文章编号:1001 - 9081(2009)05 - 1470 - 03

基于安全 E-mail 协议的电子选举研究

牛项须,崔 喆,代 翔
(中国科学院 成都计算机应用研究所, 成都 610041)
(2002piao@163.com)

摘 要:在安全邮件协议 PGP 中引入公正机构(CA),设计了一个适合大规模选举的电子选举方案。该方案不仅能满足电子选举的安全要求,而且不要求选民在固定地点投票;此外,新方案在一定程度上解决了电子选举中权威机构权力过大及绝对匿名性引发问题,可以在不泄露选票内容的情况下使选举的结果具有可验证性。

关键词:电子选举;安全 E-mail 协议;安全邮件协议
中图分类号: TP309 **文献标志码**:A

Electronic elections based on secure E-mail protocol

NIU Xiang-xu, CUI Zhe, DAI Xiang
(*Chengdu Institute of Computer Application, Chinese Academy of Sciences, Chengdu Sichuan* 610041, *China*)

Abstract: By introducing the Certificate Authority (CA) into secure E-mail protocol Pretty Good Privacy (PGP), the author designed a vote scheme for large-scale electronic elections. It fulfills the security demands of electronic elections, but does not require constituencies to the settled polling booth. Moreover, the proposed scheme resolves the problems, which result from exceeding authority of authoritative organization and absolute anonymity, in electronic elections to a certain extent. And it can provide public verifiability without disclosing the vote messages.

Key words: electronic elections; secure E-mail protocol; Pretty Good Privacy (PGP) protocol

电子选举系统以密码学为基础,运用计算机和网络技术来实现投票、计票功能。与传统的选举方式相比,它不仅具有更高的效率和更大的灵活性,而且可以节省大量的人力、物力、财力。例如,选举委员会不必像传统选举那样进行人工的选票发放和选票统计工作;投票人不必到一个固定的投票地点去投票等。由于其所具有的独特优势和其与实际应用的密切联系,目前正受到越来越广泛的关注和研究。

1 电子选举的发展及现状

文献[1]明确提出了基于公钥密码的电子邮件概念,这是首次提出基于匿名信道来设计电子选举协议的思想。随着计算机、网络和密码技术的发展,国际上众多学者开始对电子选举进行研究,并分别提出了基于不同密码技术的电子选举方案[2-7]。目前,电子选举已经在许多的国家得到了广泛的应用。据分析,现有的电子选举系统主要有以下几种:

电子计票 以电子方式计算选票,尤其是以电子方式计算纸质选票,如通过光学字符识别技术扫描选票统计选票。

投票亭投票 指在一个可以控制的场所,如大型活动中心等,使用专用的电子化投票设备,以触摸屏按键方式,让投票人使用电子形式的选票,取代现行纸质选票的方式。

网络投票 指投票人先通过网络来获取电子形式选票,表达自己的意见后再投出选票,最后在服务器端统计选票的方式。一般是通过网站或者特定的程序进行投票行为的。

国外使用的电子选举系统以投票亭投票方式最多,而国内现在的电子选举系统多是电子计票方式。这两种电子选举方式均为集中式的选举,具体表现为要求选民在固定的时间到指定的地点进行填票、投票。

1.1 电子选举的安全标准[9]

电子选举的研究学者们针对不同的选举方式对选举协议提出了不同的要求。一般认为,一个安全的电子选举协议应该满足以下基本性质。

1)合法性:只有合法的选举人才能参加投票。

2)完备性:系统应能正确地认证和统计每一张选票,杜绝篡改选票内容、漏记合法选票、添加非法选票、复制合法选票、泄露选票信息等舞弊现象的发生。

3)匿名性:投票的内容必须是保密的,除了选民自己,其他人无法把投票人和选票内容联系在一起。

4)不可重复性:任何合法选民在投票后都不能再次重复投票。

5)公正性:在最终选举结果公布前,任何机构和个人无法获得选举的中间结果。

6)可验证性:任何人(此时称为公开可校验性)或者只有投票人(此时称为原子可校验性)可以验证最后的选举结果是否正确统计了合法选票。

7)无收据性:选举者不能持有也不能构造收据以证明其投票的内容,防止贿选、胁迫投票等现象发生。

1.2 现有电子选举中存在的问题

尽管电子选举已经在实际选举中加以应用,但其安全性和可靠性仍然饱受争议,如在美国广泛使用的 Diebold Election System[10]。分析了众多的电子选举协议发现,目前电子选举协议中主要存在以下三个问题:

