一种基于全同态加密的安全电子投票方案

洪家军[1,2],崔宝江[2]
(1.莆田学院,福建 莆田 351100;2.北京邮电大学计算机学院,北京 100876)

【摘　要】 主要介绍全同态加密技术的基本原理、基于公钥的全同态加密算法的实现,以及利用全同态加密算法,结合云计算、PKI 和基于 RSA 的数据加密与数字签名等技术实现安全电子投票的技术方案,给出了方案的安全性分析。全同态加密在电子投票和云计算等领域有着巨大的应用潜力,该方案有效地解决了电子投票中的匿名性和公开可验证性难题,真正实现了安全、公开、公平和公正的电子投票。

【关键词】 全同态加密;电子投票;数字签名;云计算

A Secure Electronic Voting Scheme Based on Fully Homomorphic Encryption

HONG Jia-jun, CUI Bao-jiang

【Abstract】 Fully homomorphic encryption has great application potential in electronic voting and cloud computing and other fields. After introducing the basic principle of fully homomorphic encryption technology and the realization of fully homomorphic encryption algorithm based on public key, this paper will thoroughly illustrate a technology scheme for security electronic voting which effectively address the anonymity and public verifiability issues by adopting technology of fully homomorphic encryption algorithm, cloud computing, PKI, the data encryption and digital signature based on RSA, thus helps to realize a safe, open, fair and justice electronic voting. At the end of the paper, the analysis of the security for the scheme will be provided.

【Key words】 fully homomorphic encryption;electronic voting;digital signature;cloud computing

〔中图分类号〕TP309　　〔文献标识码〕A　　〔文章编号〕1674－3229(2015)01－0005－06

0　引言

投票是现代民主社会的重要社会活动,电子投票以密码学为基础,借助计算机和通信技术,实现公开、公平和公正的投票选举功能,在工作组织、选票搜集与统计等方面可以节省大量人力物力,还可以减少人为干预,做到更公平、安全和高效。

自从 Chaum[1] 于 1981 年提出第一个现代密码学意义上的电子投票方案后,电子投票经历了两个发展阶段,第一阶段是基于盲签名的电子投票方案的研究,这个阶段主要关注选票的匿名性问题,没有选票的公开验证信息,也没有得到实际应用。第二阶段是公开可验证的匿名电子投票方案研究,这一阶段使用不同的密码学技术来实现应用。主要有基于 mix net 协议和同态加密两种电子投票方案。文献[2]对基于 mix net 协议方案做了详细的分析,并证明了 mix 服务器作弊的可能性,而且基于 mix net 协议的方案过于复杂,需要给出零知识证明。1997 年在文献[3]中首次提出了利用 ELGamal 的乘法同态的电子投票方案,2001 年在文献[4]首次提出了基于 Paillier 的接法同态特性的电子投票方案。但 ELGamal 算法和 Paillier 算法都需要幂指运算,计算复杂,而且只能分别实现乘法同态和加法同态,属于半同态加密技术,不能在密文中进行诸如检索、比

[收稿日期] 2014－11－15
[基金项目] 福建省教育厅国内访问学者资金资助;福建省中青年教师教育科研项目(A 类)资助(JA14279)
[作者简介] 洪家军(1979－),男,硕士,莆田学院信息工程学院讲师,北京邮电大学访问学者,研究方向:网络安全与应用;崔宝江(1973－),男,博士,北京邮电大学计算机学院副教授,博士生导师,研究方向:信息安全。

较等复杂的操作,而且易被统计分析,存在服务器作弊、中间人攻击[5-6]等安全风险,不能从根本上解决选票匿名性问题。

2009 年 9 月 Craig Gentry[7]在其博士论文中首次在数学上提出了"全同态加密"的可行方法,文献[8-9]中构建了一个在整数上的基于公钥的全同态加密方案,文献[8]给出了安全性分析与证明。

