基于SEAL库的同态加权电子投票系统

杨亚涛[1),2)] 赵 阳[1)] 张奇林[2)] 马英杰[1)] 高 原[1),3)]

[1)](北京电子科技学院电子与通信工程系 北京 100070)

[2)](西安电子科技大学通信工程学院 西安 710071)

[3)](国家信息中心博士后工作站 北京 100045)

摘 要 电子投票比传统纸质投票更为灵活高效,能节省大量人力物力,在不同选举场合中的地位越来越重要.同态加密技术可以在电子投票过程中发挥重要作用,同态加密技术结合其他安全技术和手段来设计的电子投票系统,可以在计票过程中有效保护投票者的身份隐私,相比其他类型的电子投票系统也更为简洁高效.为了解决电子投票中的身份隐私保护和实现效率问题,本文提出了一种基于SEAL库的同态加权电子投票系统,通过同态操作实现密文计票,可有效抵抗来自计票中心内部的恶意攻击,保证选票保密性和计票结果正确性;通过在选票中引入投票权重,可以使电子投票系统实现加权投票;通过将选票信息密态存储在云端数据库,将计票中心部署在云端,可在保证安全的前提下借助云计算服务实现高效计票;系统中加密算法的安全性基于格上RLWE困难问题,可以抵抗量子计算攻击.对所设计投票系统的效率测试表明,完成对1000张选票的计票工作仅耗时1.867 s,相比Will等人在ICCCRI2015中提出的基于Paillier的电子投票系统计票耗时减少了32.73%,相比Wang等人在2017年提出的基于Helib的电子投票系统计票耗时减少了99.26%,相比Li在2017年提出的基于Helib的电子投票系统计票耗时减少了91.81%.本文提出的同态加权电子投票系统可以满足多个候选人投票和加权投票,能够适用于多种投票场景,且计票效率可以满足大规模投票的应用需求.

关键词 电子投票;加权投票;同态加密;SEAL;密文数据库

中图法分类号 TP309 **DOI号** 10.11897/SP.J.1016.2020.00711

Weighted Electronic Voting System with Homomorphic Encryption Based on SEAL

YANG Ya-Tao[1),2)] ZHAO Yang[1)] ZHANG Qi-Lin[2)] MA Ying-Jie[1)] GAO Yuan[1),3)]

[1)](*Department of Electronic and Communication Engineering, Beijing Electronics Science and Technology Institute, Beijing* 100070)

[2)](*School of Telecommunication Engineering, Xidian University, Xi'an* 710071)

[3)](*Postdoctoral Scientific Workstation, State Information Center, Beijing* 100045)

Abstract Electronic voting is regarded more flexible and efficient than traditional paper voting, which can save a lot of manpower and material resources. It plays an increasingly important role in various election scenarios. The solutions for electronic voting can be classified into three main paradigms: mix-type, blind signature-based and homomorphic tallying. Homomorphic encryption technology played an important role both in cloud computing and remote electronic voting system. Combining multiple security technologies, the electronic voting scheme based on homomorphic encryption can effectively protect voter's privacy during the counting ballots process; at the same time, it is simpler to be constructed and more efficient than other kinds of e-voting schemes. Microsoft SEAL based on open-source homomorphic encryption technology, provids a set of encryption

收稿日期:2019-08-26;在线出版日期:2020-02-06.本课题得到"十三五"国家密码发展基金(MMJJ20170110)资助.**杨亚涛**(通信作者),男,博士,副教授,主要研究领域为信息安全、同态加密、密码协议和算法.E-mail:yy2008@163.com.**赵 阳**,硕士研究生,主要研究领域为同态加密、信息安全.**张奇林**,硕士研究生,主要研究领域为信息安全.**马英杰**,博士,副教授,主要研究领域为信息安全与密码算法.**高 原**,女,博士,讲师,主要研究领域为信息安全与算法.

libraries, and allows homomorphic encryption computations to be performed directly on encrypted data. SEAL enables software engineers to build end-to-end encrypted data storage and computation services. In order to solve the problem of privacy preserving and working efficiency in electronic voting, a weighted electronic voting system with homomorphic encryption based on SEAL is proposed. By using ciphertext calculation, all the ballots are counted with encrypted status, which can effectively resist the insider malicious attacks, guarantee the privacy of voters and ballots. By adding voting weight to the ballot, proposed voting system can realize the weighted voting. In this scheme, the information of voters and ballots is encrypted by SEAL and stored in cloud databases, and homomorphic tallying is completed by the cloud computing service. The security of the core encryption algorithm in our scheme is based on the hardness of RLWE problem on the lattice, which is able to resist quantum computing attacks. The evaluation of performance shows that it only costs 1.867s to complete the tally of 1,000 ballots in our electronic voting system. Compared with the electronic voting system based on Paillier proposed by Will et al. at ICCCRI2015, the runtime of homomorphic tallying is reduced by 32.73%. Compared with the electronic voting system based on Helib proposed by Wang et al. in 2017, the runtime is reduced by 96.26%. Compared with the electronic voting system based on Helib proposed by Li in 2017, the runtime is reduced by 91.81%. This e-voting system can satisfy multiple candidates voting and weighted voting, it can be applied to many kinds of voting scenarios, and the efficiency of our scheme can meet the requirements of practical applications in large-scale election.

Keywords electronic voting; weighted voting; homomorphic encryption; simple encrypted arithmetic library; ciphertext database

1 引 言

投票是人们表达观点、行使权利的重要方式,传统的纸质投票方式流程比较繁琐,耗时也比较长,受限于此,难以实现大规模的投票应用,投票形式亟待电子化、信息化. 以密码学为基础,通过密码技术、网络技术和电子设备可以实现电子投票(Electronic Voting, e-voting),它比传统纸质投票更加灵活、效率更高[1],且能节省大量的人力物力. 1981年,Chaum[2]提出第一个电子投票方案. 如今的电子投票方案可按照实现方法不同分为三类:基于混合网络(mix-net)协议[3-5]的电子投票方案、基于盲签名[6-7](Blind Signature)的电子投票方案和基于同态加密(Homomorphic Encryption)技术[8-9]的电子投票方案. 其中,基于同态加密技术的电子投票方案适合解决远程网络投票应用中最受关注的安全与隐私保护问题,且相对而言构造思路比较简洁.