1)选举中权威机构权力过大,具体表现为权威机构知道

收稿日期:2008 - 11 - 11;**修回日期**:2009 - 01 - 16。
基金项目:国家 863 计划项目(2008AA01Z402);中国科学院知识创新工程重要方向项目(KGCX2-YW-105)。
作者简介:牛项须(1982 -),男,河南平顶山人,硕士研究生,主要研究方向:计算机网络、信息安全; 崔喆(1970 -),男,四川巴中人,研究员,主要研究方向:软件工程、计算机网络、信息安全; 代翔(1983 -),男,河南信阳人,硕士研究生,主要研究方向:计算机网络、信息安全。

选民的私钥,可以伪造选民的签名,而选民无法证明其伪造了自己的签名;

2)匿名性和不可重复性的矛盾;

3)可验证性和无收据性的矛盾。

随着网络和计算机的普及,目前视频会议和网络购物已经成为现实。这也使得利用网络连接,选民通过网络直接完成获取候选人信息、填票、投票的过程成为必要和可能。

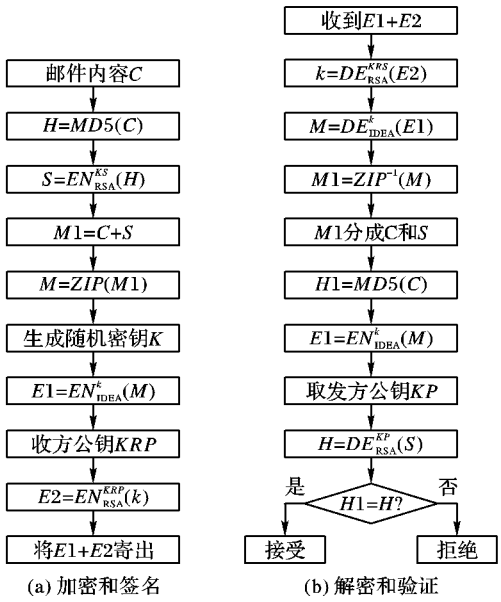
结合中国民主化进程的推进,本文在安全邮件协议(Pretty Good Privacy, PGP)中引入公正机构(Certificate Authority, CA)的基础上设计了一个适合分散式选举的电子选举方案。该方案在一定程度上解决了电子选举中权威机构造假以及匿名性和不可重复性的矛盾,并且可以在不泄露选票内容的情况下提供对选票的可验证性。

2　预备知识

2.1　PGP 工作原理[11-12]

PGP(Pretty Good Privacy)是设计用来免费保护电子邮件的程序,是专门针对电子邮件在 Internet 上通信的安全问题而设计的一种混合加密系统。用户可以使用它在不安全的通信链路上创建安全的消息和通信。PGP 包含四个密码单元:单钥密码(IDEA)、双钥密码(RSA)、单向杂凑算法(MD-5)和一个随机数生成算法。

PGP 的加密和解密原理如图 1 所示。其中 EN 为加密,DE 为解密,下标为使用的算法,上标为使用的密钥。KS 为发送方的私钥,KP 为发送方公钥,KRP 为收信方公钥,KRS 为收信方私钥。



