一种改进的预加密可验证电子投票方案*

苑 浩[1], 杨宝霖[2]

(1. 华东师范大学 计算机科学技术系, 上海 200241; 2. 皖北煤电集团有限公司 信息中心, 安徽 宿州 234000)

摘 要: 简要回顾 Morales-Rocha 等人的方案,针对这些缺陷提出相应的解决方案。经过性能分析并与原方案对比后,得出结论:改进方案解决了以上缺陷,从而具有优于原方案的性能。

关键词: 电子投票; 预加密; 可验证; 投票码; 验证码

中图分类号: TP309 **文献标志码**: A **文章编号**: 1001-3695(2012)08-3048-05

doi:10.3969/j.issn.1001-3695.2012.08.064

Improved pre-encrypted verifiable electronic voting scheme

YUAN Hao[1], YANG Bao-lin[2]

(1. *Dept. of Computer Science & Technology, East China Normal University, Shanghai* 200241, *China*; 2. *Information Centre, Wanbei Coal-electricity Group Co., LTD, Suzhou Anhui* 234000, *China*)

Abstract: This paper briefly reviewed Morales-Rocha et al.'s scheme, gave a new scheme with solutions to these flaws. After analyzing the performance and contrasting with their scheme, this paper made a conclusion that the new scheme solves the flaws above and has better performance.

Key words: electronic voting; pre-encrypted; verifiable; voting code; verification code

在传统的纸质投票系统中,投票者只需将自己的选票放入投票箱,因此可以很方便地验证自己的选票是否被正确地记录。但是,投票者无法验证自己的选票是否被正确统计。而电子投票系统除了能使投票者验证自己选票是否被正确记录以外,还能提供给投票者验证自己选票是否被正确统计的方法,从而使得投票系统的安全性更高。此外,电子投票还有高效率的选票统计、便捷的远程投票等优势。

为了保证投票系统的安全性,电子投票系统在设计的过程中需要满足一些最基本的性质[1],如保密性、完整性、认证性、不可胁迫性、可验证性等。现有的电子投票方案主要分为基于盲签名[2]、同态加密[3]、mix-net[4]三类。这些方案中,选票内容的加密主要都在客户端完成,如近期提出的对抗关系攻击的基于 mix-net 的电子投票方案[5]。而基于预加密的电子投票方案[6]是比较新颖的一种选票加密形式,主要用于防止恶意软件在客户端随意操纵选票。Morales-Rocha 等人[7]在预加密的基础之上提出了一种可验证的投票方案,此方案比同样提供可验证性的 Helios 系统[8]运算量更低。而 Morales-Rocha 等人的方案在安全性上存在一些问题,本文将分析指出这些问题,并提出改进方案。

1 预备知识

1.1 选票预加密方案

此类方案主要基于投票码,并且能有效检验选票是否被服务器接收,如文献[9]。

1)预加密方案的主要特征

(1)对同一个投票者,不同候选人由不同的字母和数字表示,而同一个候选人对于不同投票者有不同的投票码。

(2)选票生成机构将预加密的选票通过独立安全的通信信道发送给投票者。

(3)此方案的选票加密并不在投票方进行,因此投票者在投递选票之前无须使用基于密码学的选票加密软件。

(4)投票者的选择策略通过投票码来表达,即使攻击者截获了投票码也无法得知投票者的选择。

(5)此类方案还加入一些验证码以供投票者验证选票是否被投票服务器接收。验证方法是检查从投票服务器收到的验证码是否与自己给出的验证码一致,选票如图 1 所示。

ballot ID: 3643748		
candidate	voting code	verification code
Mitt Romney	f4z28p	74622
John McCain	57er94	98561

图 1 选票示意图

2)对选票预加密方案存在的主要攻击

(1)对选票进行操作。攻击者在投票者收到选票前截获选票并将某候选人的投票码、验证码等同别的候选人对调,过程如图 2 所示。

ballot ID: 3643748		
candidate	voting code	verification code
Mitt Romney	f4z28p	74622
John McCain	57er94	98561

ballot ID: 3643748		
candidate	voting code	verification code
Mitt Romney	57er94	98561
John McCain	f4z28p	74622

图 2 候选人对调过程

(2)破坏投票者的保密性。攻击者只要满足以下两点就能将投票者身份与选票一一对应:a)攻击者能通过截获或直

收稿日期: 2011-12-24; **修回日期**: 2012-01-30 **基金项目**: 国家教育部博士点基金资助项目(20070269005)

作者简介:苑浩(1986-),男,重庆人,硕士,主要研究方向为信息安全、密码学等(hao.yuan158381@gmail.com);杨宝霖(1965-),男,安徽宿州人,硕士,主要研究方向为企业信息化建设、管理.

