文章编号：1007-1423(2015)27-0006-03 DOI：10.3969/j.issn.1007-1423.2015.27.002

基于 CPK 的盲签名在电子投票中的应用

刘涤

（武汉商学院，武汉 430058）

摘要：
随着计算机和网络的广泛使用，人类进入了信息化时代。人们在工作、学习、生活中已经体会到计算机和网络带来的便利和快捷。很多传统的学习、生活模式已经逐渐由网络和计算机改变。例如电子投票已经开始广泛使用，它克服传统投票的耗费人力、物力的缺点，给人们一种新的投票方式体验。探讨一种基于组合公钥密码技术的盲签名在电子投票中的应用。

关键词：
数字签名；组合公钥密码；盲签名；电子投票
基金项目：
武汉商学院校级青年项目基金（No.2013Q012）

0 引言

随着计算机和通信网络的广泛应用，信息的安全性已受到人们的普遍重视。信息安全已不仅仅局限于政治、军事以及外交领域，而且也与人们的日常生活息息先关。密码学理论和技术已得到迅速的发展，而电子投票就是密码学的一个重要应用[1]。传统的投票需要投票人、计票方、监票方同时在场，当选票全部统计完得出结果在监票方的公证下才可证明选票有效。这种投票方式是民主选举，表达民主意见的良好方式，但这种投票存在选举时间长，人力物力消耗大，容易拉票等问题，所以研究人员不断探索尝试新的投票方式，例如电子投票。

电子投票是集合了密码学相关技术，通过计算机和网络完成投票过程。安全的电子投票协议应满足如下要求[2]：

①完整性：所有的有效选票均被正确统计，不会遗漏任何有效选票；

②合法性：只有被身份认证的人才可以参加投票；

③不可重复性：投票人最多只能投一次票，不能重复投票；

④盲性：除了投票人本身之外，没有任何其他人知道选票内容；

⑤不可追踪性：选票公开后，无法根据选票追踪到投票人；

⑥健壮性：投票的中间结果不会被提前泄露，有一定的容错能力，即一些可能影响投票的事情均不能影响最终结果；

⑦不可伪造性：不被授权的人不允许参加投票，弃权的选票不能被更改；

⑧可验证性：投票人可以查询自己的选票是否被正确统计。

为了保护投票人的合法权益，在电子投票中引入盲签名技术是很有必要的。盲签名是一种特殊的数字签名，要求签名人在不知道签名内容的情况下签名，日后签名人无法判断这个签名是何时为何人所签。

1 组合公钥密码技术理论

组合公钥密码（Combined Public Key，简称 CPK）是以椭圆曲线密码学为基础，采用基于标识的组合密钥

方式生成新的密钥对。CPK 体系采用密钥集中生成，静态分发[3]和分散存储的管理体制，直接把用户的标识作为公钥，集中生成公、私钥对后统筹配发，分散存储在各用户手中和设备中。CPK 不直接公布用户的公钥，只公布公钥因子矩阵，用户的公钥通过公钥因子矩阵和标识的映射值计算出来。本文采用椭圆曲线离散对数问题构建组合公钥体制，并以有限域 $E_p(a,b)$（p 不等于 2 和 3 的素数）上椭圆曲线群说明该密钥管理算法的构建方法和原理[4]。

2 一种基于 CPK 的盲签名

根据已经公布的组合公钥算法原理，下面提出一种基于 CPK 的盲签名方案。

(1)初始化：由注册中心为消息拥有者 A 和签名者 B 分别生成组合密钥对 (d_A,P_A)，(d_B,P_B)，通过存储介质发给 A、B。

(2)盲化：消息拥有者 A 先将消息 m 取 Hash 值得到 H(m)。A 选择一个随机数或伪随机数 δ，使得 $0<\delta<n$，并计算 $\delta G=(x',y')$，$\xi=x' \bmod n$。如果 $\xi=0$ 则重新计算。盲化后消息为 $m'=H(m)\cdot\xi+G$，Alice 将盲消息 m′ 发给用户 B。

(3)签名：签名者 B 收到盲消息 m′ 后进行签名：

$Sig(m')=d_B\cdot m'=d_B(H(m)\cdot\xi+G) \bmod n$

签名者 B 将盲签名 Sig(m′) 发送给 A

(4)去盲：用户 A 收到 Sig(m′) 后计算

$$\begin{aligned}Sig(m)&=(Sig(m')-P_B)\cdot\xi(-1)\\&=(d_BH(m)\cdot\xi+P_B-P_B)\cdot\xi(-1)\\&=d_BH(m)\end{aligned}$$