文献[10-11]利用全同态加密技术在电子投票方面作了有益的研究与探索,但并未真正解决自计票与公开验证性问题,而且通信双方仅利用一个数字签名同时实现数据加密传输与数字签名的方式并不妥当。

文中提出了一种基于公钥的全同态加密的安全电子投票方案,该方案结合云计算、PKI 技术和 RSA 数据加密与数字签名技术,对参与选举的各方实体采用 RSA 身份认证,各实体之间的数据传输均采用 RSA 数据加密和数字签名,以保证各方实体的真实性、不可抵赖性和数据完整性。各方实体的数字证书采用 PKI 进行管理与分发,选票内容采用全同态加密技术进行加密。投票结束后任何人都可以对投票的各个过程进行公开验证,每个投票人都可以验证自己的选票是否被正确地计票,也可以验证统计结果是否正确。同时解决了选票匿名性和公开可验证性以及自计票性等以往不能很好解决的问题,保证了整个投票过程安全、公开、公平和公正。

1　全同态加密技术

同态加密是由 Rivest 和 Adleman 等于 1978 年首次提出,这种技术允许对密文进行特定的代数运算得到仍然是加密的结果,将该结果解密得到的结果与对明文进行同样的运算得到的结果是一样的。这使得人们可以在加密的数据中进行诸如检索、比较等操作并能得到正确的结果,而在整个处理过程中无需对数据进行解密。

同态加密一直是密码学领域的重要课题,2009 年之前的同态加密只支持加法和乘法同态的一种,而且实现简单,易于统计分析。2009 年 Craig Gentry 在其博士论文中提出了"全同态加密"的可行方法,使得该技术取得了决定性的突破。

1.1　全同态加密的基本原理

设加密操作为 E,解密操作为 D,明文为 m,则密文 $c=E(m)$,$m=D(c)$。如果针对明文有操作 f,针对 E 可以构造 F,使得 $F(c)=E(f(m))$,则称 E 就是一个针对 f 的同态加密算法。若对任意复杂的明文操作 f,都能构造出相应的 F,则称 E 为全同态加密。

1.2　全同态加密算法的实现

由于不存在一个天然的全同态加密方案,所以需要人为构造出全同态的加密方案[12]。Craig Gentry 的构造思想是先构造一个部分(somewhat)的同态方案 ε,这种方案由以下四个算法组成:

(1)$Keygen(\lambda)$:根据安全参数 λ,生成公钥 pk 和私钥 sk。

(2)$Encrypt(pk,m)$:对二进制明文 $m\in\{0,1\}$,利用公钥 pk 加密得到密文 c。

(3)$Decrypt(sk,c)$:对于密文 c,利用私钥 sk 解密输出明文 m'。

(4)$Evaluate(pk,C,c_1,c_2,\cdots,c_t)$:输入公钥 pk,具有 t 个输入的由模 2 加法门与乘法门组成布尔电路 C,以及一组密文 $c_1,c_2,\cdots,c_t$,其中 $c_i=Encrypt(pk,m_i)$,$i\in[1,t]$。输出 $c^*=Evaluate(pk,C,c_1,c_2,\cdots,c_t)$,且满足 $Decrypt(sk,c^*)=C(m_1,m_2,\cdots,m_t)$。

方案 ε 的核心是 $Evaluate$ 算法,其作用就是对密文进行电路 C 操作,对其输出结果 c^* 进行解密,其结果刚好等于对明文进行相同的电路 C 操作。

由于方案 ε 的密文中存在噪声,使得对密文进行操作时噪声会快速增大,最终将导致解密失败。Craig Gentry 利用同态解密技术对每次 $Evaluate$ 运算后的密文 c^* 进行降噪,使得对密文的操作可以无限次地进行下去。当方案 ε 对由加法和乘法甚至更多其它运算组成的电路 C 都可以无限次正确运算时,就称该方案是全同态的。

