一种新的安全、实用的电子投票方案

赖瑾，范玉顺

（清华大学自动化系 北京 100084）

摘要: 电子选举是目前安全学界研究的一个热点问题。目前，为了满足大规模电子选举的要求，国内外学者提出了一些基于匿名通道的电子投票方案，但它们仍然存在一些重要的安全问题有待解决。针对这些问题，本文在总结“ Fujioka 方案 ”、“ Wei_Chiku 方案 ”、“ 谢金宝方案 ”和“ 姚立方案 ”的基础上，提出了一个新的电子投票方案。该方案利用在 RSA 体制下的门限多重盲签名技术来注册选票，防止签证人欺骗；并提出使用可验证的选票序列码来标识选票，保证选票唯一，并引入多个监票人来监督收票工作；从而解决了“ 选票碰撞 ”、“ 签证人欺骗 ”和“ 投票人中途退出 ”等问题，更具有安全性、实用性。

关键词: 电子投票; 数字签名; RSA; 盲签名; 门限多重签名;

中图分类号: X913

A new secure and practical electronic voting scheme

Lai Jin Fan Yushun

Department of Automation, Tsinghua University, Beijing 100084, China

Email: laijin00@mails.tsinghua.edu.cn

Abstract: These years, people have proposed several anonymous based electronic voting schemes, however there is still some security weakness in them. In this paper, A improved scheme is put forward in which we use the technology of multi_blind signature to prevent the probable cheating of visa officials, propose a kind of confirmable serial NO to identify the ballots and introduce custodians to supervise the work of ballots collector. So the scheme can resolve such problems as “ vote collision”, “ visa officials’ fraud ” and “ voter quit in the midway”, which exit in quite a lot of schemes of this type.

Key words: electronic voting; digital signature; RSA; blind signature; multisignature;

电子投票最早是 Chaul 提出的。它以各种密码学技术为理论基础，通过计算机和网络来完成投票的整个过程。使用电子投票系统，可以节省大量的人力物力资源，投票人不必到一个固定的投票中心投票，而管理机构也不必花费大量人力进行选票发放和选票统计的工作，而且电子投票系统可以减少种种人为的因素，做到更公平，更安全，更高效。如何利用电子投票的优势，设计出更具安全性、实用性的电子投票方案，是目前安全学界研究的一个热点。

1．电子投票方案的基本要求

一个安全电子投票方案 ,它应当满足以下几个基本要求：

1）**完备性** 所有合法的的投票都将计入点票结果；

2）**坚固性** 没有人能破坏投票，即：非法投票者包括签证人不能伪造选票，合法选民的中途退出以及加密参数的选取（一些随机数）都不会扰乱投票的进行；

3）**保密性** 选票内容是保密的，除了投票人本人以外，其他任何人（包括投票机构人员）不能够确定哪张选票是该投票人投的；

4）**不可重用性** 任何合法的投票人只能投一张选票；

5）**合法性** 只有具有投票权的投票人才有资格投票；

6）**公正性** 没有任何人知道投票的中间结果；

7）**可验证性** 投票人可以检验自己的投票被正确计入点票结果，投票过程之外的公

众也可以独立对投票结果进行检验，同时不需要牺牲投票参与者的个人隐私；另外，为了保证一个电子投票方案能够真正投入使用，它还应该满足：

8）**高效性** 尽量减少通讯量和计算量，使投票能在较短的时间内完成；

9）**便捷性** 投票人通过尽可能少的程序完成投票过程。

2．现有的电子投票方案分析

目前的电子投票系统总的来说可以分为两种：基于同态算法的投票系统和基于匿名信道的投票系统。基于同态算法的投票系统要求大量的通讯量和计算量，因此不适合大规模的投票活动。本文主要讨论基于匿名信道的电子投票系统。

匿名通道就是能隐藏消息来源的通道，例如抗追踪的电子邮件系统、电子公告牌等。该类型的系统，最著名的是 1992 年 Fujioka 提出来的基于盲签名 (Blind Signature)、位保证 (Bit Commitment)的投票系统[1]。这个方案的算法易于实现、网络通信量较小，是一个比较成功的电子投票方案。它在非政府部门得到了广泛的应用，如：MIT 的 EVOX 和 Washington 大学的 Sensus 系统等。但是，它在安全性方面还有一些缺陷：

