基于匿名通讯信道的安全电子投票方案

陈晓峰,王育民
(西安电子科技大学 ISN 国家重点实验室,陕西西安 710071)

摘 要: 利用群签名协议和时限承诺协议,本文给出了一种新的基于匿名通讯信道的安全电子投票方案.诚实投票者的身份无条件保持匿名,然而不诚实的投票者一定能被可信赖的注册机构追踪到.可证明:即使管理机构和计票机构勾结,在计票前可同时保证选票的秘密性和公平性.除此之外,我们的方案解决了"选票碰撞","投票者弃权或中途退出"等问题.

关键词: 电子投票; 群签名; 时限承诺
中图分类号: TP393 **文献标识码**: A **文章编号**: 0372-2112 (2003) 03-0390-04

A Secure Electronic Voting Scheme Based on Anonymous Communication Channel

CHEN Xiao-feng, WANG Yu-min
(*National Key Lab of ISN, Xidian University, Xi'an 710071, Shaanxi, China*)

Abstract: A secure electronic voting scheme based on anonymous communication channel is proposed by using group signature protocol and timed commitment protocol. The identity information of honest voters can be protected unconditionally while dishonest voters are sure to be traced by the trusted registration agent. We can also prove: Even the administrator and the counting agent conspire, the voting privacy and fairness can be realized simultaneously before the counting. Besides, we also solved the problems such as "vote collision","voter abstains from voting or quits midway" et al.

Key words: electronic voting; group signature; timed commitment

1 引言

与传统的选举方式相比较,电子投票一个显著的优点是投票者无须到一个指定的投票箱投票.随着 Internet 的迅速发展,电子投票已成为电子商务的一个主要内容,许多学者对其作了大量的研究[1~7],而且 Cranor[2]等人最近设计并实现了一个适用于 Internet 投票协议 Sensus.按选票发送的方式电子投票可分为两种:一种是投票者以加密的形式发送选票,另一种是投票者通过匿名的通讯信道发送选票.

电子投票最基本的要求是保证投票者身份的匿名性,选票的秘密性和公平性,以及方案的高效性.Benaloh[1]和 Iverson[5]利用高度剩余加密技术提出了一些电子投票方案.然而,当选举人数较多时,这些方案中数据的通讯量和计算量就无法忍受,所以这些方案都不适合于大群体的选举.

Chaum[6]和 Ohta[7]利用匿名通讯信道分别给出了一个适合于大群体选举的投票方案,而且保证了投票者的匿名性,然而这两个方案都没有解决选票的秘密性和公平性.当投票者发现自己的选票没有被正确计入时,他必须通过公开选票来要求计票机构加入自己的选票,这样就泄露了自己的选票;而且,管理者可以知道选举的一些中间结果,所以他能通过泄露这些信息影响选举的最终结果,从而破坏了选票的公平性.Asano[3]提出的方案解决了公平性的问题,但该方案对于腐败的管理者仍是不安全的.随后的方案[4]虽然解决了秘密性问题,但是又没有解决公平性的问题.

Fujioka[10]利用比特承诺协议和盲签名技术提出了一个实用的,秘密的,适合于大群体选举的电子投票方案.该方案同时保证了选票的秘密性和公平性,而且也解决了投票者身份的匿名性问题.但是,它仍然有一些缺点:首先,它没有解决"选票碰撞"的问题.如果两个投票者使用相同的随机密钥及以相同的方式投票,那么选票及其签名就完全一样.于是计票机构去掉一些重复的选票而伪造另一些"合法的"的选票,但是投票者无法察觉.其次,使用比特承诺协议虽然保证了选票的公平性,但是在计票时需要投票者提供自己的随机密钥 k.如果投票者提供一个非法的密钥,则对应的选票无法打开.为了区分不诚实的投票者和不诚实的计票机构,Fujioka 建议将该密钥发送给几个相互独立的机构(如不勾结的候选人),这不仅增加了选举中数据的通讯量和计算量,而且如果投票者中途退出,即不发送随机密钥,则对应的选票无法打开.计票机构就可能与管理机构相勾结来影响投票结果(剔除该选票而加入其它结果).最后,Fujioka 的方案要求弃权者提交一张空白选票来防止选举中的腐败行为(管理者就有可能代替这些选举者投票),但实际上如果选举者决定放弃选举,他就不愿花费时间来提交一张空白选票.