DGHV 的对称密钥方案是 Craig Gentry 等人提出的基于整数的同态加密方案,其思想描述如下:

$KeyGen(\lambda)$:根据安全参数 λ 生成一个随机素数 p 作为密钥 k。

$Encrypt(k,m)$:对于二进制明文消息 $m\in\{0,1\}$,根据安全参数 λ 选择一个随机整数 q,并随机生成一个整数 r 使其满足 $2r\in(-p/2,p/2)$,输出密文 $c=m+2r+pq$。

$Decrypt(k,c)$:对于密文 c,利用密钥 k 解密输出明文 $m=(c \bmod p) \bmod 2$。

利用该方案对二进制明文 m_1 和 m_2 进行加密,得到密文 c_1 和 c_2:

$$c_1 = m_1 + 2r_1 + pq_1$$

$$c_2 = m_2 + 2r_2 + pq_2$$

$$c_1 + c_2 = (m_1 + m_2) + 2(r_1 + r_2) + p(q_1 + q_2) \tag{1}$$

$$c_1 \times c_2 = m_1 \times m_2 + 2(r_1 r_2 + r_1 m_2 + r_2 m_1) + p(q_1 q_2 p + 2(r_1 + m_1) + 2(r_2 + m_2)) \tag{2}$$

从式(1)和式(2)可以看出,

$((c_1 + c_2) \bmod p) \bmod 2 = m_1 + m_2$,

$((c_1 \times c_2) \bmod p) \bmod 2 = m_1 \times m_2$。

因此,该算法同时具有加法同态和乘法同态特性。但由于对密文进行加法和乘法操作时,密文中的噪声 $m+2r$ 将随之变大,尤其是乘法操作。当噪声 $|m+2r| \geqslant p$ 时,解密将会出错,因此,这种方案只能进行有限次的同态运算。

2 基于公钥的全同态加密算法

2.1 算法描述

由于上面介绍的 DGHV 是基于对称密钥的,而且只能做有限次同态运算,不能满足于实际需求。于是,又提出了一种改进的基于公钥的全同态加密方案,暂且称为 P_DGHV 方案,具体算法描述如下:

设 λ 为安全参数,$\eta=\lambda^2$ 为私钥的二进制位长,$\gamma=\lambda^5$ 为公钥的二进制位长,$\rho=\lambda$ 为噪声的二进制位长,$\rho'=2\lambda$ 为另一种噪声参数位长,$\tau=\gamma+\lambda$ 为组成公钥的整数元素的个数。

$KeyGen(\lambda)$:随机生成一个 η 位长的正素数 p 作为私钥 SK,设对 p 有一个分布 $D_{q,r}(p)=\{$分别随机产生一个整数 q 和 r,输出 $x=pq+r$,其中 $q \in [0, 2^{\lambda}/p]$,$r \in (-2^{\rho}, 2^{\rho})\}$。则公钥的产生过程如下:循环执行 $D_{q,r}(p)$ 产生 $\tau+1$ 个位长为 γ 的 x 值,分别标记为 $x_0, x_1, \cdots, x_{\tau}$,重新标记该序列使 x_0 为最大值。重复以上过程直到 x_0 为奇数且 $(x_0 \bmod p)$ 为偶数,则公钥 $PK=<x_0, x_1, \cdots, x_{\tau}>$。

$Encrypt(PK,M)$:将明文 M 分为长度为 l 的分组 m,$m=m_1 m_2 \cdots m_l$,$m_i \in \{0,1\}$,$l<p$,随机选择一个子集 $S \subseteq \{1,2,\cdots,\tau\}$ 以及随机整数 r',$r' \in (-2^{\rho'}, 2^{\rho'})$,输出密文 $c_i = m_i + 2r' + \sum_{i \in S} x_i$,明文 m 对应的密文 $c = c_1 c_2 \cdots c_l$。