(5)验证：

用户 A 计算 $(Sig(m')-P_B)\cdot G\cdot P_B^{-1}\cdot H(m)^{-1}=\xi'$

如果 $\xi'=\xi$ 则接受签名，如果 $\xi'\neq\xi$，则拒绝签名。

3 盲签名在电子投票中的应用

基于 CPK 组合公钥算法的盲签名的使用，满足了电子投票协议的各种安全性能的需求，保护了投票者的隐私权和投票内容，因此在电子投票协议中的应用具有重要的意义。设投票者 V，投票管理机构为 D，计票中心为 C。

(1)初始化：投票者 V，投票管理机构 D，计票中心 C 三方均向注册管理中心申请密钥对。

(2)注册：投票者 V 向投票管理机构 D 证明自己的身份，并提交两张内容分别为“同意”和“不同意”的选票（每张选票选一随机数位序列号加入），选票分别盲化[5]。管理机构判断投票者提交的身份证明是否合格，则为其产生唯一的身份标识 ID_V 和随机数 K_V[6]，并将两张选票签名后一并连同 (ID_V,K_V) 发回给 V。

(3)投票：①投票者 V 获得投票注册机构的公钥 P_D，并按照自己的意愿选好“同意”和“不同意”两张选票中的一种取哈希值 H(m)，盲化选票得 $m'=H(m)\cdot\xi+G$，ξ 是投票者产生的随机数，作为盲签因子。将盲化选票 (m',ID_V,K_V) 发给投票管理机构 D。

②投票管理机构验证投票者的 ID_V 和 K_V，如果是第一次投票则通过验证，如果不是第一次则拒收选票。通过身份验证后，管理机构为 V 的选票签名，得到 $Sig(m')=d_D\cdot m'=d_D(H(m)\cdot\xi+G) \bmod n$，其中 d_D 为管理机构 D 的私钥。D 将签名 Sig(m′) 发给 V。

③投票者 V 接收到 Sig(m′) 后，检查其合法性，若通过，则将 Sig(m′) 脱盲得到 $Sig(m)=(Sig(m')-PD)\cdot\xi^{-1}=d_DH(m)$。

(4)计票：投票者将 (Sig(m),G) 发给计票中心 C，计票中心利用投票管理机构 D 的公钥解密的到 H(m)，并随机生成一大整数 r_C，作为 H(m) 的唯一标识并且计入选票数据库。

(5)开票：投票时间结束后由计票中心公开选票并统计结果。

4 安全性分析

(1)只有被授权的投票者才可以参加选举，从而满足合法性要求；

(2)所有被授权的投票者只能投票一次，不能重复投票，因为管理中心发给投票者 K_V，保证了投票的不可重复性；

(3)在投票中使用盲签名，并且投票与计票分开，所有保证了投票的盲性、不可追踪性以及公平性；

(4)在该协议中，投票人可以对投票结果进行验证，从而保证了投票的完整性和可验证性。

5 结语

本文基于 CPK 组合公钥签名理论构造了盲签名并将该盲签名应用到电子投票中，提出了一种电子投

票协议。该协议满足电子投票的完整性、合法性、不可重复性、公平性、可验证性等安全需求。下一步将研究如何进一步提高投票的效率和安全性，设计出更加实用的电子投票方案。

参考文献：
[1]陈鲁生，沈世镒. 现代密码学[M]. 科学出版社，2002.
[2]周利娟，王新庄，梅万祺. 新的盲签名方案在电子投票协议中的运用[J]. 太原师范学院学报(自然科学版)，2008(2)：75-77.
[3]周加法，马涛，李益发. PKI、CPK、IBC 性能浅析[J]. 信息工程大学学报，2005,9 ：26-31.
[4 邓文，邓辉舫，田文春，郑东曦. 组合公钥标识认证系统的设计及密钥生成的实现[J]. 计算机应用，2007(8):1939-1941.
[5] 杨磊，陈小龙. 盲签名在电子投票中的安全应用服务[J]. 信息网络安全技术研究，2006(3).
[6] 宋程院，张串绒，曹帅. 一种盲签名方案及其在电子投票协议中的应用[J]. 计算机工程，2012(3)：139-141.

作者简介：
刘涤(1980-)，女，湖北黄石人，研究生，讲师，研究方向为信息与编码
收稿日期：2015-08-25　　修稿日期：2015-09-20

Application of Blind Signature Based on CPK in Electronic Voting

LIU Di

(Wuhan Business University, Wuhan 430058)

Abstract：
With the wide use of computers and networks, human beings have entered the information age. People in work, study, life has realized the computer and network bringing convenience. Many of the traditional learning, life mode has gradually changed from the network and computer. For example, electronic voting has begun to be widely used, it overcomes the shortcomings of the traditional voting of human and material resources, giving people a new way to vote. Discusses the application of a blind signature scheme in the electronic voting based on the combined public key cryptography.

Keywords：
Digital Signature; Combined Public Key Cryptography; Blind Signature; Electronic Voting