利用群签名协议和时限承诺协议,本文给出了一种新的基于匿名通讯信道的安全电子投票方案.诚实的投票者可以无条件保持身份匿名,然而不诚实的投票者则一定能被可信赖的注册机构追踪到.我们还可证明即使管理机构和计票机构勾结,在计票前可同时保证选票的秘密性和公平性.除此之外,本方案解决了选票碰撞以及投票者的中途退出等问题.

收稿日期:2001-09-27;修回日期:2002-02-18
基金项目:国家重大自然科学基金资助课题(No.19931010)

© 1994-2010 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

2　电子投票的性质和研究现状

2.1　电子投票的基本性质

电子投票一般包括以下的参与者:投票者 V_i,管理机构 A,计票机构 C. 在我们给出的协议中还有一个可信赖的注册机构,假定只有在必要的时候才追踪投票者(比如不诚实的投票者提交无效的选票,或只注册而不投票). V_i 和 C 通过一个匿名的通讯信道交换信息. 一个安全的投票方案应具有下面的性质:

秘密性　除了投票者外,选票的内容不能被其他人知道.

公平性　在选举的中间过程,任何人的行为都无法影响选举的结果.

匿名性　任何人都无法将一张选票和某一投票者联系起来.

唯一性　只有有资格的人能提交一张合法的选票,冒充他人选举则一定能被追踪到.

完整性　所有合法的选票都能被正确计入.

稳固性　不诚实的投票者不能破坏选举.

可验证性　选举的结果可以被检验,任何人无法伪造选举结果. 狭义的可验证性保证合法的选票被计入,而广义的可验证性可以使任何感兴趣的第三方参与检验,同时不泄露投票者的隐私.

2.2　电子投票的研究现状

最初的方案[3,5]对于大群体选举由于效率过低,所以只具有理论上的意义,Fujioka 的方案仍是适合于大群体选举的有效的投票方案之一,其基本思想是:利用盲签名中的不可连接性保证了选票和投票者的不可连接,使用比特承诺协议隐匿选票实现了选举的公平性.

为了防止投票中的"犯罪"行为如买卖选票,Benaloh[5]引入了"无收据的电子投票"的概念:某一投票者不能向第三方证明他提交了某一特定的选票. 此外,他基于一种特定的物理假设(voting booth),利用高度剩余加密技术给出了两个无收据的投票方案. 最近,Martin[14]等证明了 Benaloh 的第二个方案不具有无收据性. 后来的一些协议[11]利用离散对数加密代替高度剩余加密提高了 Benaloh 协议的效率,然而这些协议也不具有无收据性. Sako[12]等基于一种较弱的物理设备(Untappable channel),利用混合网(Mixnet)信道给出了一个无收据的投票方案,但是不适合于大群体选举. Okamoto[13]给出了一个效率较高的无收据的投票方案,然而正如 Martin 所指出的,同时保持匿名和秘密的信道是很难得到的.

不基于任何物理假设,使用多方计算来设计无收据的投票方案是研究的另一主流. 总之,无收据性是电子投票方案设计中一个非常重要的方面. 然而正如前面所讨论的,开始提出的许多方案最后被证明不具有无收据性,这是一个非常困难的问题,本文中就不再涉及.

3　准备工作

3.1　承诺协议

A 想向 B 承诺未来发生的一个事件预测值,但在事件出现前不对 B 泄露;另一方面要使 B 确信 A 对他所做出的承诺不会改变. 通常的承诺协议包括两个过程——生成和兑现.

承诺生成:

(1) A 生成两个随机数 R_1 和 R_2.

(2) A 将 R_1 和 R_2 及承诺消息 b 组成 (R_1, R_2, b).

(3) A 计算 (R_1, R_2, b) 的单向函数值 $H(R_1, R_2, b)$,并随机选择一个数 R_1,将 $(H(R_1, R_2, b), R_1)$,送给 B.