1） 没能避免合法用户中途弃权所引起的混乱（注册选票总数不等于开票总数）；

2） 它没制止签证人的欺骗行为，由于在投票阶段选票的合法性完全由签证人的签名来验证，因此他能够伪造出合法选票，如果有投票者放权，那么他就能够进行冒名投票；

3） 位保证来区别不同的选票，很难避免“选票碰撞”，这样有些合法选民的合法选票由于该选票的位保证与别人重复，而可能不能被记入点票结果。

为了改进 Fujioka 电子投票方案的实用性，国内外许多学者做了研究。1999 年 Wei_Chiku 等人在此基础上提出了一种更复杂更精细的电子投票方案[2]。他们使用用户标志 tag_i 和单向函数处理过的选举决策 h_i 一起标识选票，试图解决“选票碰撞”的问题，以方便投票人监督，另外还使用采用多个收票监票人来监督收票工作；在这两点保证下，他们认为注册选票与计票总数的差异是选民弃权造成的，可移交权力部门处理，从而允许投票人中途退出投票。但是，它仍然没能制止签证人伪造合法选票；而且它的 tag_i 和 h_i 都使用了随机数和单向函数，由随机数的随机性和单向函数的特点可知用它们来标识选票，从本质上仍不能保证选票的唯一性，不能满足大规模选举的要求，另外，开票过程也过于繁复，不利于推广。

国内，谢金宝等人在 2001 年也提出了一个改进的电子投票方案[3]，该方案不启用签证人，而通过公证人群给选民发放匿名的成员证书，这样选民就可以直接匿名投票，这个方案有一定的新意，但是由于公证人群是给选民的盲化标志号签名，所以无法保证成员的标志号是唯一的。而且公证人群从本质上和签证人是一样的，如果处理不当，公证人也可以伪造成员证书，参与投票。另外，姚立等人在 1997 年也提出了一个简明的电子投票方案[10]，他们试图通过启用多个签证人防止签证人的欺骗，但他们采用签证人单独签名的方法（而非多重签名），而没有提出个有效的同步方案，反而为“一人多投”造成了可乘之机；而且单独签名大大增加了数字签名的长度，加大了网络通讯量；另外签证人是固定的，如果某个签证人无法工作，则注册选票的工作将无法进行。另外，这两个方案同样没能解决“选票碰撞”和“选民中途退出”等问题。

3．一种更有效的电子投票方案

3．1 方案概述

针对现有投票方案中存在的问题，本文提出了一种新的基于匿名通道的电子投票方案，它采用了 RSA 体制下的门限多重盲签名技术，使用可验证的选票系列码来标识选票，并引入了投票监票人，来解决上述的问题，而且因而更安全更实用。

- **参与者**：

(1) 投票者人 V ；

(2) 选票发放中心 D，实际上，她发放的是选票序列码及其签名；

(3) 注册中心，设有 m 个选票签证人 $E_i(i=1,\cdots,m)$ 负责检验投票人身份的合法性，并为合法选票签名；

(4) 收票人 C 负责收集选票，并统计点票结果；

(5) l 个收票监票人 $S_i(i=1,\cdots,l)$ 负责监督点票人的工作，任何时候，至少有一个监票人在工作。

- **密码系统**：

选票发放人、投票人和收票人各有自己的 RSA 数字签名系统：公钥（n,e）和私钥 d 。

为了加强注册中心的安全性，防止签证人伪造选票，我们需要采用更加复杂的加密协议，要求如下：

1）需要有 k 个或 k 个以上的签证人签名，才能计算出合法的

k 个或 k 个以上签证人的合法签名，无论是哪几个，都可以整合成一个 RSA 签名；这样如果某个签证人不能工作也不会对选举有影响了，而且最后多重签名最后输出的是一个标准 RSA 签名，这样我们构造重盲签名就比较容易了。

2）签证人无法从自己的秘钥和中心公钥中计算出其他签证人的公钥；

2）单个签名的长度被限制在一个范围内，即不会随着签证人数的增加而线性增加；

3）签证人秘钥的生成和发放有一套严格的协议；

4） 签证人之间，签证人与整合代理之间有尽量少的交互量。

我们采用基于 RSA 的门限多重盲签名，对外它公开其公钥（n_E,e_E），而内部的各个签证人 E_i 均有自己的签名秘钥 SK_i 和验证秘钥 VK_i。多重签名的门限为 k，（k 可以根据签证人的可靠度来计算）即只有收集到至少 k 的签证人的签名，才能整合成有效的注册中心签名。我们选择基于 RSA 的门限多重签名的算法满足以下几个要求[7]：

