一种基于证书的电子投票协议*)

姚 前 陈 舜 谢 立
(南京大学计算机系 南京 210008)

摘 要 本文在对RSA数字签名技术、盲数字签名技术和比特提交技术进行分析的基础上,提出了一种采用现代密码学技术的电子投票协议,该协议可以基本满足证券业类别股东投票的实际需要。

关键词 RSA数字签名,盲数字签名,比特提交,电子投票

A Digital Certificate-Based Electronic Voting Protocol

YAO Qian CHEN Shun XIE Li
(Department of Computer Science, Nanjing University, Nanjing 210008)

Abstract Based on analysis of Digital signature , Blind signature and Bit commitment, the paper poses an electronic voting protocol concerning modern cryptography technology. The protocol can basically meet the practical requirement for shareholders' voting in the securities category.

Keywords RSA Digital signature, Blind signature, Bit commitment, Electronic voting

1 引言

现代社会中经常会遇到需要投票的情况,传统方式的投票过程和规则已非常完善,但传统投票方式也受到时间、地域、成本等诸多方面的制约。随着计算机技术和网络通信技术的发展,人们设想可以借助计算机网络,提供一种可以在较短的时间、以较低的成本为广大地域的大量用户所使用的投票方式,这就是电子投票方式的提出。如何保证电子投票的公开、公平和公正,是人们关心的焦点。本文简要介绍了一种采用现代密码学技术的电子投票协议,该协议可以基本满足证券业股东投票的实际需要。

2 电子投票协议的理论基础

从理论上讲,一个投票协议是具有秘密输入值的一个多成员计算,它使得输出的正确性可检验。对于一般的投票活动而言,一个理想的电子投票协议应该满足以下的一些特性:

(1) 完全性(completeness)。所有合法票均被正确地统计。

(2) 健壮性(soundness)。不诚实的投票者不能扰乱投票。

(3) 秘密性(privacy)。所有票的内容都是保密的。

(4) 不可重用性(unreusability)。投票者不能投两次票。

(5) 合法性(eligibility)。只有合格的投票者才能投票。

(6) 公平性(fairness)。外力无法影响投票结果。

(7) 可验证性(verifiability)。投票者能检验他们的票是否被统计在投票结果中。

目前人们已经提出了一些实用的投票协议,在这些协议中,有的满足上述全部特性,有的满足上述部分特性。我们采用的投票协议基于Fujioka,Okamoto,Ohta提出的方案,该方案完全满足了上述全部特性。

协议主要用到了RSA数字签名技术、盲数字签名技术和比特提交技术,在下面的节中,我们首先对协议用到的密码技术做一个简要的回顾,然后介绍我们采用的投票协议。

3 密码技术回顾

RSA数字签名方案

一个数字签名方案主要由两个算法,即签名算法和验证算法组成。签名者能使用一个秘密的签名算法 S 签一个消息 x,使得签名 $S(x)$ 可以通过一个公开的验证算法 V 来验证。一个数字签名方案可由满足下列条件的五元组 (P,A,K,S,V) 来表示:

(1) P 是所有可能消息组成的一个有限集合;

(2) A 是所有可能签名组成的一个有限集合;

(3) K 是所有可能密钥组成的一个有限集合,即密钥空间;

(4) 对每一个 $k\in K$,有一个签名算法 $S_k\in S$ 和一个对应的验证算法 $V_k\in V$。每一个 $S_k:P\to A$ 和 $V_k:P\times A\to\{$真,假$\}$ 均满足下列要求:对每一个消息 $x\in P$ 和每一个签名 $y\in A$,有 $V_k(x,y)=$真当且仅当 $y=S_k(x)$ 对每一个 $k\in K$,S_k 和 V_k 都是多项式时间的函数,V_k 是一个公开函数,S_k 是一个秘密函数。

采用RSA公钥密码算法构造的数字签名方案就称作RSA数字签名方案,该方案描述如下:

设 $n=pq$,p 和 q 是两个素数,$P=A=Z_n$,定义 $K=\{(n,p,q,a,b)\mid n=pq,p,q$ 为素数,$ab\equiv 1(\mathrm{mod}\,\phi(n))\}$。值 n 和 b 是公开的,值 p,q 和 a 是保密的。