$Decrypt(SK,c)$:对于密文 $c=c_1 c_2 \cdots c_l$,利用私钥 SK 解密 c_i,得到 $m_i = (c_i \bmod p) \bmod 2$,$i \in [1, l]$,从而得到明文 $m = m_1 m_2 \cdots m_l$。

由于 p 是素数,所以 $(c \bmod p) \bmod 2 = (c - p \cdot [c/p]) \bmod 2 = (c \bmod 2) \oplus ([c/p] \bmod 2)$。

$Evaluate(PK, C, c_1, c_2, \cdots, c_l)$:对于给定的有 l 个输入的二进制布尔电路 C 和 l 个密文 c_i,对密文 c_i 执行电路 C 中的任意的加法和乘法门电路运算,输出一个整数结果 c^*,使得 $Decrypt(SK, c^*) = C(m_1, m_2, \cdots, m_l)$。

由于在电子投票过程中,需要提高私钥安全强度,防止服务器合谋作弊,需要将私钥 SK 分割成多个子私钥,并分布式地存储到云中的不同服务器中,任何子私钥都不能独自解密密文,只有当收集齐一定数量的子私钥后才可以重建出完整的私钥 SK,具体方法如下:

令 $\kappa = \gamma\eta/\rho'$,$\theta = \lambda$,$\Theta = \kappa \cdot \lambda$,$x_p = [2^{\kappa}/p]$。

随机选择一个 Θ 位的向量 $\vec{s} = <s_1, s_2, \cdots, s_{\Theta}>$,其元素之和为 θ,同时有集合 $S^* = \{\alpha \mid s_{\alpha} = 1\}$。随机生成一个小于 $2^{\kappa+1}$ 的非负整数 u_{α},使 $\sum_{\alpha \in S^*} u_{\alpha} = x_p \pmod{2^{\kappa+1}}$。令 $y_{\alpha} = u_{\alpha}/2^{\kappa}$,则有非负有理数向量 $\vec{y} = <y_1, y_2, \cdots, y_{\Theta}>$,其中 $y_{\alpha} \in [0,2)$,$\alpha \in [1, \Theta]$,使得 $(\sum_{\alpha \in S^*} y_{\alpha}) \bmod 2 = 1/p$。

输出私钥 $SK^* = \vec{s}$,加密公钥 $PK^* = (PK, \vec{y})$。

对 $Encrypt(PK, M)$ l 输出的每个密文 c,设 $z_{\alpha} = (c \cdot y_{\alpha}) \bmod 2$,$\vec{z} = <z_1, \cdots, z_{\Theta}>$,输出新密文 $(c, \vec{z})$。

解密时输出 $m' = (c - \lfloor \sum_{\alpha=1}^{\Theta} s_{\alpha} z_{\alpha} \rceil) \bmod 2$。

2.2 算法同态性与安全性分析

将 $x = pq + r$ 代入 $c_i = m_i + 2r' + \sum_{i \in S} s_i$ 中,可得,

$c_i = m_i + 2r' + ((pq_1 + r_1) + (pq_2 + r_2) + \cdots + (pq_\tau + r_\tau) = m_i + (2r' + r_1 + r_2 + \cdots + r_\tau) + p(q_1 + q_2 + \cdots + q_\tau) = m_i + 2r^* + pq^*$,

可见这是对称 DGHV 的加密输出形式,根据式(1)和式(2)可推知,P_DGHV 也同时满足加法和乘法同态特性。利用 Craig Gentry 的同态解密技术,该方案可以构造成全同态的,而且其安全性依赖于稀疏子集和问题,该问题目前认为是安全的,其正确性与安全性的具体证明可参见文献[7-8]。