(a) 加密和签名　　(b) 解密和验证

图 1　加密和解密原理

2.2　PGP 的不足

2.2.1　PGP 的公钥管理和信任模型

由于 PGP 使用一种分布式的公钥管理方式,没有一个统一的认证中心(CA)来管理,因此每个人都可以作为一个 CA,对某个公开密钥签名,以此来说明这个公开密钥是有效的,并且这个有效性证明是可以到处传播的。但是只有当用户信任这个签名者的时候,这个公钥的有效性证明才会被用户所接受。用户之间通过交换各自的公钥列表,从而建立起 PGP 信任网络。PGP 信任模型的不足:1)假定 A 相信 B,B 相信 C,根据 PGP 协议中的信任传递关系,A 也是相信 C 的。这种信任传递关系在现实生活中是不确定的。2)如果某个用户的私钥发生丢失或损坏,他几乎不能通知其他通信方相关的证书已不可信。

2.2.2　PGP 系统的安全问题:

系统常见的安全问题主要是:重放攻击,中间人攻击,用户名的保护,登录密码的保护,垃圾邮件以及网络中普遍存在的各种攻击,如 DoS 等。

2.3　改进的 PGP 模型

鉴于 PGP 中公钥管理和信任模型的不足,结合电子选举的实际情况,引入一个公正机构 CA 统一对系统参与者的公钥进行管理,系统中公钥采用 Diffie-Hellman 密钥交换算法,并对 PGP 中接受方公钥 KRP 定义为传输公钥 KRP,KRP 的值和 CA 的其他职责在下文中叙述。针对 PGP 系统中的安全问题,我们的新系统中通过在用户登录时要求输入随即验证码,防止重放攻击;针对伪造合法用户名发信主要通过 SPF(Sender Policy Framework)解决[13]。登录过程中先用 MD5 对密码加密然后传送到服务器,在服务器端与保存的 MD5 加密后的密码比对,完成身份认证,可以防止中间人攻击;在新系统中,针对垃圾邮件主要通过设置 SMTP 认证和限制 SMTP 的发信频率解决。另外通过对路由器正确设置和安装防火墙技术来减少 DoS 等普遍存在的攻击。

2.4　Diffie-Hellman 密钥交换算法[14]

本原元:对于一个素数 q,如果数值 $a \bmod q, a^2 \bmod q, a^3 \bmod q, \cdots, a^{q-1} \bmod q$ 是各不相同的数,并且以某种排列方式组成了从 1 到 $q-1$ 的所有整数,则称整数 a 为素数 q 的一个本原元,本原元也称为生成元。

离散对数:对于一个整数 b 和素数 q 的一个本原元 a,可以找到一个唯一的指数 i,使得:$b = a^i \bmod q$ $(0 \leqslant i \leqslant q-1)$ 成立,则指数 i 称为以 a 为底数的模 q 的离散对数。

对于给定的 a、i 和 q 容易计算出 b,但给定 b、a 和 q,计算出 i 非常困难,即离散对数问题的难解性,它是许多公钥密码算法的基础。

Diffie-Hellman 密钥交换算法:假设用户 A 和 B 希望安全地交换一个密钥,他们需要先确定并都知道两个公开的整数:一个素数 q 和一个整数 a,a 是素数 q 的一个本原元。用户 A 选择一个随机数 $X_A < q$,并计算 $Y_A = a^{X_A} \bmod q$;类似的用户 B 选择一个随机数 $X_B < q$,并计算:$Y_B = a^{X_B} \bmod q$。每一方保密存放自己的随机数 X_A 和 X_B(相当于私钥),并使 Y_A 和 Y_B(相当于公钥)的值对于对方可以公开得到。用户 A 计算:$K = (Y_B)^{X_A} \bmod q$,将其作为自己的会话密钥;用户 B 计算:$K = (Y_A)^{X_B} \bmod q$,将其作为自己的会话密钥。

