n 倍的信息扩展。因此， n 不能太大，一般取 $1\sim 10$。

2.2 一种基于椭圆曲线密码体制的类 ElGamal 公钥算法 [3]

设定义在有限域 F_p 上的一条椭圆曲线 E， H 是 E 上的一个循环子群， $\alpha\in H$ 是 H 上的一个基点 (生成元)， H 的阶为 $q(q\geq p)$。设用户 A 要向用户 B 发送的明文信息为 m。A 和 B 的秘密钥为 d_A 和 d_B，公开钥分别为 $\beta_A=d_A\cdot\alpha_A$ 和 $\beta_B=d_B\cdot\alpha_B$。

(1) 加密过程：A 首先要将明文信息 m 经过编码嵌入到 E 上 (存在这样的方法，至少存在有一种概率性嵌入方法 [3]) 变为点 P_m，然后产生一个随机数 k，并将消息 $(k\cdot\alpha_B,P_m+k\cdot\beta_B)$ 传送给 B。

(2) 解密过程： B 收到消息后，利用自己的秘密钥 d_B 解出 $P_m=(P_m+k\cdot\beta_B)-d_B\cdot(k\cdot\alpha_B)$。最后通过相应的译码规则从 P_m 中得到明文信息 m。

2.3 一种基于椭圆曲线密码体制的类 ElGamal 数字签名算法 [4]

设定义在有限域 F_p 上的一条椭圆曲线 E(所有假定同 2.2 节)，A 随机选取 $k\in F_q^*$，并计算 $Y_A=k\cdot\alpha_A$。令 $r_1=x(Y_A)(\mathrm{mod}\ q)$，其中 $x(Y_A)$ 表示 Y_A 的横坐标。利用公式 $s\cdot k=m+r_1\cdot d_A(\mathrm{mod}\ q)$ 计算出 s 的值。如果 $x(Y_A)=0$ 或 $s=0$ 则重新选择 k 值。然后将三元组 $(m,(Y_A,s))$ 作为签名消息发送给 B。 B 收到签名消息后，利用 A 的公开信息 (α_A,β_A) 计算 $s\cdot Y_A=m\cdot\alpha_A+r_1\cdot\beta_A$ 是否成立。若成立，则传送无误。

2.4 基于椭圆曲线密码体制的盲签名

当我们想得到签名者对某个文件的签名而又不想让签名者了解文件的内容时，所进行的签名就是盲签名 [1]。设 A 想让 B 对明文 m 进行盲签名，在 2.3 节中所介绍的基于椭圆曲线密码体制的数字签名算法基础上可如下进行：

(1) A 首先产生一个随机数 r 作为盲因子，并得到 r^{-1}，其中 $r\cdot r^{-1}\equiv 1(\mathrm{mod}\ q)$。对明文 m 用盲因子 r (模 q 后的值) 进行隐蔽处理得到 $r\cdot m$，送给 B。

(2) B 对 $r\cdot m$ 进行数字签名得到 $S_B(r\cdot m)=(r\cdot m,(Y_B,s'))$ 传送给 A，其中 $s'\cdot k=(r\cdot s)\cdot k=r\cdot m+r\cdot r_1\cdot d_B(\mathrm{mod}\ q)$ 成立。

(3) A 得到经 B 签名的消息 $S_B(r\cdot m)$ 后，验证 $s'\cdot Y_B=r\cdot m\cdot\alpha_B+r\cdot r_1\cdot\beta_B$ 成立后，进行解盲运算得到 B 对 P_m 的签名 $S_B(m)$，其中

$$S_B(m)=r^{-1}\cdot S_B(r\cdot m)=(r^{-1}\cdot r\cdot m,(Y_B(r^{-1}\cdot s')))=(m,(Y_B,s)).$$