同态加密允许直接在密文域进行运算,解密后可得到与明文域运算相同的结果. 同态加密源于1978年Rivset等人[9]提出的隐私同态的概念. 2009年Gentry[10]通过压缩解密电路并使用Bootstrapping技术构造出世界上第一个全同态加密(Fully Homomorphic Encryption, FHE)方案. 2010年,Dijk等人[11]延续Gentry的构造思路提出基于整数的全同态加密DGHV方案,实现了对整型数据的全同态加密,方案的安全性基于近似最大公约数[12](Approximate Greatest Common Divisor, AGCD)困难问题. 随后公钥压缩技术[13]、模交换技术[14]、批处理技术[15]被相继引入基于整数的FHE方案. 2012年Brakerski等人[16]突破Gentry的构造框架提出BGV方案,可以不使用Bootstraping技术获得层次型FHE方案,推动全同态加密研究进入了新阶段. 随后Fan等人[17]提出了BFV全同态加密方案,该方案可视为对BGV方案的优化. 近年,Microsoft基于BFV方案发布了同态加密软件库SEAL (Simple Encrypted Arithmetic Library),并对其性能不断进行完善和优化,具有很高的研究与应用价值.

Hacigumus等人[18]于2002年提出数据库即服务(Database as a Service,DaaS)的概念,即数据存储以服务的形式由第三方数据库服务器供应商提供给消费者. DaaS开启了一种新型存储模式,即云存

储.云存储模式伴随着私有数据泄露的高风险,保护隐私安全最有效的措施是加密存储,然而加密存储会破坏数据本身的数学特性,导致数据库可用性大大降低.若要在电子投票系统中借助云平台进行选票数据存储和计票,就必须解决数据库机密性与可用性之间的矛盾,找到对密文进行高效检索和计算的方法,而全同态加密的同态特性便十分契合数据库的密文运算需求.因此在云存储、云计算技术飞速发展的今天,基于同态加密技术的电子投票方案具有更为广阔的应用前景.

本文提出了一种基于SEAL库的同态加权电子投票系统,主要贡献为:

(1)设计了一个同态加权的电子投票方案.方案可有效避免传统明文计票存在的隐私泄露风险,防止内部人员在计票阶段对选票数据的恶意篡改;利用同态乘法实现加权投票,同时可支持多候选人投票,适用于多种投票场景;将选票密态存储于云端数据库中,将计票中心部署于第三方计算平台,可借助云存储和云计算技术实现数据的高效处理.

(2)基于SEAL库对本方案进行了初步实现和测试.效率测试表明本系统中同态运算效率较高,计票效率远高于其他基于同态加密技术的电子投票系统,完成对1000张选票的计票工作仅耗时1.867s,相比Will等人[19]在ICCCRI2015中提出的基于Paillier的电子投票系统计票耗时减少了32.73%,相比Wang等人[20]在2017年提出的基于Helib的电子投票系统计票耗时减少了99.26%,相比Li[21]在2017年提出的基于Helib的电子投票系统计票耗时减少了91.8%,可以满足大规模密文计票的应用需求.同时本系统加密算法BFV方案的安全性基于格上RLWE(Learning with Errors over Ring)困难问题,因此系统可以抵抗量子计算攻击.

2 相关工作

在基于混合网络的电子投票方案[22]中,首先由每个投票者生成选票并加密,然后对选票进行签名并发送到投票站(Polling Station),投票阶段一旦完成,所有被收集到的选票就会被重新"洗牌",从而隐藏投票者和选票之间的联系,但往往需要借助零知识证明(Zero-Knoledge Proof, ZKP)来验证在"洗牌"的过程中选票信息没有被篡改.在基于盲签名的电子投票方案中[23],投票者生成并加密选票后,通过可信的认证服务器对选票进行盲签名,最后将经过盲签名的选票通过匿名信道发送给投票站.

在基于同态加密技术的电子投票系统中,投票者对选票进行同态加密并发送到投票站,投票站通过同态操作将所有选票累加得到计票结果,但往往需要零知识证明来保证选票被正确编码.基于同态加密技术的电子投票系统在文献[24]中被首次提出.由于投票系统的计票过程一般情况下只涉及票数相加,所以大量电子投票系统都选择使用具有加法同态特性的部分同态加密(Partial Homomorphic Encryption, PHE)方案进行构造[25],既能满足大部分投票场景的需求,且加解密效率较高,文献[26-28]提出了基于Paillier的电子投票方案,文献[29]提出了基于Okamoto-Uchiyama的电子投票方案.此外,使用具有乘法同态特性的PHE方案也能够构造电子投票方案,文献[30-31]介绍了基于ElGamal的电子投票方案,文献[32]提出了一种适用于所有乘法PHE方案的通用电子投票架构.但基于PHE的电子投票系统存在一些共性的问题,首先是效率不高,Paillier、Okamoto-Uchiyama和ElGamal算法中都通过幂运算实现同态功能,大量幂运算会降低同态运算效率.基于加法PHE的电子投票方案难以实现高效的分布式密钥生成,基于乘法PHE的电子投票方案允许分布式密钥生成,但选票的数据量规模会随同态乘法运算次数增加呈指数形式增长,因此只能进行有限次的密文计票.针对PHE电子投票系统的效率问题,相继出现了不同的改进方案,Saadeh等人[33]通过使用多线程并行处理技术,来提高基于Paillier的电子投票系统(S-Vote)中验证选票有效性和计票两个阶段的运行效率[34],使大规模计票在可接受的时间内完成.Victor等人[35]则结合混合网络与同态加密各自的优点,提出了一种混合方案,从而提高系统效率.基于PHE设计的电子投票方案除了存在上述效率不高的问题以外,其安全性也饱受争议.2016年Tsoutsos等人[36]提出了一种针对部分同态加密电子投票系统的选票窃取攻击方案,允许恶意攻击者修改投票结果.另外,近年来随着量子计算机的发展,基于Paillier或者ElGamal的传统电子投票系统还面临着量子计算的威胁,对此,文献[37]基于LWE问题提出了一种可验证的抗量子同态电子投票系统,在保证各种安全性质的前提下还能够抵抗量子计算攻击.随着格密码理论被广泛应用于全同态加密的研究中,全同态加密技术得到迅速发展,为基于同态加密技术的电子投票系统设计也注入了新的活力.

上述工作均为基于PHE方案设计的电子投票系统,在效率和安全性上都存在许多不足,也没有实现加权投票. 本文基于全同态加密库SEAL设计实现了抗量子计算攻击的加权电子投票系统.

3 SEAL库设计原理

Microsoft SEAL是开源的同态加密软件库,使用C++语言编写,可以在不向云端提供私钥的前提下,实现云环境下端对端的密文存储和密文计算. 2016年Bajard等人[38]提出了一个BFV方案的RNS(Residue Number Systems)变体,2017年Microsoft发布SEAL2.3.0,实现了对Bajard等人方案的支持. 2018年微软发布了SEAL3.0,除了可以实现高效的整数密文运算以外,还支持Cheon等人[39]提出的CKKS方案,实现了对实数的密文运算. 在2019年最新发布的SEAL3.2.0版本中,又实现了对.NET开发的完整支持,使.NET开发人员编写同态加密应用程序更为便捷. 下面简要介绍同态加密的概念和分类,并详细介绍SEAL库的底层实现算法与BFV方案.

