基于增强型 OTP 的电子投票方案*

燕飞飞,仲 红,孙彦飞,黄宏升
(1.安徽大学 计算智能与信号处理教育部重点实验室,安徽 合肥 230039
2. 安徽大学 计算机科学与技术学院,安徽 合肥 230039)

摘 要:利用身份注册、增强型 OTP 认证和公开验证机制,提出了一种新的电子投票方案。该方案利用注册中心与认证中心的共同管理实现对投票人的身份验证,防止投票人重复投票;投票人利用简单的认证口令不仅能实现有效申诉,还避免投票人的私有信息在公开验证阶段被泄露。

关键词:增强型 OTP 认证机制;电子投票;身份认证;重复投票

中图分类号:TP309.7 **文献标识码**:A

An electronic voting scheme based on the strengthened one-time password technology

YAN Fei Fei, ZHONG Hong, SUN Yan Fei, HUANG Hong Sheng
(1.Key Laboratory of Intelligent Computing & Signal Processing, Ministry of Education, Anhui University, Hefei 230039, China;
2.School of Computer Science and Technology, Anhui University, Hefei 230039, China)

Abstract: Based on identity registration, strengthened one-time password identity authentication and publicly verifiable mechanism, a new electronic voting scheme is proposed. In the scheme, registry center collaborate with certification center to realize the authentication of voters and prevent voters to vote again. Using simple password authentication, voters can not only achieve effective complaint, but also avoid that the private information of voter are leaked in publicly verifiable phase.

Key words: strengthened one-time password identity authentication; electronic voting; authentication; multiple voting

利用计算机和网络技术实现对投票人的登记、认证、分发、收集、计票等一系列过程即为电子投票[1-3]。电子投票过程中使用计算机和网络为媒介,可以防止参与方恶意参选,同时又满足了投票结果的公开性、透明性、及时性和公正性。目前已经有很多研究人员提出了多种电子投票方案,但其中的认证机制和对重复投票问题的解决方案还不完善。

现有方案中多数采用一个注册中心进行身份认证,少数方案利用门限秘密共享协议共同认证。2007 年,日本学者 Krivoruchko 提出抗强制注册方案[4],防止了注册机构泄露投票者身份、投票者与投票之间联系,但是该方案的认证阶段使用门限方案,对每一个合法身份的判定都必须通过多个注册机构,因此在大规模电子投票中对身份的认证效率低下。若设置单个注册中心则存在重复认证问题。2008 年,西班牙学者 Jordi Girona 结合声音识别技术,提出了身份注册方案[5],可防止投票人重复认证。该方案基于投票人声音来限定身份的唯一性,但是当管理机构对投票人进行验证审查时,会泄露投票人真实的声音信息和通信地址,即私有信息被部分泄露。

本方案注册阶段,利用注册中心和认证中心共同完成对投票人的身份验证,防止了恶意方冒充认证、合法投票人重复投票;在验证阶段,利用增强型 OTP 认证中不同认证次序对应不同认证口令的特点,合法投票人不但能简单、有效地申诉,还防止公开验证阶段投票人的身份信息被泄露。

1 基础知识

1.1 参与方的名称和职能

投票人 V_i:$i \in [1, N]$。

计票中心 T:负责计票和公布选举结果。

注册中心 R:发放合法身份证书、验证 V_i 身份证书

* 基金项目:国家自然基金项目(60773114);安徽省自然基金项目(070412051);安徽高校省级重点自然科学研究项目(KJ2007A43)

的合法性、向 T 发送投票信息组成的列表。

认证中心 CA：向 V_i 提供 SOTP 认证服务；为正确认证的 V_i 提供向 R 发送投票信息的服务。

验证中心 TA：接受 V_i 的申诉，并进行检验。

1.2 方案中涉及的符号定义

Bulletin Board(BB)：电子公告板；Mix Net(MN)：混合网；

b_i：参与方 V_i 的选票；C_i：由注册中心签发的合法身份证书；

$SIGN_{V_i}(m)$：投票人 V_i 对数据 m 进行数字签名[6]；

PK_S、PK_R、PK_T：分别为 CA、R、T 的公钥；SK_S、SK_R、SK_T：分别为 CA、R、T 的私钥；

L_0：R 已经分发的 C_i 列表；

L_1：由 R 加密的 $E_{PK_S}(C_i)$列表；

L_2：合法 V_i 投票信息列表(投票信息：$E_{PK_R}(C_i)$、$E_{PK_i}(b_i)$和 $SIGN_{V_i}(E_{PK_i}(b_i))$)；