3 投票协议的设计

3.1 环境设定

(1) 投票者 $V_j(j=1,2,\cdots,h$ 即有 h 个投票者)；(2) 认证中心 A：对投票者所投的票进行认证，确保只有合法的投票者才能进行投票，并且任何人都不能投一次以上的票．要求认证中心只能对投票者所投的票进行认证而无权了解投票内容；(3) 网络中心 Mix：有 n 个子中心 $\mathrm{Mix}_i(i=1,2,\cdots,n)$，收集投票者所投的加密票 (票匿名) 进行层层解密，并将匿名票列表公布，使投票者可以检查自己的票是否正确公布．在审议无异议后，将匿名票送统计中心；(4) 统计中心 T：对网络中心送来的匿名票进行统计，得出投票结果；(5) 监督中心 1：有多个相互独立的监督子中心构成．对各网络子中心进行监督，以防止网络中心有欺骗行为；(6) 监督中心 2：由多个相互独立的监督子中心构成．对统计中心 T 进行监督，以防止统计中心进行欺骗；(7) 公告板：公布一些可以公开的信息．

投票协议中的一些实体及相关信息的符号表示如表 1．

表 1 投票协议中的一些实体及相关信息的符号表示

	公开信息	秘密信息	签名表示
投票者 $j=1,2,\cdots,h$	识别号 ID_{V_j} 公开钥 e_{V_j}	秘密钥 d_{V_j}	S_{V_j}
认证中心 A	识别号 ID_A 公开钥 e_A	秘密钥 d_A	S_A
网络子中心 Mix_i $i=1,2,\cdots,n$	识别号 ID_{Mix_i} 公开钥 β_i 公开信息有 α_i 和 N_i	秘密钥 d_i	S_{Mix_i}
统计中心 T	公开钥 β_T 公开信息有 α_T	秘密钥 d_T	S_T

3.2 协议的设计

步骤 1 预处理

(1) 各网络子中心 $\mathrm{Mix}_i(i=1,2,\cdots,n)$ 生成自己的秘密密钥 d_i，采用 Shamir 的秘密共享门限方案 [5] 生成 t_1 个子秘密钥，分发给监督中心 1 的 t_1 个独立部门．

(2) 监督中心 1 验证网络中心所分配的子秘密钥的正当性，防网络中心欺骗．

(3) 同样，统计中心生成自己的秘密密钥 d_T，并采用 Shamir 的秘密共享门限方案生成 t_2 个子秘密钥，分发给监督中心 2 的 t_2 个独立部门．

(4) 监督中心 2 验证统计中心分配其子秘密钥的正当性，防统计中心欺骗．

步骤 2 投票者生成投票内容

(1) 投票者 V_j 生成投票内容．

(2) 生成一个随机数 R'_j，用统计中心 T 的公开钥 $\beta_T=d_T\cdot\alpha_T$ 对投票内容 m_j 进行加密，得到加密后的投票内容 $M_j=(R'_j\cdot\alpha_T)\|(P_{m_j}+R'_j\cdot\beta_T)$，其中 P_{m_j} 是投票内容 m_j 编码后得到的椭圆曲线上的点．在此用到的是椭圆曲线密码体制上的类 ElGamal 公开密钥加密算法．

步骤 3 投票者将所生成的加密后的票 M_j 送认证中心 A 得到认证中心的盲签名

(1) 在票 M_j 的尾部连接上认证中心的识别号 ID_A，得到 $X_j=M_j\|ID_A$．

(2) 投票者 V_j 生成一个随机数 R''_j，在乘积 $R''_j\cdot X_j$ 上附加自己的数字签名和识别号 ID_{V_j}，得到 $ID_{V_j}\|S_{V_j}(R''_j\cdot X_j)\|(R''_j\cdot X_j)$ 送到认证中心．