3　基于安全 E-mail 协议的电子选举系统

假定电子选举系统运行于一个联网的基于 PGP 安全邮件协议的 E-mail 服务器之上,系统参与者有公正机构 CA,选民群体、选举委员会和计票机构。

公正机构 CA:负责初始化系统,发布系统参数;为合法选民分发邮箱地址和密码并发布公正机构的公钥;维护参与者公钥和身份信息对应列表。

选举委员会:制作选票;分发选票;回收选票;匿名化处理选票并转发;受理投诉;公示结果。

选民群体:填写选票;签选票;加密选票;投递选票。

计票机构:解密选票,统计选票,提供验证。

3.1 系统的信息流程

准备阶段:选民的身份认证在网络之外进行完毕,共有 n 个合法选民参加本次选举。公正机构输入安全级别参数 L 初始化系统,生成系统参数 a 和 q(a 和 q 的关系参见2.4节)。公正机构为自己分配一个信箱 CA@ EmailElection.com 并选取随机数 $i(0 \leqslant i \leqslant q-1)$ 计算公正机构的公钥 $b = a^i \bmod q$,然后根据选民的身份信息 $D_j(j = 1,2,\cdots,n)$ 不同,公正机构为将参加本次选举的选民 $D_j(j = 1,2,\cdots,n)$ 分配了一个私有电子信箱 D_j @ EmailElection.com ($j = 1,2,\cdots,n$) 并把 E-mail 地址和密码发送给每个选民;公正机构为选举委员会分配两个专用电子信箱和密码:一个 SendAndReceive @ EmailElection.com 用来发放和回收选票,一个 Appeal @ EmailElection.com 受理投诉和问询;公正机构为计票机构分配一个 StatisticalCommission@ EmailElection.com 信箱和密码;具体的发放方式可以采用现在银行系统信用卡密码的制作和发放方式;然后通过公告牌公开系统参数 a 和 q 及自己的公钥 b 和邮件地址 CA@ EmailElection.com 等信息。在系统中每个用户的邮件地址就是自己的身份标识,凡拥有系统中的已分配的邮件地址,则视为选举系统的合法用户。

选民 D_j、选委会和计票机构收到 E-mail 地址和密码后登录更改密码后,根据公告牌的信息,分别选取 s_j、s_c 和 s_s($0 \leqslant s_j$、s_c、$s_s \leqslant q-1$) 分别作为自己的私钥,分别计算 $p_j = a^{s_j} \bmod q$、$p_c = a^{s_c} \bmod q$ 和 $p_s = a^{s_s} \bmod q$ 作为自己的公钥,然后用公正机构的公钥把自己的公钥加密后通过自己的私有信箱发送给 CA@ EmailElection.com。公正机构 CA 解密所有邮件后把选民 $D_j(j = 1,2,\cdots,n)$ 的公钥 $p_j(j = 1,2,\cdots,n)$ 存储在选民公钥列表中;公正机构 CA 把选委会的两个信箱:SendAndReceive@ EmailElection.com(用来发放和回收选票),Appeal@ EmailElection.com(受理投诉和问询)和计票机构信箱 StatisticalCommission@ EmailElection.com 及选举委员会的公钥 p_c 和计票机构的公钥 p_s 发布在公告牌上,同时把所有选民的邮件地址列表转交给选举委员会。

发放选票阶段:选举委员会设计好选票 V 后,采用 $E = RSA(s_c, V)$ 加密后把 E 使用 SendAndReceive@ EmailElection.com 发送给 D_j @ EmailElection.com ($j = 1,2,\cdots,n$),选民使用选举委员会的公钥 p_c 解密选票 $V = RSA(p_c, E)$,如果不能解密可以向 Appeal@ EmailElection.com 发信投诉。

填写选票阶段:选民对选票 V 上的候选人表达意愿后形成 C,然后采用图1(a)中流程对 C 进行签名和加密形成 $E1 + E2$,其中 $KS = s_j$ 为选民 D_j 自己的私钥,图(a)中收信方的公钥 KRP 更新为会话密钥 $KRP = p_s^{s_j} \bmod q$,其中 s_j 为选民 D_j 自己的私钥,p_s 为计票机构公钥,中间过程中要求选民保存 $H = MD5(C)$ 作为收据以供验证,然后把 $E1 + E2$ 发送给选举委员会的信箱 SendAndReceive@ EmailElection.com。