3　基于全同态加密的电子投票方案

基于云端的电子投票的模型如图 1 所示,PKI 中的 CA 负责为参与投票的投票人、投票中心和计票中心等实体进行身份认证,为各方实体生成与分配公私密钥对,签发与管理数字证书,确保各实体的真实可靠。投票中心 VC 负责接受投票人的合法注册,并为投票人分发与签名选票。数据中心用于存储用户提交的选票以及其它信息。计票中心 CC 负责验证投票人提交的选票的真实性与合法性,并统计选票结果。

对于投票人 V,设有 w 个投票人 $V_1, V_2, \cdots, V_w$;并设有 h 个候选人 $O_1, O_2, \cdots, O_h$,$O_\varepsilon^{V_\mu}$ 表示投票人 V_μ 对候选人 O_ε 的投票情况,若选择了 O_ε,则 $O_\varepsilon^{V_\mu}$ 为 1,否则为 0,其中 $\mu \in [1, w]$,$\varepsilon \in [1, h]$。

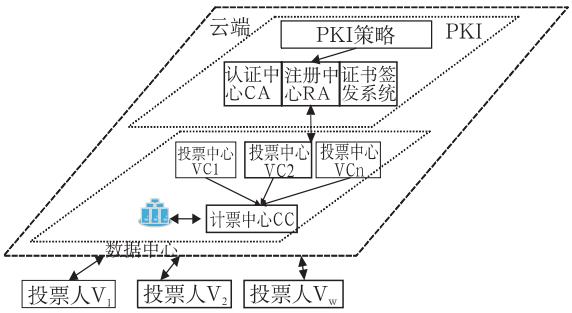

图1　基于云端的电子投票模型

3.1　具体实现过程

3.1.1　系统初始化

系统初始化阶段主要是 PKI 系统对投票人 V、计票中心 CC 和投票中心 VC 等实体进行身份认证,为每个合法实体颁发经过 CA 签名的数字证书,数字证书采用 RSA 公钥体制,其中包含各实体的公钥,并存储于 PKI 目录数据库中,任何人都可以到目录数据库查询各方实体的数字证书并对其进行验证。

设投票人 V 的公钥为 PK_V,私钥为 SK_V,其中每个投票人 V_μ 的公钥为 PK_{V_μ},私钥为 SK_{V_μ},$\mu \in [1, w]$。投票中心 VC 的公钥为 PK_{VC},私钥为 SK_{VC}。计票中心 CC 的公钥为 PK_{CC},私钥为 SK_{CC}。

另设如下几个数据表:

List1:用于保存已生成并发放的选票编号 TN_V 以及对应的投票人 ID_V。

List2:用于保存已成功投票的选票编号 TN_V 以及对应的投票人 ID_V。

List3 和 List4 分别保存有效选票和无效选票信息。

由于各实体之间的通信涉及的数据量很小,因此,实体间的通信数据采用 RSA 公钥加密,同时采用基于 RSA 的数字签名确保数据的机密性、完整性和不可抵赖性。

3.1.2　投票人注册

(1)要参与投票的人需要向 VC 发送包含 $E_{PK_{VC}}(ID_V \| RN_V, Sig_{SK_V}(H(ID_V \| RN_V)))$ 的注册请求消息,其中 $Sig_{SK_V}(H(ID_V \| RN_V))$ 表示用 SHA-1 哈希函数 H 将投票人 V 的身份标识 ID_V 和一个随机数 RN_V 进行哈希,并将结果用 V 的私钥 SK_V 作数字签名。$E_{PK_{VC}}$ 表示用 VC 的公钥 PK_{VC} 进行数据加密。

(2)VC 收到该注册请求后,用私钥 SK_{VC} 解密,然后验证签名 $Ver_{PK_V}(ID_V \| RN_V, Sig_{SK_V}(H(ID_V \| RN_V)))$ 是否为真。若通过验证,则检查 ID_V 是否具有投票资格,若任意一个检验未通过则返回警告消息。否则检查在 List1 中是否存在该 ID_V,若没有则为该 ID_V 生成一个具有唯一的选票编号 TN_V 的空白选票,将选票编号 TN_V 与 ID_V 关联,以防止一个 ID_V 拥有多张选票。