(3) 认证中心 A 有合法投票者的名单，若非合法者则不对其进行签名．对于合法的投票者，则检查数据库，看该投票者是否已经提交过选票，若是，则不对其签名；若否，则对其进行数字签名并将该投票者的识别号登录于数据库中．签名时首先用投票者的公开钥确认确实是对应于 ID_{V_j} 的投票者 V_j 送来的消息而未被窜改，或者不是其他人盗用 ID_{V_j} 冒充投票者 V_j 来取得认证，即计算 $E_{V_j}(S_{V_j}(R''_j \cdot X_j)) = (R''_j \cdot X_j)$ ？否，消息已被窜改或是他人冒充投票者 V_j，认证中心 A 不对其消息进行签名；是，投票者 V_j 的消息传递正确，认证中心对所得到的消息进行盲签名得到 $S_A(R''_j \cdot X_j)$ 返回给投票者 V_j．

(4) 投票者 V_j 从 $S_A(R''_j \cdot X_j)$ 中去掉随机数 R''_j，得到认证中心只对 X_j 的数字签名 $S_A(X_j)$，令 $W_j = S_A(X_j)$．

步骤 4　投票者将生成的投票内容匿名投给网络中心

(1) 投票者 V_j 生成一个随机数 R_j 作为匿名，R_j 要足够大以避免与别的投票者重复．V_j 为了向网络中心输入 W_j 和 R_j 而生成输入报文 $Z_{j,1}(W_j, R_j) = \mathrm{Encrypt}_1(\mathrm{Encrypt}_2(\cdots(\mathrm{Encrypt}_n(W_j, R_j))\cdots))$，即投票者 V_j 对 W_j 和 R_j 用各网络子中心的公开钥进行基于 ECC 上的层层加密．

(2) 投票者 V_j 对 $Z_{j,1}(W_j, R_j)$ 附加上自己的数字签名，并将自己的识别号 ID_{V_j} 连接在前面，得到 $ID_{V_j} \| S_{V_j}(Z_{j,1}(W_j, R_j)) \| Z_{j,1}(W_j, R_j)$ 送到公告板．

(3) 截止投票．

(4) 网络中心将输入报文 $Z_{j,1}(W_j, R_j)$ 依次解密得到 W_j 和 R_j，送公告板公开．

(a) 网络子中心 Mix_1 解密 $Z_{j,1}(W_j, R_j)$ 得到 $Z_{j,2}(W_j, R_j) = \mathrm{Encrypt}_2(\mathrm{Encrypt}_3(\cdots(\mathrm{Encrypt}_n(W_j, R_j))\cdots))$．然后 Mix_1 对其进行数字签名，并连接上自己的识别号，得到 $ID_{\mathrm{Mix}_1} \| S_{\mathrm{Mix}_1}(Z_{j,2}(W_j, R_j)) \| Z_{j,2}(W_j, R_j)$ 送到公告板公开．

(b) 同样地，网络子中心 $\mathrm{Mix}_i (i = 2, 3, \cdots, n-1)$ 将 $Z_{j,i}(W_j, R_j)$ 解密得到 $Z_{j,i+1}(W_j, R_j)$．然后 Mix_i 对其进行数字签名，并连接上自己的识别号，得到

$ID_{\mathrm{Mix}_i} \| S_{\mathrm{Mix}_i}(Z_{j,i+1}(W_j, R_j)) \| Z_{j,i+1}(W_j, R_j)$ 送到公告板公开．

(c) 网络子中心 Mix_n 由 $Z_{j,n}(W_j, R_j)$ 解密得到 R_j 和 W_j．

步骤 5　审议和公布

(1) 用认证中心 A 的加密函数 E_A 求得 $E_A(W_j) = E_A(S_A(X_j)) = X_j = M_j \| ID_A$．确认有无认证中心的数字签名 (确认有无认证中心的识别号 ID_A)．无认证中心的数字签名的票有两种情况：一是投票者没有得到认证中心的认证，即投票者不合法；另一种情况是投票者是合法的，但是由于某个网络子中心在解密过程中进行了欺骗．如果有认证中心的数字签名，则从 X_j 中去掉认证中心的识别号 ID_A，得到 M_j，并将 M_j 与相应的 R_j 在公告板上公布．