接从投票者那里得到预加密选票;b)攻击者通过截获或直接从投票服务器上得到投票者的投票码。在没有安全的连接措施的情况下,以上两个条件都有可能被攻击者实现。

(3)选票收买(或选票胁迫)。投票者投票之后,如果投票码与投票者身份被公布,或者买票者能够以一定的方式得知最终的投票码和与之对应的投票者身份,那么如果投票者再出示自己的选票给买票者,很有可能构成选票收买。

1.2　有投票回执的方案

利用投票回执,投票者能验证自己的选票是否被统计中心接收并统计。一旦投票者发现自己的选票没被正确统计,只需向相应机构出示自己的回执即可,如文献[9]。投票回执通常需要有一个安全的密码学证明,以防止第三方机构从中推测出选票内容。

对投票回执方案存在的可能攻击有:a)窜改投票回执的内容而不被发现;b)由于方案设计得不合理,选举机构可能会对有效回执否认;c)投票者、选举机构等可能自己生成虚假回执。

2　Morales-Rocha 等人的方案描述

此方案基于预加密技术,同时增加了投票回执以加强选举的安全性。假设攻击者只能截获中间传输的消息而不能直接控制、监听投票客户端和服务器。投票过程的参与者主要有五个部分:选票分发机构 *VD*、投票者 V_i、投票平台 *VP*、投票服务器 *VS*、统计中心 *CS*。投票步骤主要分为预选举阶段、投票阶段、统计阶段。

假设有 m 个候选人、n 个投票者,公开投票服务器公钥 P_{VS}、统计中心公钥 P_{CS}、与投票者身份对应的投票者公钥 P_{V_i}。投票服务器的私钥 S_{VS}、投票者自己的私钥 S_{V_i} 都由各自保存。统计中心 *CS* 由多个部分构成,*CS* 的私钥被分为许多份分发到多个统计中心,只有这些统计中心共同协作才能得到最终私钥 S_{CS},从而防止单个统计中心因密钥泄露而导致选票信息暴露,提高了安全性。

2.1　预选举阶段

1)生成预加密选票

(1)选票分发机构 *VD* 随机生成独立的选票号 $B-\mathrm{ID}_i$(运算采用二进制),对每个票号 $B-\mathrm{ID}_i$ 生成两个随机数 A_i、B_i,它们将被用于生成投票码和验证码。

(2)生成独立的候选人标号 $C-\mathrm{ID}_i$ 使其与每个候选人一一对应,对每个候选人生成一个中间值 $\mathrm{Inter}_{i,j}$:$(B-\mathrm{ID}_i \oplus C-\mathrm{ID}_i)$。

(3)投票码 $\mathrm{cod}_{i,j}$:$(\mathrm{Inter}_{i,j} \oplus A_i)$。

验证码 $\mathrm{ver}_{i,j}$:$[B_i \oplus (B-\mathrm{ID}_i \oplus \mathrm{cod}_{i,j})]$。

(4)生成随机密钥 k_{1i},用于加密 A_i,再用投票机构统计中心 *CS* 的公钥 P_{CS} 将 k_{1i} 加密得到:$KA_i=[(A_i)_{k_{1i}},(k_{1i})_{P_{CS}}]$。

(5)随机生成对称密钥 k_{2i},用其加密 B_i。k_{2i} 用投票服务器的公钥 P_{VS} 加密。最后得到:$KB_i=[(B_i)_{k_{2i}},(k_{2i})_{P_{VS}}]$。

(6)$\{(B-\mathrm{ID}_1,KA_1),(B-\mathrm{ID}_2,KA_2),\cdots,(B-\mathrm{ID}_n,KA_n)\}$ 被分发给统计中心,统计中心用 A_i 解密投票码 $\mathrm{cod}_{i,j}$,并统计投票结果。