(3)VC 计算 TN_V 的消息认证码 $MAC_V = H(ID_V \| TN_V)$,然后作数字签名 $Sig_{SK_{VC}}(H(MAC_V \| ID_V \| TN_V))$,并将 $E_{PK_V}(MAC_V \| ID_V \| TN_V$,

$Sig_{SK_{VC}}(H(MAC_V \| ID_V \| TN_V))$、空白选票以及选票加密公钥 $PK^* = (PK, \vec{y})$ 发给投票人 V。同时将 $(ID_V \| RN_V, TN_V, Sig_{SK_V}(H(ID_V \| RN_V)))$ 记入 List1 中,以便发生纠纷时核查。

(4)V 收到 VC 的返回消息后,先用私钥解密,并验证签名 $Sig_{SK_{VC}}(H(MAC_V \| ID_V \| TN_V))$ 是否真实,若验证通过,则保存 $(MAC_V \| ID_V \| TN_V, Sig_{SK_{VC}}(H(MAC_V \| ID_V \| TN_V)))$ 以证明自己是经过验证的合法投票人。

3.1.3　选票加密与投票

(1)投票人 V_μ 获得空白选票后,并决定选择候选人 O_ε,则填写完选票后,利用 P_DGHV 全同态加密算法的公钥 $(PK, \vec{y})$ 对选票内容 $O_\varepsilon^{V_\mu}$, $\mu \in \{1, w\}$, $\varepsilon \in \{1, h\}$,计算 $c_{V_\mu} = O_\varepsilon^{V_\mu} + 2r^* + pq^*$, $z_\alpha = (C_{V_\mu} \cdot y_\alpha) \bmod 2$, $\alpha \in [1, \Theta]$, $z_{V_\mu} = z_1 z_2 \cdots z_\Theta$,获得密文 $C_\varepsilon^{V_\mu} = (c_{V_\mu}, z_{V_\mu})$。令 $M_V{}^* = (C_\varepsilon^{V_\mu}, MAC_{V_\mu} \| ID_{V_\mu} \| TN_{V_\mu})$,对 $M_{V_\mu}{}^*$ 作数字签名得到 $M'_{V_\mu} = Sig_{SK_{V_\mu}}(H(M_{V_\mu}{}^*))$。因 $C_\varepsilon^{V_\mu}$ 已是密文,故可直接将 $(E_{PK_{VC}}(MAC_{V_\mu} \| ID_{V_\mu} \| TN_{V_\mu}), C_\varepsilon^{V_\mu}, M'_{V_\mu})$ 发送给 VC 且不影响机密性。

(2)VC 收到消息后首先解密 $E_{PK_{VC}}(MAC_{V_\mu} \| ID_{V_\mu} \| TN_{V_\mu})$,然后验证数字签名 M'_{V_μ},若验证通过且 (ID_{V_μ}, TN_{V_μ}) 在 List1 中,但不在 List2 中,则该选票合法,于是 VC 发送 $(E_{PK_{CC}}(MAC_{V_\mu} \| ID_{V_\mu} \| TN_{V_\mu}), C_\varepsilon^{V_\mu}, M'_{V_\mu})$ 给计票中心 CC。由于 M'_{V_μ} 是 V 的数字签名,而且 $C_\varepsilon^{V_\mu}$ 是全同态加密密文,所以不担心投票中心合谋作弊,篡改选票内容。最后向 V 返回投票成功的票据消息 $T_V = (E_{PK_V}(MAC_{V_\mu} \| ID_{V_\mu} \| TN_{V_\mu}), C_\varepsilon^{V_\mu}), Sig_{SK_{VC}}(H(C_\varepsilon^{V_\mu} \| MAC_{V_\mu} \| ID_{V_\mu} \| TN_{V_\mu}))$,同时在 List2 中记录 $(MAC_{V_\mu}, ID_{V_\mu}, TN_{V_\mu}, C_\varepsilon^{V_\mu}, Sig_{SK_{VC}}(H(C_\varepsilon^{V_\mu} \| MAC_{V_\mu} \| ID_{V_\mu} \| TN_{V_\mu})))$ 以便事后核查。

