文章编号: 1001-0920(2006)01-0107-04

非交互式可公开认证的电子选举策略

刘 媛, 刘粉林, 张利民
(信息工程大学 信息工程学院, 郑州 450002)

摘 要: 基于椭圆曲线上离散对数的难解问题提出了一种非交互式公开可认证协议, 设计了非交互式零知识证明协议, 用这两个协议作为基本工具构造出一个简单且有效的非交互式公开可认证的电子选举策略, 任何人对投票者和计票者的数据都能进行认证. 该策略可防欺诈, 适用于小规模的网络选举

关键词: 非交互; 电子选举; 椭圆曲线加密; 公开认证; 零知识证明
中图分类号: TN918.4 **文献标识码**: A

A Non-interactive Publicly Verifiable Electronic Voting Scheme

LIU Yuan, LIU Fen-lin, ZHANG Li-min
(Information Engineering Institute, Information Engineering University, Zhengzhou 450002, China. Correspondent: LIU Yuan, E-mail: liuyuan65@163.com)

Abstract: A non-interactive publicly verifiable protocol based on the intractable problems of discrete logarithm in elliptic curves cryptography is proposed. A non-interactive publicly verifiable zero knowledge proof protocol is designed. A new non-interactive publicly verifiable electronic voting scheme is established. This scheme enables anybody to verify if the shares are correctly distributed. This scheme can protect against the cheating action and is applicable to elections of smaller scale.

Key words: Non-interactive; Electronic voting; Elliptic curves cryptograph (ECC); Publicly verifiable; Zero knowledge proof

1 引 言

一个安全、公正的电子选举必须具有合法性、隐私性、不可重复性、完整性、公平性、正确性、可认证性、强固性等特性, 密码学的应用保证了电子选举的这些性质, 使其得以安全的在网络中进行. 文献[1~3]只针对选举的某一方面性质进行了研究, 不能同时满足电子选举的这8个性质, 特别是可公开认证性[4], 即指任何人(包括旁观的第3者), 皆可以认证选举投票是否为公平的、公正的. 即公开认证所有投票者投出的选票是否有效、合法(虽然无法得知其所投的内容为何); 公开认证计票是否公正(即只有合法的选票才会被计入总票数, 且一定会被加入). 对此特性还没有多少文献涉及, 可公开认证已成为公正的电子选举的必要保证, 是网络电子选举发展的迫切需要.

本文基于椭圆曲线上离散对数难解问题, 给出了一个非交互式可公开认证(PVSS)协议和一个非交互式零知识证明协议, 用这两个协议作为基本工具构造出了一个简单且有效的非交互式可公开认证的、可广播的电子选举策略, 该策略的一个重要特性就是任何人皆可认证所有投票者所投出的选票是否正确, 可认证计票是否为公正. 该策略适用于小规模的网络选举.

2 具体策略

2.1 非交互式可公开认证协议

作为一个非交互可公开认证协议(PVSS)[5], 它

收稿日期: 2004-11-03; **修回日期**: 2005-03-28.
基金项目: 国家自然科学基金项目(60374004); 河南省高校杰出科研人才创新工程项目(HAIPURT2001KYCX008); 河南省杰出青年基金项目(0412000200).
作者简介: 刘媛(1965—), 女, 江西抚州人, 博士, 从事信息安全的研究; 张利民(1952—), 男, 哈尔滨人, 教授, 博士生导师, 从事密码学等研究.

的一个重要的特色是证明者和认证者之间不需要秘密传送数据, 所有的数据都是用公开密钥加密后由公共信道传送的; 且初始化时, 也不需要证明者和认证者之间相互交互, 只要有认证者注册的公开密钥即可, 认证者可以不在线. 下面给出一个非交互可公开认证协议, 记为 ECEQ (G_1, Q_1, G_2, Q_2):

系统初始化: 选取一个大素数 p 和 Z_p 上的一条椭圆曲线 E, 并且 $|E(Z_p)| = q$, q 是一个素数, $q > 2^{160}$ 且 $q > 4\sqrt{p}$. 选取一个安全的强 hash 函数 H_d: $\{0,1\}^* \to \{0,1\}^d$. 选取 E 上的点 G_1, G_2. 公开 q, H_d, G_1, G_2.

证明者 P 的密钥生成: 证明者 P 选取自己的私钥 $a \in Z_q$, 计算 $Q_1 = aG_1, Q_2 = aG_2$. 公开 $G_i, Q_i (i = 1, 2)$, 私钥 a 保密.