(7)$\{(B-\mathrm{ID}_1,KB_1),(B-\mathrm{ID}_2,KB_2),\cdots,(B-\mathrm{ID}_n,KB_n)\}$ 被存放在投票服务器 *VS* 上,从而由 B_i 可以计算得到验证码 $\mathrm{ver}_{i,j}$,便于以后返还给投票者验证。

2)打印投票者信息

投票者信息如姓名、地址、投票注意事项等被打印在另外一张表上。

3)分发预加密的选票和投票者信息

随机分配预加密选票给投票者,将选票封装好之后,随机将其和投票者信息组合在一起形成一个包裹,通过邮局或者其他方式投递给投票者。

为了防止攻击者因中途截获选票得到验证码而对选票进行窜改和操纵,验证码并不打印在选票上,投票者可以通过特定网站获得验证码。此时需要投票者输入打印在选票上的密码,该密码用涂层覆盖,需要刮开才可见,如图 3 所示。

ballot ID:3643748		
candidate	voting code	password
Mitt Romney	f4z28p	
John McCain	57er94	

图 3　用涂层覆盖的选票

2.2　投票阶段

假设投票者之前已经获得相关机构颁发的电子证书,通过证书认证后,投票者通过投票平台 *VP* 投票。

1)生成选票与投票回执

(1)投票者通过对应的投票码 $\mathrm{cod}_{i,j}$ 确定自己支持的候选人。

(2)随机生成一个随机数 $R-\mathrm{ID}_i$。

(3)通过哈希函数 H 计算

$$r_i=[H(R-\mathrm{ID}_i|E-\mathrm{ID}_i)|[H(R-\mathrm{ID}_i|E-\mathrm{ID}_i)]_{S_{V_i}}]$$

其中,$E-\mathrm{ID}_i$ 是此次选举的选举号。

(4)投票者生成一个秘密消息:

$$S_i=[[H(\mathrm{cod}_{i,j})|R-\mathrm{ID}_i]_{S_{V_i}}]_{P_{CS}}$$

2)发送选票和投票回执

投票者发送消息 M_i 给投票服务器:

$$M_i=[\mathrm{cod}_{i,j}|r_i|S_i|B-\mathrm{ID}_i]$$

3)投票服务器检测回执的有效性并计算验证码

(1)通过 r_i 上的电子签名来验证投票者合法性。

(2)通过对 r_i 再签名得到 $R_i=[r_i]_{S_{VS}}$。

(3)由 B_i、$B-\mathrm{ID}_i$ 和 $\mathrm{cod}_{i,j}$ 计算得到:

$$\mathrm{ver}_{i,j}=[B_i \oplus (B-\mathrm{ID}_i \oplus \mathrm{cod}_{i,j})]$$

(4)投票回执 R_i 与 $\mathrm{ver}_{i,j}$ 被发回给投票者。

(5)将 $\mathrm{cod}_{i,j}$ 用统计中心的公钥 P_{CS} 加密得到:

$$\mathrm{cod}'_{i,j}=[\mathrm{cod}_{i,j}]_{P_{CS}}$$

(6)将 $\mathrm{cod}'_{i,j}$、S_i、$B-\mathrm{ID}_i$ 用投票服务器 *VS* 的私钥 S_{VS} 签名,并附上由哈希函数 H 得到的哈希值得出 com,将其与 R_i 一起保存:

$$\mathrm{com}=[H(\mathrm{cod}'_{i,j}|S_i|B-\mathrm{ID}_i|[\mathrm{cod}'_{i,j}|S_i|B-\mathrm{ID}_i]_{S_{VS}}]$$

4)投票者验证验证码 $\mathrm{ver}_{i,j}$,通过后保存 R_i。

2.3　统计阶段

1)统计中心解密投票码

(1)统计中心下载保存在投票服务器中的 com 和 R_i。

(2)将 com 与 P_{VS} 计算得到$[\mathrm{cod}'_{i,j}|S_i|B-\mathrm{ID}_i]$,将其哈希后与 com 中的 $H(\mathrm{cod}'_{i,j}|S_i|B-\mathrm{ID}_i)$ 比较是否一致。若验证通过,统计中心用私钥解密 $\mathrm{cod}'_{i,j}$ 得到 $\mathrm{cod}_{i,j}$。