(3)V 对 T_V 进行解密和签名验证,确保已成功投票并保留 T_V,以后若有纠纷,可持 T_V 申诉。

3.1.4　验票与计票

(1)计票中心 CC 解密由 VC 发来的消息 $E_{PK_{CC}}(MAC_{V_\mu} \| ID_{V_\mu} \| TN_{V_\mu})$,并用公钥验证 V 的签名 M'_{V_μ},若验证通过则表明该选票有效,并将 $(MAC_{V_\mu}, ID_{V_\mu}, TN_{V_\mu}, C_\varepsilon^{V_\mu}, M'_V)$ 保存在 List3 中,否则该选票视为无效并将其保存到 List4 中。

(2)投票结束后,统计有效票数时,由于对于候选人 O_ε 的选票内容 $O_\varepsilon^{V_\mu}$ 都是经过同态加密的 $C_\varepsilon^{V_\mu}$,利用同态加法操作就可以统计出有效票数,设 $Sum_{C_\varepsilon} = Evaluate(PK^*, C, C_\varepsilon^{V_1}, C_\varepsilon^{V_2}, \cdots, C_\varepsilon^{V_w})$,这里的电路 C 就是对选票密文 $C_\varepsilon^{V_\mu}$ 执行加法运算的门电路,Sum_{C_ε} 为候选人 O_ε 的有效票总票数的同态加密密文。根据全同态加密的定义,将 Sum_{C_ε} 解密就是候选人 O_ε 的总有效票数。于是计票中心 CC 收集分布式存储在云端服务器上的子私钥,并生成私钥 $\vec{s} = < s_1, s_2, \cdots, s_\Theta >$,利用该私钥就可以解密 Sum_{C_ε}。

(3)计票结束后,计票中心 CC 将公布各候选人有效票数的明文形式。

3.2　安全性分析

一个电子投票方案是否安全有效,一般要满足合法性、匿名性、公正性、完备性、机会唯一性、自计票性以及公开可验证性等安全特性[11,13,14]。针对文中所提方案的安全性分析如下:

(1)合法性:就是要确保合法有效的投票人才能投票,方案中的 PKI 系统和投票人注册过程确保了投票人的有效身份和投票资格的确认,投票过程中的数据加密与数字签名确保了数据的机密性和可靠性,假冒者即使获得了一张空白选票,但因为没有真正投票者的私钥而无法通过数字签名验证。

(2)匿名性:选票内容均经过全同态加密技术加密,攻击者甚至是投票中心都无法从密文中获得选票内容信息,从而确保选票的匿名性。

(3)公正性:由于采用全同态加密技术,选票的统计只有在最后阶段由计票中心通过对密文操作,由私钥对操作结果解密获得选举结果,全程没有相关选票内容的明文出现。而且私钥被分割为多个子

私钥并分布式存储于云端的各服务器中,防止了服务器合谋作弊,攻击者即使获取了若干个子私钥也无法解密,从而保障全过程的公正性。

(4)完备性:就是要保证合法选票不能被投票中心拒绝,由于每张选票均有唯一的编号 TN_V,防止了重复选票的问题,而且所有选票从生成到投票结束的过程中都有经过数字签名,只有通过签名验证才可以进入下一步操作,伪造的选票将无法通过验证。

(5)机会唯一性:通过将投票人 ID_V 与选票编号 TN_V 关联,并在 List2 中记录投票人 ID_V 和选票编号 TN_V,防止一人多投或一票多投的现象,确保一个 ID_V 只有一张合法的选票和一次投票机会,也规避了"选票碰撞"问题。