3.1 同态加密

通常一个同态加密方案包含四个算法:密钥生成算法(*KeyGen*)、加密算法(*Enc*)、解密算法(*Dec*)和密文计算算法(*Eval*). 其中密文计算(Ciphertext Computation)是指在密文域上进行的运算. 将一个函数f等效为一个电路模型$C(c_1, c_2, \cdots, c_k)\in C_\lambda$,其中$C_\lambda$为电路集合,$\lambda$为安全系数,则算法描述如下:

(1)密钥生成算法$KeyGen(\lambda)$是一个随机化的算法,输入安全系数λ,输出解密私钥sk、加密公钥pk以及用于密文计算的公开密钥ek.

(2)加密算法$Enc(pk, m)$是一个随机化的算法,输入公钥pk和明文m,输出密文c,对于相同的明文,每次加密得到的密文都是不同的.

(3)解密算法$Dec(sk, c)$是一个确定性的算法,输入私钥sk以及密文c,输出明文m.

(4)密文计算算法$Eval(ek,(c_1, c_2, \cdots, c_k), C)$输入密文计算密钥$ek$,电路$C(c_1, c_2, \cdots, c_k)\in C_\lambda$和密文$(c_1, c_2, \cdots, c_k)$,输出为密文计算结果$c^*$.

以上四个算法都是概率多项式时间(Probabilistic Polynomial Time, PPT)算法.

定义1. (同态性)对于加密方案α及其明文域M上的运算$\circ$,若对于$\forall m_1, m_2, \cdots, m_k\in M$都满足式(1),则表明该加密方案对于运算$\circ$满足同态性.

$$Dec(sk, Eval(ek,(c_1, c_2, \cdots, c_k),\circ)) = (m_1, m_2, \cdots, m_k)\circ \tag{1}$$

定义2. (正确性)对于$KeyGen(\lambda)$生成的公私钥对(pk, sk),电路集合C_λ中的任意电路C,明文域M中的任意明文$m_1, m_2, \cdots\cdots, m_k$以及加密得到的密文$(c_1, c_2, \cdots, c_k)$,其中$Enc(pk, m_i)\rightarrow c_i$,如果对输出的$c^* = Eval(ek,(c_1, c_2, \cdots, c_k), C)$,都有$Dec(sk, c^*) = C(m_1, m_2, \cdots, m_k)$.

那么,就认为同态加密方案α关于电路集合C_λ中的电路是正确的.

定义3. (紧凑性)对于任意的安全参数λ,假如存在一个多项式f,使得α的解密算法能够用一个规模至多为$f(\lambda)$的电路D来表示,那么,同态加密方案α便是紧凑的.

通俗来讲,满足紧凑性意味着算法的解密电路不依赖于密文或密文运算函数.

定义4. (安全性)通过选择明文攻击(Chosen Plaintext Attacks, CPA)来定义同态加密的安全性. 若式(2)对任意多项式时间敌手A在λ上都是可忽略的,则该同态加密方案为不可区分选择明文攻击安全的(也称为IND-CPA安全):

$$\left|\Pr[\mathrm{A}(pk, Enc(pk, 0))=1]-\Pr[\mathrm{A}(pk, Enc(pk, 1))=1]\right| = negl(\lambda) \tag{2}$$

其中$(pk, sk)\leftarrow KeyGen(1^\lambda)$.

按照各种同态加密方案允许密文计算的种类和次数,可以将其分为三类:部分同态加密(Partial Homomorphic Encryption, PHE)方案、类同态加密(Somewhat Homomorphic Encryption, SWHE)方案和全同态加密(Fully Homomorphic Encryption, FHE)方案. PHE仅满足加法或乘法的密文同态运算,SWHE可同时满足加法和乘法有限次的密文同态运算,FHE可同时满足加法和乘法无限次的密文同态运算.

定义5. (部分同态加密)若加密方案α仅对于加法(+)满足同态性或者仅对于乘法(×)满足同态性,则称该方案为部分同态加密方案. 即仅满足式(3)或式(4).

$$Dec(sk, Eval(ek,(c_1, c_2, \cdots, c_k),\circ)) = (m_1, m_2, \cdots, m_k)+ \tag{3}$$

$$Dec(sk, Eval(ek,(c_1, c_2, \cdots\cdots, c_k),\circ)) = (m_1, m_2, \cdots\cdots, m_k)\times \tag{4}$$

定义6. （类同态加密）若加密方案α对于加法(+)和乘法(×)都满足同态性,但是由于噪声限制只能进行有限次的同态运算,则称该方案为类同态加密方案. 即同时满足式(3)和式(4),但只能进行有限次运算.

定义7. （全同态加密）若加密方案α对于加法(+)和乘法(×)都满足同态性,且能在无限次运算后依然保持同态性,则称该方案为全同态加密方案. 即同时满足式(3)和式(4),且能进行无限次运算. 或者可以说对于任意电路$C\in C_\lambda$都满足正确性和紧凑性的同态加密方案为全同态加密方案.

3.2 BFV全同态加密方案

Microsoft SEAL库的底层实现算法是BFV全同态加密方案,BFV方案是由Fan等人[17]在2012年提出的,该方案可以看作是对Brakerski所提方案[16]的优化. 下面简要介绍BFV方案的原理.

令λ为安全系数,ω为对数的底数,$a\xleftarrow{\$}S$表示$a$是有限集合$S$的一个均匀抽样,BFV方案共包括私钥生成、公钥生成、计算密钥生成、加密、解密、加法和乘法7个算法.

私钥生成($SecretKeyGen(\lambda)$):均匀选取$s\xleftarrow{\$}R_2$并输出$sk=s$.

公钥生成($PublicKeyGen(sk)$):输入$s=sk$,选取$a\xleftarrow{\$}R_q$和$e\leftarrow\chi$,输出$pk=([-(as+e)]_q,a)$.

计算密钥生成($EvaluationKeyGen(sk,\omega)$):选取$a_i\xleftarrow{\$}R_q$和$e_i\leftarrow\chi$,其中$i\in\{0,\cdots,\ell\}$,输出$evk=([-(a_is+e_i)+\omega^is^2]_q,a_i)$.