(3)解密 S_i,验证投票者身份,得到[$H(\mathrm{cod}_{i,j})\,|\,R-\mathrm{ID}_i$]。

(4)将 $\mathrm{cod}_{i,j}$哈希后与[$H(\mathrm{cod}_{i,j})\,|\,R-\mathrm{ID}_i$]中的$H(\mathrm{cod}_{i,j})$比较是否被窜改。同时,将[$H(\mathrm{cod}_{i,j})\,|\,R-\mathrm{ID}_i$]中的 $R-\mathrm{ID}_i$ 取出并计算 $H(R-\mathrm{ID}_i\,|\,E-\mathrm{ID}_i)$,将其与 r_i 中的 $H(R-\mathrm{ID}_i\,|\,E-\mathrm{ID}_i)$比较是否一致。

(5)由统计中心已知的 A_i 和 $B-\mathrm{ID}_i$ 将 $\mathrm{cod}_{i,j}$解密得到 $C-\mathrm{ID}_i$,即候选人号码。

2)统计并公布结果

公布统计的总结果和所有的随机数 $R-\mathrm{ID}_i$。

3)投票者用自己的回执验证

投票者通过查看自己的 $R-\mathrm{ID}_i$ 是否被公布来判断选票是否被统计。如果没有被统计,投票者出示自己的 R_i。

3 原方案的缺陷分析

3.1 选票的分发方式

分发选票是通过邮寄的方式,这种方式可能会在选票邮寄的过程中丢失选票。同时,选票是纸质,投票者太多、分布太广时邮寄成本比较高,不适用于大型投票。

3.2 选票分发机构的权限

因为选票分发机构权限太大,其有可能跳过随机打包步骤,而将投票者身份与选票联系起来,并且消息 M_i 在传送过程中没有加密,一旦该机构截获到投票者发送出的投票码,就能从选票中发现投票者实际选择的候选人,从而增加了投票者隐私泄露的危险性,不能保证电子投票的保密性。

3.3 统计过程中的投票者隐私

设计 S_i 时用到了投票者签名因而统计中心能够将 $\mathrm{cod}_{i,j}$与投票者身份联系起来,将 $\mathrm{cod}_{i,j}$解密后,统计中心就能将投票者身份与该投票者选择的候选人一一对应。由此,统计过程严重暴露了投票者隐私,不能保证电子投票的保密性。

3.4 统计结果的窜改

统计中心只公布最后的 $R-\mathrm{ID}_i$ 和总的统计结果,投票者只能看到自己的选票是否到达统计中心,不能确定自己的选票是否真正被统计中心统计到最终结果中,统计中心对最终投票结果的肆意窜改无法被发现,即不满足可验证性。

4 改进方案

投票过程的参与者主要有五个部分:选票生成机构 *VG*、选票分发机构 *VD*、投票者 $V_1,V_2,\cdots,V_i,\cdots,V_n$、投票平台 *VP*、投票服务器 *VS*、统计中心 *CS*。投票步骤主要包括预选举阶段、投票阶段、统计阶段。

假设参与投票的五个部分不存在联合作假,即如果出现选举过程的参与者作假,只可能是该五个部分中的一个。假设有 m 个候选人,n 个投票者,$K_1,K_2,\cdots,K_i,\cdots,K_n$ 为与 *VG* 生成选票对应的密钥,公开投票服务器公钥 P_{VS}、统计中心公钥 P_{CS}、投票平台公钥 P_{VP}。选票生成机构的私钥 S_{VG}、投票服务器的私钥 S_{VS}、投票平台私钥 S_{VP}由它们自己妥善保管。统计中心 *CS* 由多个部分构成,*CS* 的私钥被分为许多份分发到多个统计中心,只有这些统计中心共同协作才能得到最终私钥 S_{CS}。P_{system}为整个投票系统公钥,对应的私钥分为许多份分发到整个投票系统的各个部门,只有这些部门共同协作才能最终得到对应的私钥 S_{system}。

4.1 预选举阶段

1)投票者注册

在进行选举之前,所有投票者 V_i 到一个指定机构注册,由该机构颁发给每位投票者一份电子证书。

2)生成预加密选票

(1)选票生成机构 *VG* 随机生成独立的选票号 $B-\mathrm{ID}_i$(运算采用二进制),对每个票号 $B-\mathrm{ID}_i$ 生成两个随机数 A_i、B_i,它们将被用于生成投票码和验证码。