(2) 审议各网络子中心．若没有认证中心的签名，则首先跟踪从 Mix_n 到 Mix_1 的各网络子中心．对所得到的 (W_j, R_j) 用各网络子中心的公开钥依次进行层层加密并检查与公开 $Z_{j,i}(W_j, R_j)$ 是否一致，若在某个环节上不一致，则相应的那个网络子中心 Mix_i 有欺骗行为，去掉该网络子中心 Mix_i，用监督中心 1 的各部门的分散子秘密钥恢复 Mix_i 的秘密钥．并用恢复的秘密钥重新解密，然后返回步骤 5 的第 (1) 步．若各网络子中心 Mix_i 所公布的 $Z_{j,i}(W_j, R_j)$ 都是正确的，则认为投票者没有得到认证中心的认证，即投票者不合法，将没有认证中心签名的票取消．

(3) 投票者从公布的 R_j 和 M_j 列表中找到自己的随机数 R_j 和相应的 M_j，确认 R_j 和 M_j 是否正确公布了．若没有正确公布就将票 M_j 与其持有的 R_j 提出异议．投票者提出异议

有两种情况：一种是投票者对 M_j 的加密票 $Z_{j,i}(W_j, R_j)$ 没有得到某个或某几个网络子中心的正确解密，即有网络子中心进行了欺骗；另一种情况是投票者无理取闹. 类似第 (2) 步，检验是提出异议的投票者无理取闹还是网络子中心有欺骗行为. 去掉有欺骗行为的网络子中心，用监督中心相应的分散子秘密钥重新解密后公开，然后返回步骤 5 的第 (1) 步.

步骤 6 统计票

(1) 统计中心 T 将自己的秘密钥 d_T 公开.

(2) 监督中心 2 对统计中心所公布的秘密钥 d_T 进行检查，如果统计中心没有正确公布，则监督中心 2 将自己各部门的相应的分散子密钥恢复秘密钥 d_T 并公开.

(3) 用公开的秘密钥 d_T ，从票文 $M_j = (R'_j \cdot \alpha_T) \| (P_{m_j} + R'_j \cdot \beta_T)$ 中解密出 $P_{m_j} = (P_{m_j} + R'_j \cdot \beta_T) - (R'_j \cdot \alpha_T) \cdot d_T$ 后对 P_{m_j} 进行译码恢复出投票内容 m_j .

(4) 去掉有不合理内容的票只统计正确的票.

4 投票协议的分析

该协议中有三个相互独立的部门和两个监督部门：认证中心、网络中心、统计中心、监督中心 1 和监督中心 2 ，可以有效地防止权力过分集中而可能导致的欺骗行为.

认证中心保存有合法投票者的清单，非法投票者不可能得到认证中心的认证. 任何人想投票必须得到认证中心的认证，如果某人想不经认证中心的认证就投出选票，选票则在步骤 5 的第 (1) 步不能通过审议而被摒弃. 这就保证了只有合法的投票者才能投票.

认证中心对所有经其签名认证过的投票者进行登记，可以确保每个合法投票者只投一次票. 任何已被签名认证过的投票者想再得到一张经认证中心认证的票都是不可能的，因为认证中心在步骤 3 的第 (3) 步会发现数据库里已有投票者的名字了，所以不再对其进行签名认证.

任何人都不能窜改投票者的消息或者冒充某投票者的名字发投票信息，这一点由投票者对其要发的消息进行数字签名来保证. 因为其他人不知道投票者的秘密钥因而不能冒充投票者对所发消息进行数字签名. 收方用投票者的公开钥对收到的消息解签名，可以验证所传消息是否被窜改或是冒充.