回收选票阶段:选举委员会通过邮件过滤只接受合法选民的 E-mail 发送的选票,并且在收到每个选民包含选票信息的邮件后,把该选民的邮件地址加入过滤名单,使其不能重复发送选票(所有选民在选举期间随时都可以通过给选举委员会受理投诉的信箱发送投诉信息)。在回收选票阶段结束后,选举委员会把收到邮件的地址列表公开,供所有选民验证自己的选票信息是否被选举委员会收到。如果没有投诉,选举委员会把所有邮件进行匿名化处理,然后把匿名化后的邮件转发到计票机构的信箱 StatisticalCommission @ EmailElection.com,并公布参加投票的选民邮件地址列表。

统计选票阶段:此时公正机构 CA 把选民公钥列表转交给计票机构,计票机构把收到的邮件内容 $E1 + E2$ 按照图1(b)中的流程对所有邮件进行解密验证,其中 $KP = p_j(j = 1,2,\cdots,n)$ 为选民 D_j 公钥,图(b)中收信方私钥 KRS 更新为会话密钥 $KRS = p_j^{s_s} \bmod q$,其中 $p_j(j = 1,2,\cdots,n)$ 为选民 D_j 公钥,s_s 为计票机构私钥。对符合验证的选票 C 把 $H1 = MD5(C)$ 和对应的公钥 p_j 保存到一个列表 ValidateTable 中;同时进行候选人选票统计,得到最后选举结果 R。统计完成后,计票机构把列表 ValidateTable 和选举结果 R 转发给选举委员会。

公示结果阶段:选举委员会审核选举结果 R 后,把列表 ValidateTable 和选举结果 R 公开发布。

3.2 系统的安全性分析

基于安全电子邮件协议 PGP 的安全性和计算 Diffe-Hellman 问题是困难的假设,对本文设计的电子选举系统进行安全性分析。

1)合法性。本文系统对选民资格的认定这一项放在网络之外(可以委托当地派出所机构认定)进行,根据认定的结果为每个合法选民分配对应的电子信箱,在系统运行过程中 E-mail 地址即合法选民的身份标识,SBF 提供了识别伪造邮件地址的解决方案。通过电子邮件完成选举过程。有效保证了只有合法的选举人才能参加投票。

2)完备性。系统中所有选民的私有信箱即是选民的身份象征,要利用弃权选民来代替合法选民投递选票时,必须同时拥有该选民的私有信箱地址、信箱密码和的私密密钥。假定某弃权选民没有更改邮箱密码,则公正机构 CA 知道选民的邮件地址和初始密码及其公钥,但不知道选民的私钥,故无法完成伪造合法选民投票过程;选举委员会在选举时仅知道选民的信箱地址,也无法独立完成伪造合法选民投票。在回收选票阶段结束后,选举委员会公开参与投票的选民邮件地址,可以让选民监督选举委员会和公正机构 CA。如果选委会和 CA 勾结,删除选民 D_j 的选票,然后伪造选民 D_j 私钥,并使用选民 D_j 的私有信箱投票,选民 D_j 可以根据自己选票内容的 hash 值和他们投出的选票 hash 值不同,指出他们的作弊行为;如果选民 D_j 弃权未参与投票过程时,当选委会公开邮件地址列表时可以指出他们的作弊行为。因此系统符合电子选举的完备性标准。

3)匿名性。选举委员会拥有选民的邮件地址,但没有计票机构的私钥,故不能看到选票的内容;计票机构看到的邮件是匿名化处理过的,计票机构只有选民的公钥列表,没有公钥列表和邮件地址的对应信息,故不能把选票内容与投票人联系起来;当选举委员会和计票机构勾结时,只能把邮件地址和选票内容配对,但没有邮件地址和具体选民的对应信息,依然无法把选票内容和具体投票人联系起来。