加密算法($Encrypt(pk,m)$):输入明文$m\in R_t$,将公钥表示为$pk=(p_0,p_1)$. 进行抽样$\mu\xleftarrow{\$}R_2$和$e_1,e_2\leftarrow\chi$,计算$ct=([\Delta m+p_0u+e_1]_q,[p_1u+e_2]_q)$.

解密算法($Decrypt(sk,ct)$):令$s=sk$,$c_0=ct[0]$,$c_1=ct[1]$. 输出$\left[\frac{t}{q}[c_0+c_1s]_q\right]_t$.

同态加法运算($Add(ct_0,ct_1)$):输出$(ct_0[0]+ct_1[0],ct_0[1]+ct_1[1])$.

同态乘法运算($Multiply(ct_0,ct_1)$):计算

$$c_0=\left[\frac{t}{q}ct_0[0]ct_1[0]\right]_q,$$

$$c_1=\left[\frac{t}{q}(ct_0[0]ct_1[1]+ct_0[1]ct_1[0])\right]_q,$$

$$c_2=\left[\frac{t}{q}ct_0[1]ct_1[1]\right]_q.$$

将c_2以ω为底表示为$c_2=\sum_{i=0}^{\ell}c_2^{(i)}\omega^i$,令

$$c_0'=c_0+\sum_{i=0}^{\ell}evk[i][0]c_2^{(i)},$$

$$c_1'=c_1+\sum_{i=0}^{\ell}evk[i][1]c_2^{(i)},$$

输出(c_0',c_1').

4 基于SEAL库的同态加权电子投票系统设计

4.1 传统电子投票系统与同态加密电子投票系统对比

云环境下,电子投票系统的计票中心往往会部署在不可信的第三方计算平台上,此时使用传统电子投票系统进行计票操作时,会产生选票的机密性和计票结果正确性难以确保的问题,即使将计票中心部署在本地,传统电子投票系统也会在计票时面临内部攻击的威胁,如图1所示.

其中,应用服务器对应于各类投票客户端,代理服务器用于实现加解密功能,数据库服务器对应于云端计票中心(或本地计票中心). 利用传统电子投票系统在投票时,首先对选票数据进行加密,然后将密文选票交由计票中心进行存储和计票,计票中心在计票前需将密文选票解密为明文,计票完成后再将结果重新加密. 这为恶意破坏者提供了窃取甚至篡改选票数据的可能,使得选票的机密性难以得到保障.

基于同态加密技术的电子投票系统使得计票中心可以直接对密文选票进行计票,从而在计票阶段杜绝了选票的机密性和投票匿名性面临的威胁,且具有设计简单、思路清晰的优点,如图2所示.

与图1中的传统电子投票系统进行比较,可以发现,基于同态加密技术的电子投票系统无需在计票前解密选票,这就有效防止了来自计票中心内部的恶意攻击. 同时,基于同态加密技术的电子投票系统更为契合当下云存储、云计算模式的大发展趋势,可以实现在保证安全的前提下将本地计票中心部署在云端,借助云端强大的计算资源实现高效的密文计票.

4.2 云环境下电子投票系统的网络架构

分析电子投票系统的基本数据处理流程,可以得到云环境下电子投票系统的网络架构如图3所示.

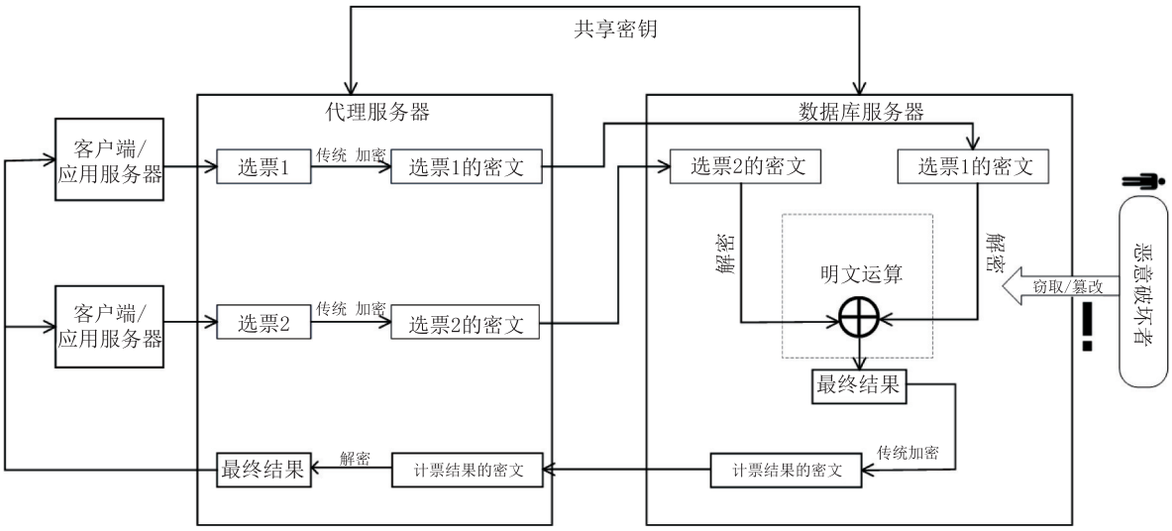

图1 采用传统加密的电子投票系统

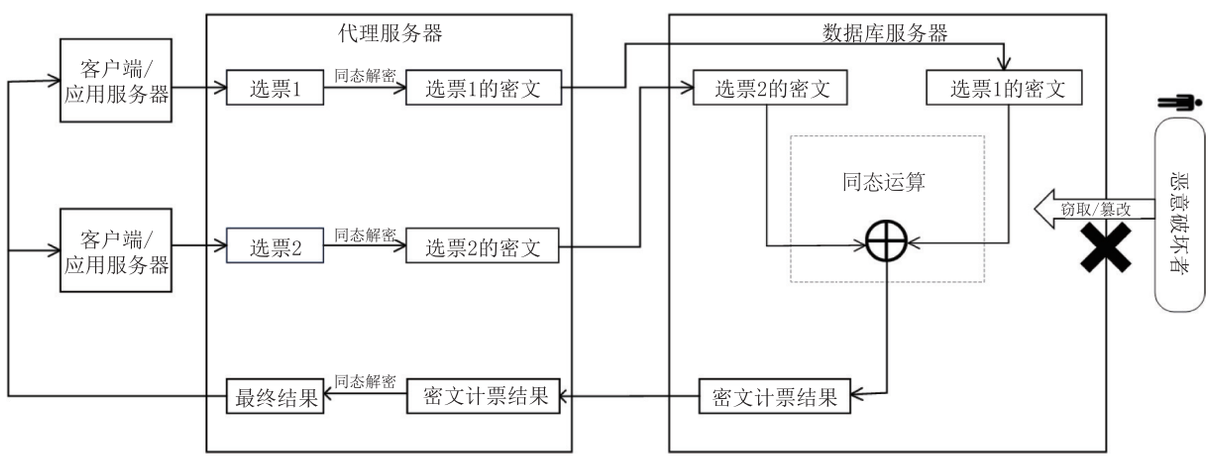

图2 采用同态加密的电子投票系统

其中,应用服务器、代理服务器和数据库服务器的功能分别为:

应用服务器:该服务器提供电子投票系统的功能模块实现,用于接收、响应用户注册、登录、查询、处理请求,以可视化方式进行信息的动态发布和更新.