任何人都不能确定别人的投票内容. 认证中心对投票者的投票内容进行的是盲签名，因此，虽然知道投票者的名字却不知道相应的投票内容；投票者秘密地产生一个能够识别自己的随机号码，投票者将自己的投票内容和随机号码层层加密后送网络中心解密. 网络子中心 1 知道发送消息的相应投票者，但不知道真正投票内容，因为经它解密后投票消息还有 $n-1$ 重加密. 网络子中心 2 收到网络子中心 1 发的解密消息后，经解密后已经不知收到的加密消息所对应的投票者. 只有当网络子中心 1 和 2 相互勾结时，才能确定经两者解密后的投票消息相对应的投票者，但还是不知道投票内容，因为投票内容还有 $n-2$ 重加密. 仅网络子中心 n 最终解密得到投票内容，但是要想知道相应的投票者的名字则需要所有的 n 个网络子中心的合作，而这一般是不可能的.

任何合法投票者都可以确信他的票被统计上，因为在统计票之前，所有经网络中心解密的合法投票消息都将公布出来. 如果投票者发现自己的票被遗漏或没有正确地公布则可以在步骤 5 的第 (3) 步中提出异议，最终得以正确公布.

由于各网络子中心有监督中心 1 对它们进行监督，所以各网络子中心都不能进行欺骗. 一旦有欺骗行为，则在步骤 5 审议时监督中心 1 会将其查出，并用分散的子密钥恢复相应的秘密钥，代替网络子中心进行解密.

统计中心有监督中心 2 对其进行监督，因而在对所公布的投票内容进行解密时，难以有欺骗行为.

5 结 束 语

本文所介绍的投票协议中加解密和数字签名都是基于椭圆曲线密码体制上的，因此能在保证速度的同时，大大压缩密钥量而且还提供良好的安全性．但是椭圆曲线密码体制本身还有许多尚未解决的问题：例如，寻找明文嵌入的高效算法，确定椭圆曲线上点加群的阶的有效算法等．这些问题都有待于进一步研究．

与现有的其它投票协议[1]相比，本文所设计的投票协议能够有效地实现投票者匿名并可以防止各种欺骗．但是，其中统计中心的作用似乎不大。一种更有效的方法是将投票者将其投票内容分割成多份，分别加密、认证，由网络中心层层解密后送多个统计子中心分别统计．这样的协议更加有效而可靠，但是更加复杂而且还有许多问题需要解决．所以，如何设计简单、有效、安全而可靠的投票协议仍是一个值得研究的课题．

参 考 文 献

[1] Schneier B. Applied Cryptography, New York: John Wiley & Sons, Inc., 1994: 125-137.
[2] Stinson D R. Cryptography Theory and Practice, CRC Press, Inc., 1995: 177-190.
[3] Koblitz N. A Course in Number Theory and Cryptography, Beijing: Springer-Verlag World Publish Corp, 1990, 150-169.
[4] Miyaji A. A Message Recovery Signature Scheme Equivalent to DSA over Elliptic Curves, In K. Kim, T. Matusmoto (Eds.), Advances in Cryptology-ASIACRYPT'96(Lecture Notes in Computer Science), Berlin: Springer-Verlag, 1996, 1-14.
[5] Desmedt Y, Frakel Y. Threshold Cryptosystems, In G. Brassard, editor, Advances in Cryptology, Proc. of Crypto' 89(Lecture Notes in Computer Science 435), Berlin: Springer-Verlag, 1990, 307-315.

A VOTING PROTOCOL BASED ON ELLIPTIC CURVE CRYPTOSYSTEMS

Liu Shengli　Yang Bo　Wang Yumin

(*National Key Lab. on ISN, Xidian University, Xi'an* 710071)

Abstract　A voting protocol is designed based on elliptic curve cryptosystems. This protocol enables each anonymous voter to vote on computer network, defends any cheat and makes secure elections possible.

Key words　Elliptic curve cryptosystems, Voting protocol, Secure elections

刘胜利：女，1974 年生，博士生，密码学专业，研究方向为通信网的安全保密．
杨　波：男，1963 年生，博士，副教授，研究方向为通信网的安全保密．
王育民：女，1936 年生，教授，博士生导师，长期从事信息论、信道编码、密码学以及通信网的安全等方面的研究．