(6)自计票性:投票人可验证自己的选票是否被正确地计入到有效票中且选票内容未被篡改。投票人只需要验证有效选票中的自己选票的签名消息 M'_V 与自己持有的 T_V 中的 M'_V 是否一致,若一致,则表明选票无误,否则就可以持 T_V 进行申诉。

(7)公开可验证性:由于所有选票都存储在云端数据中心的 List3 和 List4 中,各方实体的公钥存放于 PKI 证书数据库中,任何人都可以访问、查询和验证投票的各个过程产生的数据是否合法。另外,用户可以对有效选票同样执行 $Sum_{C_\varepsilon} = Evaluate(PK^*, C, C_\varepsilon^{V_1}, C_\varepsilon^{V_2}, \cdots, C_\varepsilon^{V_w})$ 操作得到候选人 O_ε 的有效票数的加密密文 Sum_{C_ε},然后将计票中心公布的该候选人的有效票数经公钥 $(PK, \vec{y})$ 全同态加密,若加密结果与 Sum_{V_ε} 相同,则说明公布的结果是正确的。

4　总结

文中提出了一种基于全同态加密技术的电子投票方案,它综合利用了云计算的分布式特点、强大的计算能力以及安全的数字证书、数字签名、PKI 等安全技术,实现了一种安全的电子投票方案,同时解决了匿名性和公开可验证的难题,特别是自计票性,保证了选举过程的安全、公开、公平和公正。但由于当前全同态加密技术方案计算效率不高,目前还难以在真实环境中实现。不过,相信但随着全同态加密技术研究的深入以及云计算的广泛应用,采用全同态加密技术的电子投票方案将会得到广泛应用。

[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] Boneh D, Golle P. Almost entirely correct mixing with applications to voting[C]//Proceedings of the 9th ACM conference on Computer and communications security. ACM, 2002: 68－77.

[3] Cramer R, Gennaro R, Schoenmakers B. A secure and optimally efficient multiauthority election scheme[J]. European transactions on Telecommunications, 1997, 8(5): 481－490.

[4] Baudron O, Fouque P A, Pointcheval D, et al. Practical multi-candidate election system[C]//Proceedings of the twentieth annual ACM symposium on Principles of distributed computing. ACM, 2001: 274－283.

[5] 张鹏,喻建平,刘宏伟. 同态签密方案及其在电子投票中的应用[J]. 深圳大学学报(理工版), 2011, 28(6): 489－494.

[6] 任福乐,朱志祥,王雄. 基于全同态加密的云计算数据安全方案[J]. 西安邮电学院学报, 2013, 18(3): 92－95.

[7] Gentry C. A fully homomorphic encryption scheme[D]. Stanford University, 2009.

[8] Van Dijk M, Gentry C, Halevi S, et al. Fully homomorphic encryption over the integers[M]//Advances in Cryptology-EUROCRYPT 2010. Springer Berlin Heidelberg, 2010: 24－43.

[9] Mitchell Harper. Fully Homomorphic Encryption[EB/OL]. http://www.math.washington.edu/~morrow/336_14/papers/mitchell.pdf. 2014－6－2/2014－11－10.

[10] 朱正阳. 一种基于全同态加密的电子投票方案[D]. 广州大学, 2013.

[11] 朱正阳,刘镓,唐春明,等. 基于 LWE 同态加密的电子投票方案[J]. 信息网络安全, 2013, (5): 8－11.

[12] 陈智罡,王箭,宋新霞. 全同态加密研究[J]. 计算机应用研究, 2014, 31(6): 1624－1630.

[13] Bruce Schneier. Applied cryptography: protocols, algorithms, and source code in C[M]. john wiley & sons, 2007.

[14] 丛清日,胡金初. 基于椭圆曲线盲数字签名的电子选举[J]. 计算机工程, 2010, 36(13): 156－158.