L_2'：是 L_2 经过 MN 后得到的列表；

A→B：(m)表示参与方 A 向参与方 B 发送消息 m。

$H^N(spp \| seed)$：对数据 spp 和 seed 进行 N 次哈希运算。

1.3 增强型 OTP 身份认证

2008 年，国内研究人员提出了基于一次性口令 OTP[7](One-Time Password)的增强型认证系统 SOTP[7](Strengthened OTP)，在 C/S 模式下设置单个认证中心，实现客户端的身份认证。不但减少了认证系统中信道安全性假设，还防止了恶意者利用公开信道冒充认证服务器，截获认证口令仿冒认证，使 SOTP 可用于大规模电子投票中的身份认证。

此 C/S 模式中，客户端保存秘密口令 spp、seed 和相应的认证次序，而服务器端保存客户端的 ID、seed、客户端认证次序和 $H^N(spp \| seed)$的值。协议执行时，客户端与服务器端进行简单的相互通信，双方对秘密信息进行加/解密和 $H(spp \| seed)$运算，比较已存信息与接收的秘密信息是否相同，判断出两端身份的合法性。不仅完成了相互认证，还修改了下次认证口令，提高了安全性。

1.4 身份注册机制

R 通过安全性信道向合法 V_i 发放唯一的 C_i，V_i 在注册阶段向 R 提供其收到的 C_i，R 按照自己已经发放的证书列表进行证书检查，根据检查的结果来判断 V_i 身份的合法性。

2 具体的投票方案

该方案中 V_i 只有同时拥有合法 C_i 和正确认证口令时才能投票。利用剩余的秘密认证口令，在公开验证阶段向 TA 提出有效申诉，确保 V_i 的投票被正确计票。对图 1 的方案框图解释如下：

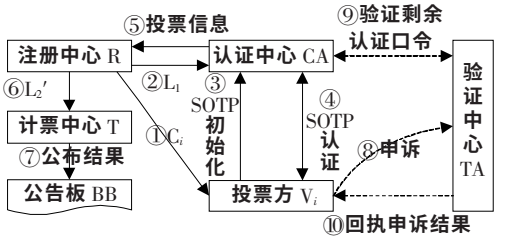

图 1 方案框架图

初始化阶段：

①R→V_i：C_i；//R 经过 MN 混合后，通过安全信道为每个 V_i 核发唯一的匿名证书 C_i。

②R：$L_1=E_{PK_S}(L_0)$；R→CA：L_1；CA：$L_0=D_{SK_S}(L_1)$；

SOTP 认证阶段：

③SOTP 初始化：

V_i：$(ver=H^N(spp \| seed), E_{PK_S}(ver))$；//其中 spp、seed 是 V_i 随机选择秘密口令。

V_i：(保存 N、spp、seq′)；//seq′是迭代次数 seq 的备份值，N 是迭代次数的初值。

V_i→CA：$(C_i, spp, seed, N, E_{PK_S}(ver))$；//通过安全信道传输。

④SOTP 认证：

V_i：随机选择 S 和对称加密密钥 K，保存 S′=S；

V_i→CA：$(E_{PK_S}(K), E_K(C_i, S))$；

CA：$D_{SK_S}(E_{PK_S}(K))=K$；

$D_K(E_K(C_i, S))=(C_i, S)$；

If(C_i 有效)

{ CA→V_i：$E_K(seq, S, seed)$；

} Else exit；

V_i：$D_K(E_K(seq, S, seed))=(seq, S, seed)$；

If(S==S′&&seq==seq′)