代理服务器:核心处理模块,部署在本地数据中心,被认为是安全可信的.代理服务器接收应用服务器的操作请求,调用用户自定义函数.发送可执行的SQL操作语句和密文参数给数据库服务器,由代理服务器和数据库服务器联合完成密文的运算处理.代理服务器除了支持对数据的加解密,还承担身份认证和密钥管理功能,密钥由用户口令加密保护.

数据库服务器:提供数据密文存储和密文操作功能.数据库中的数据始终密态存储,通过调用用户自定义函数,支持对密文数据的同态运算.

在电子投票系统中,数据库服务器中存储使用SEAL库进行加密后的密文选票,支持直接进行密文计票.数据库中的实体关系图(Entity Relationship Diagram, ERD)如图4所示.

数据库共包含投票人、选票、投票人_投票、候选人、计票5个主要实体.其中,投票人实体包含投票人ID、由代理服务器分配的SM2算法公私钥对、选票ID、姓名、口令等属性;选票实体包含选票ID、选票信息等属性;投票人_投票实体包含投票人ID、选票ID等属性;候选人实体包含候选人ID、姓名、简介、照片路径等属性;计票实体包含候选人ID、票数等属性.

4.3 同态加权电子投票方案设计

目前的投票机制(Voting Mechanism)大体可以分为两类:一类是一票制,强调平等原则.另一类则是加权投票制,强调角色和效率原则.很多机构和部门越来越多地采用加权投票制,即根据一定标准

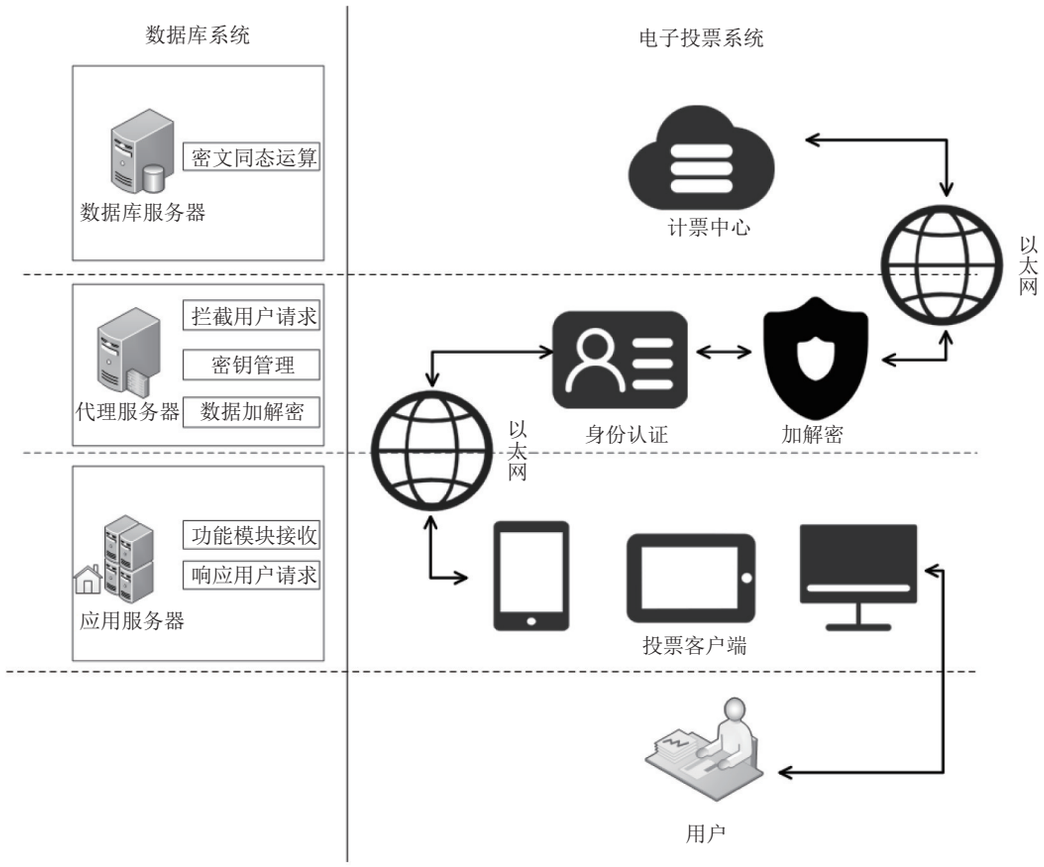

图3　云环境下电子投票平台网络架构设计

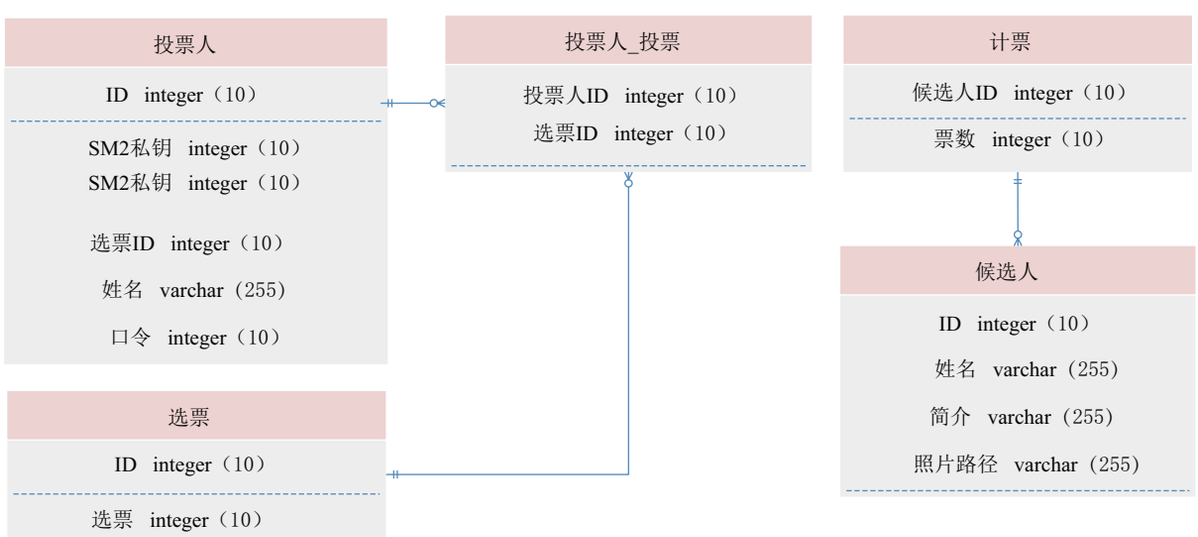

图4　数据库中的实体关系图

给予投票人不同的投票权重,以此实现公平、角色、效率的投票综合需求.