证明者 P 要向认证者证明其拥有密钥 $a \in Z_q$, 认证步骤如下:

1) 对于 $v = 1, \cdots, d$, 证明者 P 随机选取 $\omega_v \in Z_q$, 计算并公开 $R_{1v} = \omega_v G_1, R_{2v} = \omega_v G_2$. 计算

$$R = (r_1, r_2, \cdots, r_d) = (\omega_1 - ac_1, \omega_2 - ac_2, \cdots, \omega_d - ac_d).$$

其中 c_v 为 c 的第 v 比特位, 公开 (R, c).

$$c = H_d(R_x(Q_1) \| R_x(Q_2) \| R_x(R_{11}) \| R_x(R_{21}) \| \cdots \| R_x(R_{1d}) \| R_x(R_{2d})).$$

这里: 记号 $(\cdot \| \cdot)$ 是两个比特串连接, $R_x(A)$ 是表示取 A 点的 x 坐标.

2) 对于 $v = 1, \cdots, d$, 认证者 V 检验 $R_{1v} = r_v G_1 + c_v Q_1, R_{2v} = r_v G_2 + c_v Q_2$, 并检验 c 是否相等.

2.2 非交互零知识证明协议

所谓零知识证明[6], 是指证明者向认证者证明某个论断是正确的, 同时在证明过程中不暴露证明方任何其他信息. 本文给出了一个非交互式零知识证明协议, 简记为 ECDEQ (G_1, U, G_2, Q).

系统初始化同上.

证明者的密钥生成: 证明者 P 选取自己的私钥 $s \in Z_q$, 计算 $Q = sG_2, U = (s + v)G_1$. 私钥 $s, s + v$ 保密. 公开 $G_i (i = 1, 2), Q, U$.

证明者 P 欲向认证者 V 证明他的 U 中存在 $v \in \{0, 1\}$ 这个信息, 认证步骤如下:

1) 对于 $i = 1, \cdots, d$, 证明者 P 随机选取 $w_i, r_{1-v,i}, d_{1-v,i} \in Z_q$, 计算并公开

$$A_{v,i} = w_i G_1, B_{v,i} = w_i G_2,$$

$$A_{1-v,i} = r_{1-v,i} G_2 + d_{1-v,i} Q,$$

$$B_{1-v,i} = r_{1-v,i} G_1 + d_{1-v,i}(U - (1 - v)G_1).$$

然后计算

$$D = (d_{v,1}, d_{v,2}, \cdots, d_{v,d}) = (c_1 - d_{1-v,1}, \cdots, c_d - d_{1-v,d}),$$

$$R = (r_{v,1}, r_{v,2}, \cdots, r_{v,d}) = (w_1 - sd_{v,1}, \cdots, w_d - sd_{v,d}).$$

其中 c_i 为

$$c = H_d(R_x(Q) \| R_x(U) \| R_x(R_{11}) \| R_x(R_{21}) \| \cdots \| R_x(R_{1d}) \| R_x(R_{2d}))$$

的第 i 比特位, 公开 (D, R, c).

2) 对于 $i = 1, \cdots, d$, 认证者 V 检验 $c_i = d_{0,i} + d_{1,i}$, $A_{1,i} = r_{1,i} G_2 + d_{1,i} Q$, $A_{0,i} = r_{0,i} G_2 + d_{0,i} Q$, $B_{0,i} = r_{0,i} G_1 + d_{0,i} U$, $B_{1,i} = r_{1,i} G_1 + d_{1,i}(U - G_1)$ 成立与否, 并检验 c 是否相等.

2.3 非交互式可公开认证的电子选举策略

可广播的电子选举模式[7], 要求系统里的参与者宣告他们的信息. 参与者由一个计票集合 $(A_1, \cdots, A_n)$, 一个投票集合 $(V_1, \cdots, V_n)$ 和一个监督集合组成, 这些集合是可交的, 参与者可以既是投票者同时也是计票者. 一般的电子选举分两个过程. 第 1 过程: 投票者将自己的选票加密, 然后投上他们的选票并广播. 由于该系统中投票者不是匿名的, 所以很容易防止双重投票, 仅仅合法且有效的投票才被接受. 第 2 过程: 计票者使用自己的私钥解密, 共同计算出所有合法投票的票数. 本文电子选举策略为:

1) 初始化. 首先每个计票者 A_i 用公钥密码算法 E_i 登记注册了一个公开密钥, 即参加可公开认证电子选举协议的授权计票者必须是注册登记了的, 设为 $A_1, A_2, \cdots, A_n$.

2) 投票协议.