{ V_i：$H^{N-seq}(spp \| seed)$；

$H'=H^{N-seq}(spp \| seed) \oplus H^N(spp \| seed)$；

} Else exit；

V_i→CA：H′；

CA：$H^{N-seq}(spp \| seed)=H' \oplus H^N(spp \| seed)$；

$temp=H^{N-seq}(spp \| seed)$；

$H(H^{N-seq}(spp \| seed))=H^{N-seq+1}(spp \| seed)$；

If $(H^{N-seq+1}(spp \| seed)==D_{SK_S}(ver))$

{认证成功；ver=temp；//temp 是保存 $H^{N-seq}(spp \| seed)$ 的变量，用以改变下次认证中的参数值 ver。

} Else exit；

注册阶段：

⑤R：If(SOTP 认证成功)；//SOTP 认证成功后 V_i 才能通过 R 向 CA 转发投票信息。

{ V_i：$(E_{PK_T}(b_i), SIGN_{V_i}(E_{PK_T}(b_i)), E_{PK_R}(C_i))$；

V_i→CA：$(E_{PK_T}(b_i), SIGN_{V_i}(E_{PK_T}(b_i)), E_{PK_R}(C_i))$；

CA→R：$(E_{PK_T}(b_i), SIGN_{V_i}(E_{PK_T}(b_i)), E_{PK_R}(C_i))$；

If(R 验证 $E_{PK_R}(C_i)$合法)，将$(E_{PK_R}(C_i)$、$E_{PK_T}(b_i)$、$SIGN_{V_i}(E_{PK_T}(b_i)))$写入 L_2 中；

Else 丢弃 V_i 发送的所有信息。

} Else exit;

计票阶段:

⑥注册结束时R利用MN使L_2转换为L_2';R→T:L_2';

T:If(T检查L_2'有相同的$E_{PK_R}(C_i)$)

{T删除($E_{PK_R}(C_i)$,$E_{PK_T}(b_i)$,$SIGN_{V_i}(E_{PK_T}(b_i))$);//防止有合法的$V_i$重复投票。

} Else exit;

⑦T:$D_{SK_T}(E_{PK_T}(b_i))$;

T→BB:($E_{PK_R}(C_i)$,$SIGN_{V_i}(E_{PK_T}(b_i))$);//公布选举结果,为$V_i$验证提供相关数据。

公开验证阶段:

⑧R:根据BB公布的$E_{PK_R}(C_i)$检查是否有非法的注册信息;

V_i:If(BB中无$SIGN_{V_i}(E_{PK_T}(b_i))$)

{V_i向TA提出申诉请求;

V_i→TA:(V_i的剩余认证口令,$E_{PK_T}(b_i)$,$SIGN_{V_i}(E_{PK_T}(b_i))$,$E_{PK_R}(C_i)$);

}

⑨TA:利用V_i提供的剩余认证口令进行$N-1$次认证;

For ($j=1$; $j<N$; j++)

{If(认证失败) exit;

}

If($j==N-1$);//只有$N-1$次口令都正确才表明V_i申诉的正确性。

{TA:直接向T提出仲裁;

b_i被正确计票;

BB:($SIGN_{V_i}(E_{PK_T}(b_i))$,$E_{PK_R}(C_i)$);//以便合法$V_i$进行公开验证。

} Else 申诉失败

⑩TA通知V_i利用BB查看公开验证结果。

3 安全性分析

初始化阶段:R利用MN混合后,通过安全信道为每个V_i核发唯一的C_i,既保证了C_i的传输安全,也完成了C_i的匿名分发,防止恶意方获取C_i与V_i之间的对应关系,进行恶意攻击;R用PK_S对L_0进行加密,实现了安全的SOTP初始化。

注册阶段:本方案中CA和R共同验证V_i的合法性。在恶意方无法获得C_i的情况下,无法通过SOTP认证,即使恶意方非法避开SOTP阶段也不能完成注册,因为R在⑤中检查$E_{PK_R}(C_i)$的合法性;由于SOTP的特点是不同认证次序对应不同的认证口令,即使恶意方拥有SOTP认证口令也不能完成注册;假设恶意方非法避开整个注册阶段,利用伪造C_i直接投票也会失效,因为在公开验证时R检查BB中$E_{PK_R}(C_i)$的合法性,会发现虚假的注册信息。