(2)生成独立的候选人标号 $C-\mathrm{ID}_i$ 使其与每个候选人一一对应,对每个候选人生成一个中间值 $\mathrm{Inter}_{i,j}$:$(B-\mathrm{ID}_i\oplus C-\mathrm{ID}_i)$。

(3)投票码 $\mathrm{cod}_{i,j}$:$(\mathrm{Inter}_{i,j}\oplus A_i)$。

验证码 $\mathrm{ver}_{i,j}$:$[B_i\oplus(B-\mathrm{ID}_i\oplus\mathrm{cod}_{i,j})]$。

(4)生成随机密钥 k_{1i},用于加密 A_i,再用投票机构统计中心 *CS* 的公钥 P_{CS}将 k_{1i}加密得到:$KA_i=[(A_i)_{k_{1i}},(k_{1i})_{P_{CS}}]$。

(5) 随机生成对称密钥 k_{2i},用其加密 B_i。k_{2i}用投票服务器的公钥 P_{VS}加密,最后得到:$KB_i=[(B_i)_{k_{2i}},(k_{2i})_{P_{VS}}]$。

(6)$\{(B-\mathrm{ID}_1,KA_1),(B-\mathrm{ID}_2,KA_2),\cdots,(B-\mathrm{ID}_n,KA_n)\}$被分发给统计中心,统计中心用 A_i 解密投票码 $\mathrm{cod}_{i,j}$,并统计投票结果。

(7)$\{(B-\mathrm{ID}_1,KB_1),(B-\mathrm{ID}_2,KB_2),\cdots,(B-\mathrm{ID}_n,KB_n)\}$被存放在投票服务器 *VS* 上,从而由 B_i 计算得到验证码 $\mathrm{ver}_{i,j}$返还给投票者验证。

(8)将选票生成好之后,分别再用各自对应的密钥 K_1,$K_2,\cdots,K_i,\cdots,K_n$ 对各选票信息加密,从而防止分发机构看到此信息。用自己的私钥 S_{VG}对所有已加密选票签名后,将选票传给原方案中的分发机构 *VD*。由 K_i 加密后的选票如图 4 所示。

ballot ID: 3643748		
candidate	voting code	verification code
8pe4vf6l	fxd4sf9	r5kw03
sd8cw5u	rtu86yk	m94gx5

图 4 加密后的选票

(9)选票生成机构 *VG* 在特定的服务器上提供一个查询系统,该系统能使投票者查询与选票号对应密钥 K_i。在通过电子证书进行身份认证之后,投票者往系统中输入选票号、选票上第一行编码(如 8pe4vf6lfxd4sf9r5kw03)以确定自己确实拥有此选票,即可获得与自己选票号对应的密钥并解密自己的选票,一个投票者成功获得一次自己的密钥后不能再从该系统进行查询。

3)打印投票者信息

投票者信息(如姓名、邮件地址、投票注意事项等)被打印在另外一张表上。

4)分发预加密的选票和投票者信息

分发机构 *VD* 随机分配预加密选票给投票者,将选票封装好之后,随机将其和投票者信息组合在一起通过电子邮件等方式传送给投票者。

4.2 投票阶段

投票者解密选票后,再经投票平台 *VP* 电子证书认证通过,就能由投票平台从客户端投票了。

1)生成选票与投票回执

(1)投票平台 *VP* 返回给投票者 V_i 一个随机数 X_i,并对 X_i

用自己的私钥签名得到 $X_{iS_{VP}}$。

(2)投票者通过选票上对应的投票码 $\mathrm{cod}_{i,j}$确定自己支持的候选人。

(3)生成一个随机数 $R-\mathrm{ID}_i$。

(4)通过哈希函数 H 计算

$$r_i = H(R-\mathrm{ID}_i \mid E-\mathrm{ID}_i)$$

其中,$E-\mathrm{ID}_i$ 是选举号。

(5)投票者生成一个秘密消息:

$$S_i = [H(\mathrm{cod}_{i,j}) \mid R-\mathrm{ID}_i]_{P_{CS}}$$

2)发送选票和投票回执

投票者将消息 M_i 用投票服务器 VS 公钥 P_{VS}加密后发送给投票服务器

$$M_i = [\mathrm{cod}_{i,j} \mid r_i \mid S_i \mid B-\mathrm{ID}_i \mid X_i \mid X_{iS_{VP}}]_{P_{VS}}$$