承诺兑现:

(4) A 将原消息 (R_1, R_2, b) 送给 B.

(5) B 计算 (R_1, R_2, b) 的单向杂凑值,并与(3)中收到的值相比较. 同时还将(4)中的 R_1 与(3)中收到的 R_1 比较,如果一致,证明 A 的承诺合法.

在上述的协议中,如果 A 拒绝兑现承诺,则 B 无法得到消息 b. 于是 D Bonch[8]等引入了"时限承诺"的概念. 它在通常承诺的协议的基础上增加了一个"强迫打开承诺"的过程:经过一个时间段 T 后,无须 A 的参与 B 就可以恢复出消息. 但在任何的时间段 $t < T$,即使 B 有一个多项式数量级处理器的并行机,他恢复出消息的概率可以忽略. 具体的说,时限承诺协议包括以下三个过程:

承诺生成　对消息串 $s \subset \{0,1\}^n$,A 与 B 执行承诺协议得到承诺串 C,A 发送 C 给 B.

公开承诺　经过一段时间后,A 泄露消息串 s 给 B,并且要给 B 证明 s 确是所承诺的值.

强迫打开承诺　如果 A 拒绝泄露消息串 s 给 B,则 B 运行所谓的"强迫公开算法",经过时间 T 后可得到消息串 s 及 s 是所承诺值的证据.

时限承诺主要有以下的性质:

可证实的恢复性　只要正确地执行承诺生成过程,那么 B 就一定在强迫打开承诺过程后得到消息 s.

有证据的恢复性　B 不仅可以恢复出消息 s,而且得到关于 s 的一个证据,任何人都可以验证 s 确实是所承诺的消息.

抗并行攻击性　即使 B 有更多的处理器(多项式数量级),他也无法更快的计算出消息 s.

时限承诺协议在电子合同签署,电子拍卖中有着重要的作用. 本文利用时限承诺协议来隐匿选票,即使某些投票者中途退出选举或拒绝打开承诺,相对应的选票也可计入选举.

3.2　群签名

群签名的概念最早由 Chaum 和 Van Hegst[15]提出,之后又有许多人对它进行了研究. 一个群签名方案允许群体中的任一个成员代表该群体签名,这个签名是可用一个群公钥公开验证的,同时它还实现了签名者的匿名性以及签名文件的不可连接性.

群签名协议主要包括以下几个过程:

创建　是产生群公钥 Y 和群管理员的管理密钥 S 的一个概率算法.

加入　是群管理员和新的群成员 Alice 之间的一个交互式协议,它产生 Alice 的密钥 x,成员证书 v 和她的公开钥.

签名　是群成员 Alice 和一个用户之间的一个交互式协

© 1994-2010 China Academic Journal Electronic Publishing House. All rights reserved.　http://www.cnki.net

议,输入是用户的信息 m 和 Alice 的密钥 x,输出是对 m 的签名 s.

验证 是一个输入 (m, s, Y),用群公钥 Y 确定 s 是否是对 m 的一个合法的签名的算法.

打开 是一个给定一个签名信息和群密钥,确定签名者身份的算法.

一个群签名必须满足下列安全性质:

匿名性 给定一个签名,确定实际签名者的身份除了惟一的群管理员之外,对任何人都是计算困难的.

不可伪造性 只有合法的群成员才能代表群体来签名;任何一个群成员,甚至群管理员也不能代表其他成员签名.

无关性 确定两个不同的签名是否是由同一个群成员签署的,在计算上是困难的.

可跟踪性 群管理员可以打开任意一个签名,识别出实际签名者的身份;此外,签名者不能阻止一个合法签名的打开.

抵抗联合攻击 群成员中的部分成员串通起来也不能生成一个不可跟踪的合法的群签名,即不能生成一个合法群签名,这个签名不能由群管理员打开.

基于双重离散对数知识证明签名(SKLOGLOG)和离散对数的 e-次根知识证明签名(SKROOTLOG)技术,Camenisch[16]提出了一个适用于大群体的有效的群签名方案. 这两个签名所用的离散对数都是一般乘法群上的,签名过程中所需传输的数据量较大,签名数据较大. 张氏[9]将之推广到椭圆曲线上,使得传输的数据量和签名长度大大降低,提高了效率.