假设Alice是投票发起者,Bob是合法投票者,加权投票制电子投票方案实施过程如图5所示.

同态加权电子投票方案描述如下:

(1)初始化阶段

首先,Alice使用私有的初始化参数构建同态加密环境Env_{FHE}以及与之对应的公钥pk_{SEAL}和私钥sk_{SEAL},将Env_{FHE}和pk_{SEAL}部署在第三方计算平台.另外,Alice设置合法投票人V并为每个合法投票人分配唯一注册凭证$Cer[i]\leftrightarrow V[i]$及投票权重$w[i]\leftrightarrow Cer[i]$. 之后,Alice定义候选人被选中或

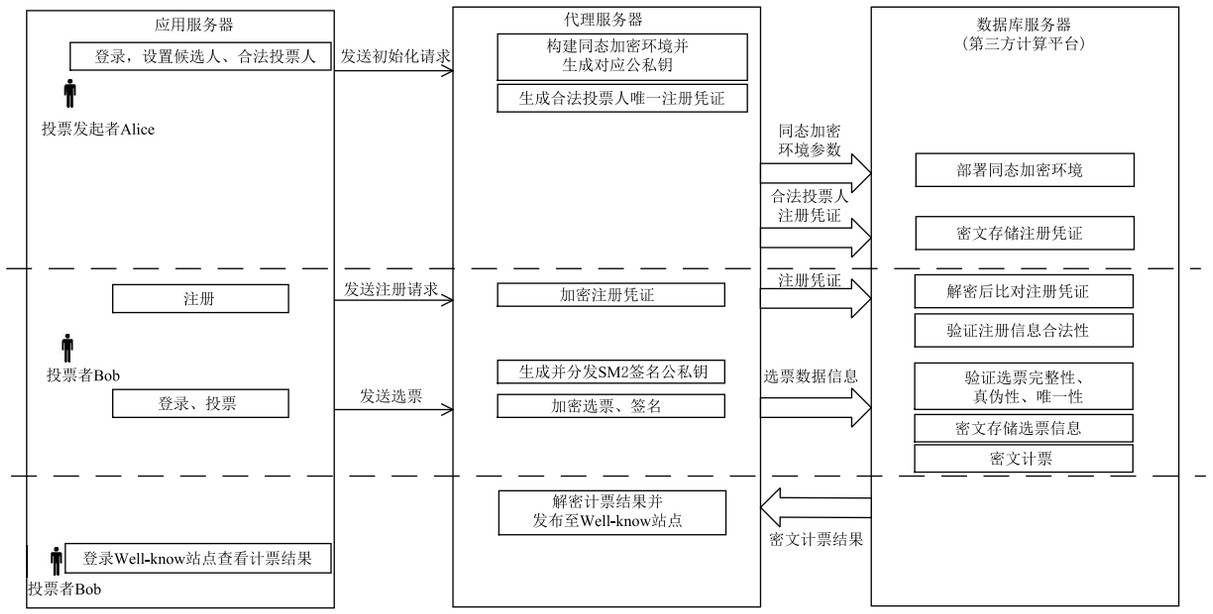

图5 同态加权电子投票系统流程图

未被选中的表示数据形式S,对应n个候选人$G=[g_1,g_2,\cdots,g_n]$和m个合法投票者$V=[v_1,v_2,\cdots,v_m]$有选票:

$$Ballot_i=[B_i,w_i].$$

其中,$B_i=\{b_1,b_2,\cdots,b_j,\cdots,b_n\}$,$i=1,2,\cdots,m$,$b_j\in\{0,1\}$,$j=1,2,\cdots\cdots,n$. 默认选票数据$b_i$为"0",表示对$g_i$不选;投票者选择某个候选人之后,选票数据$b_i$会被置为"1". 最后Alice设置候选人信息并将其写入公告牌.

(2)注册阶段

Alice开启注册服务,合法投票人Bob递交注册凭证Cer_{Bob},代理服务器对其身份进行验证$Verf(Cer_{Bob},Cer)$,通过验证后为其生成唯一的公钥pk_{SM2_Bob}和私钥sk_{SM2_Bob}.

(3)投票和计票阶段

投票:Bob从候选人中选出自己的支持者并生成选票$Ballot_{Bob}$,使用同态加密公钥pk_{SEAL}加密后得到密文选票$Ballot_{Bob_Ctxt}$,同时使用sk_{SM2_Bob}对选票$Ballot_{Bob}$的哈希值进行签名得到Sig_{Bob},最后通过网络向计票中心提交投票数据信息$[Ballot_{Bob_Ctxt},Sig_{Bob}]$,其中

$$Ballot_{Bob\_Ctxt}=Enc[pk_{SEAL},Ballot_{Bob}].$$

$$Sig_{Bob}=Sig[sk_{SM2\_Bob},H(Ballot_{Bob})].$$

计票:计票中心对选票进行完整性、真伪和唯一性验证,完整性通过比对哈希值进行验证,真伪性通过对数字签名验签来实现,唯一性通过比对注册凭证进行验证,只有通过验证的选票才会被存储在密文数据库中,并参与计票. 计票时首先将所有选票中的密态选票信息B_{i_Ctxt}与密态选票权重w_{i_Ctxt}分别同态相乘得到$B_{i_Ctxt}w_{i_Ctxt}$,再将所有乘积同态相加得到候选人G的密文计票结果为:

$$Result_{Ctxt}=\sum_{i=1}^{m}(B_{i\_Ctxt}\times w_{i\_Ctxt}).$$

进行一次解密后,得到明文计票结果为

$$Result=Dec(sk_{SEAL},\sum_{i=1}^{m}(B_{i\_Ctxt}\times w_{i\_Ctxt})).$$

(4)获得投票结果

计票结果采用集中式公布,代理服务器获取密文计票结果后,进行同态解密得到明文计票结果并公布,投票者可以主动查看获取选举结果.