3)投票服务器检测回执的有效性并计算验证码

得到 M_i 以后,投票服务器进行以下步骤:

(1)用投票平台的公钥解密 $X_{iS_{VP}}$,看是否等于 X_i。

(2)如果验证通过,用整个投票系统的公钥 P_{system}加密 r_i(如采用 ElGamal 加密),再用私钥 S_{VS} 签名得到 $R'_i = [[r_i]_{P_{\mathrm{system}}} \mid [[r_i]_{P_{\mathrm{system}}}]_{S_{VS}}]$。

(3)由 B_i、$B-\mathrm{ID}_i$ 和 $\mathrm{cod}_{i,j}$计算得到

$$\mathrm{ver}_{i,j} = [B_i \oplus (B-\mathrm{ID}_i \oplus \mathrm{cod}_{i,j})]$$

(4)投票回执 R'_i 与 $\mathrm{ver}_{i,j}$被发回给投票者。

(5)将 $\mathrm{cod}_{i,j}$用统计中心的公钥 P_{CS}加密得到:$\mathrm{cod}'_{i,j} = [\mathrm{cod}_{i,j}]_{P_{CS}}$,并重新计算 $R_i = [r_i]_{S_{VS}}$。

(6)将 $\mathrm{cod}'_{i,j}$、S_i、$B-\mathrm{ID}_i$ 用投票服务器 VS 签名得到 $[\mathrm{cod}'_{i,j} \mid S_i \mid B-\mathrm{ID}_i]_{S_{VS}}$,计算 com 并与 R_i 一起保存:

$$\mathrm{com} = [H(\mathrm{cod}'_{i,j} \mid S_i \mid B-\mathrm{ID}_i) \mid [\mathrm{cod}'_{i,j} \mid S_i \mid B-\mathrm{ID}_i]_{S_{VS}}]$$

4)投票者验证 $\mathrm{ver}_{i,j}$,验证通过后保存 R'_i

发生分歧时,投票者出示 r_i、R'_i 给相关部门,最终由整个投票系统协作恢复出 P_{system}的私钥,进而确定 r_i 的有效性。

4.3　统计阶段

1)统计中心解密投票码

(1)统计中心从投票服务器下载 com 和 R_i。

(2)将 com 与 P_{VS}计算得到$[\mathrm{cod}'_{i,j} \mid S_i \mid B-\mathrm{ID}_i]$,将其哈希后与 com 中的 $H(\mathrm{cod}'_{i,j} \mid S_i \mid B-\mathrm{ID}_i)$ 比较,看是否一致。若验证通过,统计中心用私钥解密 $\mathrm{cod}'_{i,j}$得到 $\mathrm{cod}_{i,j}$。

(3)解密 S_i 得到 $H(\mathrm{cod}_{i,j}) \mid R-\mathrm{ID}_i$。

(4)将解密得到的 $\mathrm{cod}_{i,j}$哈希之后与 $H(\mathrm{cod}_{i,j}) \mid R-\mathrm{ID}_i$ 中的 $H(\mathrm{cod}_{i,j})$ 比较,看是否被窜改。同时,将 $H(\mathrm{cod}_{i,j}) \mid R-\mathrm{ID}_i$ 中的 $R-\mathrm{ID}_i$ 取出并计算 $H(R-\mathrm{ID}_i \mid E-\mathrm{ID}_i)$,将其与 r_i 中的 $H(R-\mathrm{ID}_i \mid E-\mathrm{ID}_i)$ 比较看是否一致,由此保证 r_i 的有效性。

(5)由 A_i、$B-\mathrm{ID}_i$ 将 $\mathrm{cod}_{i,j}$解密得到 $C-\mathrm{ID}_i$。由于发送了 $B-\mathrm{ID}_i$ 并且能解密出 $C-\mathrm{ID}_i$,此 $B-\mathrm{ID}_i$ 是有效的,以后遇到的相同有效 $B-\mathrm{ID}_i$ 对应的候选人编号 $C-\mathrm{ID}_i$ 将忽略不计,以保证投票者不能重复投票。