4 安全的电子投票方案

这一节给出投票方案,首先给出所需要的参数和符号:

4.1 参数

注册机构 注册机构 RA 作为一个群体的群管理员,他选择如下参数:RSA 公钥 (n, e),定义在 $GF(p)$ 上的椭圆曲线 $E_{(a,b)}$,p 是一个大素数. G 是 $E_{(a,b)}$ 中的一个 q 阶元素,q 是一个至少为 160 比特的素数. $c \in Z_n^*$,它模 n 的两个素因子都有大的乘数阶. 密钥上界 λ,常数 ε. 群公钥是 $\Omega = (n, e, c, E_{(a,b)}, P, q, \lambda, \varepsilon)$. 规定 t_0 为开始投票的时刻,t_1 为结束集票的时刻.

投票者 投票者 V_i 作为 RA 的一个群成员,他的群签名私钥为 x_i,身份为 ID_i. V_i 使用时限承诺协议隐匿选票后的承诺记为 $m_i = TC(v_i, T, \varepsilon)$,其中 v_i 是 V_i 的选票,T 是使用强迫公开算法打开 v_i 所需的时间,ε 是任意小的正数. 当 $t < T$ 时,恢复出 v_i 的概率为 ε. 我们设注册的总人数为 $Total$.

管理机构 管理机构 A 的签名私钥为 SK_A,对应的公钥记为 PK_A. $f(\cdot)$ 是一个无碰撞的函数.

计票机构 计票机构记为 C,他的加密密钥为 PK_C,解密密钥为 SK_C.

4.2 投票方案

我们的方案包括以下几个协议:

注册协议 有选举资格的成员 V 到 RA 处注册(不注册者认为是弃权,然而注册过的成员必须提交一张合格的选票). 他提交自己的身份 ID,RA 验证他具有选举资格后允许他加入群体. V 选择自己的私钥 $x \in \{0, 1, 2, \cdots, 2^{\lambda} - 1\}$,并计算 $y = c^x$ 及身份密钥 $z = (y \bmod q)\ G$. 然后他对 y 承诺并发送 y, z 给 RA,当 RA 确信 V 知道 x 后(RA 不能知道 x,这可以通过离散对数的知识签名完成),他发送 V 的身份证书 $Cer = (y + 1)^d \bmod n$ 和一个随机比特串 B 给 V. 最后,RA 公布所有的 B. 在 t_0 时刻,RA 宣布开始投票.

管理协议 V_i 首先计算 $M_i = f(m_i \| B_i)$,其中 $\|$ 表示级联;$G' = rG$,$r \in_R Z_p^*$;$Z' = yG$;$s_1 = \mathrm{SKLOGLOG}[\alpha: Z' = c^{\alpha} G](M_i)$ 和 $s_2 = \mathrm{SKROOTLOG}[\beta: Z \wedge G' = \beta G](M_i)$,然后发送 B_i,M_i 及 (G', Z', s_1, s_2) 给 A. A 首先验证 M_i 的签名 (G', Z', s_1, s_2) 是否成立,若不成立,则拒绝接受数据;否则再检验 B_i 是否已经存储在数据库中,若已经存储,则说明有人冒充他人投票,A 发送 B_i 和对应的两个签名给 RA,则可追踪出不诚实的投票者的身份;否则存储 B_i,M_i 和签名 (G', Z', s_1, s_2). 然后 A 发送 $SK_A(B_i \| M_i)$ 并给 V_i.

投票协议 如果 V_i 检验签名 $SK_A(B_i \| M_i)$ 正确,则通过匿名通讯信道发送 $:\{m_i, PK_C(B_i \| SK_A(B_i \| M_i))\}$ 给 C. C 首先计算出 $M_i = f(m_i \| B_i)$,然后再验证签名是否正确. 如果检验通过,则公布 (N_i, m_i),其中 N 是公布的序列号.

集票协议 如果投票者 V_i 发现自己的 m_i 没有被公布,则提交 $(m_i, SK_A(B_i \| M_i))$ 给 A 表示抗议,于是 A 要求 C 加入 m_i.