① 分配碎片: 投票者投票 v 并计算要分配给计票者 A_i 的碎片 s_i, $i = 1, \cdots, n$, 零知识证明自己投入了正确的选票. 投票者广播用计票者 A_i 公开密钥嵌入了的碎片 $E_i(s_i)$, 也广播 $E_i(s_i)$ 的认证策略, 可让人认证其中含有密钥 s, 且保证能重构出嵌入后密钥 S 的同样数值.

② 碎片的认证: 任何认证者都能用非交互式认证策略认证加密后碎片的正确性, 不正确则抱怨和拒绝, 如果抱怨超过一定的数目则可认定投票者作假.

3) 计票协议.

① 解密碎片: 每个通过认证策略的计票者 A_i 用自己注册的公钥所对应的私钥从 $E_i(s_i)$ 解出嵌入后的碎片 S_i. 计票者广播碎片 S_i, 也广播 S_i 的认证方案, 以供人认证 S_i 是正确的.

② 恢复密钥: 经过认证后, 除去不正确的碎片, 一定数目的正确碎片集合在一起恢复出嵌入后的密钥 S.

③ 计算票数:

具体算法如下: 设计票集合$A = (A_1, \cdots, A_n)$, 投票集合$V = (V_1, \cdots, V_m)$, $ID_i \in Z_q$ 为V_i 的身份公开识别号.

系统初始化: 与上相同

参与者的密钥生成: 每个计票者$A_i (i = 1, \cdots, n)$ 随机选取私钥$k_i \in Z_q$, 注册$X_i = k_i G_1$ 作为自己的公开密钥

投票:

1) 投票者$V_i (i = 1, \cdots, m)$ 投入选票$v \in \{0, 1\}$ 和随机选取一个私钥s_i, 计算并公开$Q = s_i G_2, U = (s_i + v) G_1$.

2) 投票者$V_i (i = 1, \cdots, m)$ 随机选取一个Z_q 上的$l - 1$ 次多项式$f_i(x) = \sum_{k=0}^{l-1} a_{ik} x^k \pmod p$, 其中$s_i = a_{i0}$ 为V_i 的私钥, 分发者对多项式保密, 计算并公开$C_{ik} = a_{ik} G_2 (0 \leq k \leq l - 1)$, 保密$a_{ik}$.

3) 投票者V_i 对$s_{ij} = f_i(ID_j), j = 1, \cdots, n$, 用$A_j (j = 1, \cdots, n)$ 的公开密钥进行碎片嵌入, 得$Y_{ij} = s_{ij} X_j, 1 \leq j \leq n$, 公开$Y_{ij}$, 保密$s_{ij}$.

4) 对参数$s_{ij} (j = 1, \cdots, n)$, 投票者$V_i$ 随机选取$\omega_{jv} \in Z_q, v = 1, \cdots, d$, 并计算

$$R_{ijv} = \omega_{jv} X_i,\ R_{2jv} = \omega_{jv} G_2,$$

$$R_{ij} = (r_{ij1}, r_{ij2}, \cdots, r_{ijd}) = (\omega_{j1} - s_{ij} c_{i1}, \omega_2 - s_{ij} c_{i2}, \cdots, \omega_d - s_{ij} c_{id}),$$

$$c_{ij} = H_d(R_x(Z_{i1}) \| R_x(Y_{i1}) \| \cdots \| R_x(Z_{in}) \| R_x(Y_{in}) \| R_x(R_{ij1}) \| R_x(R_{2j1}) \| \cdots \| R_x(R_{ijd}) \| R_x(R_{2jd})),$$

其中$Z_{ij} = \sum_{k=0}^{l-1} ID_j^k C_{ik}$, c_{ijv} 为c_{ij} 的第v 比特位. 公开$R_{ijv}, R_{2jv}, c_{ij}, R_{ij}$. 保密$\omega_{jv}$.

认证者认证投票者分配碎片的正确性:

1) 认证者首先用 ECDEQ (G_1, U, G_2, Q) 协议认证V_i 投了正确的票v. 如果认证正确则计入选票进行下一步, 否则选票作废, 以下步骤不进行.

2) 认证者用 ECEQ $(G_2, Z_{ij}, X_j, Y_{ij})$ 认证协议认证投票者分发碎片的正确性

解出碎片:

1) 计票者A_i 用自己的私钥k_i 解出嵌入的碎片$S_{ij} = k_j^{-1} Y_{ij} \pmod p = s_{ij} G_1$, 广播$S_{ij}$, 保密$k_j$.