近几年人们提出了很多改进的基于 RSA 的门限多重签名方案，比较有代表性的有 IBM 提出的门限多重签名标准[7]和 Ivan B. Damgard[8]等人提出的不需要庄家的多重签名协议等。

- **投票过程**：

投票过程包括三个阶段：选票发放阶段、注册阶段、收票阶段、。投票人可能参加全部投票过程，也可能中途退出投票。假定：注册过但却没有投出选票的投票人同意把投票权转让给权力部门。

方案的框架图如下：

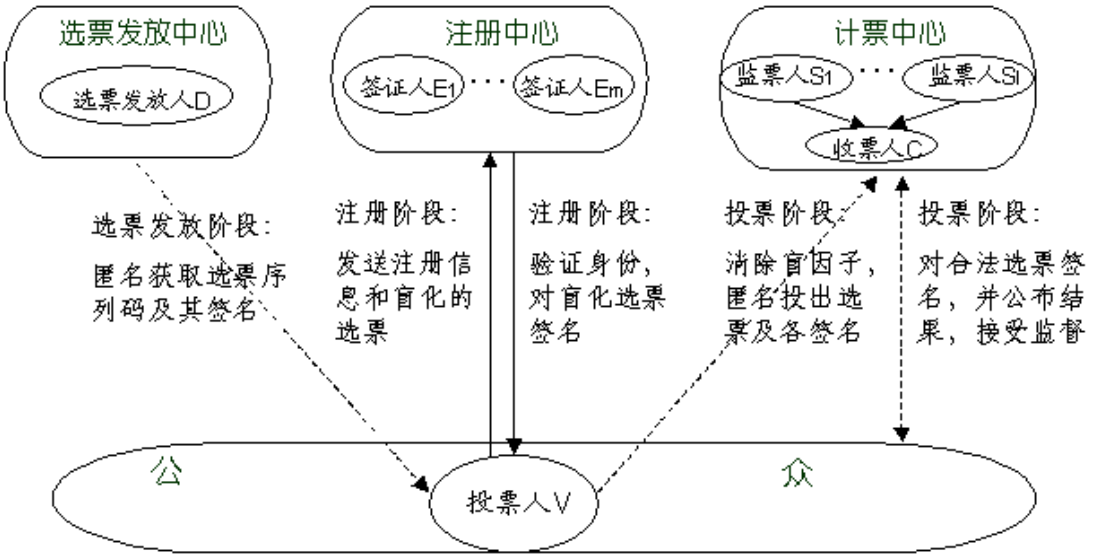

图 2：电子投票方案框架图

3．2 选票发放阶段

投票人以匿名的身份向选票发放中心申请序列码 $SerNO_i$ 及其签名：$S_D(SerNO_i) = (SerNO_i)^{e_D} \bmod n_D$。发放人 D 应保证：一个合法序列码只发放一次。当然，这个阶段投票人如果乐意可以申请多个选票序列码，但在下一个阶段他只能注册其中的一个。注意选票序列码应包括选举号，用于区别不同的选举。

3．3 注册阶段

第一步：投票人 V_i

(1) 计算电子选票 $b_i : b_i = \{SerNO_i \,\|\, sel_i\}$；其中 $SerNO_i$ 是选票序列码，sel_i 是选民填写的选票内容，‖是附加号，A‖B，表示把 B 串附在 A 串后面。

(2) 产生随机大数 k_i 满足 $k_i < n_E$，用 k_i 作为盲因子对 b_i 进行盲化，计算盲化选票 sb_i 得：$sb_i = (k_{2i})^{e_E}(b_i) \bmod n_E$，其中（$e_E$，$n_E$）是选票中心公布的公钥。

(3) 对 sb_i 进行签名，计算：$req_i = (Q \,\|\, sb_i)^{d_{V_i}} \bmod n_{V_i}$，Q 是选举序列号，用于验证投票人的签名；