计票协议 在 t_1 时刻,C 宣布终止集票. V_i 通过匿名通讯信道与 C 执行承诺公开协议,则 C 得到选票 v_i 和相应的证据. 如果某些投票者不执行承诺公开协议,则 C 运行强迫公开算法得到 v_i 和相应的证据.

4.3 简单的性能分析

4.3.1 选票碰撞 选票碰撞的问题在 Fujioka 的方案中没有提到,后来的一些方案注意到了这个问题,并给出了一些解决的方法. 在我们的方案中也存在类似的问题,如果两个投票者的 m_i 相同,而且 A 和 C 勾结,只公布一张有效的选票 (N_i, m_i),那么他们就可以伪造一张选票而不被察觉. 通过如下的办法来解决这个问题:令 $m_i = TC(v_i^*, T, \varepsilon)$,其中 $v_i^* = v_i \| f(B_i, R_i)$,$R_i$ 是 V_i 所选的随机数.

4.3.2 可信赖的注册机构的安全性分析

正如基于可信赖的托管者的公平电子现金方案一样,如果托管者与银行相互勾结,则他一定能追踪所有用户的信息,匿名性就不可能保证. 在我们的方案中,如果 RA 与 A 或 C 不勾结,则投票者可以无条件的保持匿名. 否则,他在计票结束后就知道 V_i 的选票,但是在计票结束前,他无法知道 V_i 的投票(这是由承诺协议所保证的).

在公钥密码基础设施中,都假定有一个可信赖的主体. 当然,也可以利用门限秘密分享技术,使用多个注册机构的方案来保护投票者的隐私.

5 安全性分析

匿名性 使用群签名协议,使得 A 无须验证 V_i 的身份就可以确定该投票人是否具有选举资格,使用匿名通讯信道使得任何人无法追踪投票者. 当然,我们的方案是基于可信赖的

© 1994-2010 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

注册机构,只要他与 A 或 C 不勾结,则投票者可以无条件的保持匿名.

秘密性和公平性　使用了时限承诺协议来隐匿选票,只要保证 $T > t_1 - t_0$,则在计票前任何人无法知道选票的内容.而且计票是在投票完全结束之后,所以,计票结果就不会影响选举和投票.

稳固性　规定未注册的有选举资格的成员作弃权处理,而注册的成员必须提交一张合法的选票.对于注册而不投票或提交不合法选票或不开票的选民,使用群签名协议保证了可以追踪出其身份.使用时限承诺协议可以保证能打开所有的选票,从而阻止了破坏选举的行为.

合法性　使用群签名协议,保证了只有选举资格者才能提交合法的选票.假设 A 与某无资格者勾结,提交一张不合法的选票,但此时选票数就大于注册者的人数,从而被发现.

唯一性　每个投票者只能提交一张合法的选票,否则他必须提交重复的 B_i;如果他盗用别人的 B_i 来提交选票,则一定会被发现(在管理协议中我们已讨论过这个问题).

广义可验证性　使用时限承诺协议保证每个人都可以检验选票及选举的结果.即使 A 与 C 相勾结也无法改变选举的结果.

实用性　使用一个适用于大群体的群签名协议,而且将其推广到椭圆曲线密码上,所以效率较高.

6　结论

本文利用群签名技术和时限承诺协议提出了一个安全的电子投票方案.其主要贡献是不仅同时保证了诚实投票者身份的匿名性与选票的秘密性和公平性,而且解决了"选票碰撞"问题及投票者中途退出的问题.诚实投票者的选票一定会被计入选举结果,而不诚实的投票者则一定能被可信赖的注册机构恢复出其身份,从而防止了投票者,管理机构或计票机构的欺诈行为.

当然,如何进一步提高群签名协议的效率,设计出更为有效的适用于大群体选举的电子投票方案需要更深入的工作.其次,为了防止选票的买卖活动,无收据的投票协议成为研究的一个主流,如何设计一个真正有效的方案仍是一个棘手问题.而且现有的方案大多都依赖于一个基于过强的物理设备—匿名的通讯信道来保护投票者的隐匿信息,但实际上在 Internet 上很难保证匿名性,设计出实用的匿名投票方案仍需要深入研究.