2)统计并公布结果

公布统计的总结果和所有的随机数 $R-\mathrm{ID}_i$ 与对应的候选人,让投票者验证。

3)投票者用自己的回执验证

投票者通过查看自己的 $R-\mathrm{ID}_i$ 与对应的候选人是否被公布来判断选票是否被统计。如果没有被统计,投票者出示自己的 R'_i。

5　安全性分析与对比

改进后的方案满足电子投票需要保证的安全性质:

a)保密性。投票的过程中,选票内容都不能与投票者身份相联系。

改进方案中,选票信息通过加密后再随机分发给投票者,因此即使是分发机构也无法确定投票者具体的选票内容,更加无法将选票信息同投票者身份联系起来。

b)完整性。投票过程中的不诚实行为都会被发现。

在改进方案中,选票的生成与随机分发由不同机构完成,并且分发前已对选票加密。因此选票生成机构与选票分发机构无法将投票者与对应选票联系起来;选票是预加密的,因此投票者无法对选票信息作任何窜改,同时如果投票者截获到其他投票者的加密选票,因为系统只允许解密一次自己选票,因此无法获得他人选票信息,并且由于 $B-\mathrm{ID}_i$ 对每个投票者来说是唯一的,投票者无法重复投票;如果投票服务器伪造发送给统计中心的 $\mathrm{cod}_{i,j}$,那么投票服务器同时将伪造一个新的 S_i 发送给统计中心,于是同时需要伪造 $R-\mathrm{ID}_i$。而统计中心最终会公布 $R-\mathrm{ID}_i$,投票者一旦发现 $R-\mathrm{ID}_i$ 被伪造,将出示自己的 r_i、R'_i。经投票系统确定其有效性后,统计中心会出示 com,投票者发现其中 S_i 与自己生成的 S_i 不同而确定投票服务器实施了伪造;统计中心最后会公布所有 $R-\mathrm{ID}_i$ 与对应的候选人以及最终的统计结果,$R-\mathrm{ID}_i$ 与对应候选人可由投票者验证,统计总结果可以由投票过程中所有成员计算验证,因此统计中心无法私自窜改投票结果而不被发现。

c)认证性。通过认证的投票者才能进行投票。

投票者投票之前都要到特定机构申请证书,通过证书认证的投票者才能使用投票系统进行投票。

d)不可胁迫性。投票者不能向他人证明自己的投票内容。

投票者只有将接收到的回执 R'_i、$R-\mathrm{ID}_i$ 发送给买票者,才能使买票者由投票服务器签名确定 R'_i 的有效性,进而解密得出 r_i 以确定 $R-\mathrm{ID}_i$ 的有效性,从而由统计中心公布的信息中得到投票者投递的候选人。而在改进方案中 R'_i 的解密需要整个投票系统的共同协作,因此对买票者而言无法实现 R'_i 的解密,从而保证了不可胁迫性。

e)可验证性。投票者能验证自己选票是否被正确统计。

在改进方案中,投票者最终可以由统计中心公布的$R-\mathrm{ID}_i$ 与对应的候选人信息确认自己的选票是否被正确统计。因为投票过程中的参与者都可以根据统计中心公布的候选人信息自行计算出每个候选人的得票总数。将自行计算的总结果与投票中心公布的总结果比较即可知道统计中心是否统计了所有选票。

f)公平性。在投票过程中没人可以对选票进行部分统计。

在改进方案中,选票最终由统计中心统一解密并发布,因此只有统计中心才能最终解密并统计所有选票,从而保证了公平性。表 1 给出了改进方案与原方案在安全性上的比较。

表 1　与原方案的安全性对比

满足的安全性质	Morales-Rocha 等人的方案	改进方案
保密性	No	Yes
完整性	No	Yes
认证性	Yes	Yes
不可胁迫性	Yes	Yes
可验证性	No	Yes
公平性	Yes	Yes