(4) 发送 (ID_i, req_i) 给注册中心，ID_i 是投票人的身份证 ID 号。

第二步：注册中心

注册中心采用门限多重签名，其中门限数为 k，即只有收集至少 k 个签证人的签名才能获得注册中心的合法签名。注册中心的工作流程如下：

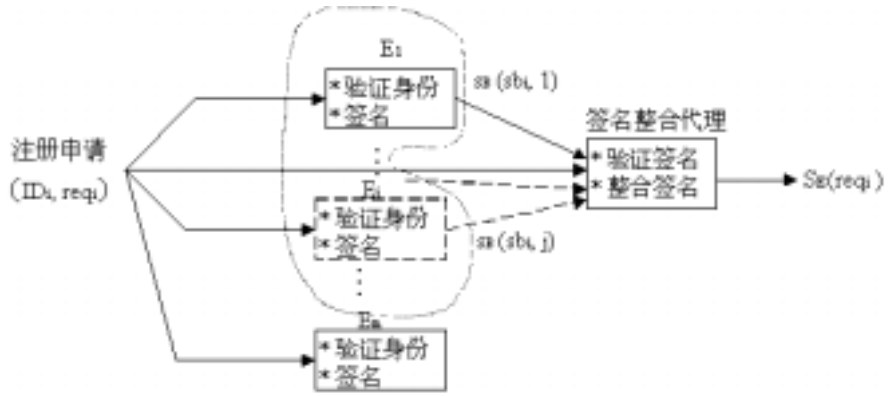

图 3 注册中心的工作流程图

注册申请被发送到各个签证人，签证人启动验证身份算法，判断是否能够签名，如果可以则对 req_i 签名，并将其发送到签名整合代理。整合代理先用签证人的验证密码验证签名是否有效，如果是则接受它，否则抛弃它。等到它收集到 k 个以上有效签名时，它将启动整合算法，把这些签名整合成一个签名，并在注册信息表登记注册信息：$(ID_i, req_i, S_E(sb_i))$，最后把签名 $S_E(sb_i)$ 发还给申请人。

其中签证人 E_j 的**验证算法**是如下：

（1）判断 ID_i 是否为合法选民的身份证号，如果是转入下一步，否则发回警告信息；

（2）判断 ID_i 是否在注册信息表里面，如果是，则把原有的签名发还给申请者；否则转下一步；

（3）用申请人的公钥解开 req_i，获得 Q 和 sb_i，判断 Q 是否正确，如果是，则证明此申请的确是 ID_i 对应的选民发出的，转入下一步，否则发回警告信息；

(4) 用 SK_j 对 sb_i 签名得，$SB(sb_i, j) = (sb_i)^{SK_j} \bmod n_E$，并把 $SB(sb_i, j)$ 发给整合代理。

而整合代理的验证算法和整合算法因采用的门限群签名方案而异，请参看[7],[8],[9]。

第三步：投票人 V_i

（1）用注册中心的公钥解开 $S_E(sb_i)$，验证是否为她的合法签名，如果是，则转下一步，否则重新申请；

（2）启动盲逆运算，计算注册中心对选票的签名：

$$
\begin{aligned}
& k_i^{e_E} \cdot S_E(sb_i) \bmod n_E \\
&= k_i^{e_E} \cdot S_E(k_i \cdot b_i) \bmod n_E \\
&= S_E(b_i) \bmod n_E \qquad \because \text{ 门限多重签名最后得到的是一个} \\
&= S_E(b_i) \qquad \text{RSA 签名，根据 RSA 签名系统的性质}
\end{aligned}
$$

3．4 收票阶段

第一步：投票人V_i通过匿名信道将$(SerNO_i, S_D(SerNO_i), sel_i, S_E(b_i))$发送给收票中心$C$。

第二步：收票人C在 l 个监票人的监督下：

(1) 验证$SerNO_i$是否唯一，如果是，则转入下一步，否则抛弃该非法选票；

(2) 利用选票发放人 D 的公钥，解开$S_D(SerNO_i)$验证其是否 D 对为选票序列码的合法签名，如果是则转入下一步，否则抛弃该非法选票；

(3) 用注册中心 E 的公钥，解开$S_E(b_i)$，验证其是否为 E 对$b_i = \{SerNO_i \| Sel_i\}$的合法签名，如果是则转入下一步，否则否则抛弃该非法选票；

(4) 对选票b_i签名得$S_C(b_i)$,并把$(SerNO_i, S_D(SerNO_i), sel_i, S_E(b_i), S_C(b_i))$写入选票信息表（CT）里，接受公众的监督。

注意：在这个阶段，l个收票监票人$S_i(i = 1,2,\cdots l)$负责监视每一张选票，保证每一项合理的$(SerNO_i, vote_i, z_i, CerSer_i, k_{1i}, g_i)$都能准确纪录到投票信息数据库，另外公众可以查看选票信息表（CT）确保自己的合法选票被记录在案。在这种保证下，ET 和 CT 选票总数的差异（如果存在这个差异）就是合法选民中途弃权造成的，权利机关将有权补足这个差异。