2) 计票者随机选取$\tilde{\omega}_{jv} \in Z_q, v = 1, \cdots, d$ 并计算

$$\tilde{R}_{ijv} = \tilde{\omega}_{jv} S_{ij},\ \tilde{R}_{1jv} = \tilde{\omega}_{jv} G_1,$$

$$\tilde{c}_{ij} = H_d(R_x(X_1) \| R_x(Y_{1i}) \| \cdots \| R_x(X_n) \| R_x(Y_{in}) \| R_x(\tilde{R}_{ij1}) \| R_x(\tilde{R}_{1j1}) \| \cdots \| R_x(\tilde{R}_{ijd}) \| R_x(\tilde{R}_{1jd})),$$

$$\tilde{R}_{ij} = (\tilde{r}_{ij1}, \tilde{r}_{ij2}, \cdots, \tilde{r}_{ijd}) = (\tilde{\omega}_{j1} - k_j \tilde{c}_{ij1}, \tilde{\omega}_{j2} - k_j \tilde{c}_{ij2}, \cdots, \tilde{\omega}_{jd} - k_j \tilde{c}_{ijd}).$$

公开$\tilde{R}_{ijv}, \tilde{R}_{1jv}, \tilde{c}_{ij}, \tilde{R}_{ij}$.

认证者进行认证: 认证者用 ECEQ $(G_1, X_j, S_{ij}, Y_{ij})$ 认证协议认证计票者A_j 的身份和其广播的数据的正确性

统计选票:

1) 恢复密钥: l 个计票者A_i 给出的数据$S_i (i = 1, \cdots, l)$ 通过认证其正确性后, 密钥sG_1 可由 Lagrange 插值公式获得, 即

$$sG_1 = \sum_{i=1}^{l} \lambda_i S_i,$$

其中$\lambda_i = \prod_{j \neq i} \frac{j}{j - i}$ 是 Lagrange 系数

2) 计算票数: 计票者计算

$$\sum_{j=1}^{m} S_j = G_1 \sum_{j=1}^{m} p_j(0) = G_1 \sum_{j=1}^{m} s_j,$$

$$\sum_{j=1}^{m} U_j = G_1 \sum_{j=1}^{m} (s_j + v_j),$$

则可获得$G_1 \sum_{j=1}^{m} v_j$, 得到有效的选票数

定理 1　每个认证者V 都能利用 ECEQ (G_1, Q_1, G_2, Q_2) 或 ECDEQ (G_1, U, G_2, Q) 协议, 检验等式成立与否来认证证明者P 的合法身份或某个论断的正确性

定理 2　l 个合格的计票者才能用 Lagrange 插值公式恢复出密钥, 少于l 个计票者得不到密钥

定理3　加密策略是同态的, 即$E_i(s_i) + E_i(s_i') = E_i(s_i + s_i')$, 所以可用于电子选举

证明略

3　性能分析

1) 安全性　此策略的所有通信都不需要使用安全的秘密通道, 可在公共信道上进行, 从而提高了系统的安全性. 而投票者和计票者之间发送的信息可以在不泄漏秘密的情况下向第 3 方证明秘密的有效性, 所有的数据都是在处理后由公共通道传送的, 且是安全的.

2) 可公开认证性　此策略可以让任何验证者通过两个非交互的可公开认证协议, 公开认证投票者投入了有效的选票以及传送数据的正确性, 它防止了非法者的破坏; 任何人也可通过 ECEQ (G_1, Q_1, G_2, Q_2) 认证计票者的合法身份以及解密数据的正确性, 可防止非法成员的参与和欺骗

3) 不可伪造性　只有l(或多于l) 个诚实的计票者联合才能恢复出密钥, 任何人或少于l 个参与者是无法生成一个有效的密钥, 且得不到密钥的任何信息. 因为若计票者是诚实的, 由$S_i = k_i^{-1} Y_i \pmod$

p) 可得 $f(ID_i)G_1$, 从而用 Lagrange 插值公式恢复出密钥, 才能计算出票数. 而求解 $f(ID_i)G_1$ 时需用到参与者的私钥 k_i, 用公钥 $X_i = k_iG_1$ 计算 k_i 是求解椭圆曲线上离散对数难解问题, 是困难的.

4) 隐私性. 验证者认证投票者的投票有效, 使用的是非交互公开可认证的零知识证明协议 ECDEQ (G_1, U, G_2, Q), 认证时没泄露出 v 的任何信息. 投票者既可让人认证自己投入了有效的选票, 又不必泄露自己投了谁的票, 保护了隐私.