相比于 Morales-Rocha 等人的方案,改进方案是为进一步保证安全性而进行的改进。

(1)原方案中选票是邮寄的,改进方案中选票直接通过 email 传送,便捷可靠,节省成本。

(2)改进方案中加入选票生成机构以生成选票,同时会在选票分发前对选票加密。削弱了选票分发机构的权限,降低了投票者身份泄露的危险性。

(3)改进方案没有用到投票者签名,而是由投票平台 *VP* 对投票者身份进行认证,相比于 Morales-Rocha 方案,改进方案因不使用投票者签名,统计阶段就不会暴露投票者身份,并且改进方案中,投票阶段公布了与 $R-\mathrm{ID}_i$ 对应的候选人,如果继续使用 Morales-Rocha 等人的方案中投票者的签名方式,投票服务器将能直接由 S_i 将投票者与所选候选人联系起来。

(4)改进方案中,统计中心公布和 $R-\mathrm{ID}_i$ 对应的候选人。由此,投票者能确定自己的选票是否被正确接收并统计。如果统计中心公布了与 $R-\mathrm{ID}_i$ 对应的候选人而并未统计,那么从最终的总结果中可以看出统计中心进行了错误统计。

(5)在改进方案中,统计中心公布了与 $R-\mathrm{ID}_i$ 对应的候选人。而在原方案中 $R_i=[r_i]_{S_{VS}}$,投票者只要将 $R_i=[r_i]_{S_{VS}}$、$R-\mathrm{ID}_i$ 发送给买票者,买票者通过解密 r_i,再验证 $r_i=[H(R-\mathrm{ID}_i\mid E-\mathrm{ID}_i)]$ 是否成立,即可确定 $R-\mathrm{ID}_i$ 有效性,并从公布的数据中找到对应的候选人。改进方案加入了整个投票系统的公钥 P_{system},除非由所有投票系统共同恢复出对应私钥,否则无法确认 r_i,从而是在防止选票收买的前提下对原方案进行的改进。

6 结束语

本文回顾了文献[6]中的预加密可验证电子投票方案,在原方案的预加密基础上,采用分发选票前再进行一次加密的策略,改进了该方案中分发机构权限过大,容易得到投票者隐私的漏洞。同时,通过投票平台 *VP* 验证投票者的合法性,避免了统计选票时投票者身份不必要的暴露。因原方案的统计过程事实上不可验证,本文在统计过程中公布了最终候选人结果以保证可验证性,同时在原方案中创建一个投票系统的公钥 P_{system} 并将私钥成分分发以协作解决纠纷,这种方式很好地解决了为保证可验证性而带来的买卖选票问题。

参考文献:

[1] SAMPIGETHAY K, POOVENDRAN R. A framework and taxonomy for comparison of electronic voting schemes[J]. Computers & Security, 2006,25(2):137-153.

[2] FUJIOK A, OKAMOTO T, OHATA K. A practical secret voting scheme for large scale election[C]//Proc of Workshop on the Theory and Application of Cryptographic Techniques. London: Springer-Verlag,1993:244-251.

[3] COHEN J D,FISCHER M J. A robust and verifiable cryptographically secure election scheme[C]//Proc of the 26th Annual IEEE Symposium on Foundations of Computer Science. Washington DC:IEEE Computer Society, 1985:372-382.

[4] CHAUM D. Untraceable electronic mail, return address and digital pseudonyms[J]. Communications of the ACM,1981,24 (2):84-88.

[5] KUN P. A general and efficient countermeasure to relation attacks in mix-based e-voting[J]. International Journal of Information Security,2011,10(1):49-60.

[6] STORE T, DUNCAN I. Pollsterless remote electronic voting[J]. Journal of E-Government, 2004,1(1):75-103.

[7] MORALES-ROCHA V,SORIANO M,PUIGGALI J. New voter verification scheme using pre-encrypted ballots[J]. Computer Communications, 2009,32(7-10):1219-1227.

[8] ADIDA B. Helios: Web-based open-audit voting[C]//Proc of the 17th Conference on Security Symposium. Berkeley: USENIX Association,2008:335-348.

[9] JOAQUIM R,RIBEIRO C. Code voting: protection against automatic vote manipulation in an uncontrolled environment[C]//Proc of the 1st International Conference on E-voting and Identity. Berlin:Springer-Verlag, 2007:178-188.

[10] RIERA A,RIFA J,BORRELL J. Efficient construction of vote-tags to allow open objection to the tally in electronic elections[J]. Information Processing Letters,2000,75 (4):211-215.