4．性能评价

1）完备性

我们引入多个监票人监督收票工作，就是为了保证所有合法的选票都将纪录并公布。另外，我们使用选票序列码 $SerNO_i$ 来标识选票，由于一个选票序列码只发放一次而合法序列码必须带有发放人 D 的签名（没有人能伪造序列码），而且一个人只能注册一张选票，因此每一张合法选票的标识都不一样，这样就能解决选票冲突的问题，保证合法选民的合法选票不会因为选票标识重复而被淘汰。

2）坚固性

在本案中，一张合法的选票需要经过多个签证人的签名，而且签证人无法猜测其他签证人的秘钥，而多重签名的门限是由签证人的可靠度计算出来的，这样签证人伪造合法选票的可能性就很小了。

对于其他非法投票者，本方案的坚固性等同于 RSA 秘钥系统，没有获得相应的签名私钥，他就不能伪造序列码签名、伪造合法用户身份、伪造注册中心签名，也就无法伪造选票。

而合法选民中途退出，主要有两种可能：第一，只申请序列码不注册；第二，只注册不

投票。对于第一种，它不会引起混乱，只是增加了一个废的序列码。第二种危害最大，它会使注册信息表 ET 和选票信息表 CT 的选票总数不一致，选民有弃权的权利，在所有安全措施下，我们可以认为 ET 表和 CT 表的差异就是弃权造成的。

3）保密性

选票发放阶段：投票人一匿名身份申请并下载序列码，不会暴露投票人的真实身份；注册阶段：使用盲签名技术，在盲因子 $(k_i)^{d_E}$ 的掩盖下，签证人并不能读取选票的真正内容；收票阶段：采用匿名信道发出选票，也不会暴露投票人的身份。

4）不可重用性

即一名合法投票人只能投一张票。本方案在注册阶段，签证人的职责之一验证注册人 ID 是否已经记录在注册信息表 ET 里，如果是，将拒绝为其选票签名，而收票人也会验证选票是否有注册中心的合法签名，如果没有，选票不予记录。在这种情况下一个投票人不可能投出多张选票，干扰选举过程。

5）合法性

只有合法投票者才能获得签证人的签名。

6）公正性

选票在送往注册中心前经过盲化，因此选票的内容中是不可见的，只有投票人本人才能够验证选票的内容。

7) 可验证性

系统将公开注册信息表 ET 和选票信息表 CT。通过查看选票信息表 CT，投票人可以查看自己的选票是否被正确记录。所有数字签名的公钥都是公开的，这样就可以验证每一阶段的数据。

8）实用性

首先，本方案建立在匿名通道之上，匿名通道方案相对同态算法方案具有通讯量小，计算量小的优点；我们还采用 RSA 公钥体制，它是目前比较流行的公钥体制，普及起来比较容易，而且签名数据量比较少，速度也比 DSS 快。

5．结论

本文提出的方案可以说是方“ Fujioka 方案 ”、“ Wei_Chiku 方案 ”、“ 谢金宝方案 ”和“ 姚立方案 ”的综合和发展。这个方案利用 RSA 体制下门限多重盲签名技术和可验证的选票序列码等技术，解决了“ 投票人中途退出 ”、“ 签证人欺诈 ”、“ 选票碰撞 ”三大难题，并简化了投票过程，因而很具安全性、实用性。

参考文献

[1] A. Fujioka,T. Okatoma,and K. Ohta. A Practical Secret Voting Scheme for Large Scale Elections[J]. Proceedings of Auscrypt,1992,92 :244－251.

[2] Wei-Chi Ku, Sheng-De Wang. A secure and practical electronic voting scheme[J]. Computer Communications,1999, 22: 279－286.

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

[4] Andreu Riera, JosepRifà and Joan Borrell. Efficient construction of vote-tags to allow open objection to the tally in electronic elections[J]. Information Processing Letters, 2000, 75 :211--215.

[5] 段 琪, 孙淑玲．电子选举研究概况[J]．计算机应用,1998, 18(4): 23—25.

[6] 卢开澄．计算机密码学．北京：清华大学出版社[M]，1999.
[7] Victor Shoup. Practical Threshold Signatures. [EB/OL]. http://citeseer.nj.nec.com/512.html.
[8] Ivan B. Damgard and Maciej Koprowski. Practical Threshold RSA Signature without a trusted dealer. [EB/OL] http://www.brics.dk/RS/00/30/BRICS-RS-00-30.pdf
[9] Yair Frankel and Yvo G. Desmedt. Prallel reliable threshold multisignature. http://citeseer.nj.nec.com/frankel92parallel.html
[10] 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—99.