4)不可重复性。在系统中合法选民的私有邮件地址是其身份标识,当选民第一次投票后其邮件地址寄加入邮件过滤地址列表,根据邮件地址设立的邮件过滤有效避免了合法选民的重复投票问题。

5)公正性。计票过程具体操作要求计票机构输入私钥和选民公钥列表,系统根据选票的结构自动化完成选票的解密验证和统计过程,整个过程无人工干预,在很短时间内即可完成选票的验证和统计工作,有效避免了选举中间结果的泄露。

(下转第1476页)

[12]一样采用凸规划问题求解器来求解初值。因为改进的CCL将求得的增益矩阵作为已知的,未知的Lyapunov矩阵作为决策变量,在迭代过程中作为迭代终止条件,使得未知的Lyapunov矩阵具有更大的自由度,从而可以很好地减少迭代次数(如本文仅迭代54次),所以可以任意取初值。

5 结语

本文研究了一类关联时滞大系统分散鲁棒 H_∞ 控制问题,设计了状态反馈控制器,导出了此类关联时滞大系统分散状态反馈控制器存在的线性矩阵不等式充分条件,将结果扩展到了输出反馈中,数值仿真说明了该方法的有效性。

参考文献:

[1] NICULESCU S I. Delay effects on stability: A robust control approach[M]. Berlin: Springer-Verlag, 2001.

[2] LEE Y S, MOON Y S, KWON W H, *et al.* Delay-dependent robust H_∞ control for uncertain systems with a state-delay [J]. Automatica, 2004, 40(1): 65 - 72.

[3] MOON Y S, PARK P G, KWON W H, *et al.* Delay-dependent robust stabilization of uncertain state-delayed systems [J]. International Journal of Control, 2001, 74(14): 1447 - 1455.

[4] WU M, HE Y, SHE J H, *et al.* Delay-dependent criteria for robust stability of time-varying delay systems [J]. Automatica, 2004, 40(8): 1435 - 1439.

[5] KHARITONOV V L, ZHABKO A P. Lyapunov-krasovskii approach to the robust stability analysis of time-delay systems [J]. Automatica, 2003, 39(1): 15 - 20.

[6] PARK J H, JUNG H Y. On the exponential stability of a class of nonlinear systems including delayed perturbations [J]. Journal of Computational and Applied Mathematics, 2003, 159(2): 467 - 471.

[7] ZHANG XIAN-MING, WU MIN, SHE JIN-HUA, *et al.* Delay-dependent stabilization of linear systems with time-varying state and input delays [J]. Automatica, 2005, 41(8): 1405 - 1412.

[8] GHAOUI L E, OUSTRY F, AITRAMI M. A cone complementarity linearization algorithm for static output-feedback and related problem [J]. IEEE Transactions on Automatic Control, 1997, 42(8): 1171 - 1176.

[9] GAO HUI-JUN, WANG CHANG-HONG. Comments and further results on: A descriptor system approach to H_∞ control of linear time-delay systems[J]. IEEE Transactions on Automatic Control, 2003, 48(3): 520 - 525.

[10] GAO HUI-JUN, LAM J, WANG CHANG-HONG, *et al.* Delay-dependent output feedback stabilization of discrete-time systems with time-varying state delay[J]. IEE Proceedings: Control Theory and Applications, 2004, 151(6): 691 - 698.

[11] 孙敏慧, 邹云, 徐胜元. 随机马尔可夫切换系统的 H_∞ 模型降阶[J]. 控制理论与应用, 2006, 23(2): 269 - 274.

[12] 彭程, 王永. 智能悬梁臂的降阶 H_2 控制[J]. 中国科学技术大学学报, 2008, 38(3): 252 - 256.