致谢　作者衷心的感谢西安电子科技大学 ISN 国家重点实验室的张方国博士,在椭圆曲线密码知识签名方面的有意义的讨论,以及中国科学院软件研究所的张文涛博士提供的文献和帮助.

参考文献:

[1] J Benaloh, M Yung. Distributing the power of a government to enhance the privacy of voters [A]. Proc of the 5th ACM of Distributed Computing [C]. Calgary, 1986: 52 - 62.

[2] L Cranor. Electronic voting: Computerized polls may save money, protect privacy [A]. Proc of the Hawaii Internet of Conference on System Science [C]. Huawaii, 1997. 116 - 124.

[3] T Asano, T Matsumoto, H Imai. A study on some schemes for fair election secret voting [A]. Proc of the 1991 Symposium on Cryptography and Information Security [C], Japan, 1991: SCIS91 - 12A.

[4] K Sako. Electronic voting system with objection to the center [A]. Proc of the 1992 Symposium on Cryptography and Information Security [C]. 1992: SCIS92 - 13C.

[5] K R Iverson. A cryptographic scheme for computerized general elections [A]. CRYPTO '91 [C]. LNCS 576, Berlin: Springer-verlag, 1991. 405 - 419.

[6] D Chaum. Elections with unconditionally-secret ballots and disruption equivalent breaking RSA [A]. EUROCYPT '88 [C]. LNCS 330, Berlin: Springer-verlag, 1988. 177 - 182.

[7] K Ohta. An electrical voting scheme using a single administrator [A]. 1988 Spring National Convention Record [C]. Berlin: IEICE, 1988. A-294.

[8] D Bonch, M Naor. Timed commitments [A]. CRYPTO '00 [C]. LNCS1880, Berlin: Springer-Verlag, 2000. 236 - 254.

[9] Fangguo Zhang, Futai Zhang, Yumin Wang. Fair electronic cash systems with multiple banks [A]. The sixteenth annual working conference on information security [C]. Beijing: Kluwer, 2000. 461 - 470.

[10] A Fujioka, T Okamoto, K Ohta. A practical secret voting scheme for large scale elections [A]. AUSCRYPT '92 [C]. LNCS 718, Berlin, Springer-verlag, 1993: 244 - 251.

[11] K Sako, J Kilian. Secure voting using partially compatible homomorphism [A]. CRYPTO '94 [C]. LNCS 839, Berlin: Springer-verlag, 1994. 411 - 424.

[12] K Sako, J Kilian. Receipt-free mix-type voting scheme: A practical solution to the implementation of a voting booth [A]. EUROCRYPT '95 [C]. LNCS 921, Beilin: Springer-verlag, 1995. 393 - 403.

[13] T Okamoto. Receipt-free electronic voting schemes for large scale elections [A]. Proc of Workshop on Security Protocols '97 [C]. Berlin: LNCS 1361, 1997. 25 - 35.

[14] H Martin, K Sako. Efficient receipt-free voting based on homomorphic encryption [A]. EUROCRYPT '00 [C]. LNCS 921, Berlin: Springer-verlag, 2000. 393 - 403.

[15] D Chaum, E van Heijst. Group signatures [A]. EUROCRYPT '91 [C]. LNCS 547, Berlin: Springer-Verlag, 1991. 257 - 265.

[16] Jan Camenisch, Markus Stadler. Efficient group signature schemes for large groups [A]. CRYPTO '97 [C]. LNCS 1294, Berlin: Springer-Verlag, 1997. 410 - 424.

作者简介:

陈晓峰　男,1976 年 2 月生于陕西宝鸡,现为西安电子科技大学 ISN 国家重点实验室博士研究生,研究方向为电子商务安全,椭圆曲线密码.

王育民　男,1936 年生于北京,教授,西安电子科技大学博士研究生导师,IEEE 高级会员,研究领域为信息理论安全及编码,密码学.

© 1994-2010 China Academic Journal Electronic Publishing House. All rights reserved.　http://www.cnki.net