计票阶段:T利用⑥判断是否有重复认证和重复投票,同时公开$E_{PK_R}(C_i)$和$SIGN_{V_i}(E_{PK_T}(b_i))$以便R和$V_i$验证计票阶段的合法性,增强了方案的健壮性。

公开验证阶段:V_i比较$SIGN_{V_i}(E_{PK_T}(b_i))$与$E_{PK_R}(C_i)$是否对应,判断$C_i$是否被非法利用、选票被正确计票;R检查BB中$E_{PK_R}(C_i)$的合法性,防止恶意方绕过注册阶段,伪造$C_i$进行投票,同时R检查BB中$E_{PK_R}(C_i)$的数量,以掌握废弃$C_i$的具体比例,衡量此次投票的有效性;TA接受$V_i$申诉时,$V_i$利用剩余的SOTP秘密口令,既能完成有效申诉,又防止私有信息泄露。

4 性能比较

从通信的安全性的角度对比,参考文献[8]中使用了一次容易泄密的电话通信,但本方案利用安全信道和数据加密的方法实现了信息安全传输;本方案中利用SOTP机制实现了V_i对认证机构诚实性的判断过程,而参考文献[8]没有V_i对认证机构的验证过程;参考文献[8]增加了保存声音特征的步骤,即V_i与认证机构电话通信时V_i的声音特征,不但增加了通信代价、数据存储代价,而且声音特征的录入与普通数字相比,录入的工作量大、误差率高;从认证的准确性角度分析,参考文献[8]中认证机构对V_i身份的真实性检查、V_i认证信息的完整性检查,都是基于生物特性的比对,由于当前生物认证技术的限制,在V_i认证阶段仍会存在2%以上的错误率[8];从公开验证的角度比较,本方案公开验证数据都是秘密数据,即利用秘密挑战口令进行验证,不会泄露V_i的私有信息,而参考文献[8]身份检查时涉及了V_i的录音或者电话号码。

综上所述,本方案仅在认证机构中增加一个挑战中心,却比参考文献[8]多了以下特点:(1)避免恶意方通过监听V_i电话而造成私有信息泄露;(2)增加了投票方V_i对认证机构诚实性判定功能;(3)认证阶段验证准确率高于基于声音特征的准确率;(4)验证阶段对保护V_i的私有信息更加合理,验证过程更加简单、准确;(5)增加了具体的计票方案,完善了公开验证中的申诉方法。

本方案不但满足了一般电子投票的要求,还增加了防止重复认证、重复投票以及保密申诉的功能。方案也存在一些不足之处,如对投票人诚实性要求较高,不能防止V_i与恶意方合谋,这将是作者下一步的研究重点。

参考文献

[1] FUJIOKA A, OKAMOTO T, OHTA K. A practical secret voting scheme for large scale elections [C]. In Advancesin Cryptology(-AUSCRYPT9 2), LNCS 718, Berlin: S pringer-Verlag, 1992:244-251.

[2] 仲红,黄刘生,罗永龙.一个实用的电子评审方案[J].小型微型计算机系统,2007,43(1):178-181.

[3] ZHONG H, HUANG L S, XIONG Y. A weighted e-voting scheme with secret weights [J]. Chinese Journal of Electron-

ics, 2006,15(3):413-416.

[4] KRIVORUCHKO T. Robust coercion-resistant registra tion for remote e-voting [C]. Proceedings of the IAVoSS Workshop on Trustworthy Elections(WOTE 2007), 2007.

[5] JORDI G. Secure remote voter registration [DB/OL]. 2008. http://www.e-voting.cc/files/Session03_JordiPuiggali.

[6] 赵泽茂.数字签名理论[M].北京:科学出版社,2007.

[7] 张丽,赵洋,史丽敏.基于OTP的增强型身份认证系统的研究与设计[J].计算机工程与科学,2008,30(6):1007-130.

[8] HALLER N, METZ C, NESSER P. A one-time password system[M]. RFC 2289,1995(2).

(收稿日期:2009-11-03)

作者简介:

燕飞飞,男,1981年生,硕士研究生,主要研究方向:网络与信息安全。

仲红,女,1965年生,硕士,教授,主要研究方向:网络与信息安全、分布式计算。

孙彦飞,男,1982年生,硕士研究生,主要研究方向:网络与信息安全。