[13] HE YONG, WU MIN, LIU GUO-PING, *et al.* Output feedback stabilization for discrete-time systems with a time-varying delay [C]// The 26th Chinese Control Conference: CCC 2007. Washington, DC: IEEE Press, 2007: 64 - 70.

[14] HE YONG, WU MIN, LIU GUO-PING, *et al.* New delay-dependent H_∞ Control for Systems with a time-varying delay [C]// The 17th World Congress. Seoul: [s.n.], 2008: 4 - 7.

[15] 张先明, 吴敏, 何勇. 不确定线性多时变时滞系统的时滞相关鲁棒控制[J]. 控制与决策, 2004, 19(5): 496 - 500.

(上接第1472页)

6)可验证性。选民本人根据填写选票阶段保存的 $H = MD5(C)$ 和自己的公钥 p_j 比对列表 ValidateTable 中的选项,验证自己的选票是否被正确统计,此时满足原子可校验;当选民对选举结果感到怀疑时,可以申请有CA和计票机构参加,重新统计收到的选票,并和公布的选举结果比对,能有效指出选举机构直接修改选举结果,公开正常列表的情况,此时满足公开可校验性。

7)无收据性。在填写选票阶段选民保存的 $H = MD5(C)$ 是选票内容的hash值,根据hash值是无法构造出原始选票内容的,选民无法构造出原始选票的内容就避免了贿选的可能。因此系统满足无收据性的含义。

4 结语

本文基于安全电子邮件协议PGP,设计了一个适合分散式选举的电子选举系统,并对其安全性进行了分析。系统符合电子选举的安全标准,并有效解决了大多数电子选举系统中存在的三个问题。新的电子选举系统操作流程规范,工程实现相对简单,为在国内正在进行的选举改革提供了一个好的解决方案。

参考文献:

[1] CHAUM D L. Untraceable electronic mail, return addresses, and digital pseudonyms [J]. Communications of the ACM, 1981, 24(2): 84 - 90.

[2] Electronic voting. [EB/OL]. [2008 - 03 - 20]. http://en.wikipedia.org/wiki/Electronic_voting.

[3] CHEN Y Y, JAN J K, CHEN C K. The design of a secure anonymous Internet voting system[J]. Computer and Security, 2004, 23(4): 330 - 337.

[4] 李秉礼. 具选票验证之匿名电子投票机制[D]. 宜兰, 台湾: 佛光大学, 2007.

[5] 秦为海. 基于匿名信道的电子选举协议的研究[D]. 成都: 西南交通大学, 2007.

[6] 姚立, 李仲麟. 一个实用的电子投票协议的设计[J]. 华南理工大学学报: 自然科学版, 1997, 25(5): 96 - 10.

[7] 谢金宝, 刘晖波. 基于盲、群签名和秘密共享的新型电子完全选举模型[J]. 微型机与应用, 2000, 19(9): 38 - 42.

[8] 中国选举科技网. 全球对智能电子选举的应用[EB/OL]. [2008 - 04 - 10]. http://www.electiontech.com.cn/displayinfo.php?id=55.

[9] 王思佳, 韩玮, 陈克非. 电子选举研究的挑战和进展[J]. 计算机工程, 2006, 32(15): 7 - 9.

[10] KOHNO T, STUBBLEFIELD A, RUBIN A D. Analysis of an electronic voting system [C]// IEEE Symposium on Security and Privacy. Washington, DC: IEEE Computer Society Press, 2004: 27 - 40.

[11] 廖正辉. PGP的研究与讨论[D]. 台中, 台湾: 逢甲大学, 2002.

[12] 张文东. 基于Web的安全电子邮件系统的研究与实现[D]. 乌鲁木齐: 新疆大学, 2005.

[13] Sender Policy Framework (SPF) for authorizing use of domains in E-Mail, Version 1 [S/OL]. [2008 - 08 - 10]. http://www.ietf.org/rfc/rfc4408.txt.

[14] 胡向东, 魏琴芳. 应用密码学[M]. 北京: 电子工业出版社, 2006.