5) 不可重复性. 用了投票者的公开身份识别号作为 x 值, 可进行认证以防止投票者重复投票.

6) 不可抵赖性. 投票者和计票者都不可否认自己的身份, 只有他们自己才有私钥能算出碎片及密钥.

7) 重复使用性. 此策略参与者 A_i 不需要知道 $f(ID_i)$ 的值, 只要知道相关的 $S_i = f(ID_i)G_1$ 便可重新恢复出密钥 sG_1, 而 s 并没有泄露, 同时参与者 A_i 也不要公开他的私钥 k_i. 所以密钥 s 和参与者的私钥可以同时用在几个不同的选举中, 有利于密钥的复制和更新.

8) 此策略进行的解密、加密、认证都是椭圆曲线上的加减法运算, 运算速度快. 计票者的密钥位数短, 存贮量小: 长度为 160 bit 的素数 p 即可(相当于大数分解 RSA 中长度为 1 024 bit 素数的难度). 因而此策略速度快、安全性能高、方便简洁.

4 结 语

本文基于椭圆曲线上难解问题, 构造出了一个新的非交互可公开认证的电子选举策略, 该策略的一个特点就是任何人皆可认证所有投票者所投出的选票是否为正确(选票是否有效但无法得知其所投的内容为何), 任何人皆可认证计票是否公正(只有合法的选票才会被加入到最后的总票数内, 且一定会被加入). 也解决了计票人权力过于集中的问题, 还能对计票人的身份和数据进行公开认证, 防止了计票人的欺诈行为. 另外, 在投票中随时认证将非法选票去除, 降低了存贮量. 该方案适用于重要的、小型的电子选举, 有一定的实用价值.

参考文献(References)

[1] Benaloh J, Tuinstra D. Receipt-free Secret-ballot Elections [A]. *Proc of the Twenty-sixth Annual ACM Symposium on Theory of Computing* [C]. Montreal, Quebec, 1994: 544-553.

[2] Jan J K, Chen Y Y, Lin Y. The Design of Protocol for e-Voting on the Internet [A]. *Proc of IEEE 35th International Carnahan Conference on Security Technology* [C]. London, 2001: 180-189.

[3] Ku W C, Wang S D. A Secure and Practical Electronic Voting Scheme [J]. *Computer Communications*, 1999, 22(3): 279-286.

[4] Pedersen T P. Non-interactive and Information-theoretic Secure Verifiable Secret Sharing [A]. *Lecture Notes in Computer Science* [C]. Berlin: Springer-Verlag, 1992, 576: 129-140.

[5] Chaum D, Pedersen T P. Wallet Databases with Observers [A]. *Lecture Notes in Computer Science* [C]. Berlin, 1993: 740: 89-105.

[6] Blum M, De Santis A, Micali S, et al. Non-interactive Zero-knowledge Proof Systems [J]. *SIAM J on Computing*, 1991, 20(6): 1084-1118.

[7] Benaloh J, Yung M. Distributing the Power of a Government to Enhance the Privacy of Voters [A]. *Proc of 5th ACM Symposium on Principles of Distributed Computing* [C]. New York, 1986: 52-62.

(上接第 106 页)

[2] Mullhaupt P, Srinivasan B, Bonvin D. Analysis of Exclusively Kinetic Two-link Underactuated Mechanical Systems [J]. *Automatica*, 2002, 38(3): 1565-1573.

[3] Ho-Hoon Lee. Modeling and Control of a Three-dimensional Overhead Crane [J]. *J of Dynamic Systems Measurement and Control*, 1998, 120(4): 471-476.

[4] Fang Y, Dixon W E, Dawson D M, et al. Nonlinear Coupling Control Laws for an Underactuated Overhead Crane System [J]. *IEEE/ASME Trans on Mechatronics*, 2003, 8(3): 418-423.

[5] Yabuno H, Goto K, Aoshima N. Swing-up and Stabilization of an Underactuated Manipulator Without State Feedback of Free Joint [J]. *IEEE Trans on Automatic and Control*, 2004, 20(2): 359-365.

[6] Reyhanoglu M, Van Der Schaft A, McClamroch N H, et al. Dynamics and Control of a Class of Underactuated Mechanical Systems [J]. *IEEE Trans on Automatic and Control*, 1999, 44(9): 1663-1671.

[7] Isidori A. *Nonlinear Control Systems* [M]. Berlin: Springer-Verlag, 1992.

[8] Vikramaditya B, Rajamani R. Nonlinear Control of a Trolley Crane system [A]. *Proc of the American Control Conference* [C]. Chicago, 2000: 1032-1036.