对 $K=(n,p,q,a,b)$,定义 $S_k(x)=x^a \bmod n, x\in Z_n$

$V_k(x,y)=$真$\Leftrightarrow x\equiv y^b \bmod n$ $x,y\in Z_n$

签名算法使用RSA解密过程 D_k,由于 D_k 是保密的,因

*)基金项目:国家十五科技攻关项目(金融示范工程),课题编号:2001BA102A04。姚 前、陈 瞬 博士生,主要研究方向为分布式系统和计算机安全。谢 立 教授、博士生导师,主要研究方向为分布式计算、并行处理、先进操作系统等。

此 B 是唯一能产生签名的人。验证算法使用 RSA 加密过程 E_k。因为 E_k 是公开的，所以任何人都可以验证签名。

盲数字签名

盲数字签名技术是指具有下面两种特性的一种数字签名技术：

(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。

为达到上述要求，请求者首先将被签的消息进行盲变换，把变换后的消息(称为盲消息)提交给签名者，签名者对盲消息进行签名并把消息送还给请求者，请求者对签名再做逆盲变换，得出的消息即为原消息的盲签名。

盲数字签名技术在某些有参加者匿名性需求的场合具有重要意义，目前已有几种实现方案。在本协议中我们采用的是基于 RSA 体制的盲数字签名方案，其实现方法如下所述：

签名者 B 选择两个大素数 p 和 q，以及一个单向函数 f，并随机选择一个 e，使得 $\gcd(e,\phi(n))=1$，其中 $n=pq$。由 $ed\equiv 1(\bmod \phi(n))$ 求出 $d\equiv e^{-1} \bmod \phi(n)$。B 公开 n，e 和 f，保密 p，q 和 d。

如果请求者 A 想让 B 给他盲签一个消息 x，那么 A 先随机选择一个数 $k\in Z_p^*$ (k 称为盲因子)，计算 $x'=f(x)k^e \bmod n$，并将 x' 发送给 B。B 收到 x' 进行签名得到 $y'=Sig_B(x')=(x')^d \bmod n$。然后 B 将签名 y' 发送给 A，A 计算：

$$y'=y'/k \bmod n=(f(x)k^e)_d/k \bmod n=f_d(x) \bmod n$$

现在 A 得到了 B 对 x 的一个盲签名。显然 y 是 x 的一个合法签名。但 B 在签名过程中从来没有看到过 x 和 y，他无法将 (x,y) 和 (x',y') 联系起来。因此，该方案满足了盲数字签名的两个特性。

比特提交技术

比特提交方案是一个函数：$f:\{0,1\}\times X\to Y$，这里 X 和 Y 是两个有限集。$f(b,x)$，$x\in X$ 称作 $b\in\{0,1\}$ 的一个加密。函数 f 满足以下两个特性：

(1)隐蔽性(Concealing)：对 $b\in\{0,1\}$，接收者不能从 $f(b,x)$ 确定出 b 的值；

(2)约束性(Binding)：发送者能通过公开用于加密 b 的 x 的值，使接收者相信 b 确实为 0 或为 1。

如果发送者想提交任何比特串 s，他可以通过独立地提交比特串 s 中的每一个单比特位来完成，记为 $f(s,k)$。实现比特提交的方案有几种，本协议中采用基于离散对数的比特提交方案。根据离散对数的安全特性可知，当 $p\equiv 3(\bmod n)$ 是一个使得在 Z_p^* 上计算离散对数问题是不可行的素数时，一个离散对数的第二个低位比特是安全的，其方法如下：

设 $X=\{1,2,3,\cdots,p-1\}$，$Y=Z_p^*$，用 SLB(x)表示整数 x 的第二个低位比特，则

$$\mathrm{SLB(x)}=\begin{cases}0 & x\equiv 0,1 \bmod 4\\ 1 & x\equiv 2,3 \bmod 4\end{cases}$$

比特提交方案 f 定义为

$$f(b,x)=\begin{cases}a^r \bmod p & SLB(x)=b\\ a^{p-r} \bmod p & \mathrm{SLB(x)}\neq b\end{cases}$$