5 安全性分析

一个安全的电子投票系统必须满足正确性、匿名性、机密性、无收据性、公平性、可验证性等安全需求. 保证本文电子投票系统安全性的前提是代理服务器要安全可靠.

BAN逻辑是由Burrows,Abadi和Needham提出的一种基于信仰的形式化证明逻辑[40]. 这里现在假定,投票人V的公私钥对为(pk_{SM2},sk_{SM2}),计票中心为T,代理服务器P的公私钥对为(pk_{SEAL},sk_{SEAL}). 下面利用BAN逻辑对电子投票系统的安全性进行形式化证明. 本文提出的方案主要目的是正确进行投票和计票,该方案的初始假设为:

(1)$P|\equiv \overset{pk_{SM2}}{\mapsto} V$,即$P$相信$V$的公钥是$pk_{SM2}$;

(2)$V|\equiv \overset{pk_{SEAL}}{\mapsto} P$,即$V$相信$P$的公钥是$pk_{SEAL}$;

(3)$V|\equiv P$,即V相信P是安全可信的.

同态加权投票过程可以形式化为:

(1)$P \lhd ID_V$;

(2)$V \lhd pk_{SM2}$, $V \lhd sk_{SM2}$;

(3)$P \lhd Ballot_i$,P对$Ballot_i$进行加密和签名;

(4)$T \lhd Ballot_{i\_Ctxt}$,将密文选票发送给计票中心;

(5)$P \lhd Result_{Ctxt}$,P对$Result_{Ctxt}$进行解密;

(6)$V \lhd Result$,V得到明文选票信息;

由新鲜规则和看见规则可以得到:

(7)$V|\equiv P|\equiv Result$,即$\boldsymbol{V}$相信"$\boldsymbol{P}$相信计票结果是正确的".

由上述步骤看出,提出的方案是安全的,可以实现密文投票和正确计票.

对本方案其他属性的分析如下:

(1)正确性:每一位被投票发起者授权的投票者v_i只能进行一次投票,多次投票无法通过唯一性验证,如果有恶意攻击者试图伪造选票,就必须伪造由代理服务器授权的数字签名,这在计算上是不可行的,所以攻击者无法伪造选票或者干预投票结果.计票过程中所有合法选票都会被计入在内,方案满足正确性.

(2)匿名性和机密性:为实现密文计票,将选票内容全部用整数表示,经代理服务器加密后发送至云端存储并计票,投票者的身份信息和选票信息在计票阶段始终处于密文状态,任意恶意攻击者即便截获选票,也无法获得明文信息,从而保证选举过程的匿名性和机密性.

(3)无收据性:投票者的选票一旦投出,就会经代理服务器加密,并在后续的选票存储、计票阶段始终处于密文状态,投票者无法重构自己的选票,因此也不能向恶意第三方证明自己的选票内容,该方案满足无收据性.

(4)公平性:每个投票者都有唯一的注册凭证$Cer[i]$,注册成功的投票者的注册凭证加密后会在云端存储,通过核对凭证来保证每位合法投票者只能投出一张选票;同时,投票者之间互不知道选票的具体内容,且均不参与计票过程,因此,该方案满足公平性.

(5)可验证性:方案采用了常用的公告板机制,在注册结束后,会公布所有合法投票者的ID_i,计票结束后会再次公布投票者的ID_i和选票编号,投票者可以跟踪验证自己的选票是否被正确计入在内.

6　性能测试

测试环境均为配置为英特尔i5、1.6 GHz处理器,8 GB内存,Windows 10操作系统的笔记本电脑,分别对SEAL库进行重线性化测试、安全参数测试,对投票系统进行密文计票效率测试.

6.1　SEAL库重线性化测试

在进行同态运算的过程中会产生密文膨胀问题,密文膨胀不仅会降低同态运算效率,同时还会导致噪声加速增长.BFV方案使用重线性化技术来解决密文膨胀问题,下面对SEAL库重线性化技术的实际优化效果进行测试.模拟选举有投票者200名、候选人1名,直接进行密文计票和先对密文进行重现性化操作后再进行密文计票的效率测试结果分别如图6、图7所示.

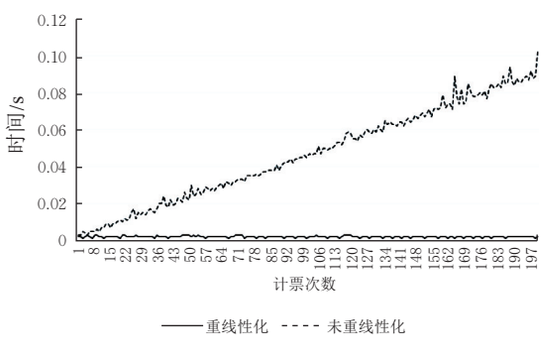

图6　计入单张新选票耗时

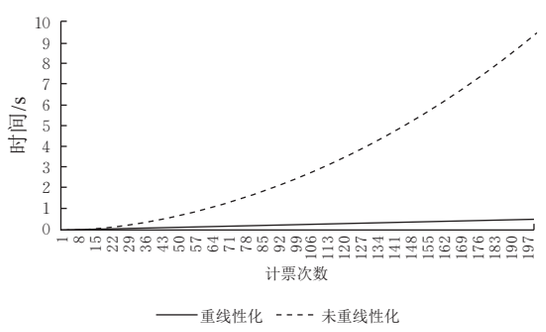

图7　计入多张选票累计耗时

从图6中可以看出,若不使用重线性化技术,计入单张新选票耗时会随计票次数增加而线性增加,而先对密文进行重线性化处理后再计票,计入单张新选票耗时大约恒定在2 ms.相应从图7中可以看到,若不使用重线性化处理密文,计入多张选票累计耗时会随着计票次数的增加而呈指数形式增长,若先对密文进行重线性化处理再计票,计入

多张选票累计耗时随计票次数增加呈线性增长.

密文膨胀不仅会降低同态运算效率,还会导致密文噪声加速增长,导致解密失败,测试结果显示若不使用重线性化解决密文膨胀问题,当设置参数poly_modulus_degree为2048时,最多只能计入381张选票,相同参数下引入重线性化技术,可以计入70000余张选票,如表1所示.

经过重线性化后,计入单张新选票所需的平均时间从110 ms缩短至1.8 ms,重线性化技术的优化效果非常显著,可使密文计票的时间缩短98.36%,因此在进行密文运算前先对密文进行重线性化处理是实际应用SEAL库进行同态运算的必要步骤.