由于 $p\equiv 3(mod\ 4)$，因此可证明 $SLB(p-x)\neq SLB(x)$。

4 电子投票协议

我们的投票协议中主要有三个参与方，即投票者 V_i、投票管理中心 A 和计票者 C。

前提条件：每个投票者 V_i 均持有证书及相应的私钥，证书上具有其唯一标识 ID_i，V_i 用私钥签名的函数标记为 σ_i。

预备阶段：投票者 V_i 填写投票内容 v_i，随机选择一个密钥 k_i，用比特提交方案 f 加密 v_i，即计算 $x_i=f(v_i,k_i)$。然后随机选择一个盲因子 $r_i\in Z_n^*$ 盲化 x_i，即计算 $e_i=r_i^eH(x_i) \bmod n$，并对 e_i 签名得 $s_i=\sigma_i(e_i)$。然后将 (ID_i,e_i,s_i) 发送给投票管理中心 A。其中 H 是一个公开的单向函数。

签证阶段：投票管理中心 A 检查投票者 V_i 有无权力投票，如果 V_i 无权参加投票，则 A 拒绝给 V_i 签证。否则，A 检查 V_i 是否已经申请过签证，如果 V_i 已申请过签证，则 A 拒绝再给 V_i 签证。否则，A 检查 s_i 是否是消息 e_i 的合法签名，如果是，则 A 对 e_i 签名，即计算 $d_i=e_i^d \bmod n$ 并将 d_i 发送给 V_i。在签证阶段结束后，A 宣布已获得签证的投票者总数并公布包含有 (ID_i,e_i,s_i) 的一张表。

投票阶段：投票者 V_i 通过对 d_i 脱盲恢复 x_i 的签名 $y_i=d_i/v_i \bmod n_i$。V_i 检查 y_i 是否是 A 对 x_i 的合法签名，如果不是，V_i 通过向 A 证明 (x_i,y_i) 的不合法性并重复以上两步过程直到得到一个合法的签证，然后 V_i 匿名地将 (x_i,y_i) 发送给计票者 C。

验票阶段：计票者 C 通过使用 A 的签名验证密钥检查 y_i 是否是 x_i 的合法签名，如果是，C 将 (l,x_i,y_i) 填入表中，其中 l 是 (x_i,y_i) 的编号。在所有投票者投完票后，C 公开该表。

公开阶段：投票者 V_i 检查票的数量是否等于投票者的数量，如果不相等，V_i 检查他的票是否被计入表中，如果没有被列在表中，V_i 公开 (x_i,y_i) 并要求列入表中。然后 V_i 根据序号 l 将密钥 k_i 发送给 C。

计票阶段：计票者 C 用 k_i 将票 x_i 恢复为 v_i 并检查是否合法，统计并宣布投票结果。

结束语 上述协议基本上可以满足我们通过网络进行电子投票的需求，未来我们希望能够在证券股东投票系统等环境中进行实际的应用，进一步验证该协议的实用性、效率及实现成本，发现其潜在的问题，以便不断地对其进行改进和完善。

参 考 文 献

1 Chaum D, Crepeau C, Damgard I. Multiparty Unconditionally Secure Protocols. In: Proc. of the Twentieth Annual ACM Symposium on theory of Computing, 1988

2 Schneier B. Applied Cryptography: Protocols, Algorithms and Source Code in C John Wiley&-Sons, 1996

3 Fujioka A, Okamoto T, Ohta K. A Practical Secret Voting Scheme for Large Scale Elections. Advances in Cryptology-Ausocrypt'92, Springer-Verlag, 1993

4 Rivest R L, Shamir A, Adleman L. A Method for Obtaining Digital Signatures and Public-key Cryptosystem. Comm. ACM 1978, 2 (22)

5 Stadler M, Pivetear J M, Camenisch J. Fair Blind Signatures. Advances in Cryptology-Eurocrypt'95, Springer-Verlag, 1996

6 Naor M. Bit Commitment Using Pseudo-randomness. Advances in Cryptology-Crypto'89, Springer-Verlag, 1990