表1 重线性化测试

重线性化	可计入票数	计入单张票所需平均时间/s
是	76913	0.0018
否	381	0.11

6.2 安全参数选择测试

将实验参数选取为

coeff_modulus_128(poly_modulus_degree),

plain_modulus(1≪20),

测试不同的poly_modulus_degree对同态操作效率的影响.

安全参数是影响算法安全级别的主要指标,poly_modulus_degree代表分圆多项式的次数,它的值取2的整数次幂.poly_modulus_degree取值越大,则方案越安全,但也会使密文体积变大,导致初始化、加密、同态加、同态乘、解密等操作效率降低,如表2所示.

表2 安全参数选择测试

安全参数poly_modulus_degree	初始化时间/ms	加密时间/ms	加法时间/ms	乘法时间/ms	加法解密时间/ms	乘法解密时间/ms
2048	14.42	2.38	—	1.36	0.2	0.16
4096	72.16	5.48	—	4.7	0.5	0.66
8192	424.2	14.94	0.18	17.64	1.54	2.48
16384	2760.88	44.78	1.08	71.62	6.32	9.84

表2中数据均为50次测试结果的平均值,从表2中可以明显看到,随着poly_modulus_degree取值增大,同态操作的耗时都普遍随之增加,且呈指数形式增加,因此应根据实际情况选取合适的安全参数,一般情况下设置poly_modulus_degree为2048较为合适.

6.3 明文空间选择测试

将实验参数选取为

poly_modulus_degree(2048),

coeff_modulus_128(2048),

测试不同的plain_modulus对同态操作效率的影响.

明文空间plain_modulus在电子投票中代表选民的规模,它可以被设置为任意的正整数.plain_modulus不仅决定着明文数据的大小,同时也会影响新鲜密文的噪声以及同态乘运算后的噪声增长.新鲜密文所允许的噪声增长上限可以表示为$\log_2$(coeff_modulus/plain_modulus)(bits),单次同态乘引起的噪声增量可以表示为$\log_2$(plain_modulus)+(other terms)的形式.明文空间选择测试结果如表3所示.

从表3的测试结果中可以看出,随着明文空间的增大,乘法解密时间也随之增加,因此,为了提高运算效率,明文空间需在满足实际情况的前提下尽可能最小.

6.4 相似类型的电子投票系统对比分析

将本方案与其他基于同态加密技术的电子投票系统进行对比,结果如表4所示.

表3 明文空间选择测试

明文空间plain_modulus	初始化时间/ms	加密时间/ms	加法时间/ms	乘法时间/ms	加法解密时间/ms	乘法解密时间/ms
101	0.01462	0.00242	2.00E-05	0.00148	0.00018	0.0001
5101	0.01442	0.00238	—	0.00136	0.0002	0.00016
15101	0.01432	0.00228	—	0.0015	0.00012	0.00016
20101	0.01424	0.00242	—	0.00132	0.00016	0.0002

表4　与其他相似方案比较

投票方法	同态加密算法	抗量子计算攻击	加权投票	计票效率(时间/票数)	困难问题
文献[19]	Pallier	NO	NO	2.78ms	N次剩余类问题
文献[33]	Pallier	NO	NO	39.94ms	N次剩余类问题
文献[20]	BGV	YES	NO	253.33ms	RLWE问题
文献[21]	BGV	YES	NO	21.10ms	RLWE问题
本方案	BFV	YES	YES	1.87ms	RLWE问题

文献[19]中由于Paillier加密算法需要执行幂运算来实现同态操作,效率低于本方案,本方案的计票耗时相较于文献[19]减少了32.73%.文献[33]通过使用多线程技术对基于Pallier的电子投票方案进行了优化,表中的计票时间包含借助零知识证明对选票进行有效性验证的耗时,本文通过代理服务器对选票统一编码和加密,省去了零知识证明引入的耗时.文献[20-21]均提出了一种基于Helib库设计实现的电子投票系统,由于需要引入密文全加器,计票效率均低于本方案,本方案的计票耗时相较于文献[20]减少了99.26%,相较于文献[21]减少了91.81%.

7　结束语

本文通过将全同态加密技术应用于数据库中,实现了数据库中数值型数据的密文同态计算,并在此基础上设计实现了基于SEAL库的同态加权电子投票系统,系统在保证投票匿名性、可认证性的同时,可以有效保护计票过程的隐私安全,防止来自计票中心内部的恶意攻击.由于SEAL库的安全性基于RLWE格困难问题,系统可以抵抗量子计算攻击.同时,将计票中心部署在云端可以充分发挥云计算优势而进行高效计票.测试结果表明本方案运行效率较高,可以满足大规模选举的计票需求,具有一定的应用价值.下一步的研究方向,一是可结合同态签名技术实现投票系统的公开可验证性,二是可引入批处理技术进一步提高计票效率.

参　考　文　献

[1] Clarkson M R, Chong S, Myers A C. Civitas: toward a secure voting system//Proceedings of the IEEE Symposium on Security and Privacy. Oakland, USA, 2008: 354-368

[2] Chaum D L. Untraceable electronic mail, return addresses, and digital pseudonyms. Communications of the ACM, 1981, 24(2): 84-90

[3] Park C, Itoh K, Kurosawa K. Efficient anonymous channel and all/nothing election scheme//Proceedings of 1993 Workshop on the Theory and Application of Cryptographic Techniques. Lofthus, Norway, 1993: 248-259

[4] Golle P, Zhong S, Boneh D, et al. Optimistic mixing for exit-polls//Proceedings of the 8th International Conference on the Theory and Application of Cryptology and Information Security. Queenstown, New Zealand, 2002: 451-465

[5] Jakobsson M. Flash mixing//Proceedings of the 18th Annual ACM Symposium on Principles of Distributed Computing. Atlanta, USA, 1999: 83-89

[6] Fujioka A, Okamoto T, Ohta K. A practical secret voting scheme for large scale elections//Proceedings of 1992 Workshop on the Theory and Application of Cryptographic Techniques. Gold Coast, Australia, 1992: 244-251

[7] Chen T S, Liu T P, Chung Y F. A proxy-protected proxy signature scheme based on elliptic curve cryptosystem//Proceedings of the IEEE Region 10 Conference on Computers. Beijing, China, 2002: 184-187

[8] Zhang Peng, Yu Jian-Ping, Liu Hong-Wei, et al. A homomorphic signcryption scheme and its application in electronic voting. Journal of Shenzhen University (Science & Engineering), 2011, 28(6): 489-494 (in Chinese)
(张鹏, 喻建平, 刘宏伟等. 同态签密方案及其在电子投票中的应用. 深圳大学学报(理工版), 2011, 28(6): 489-494)

[9] Rivest R L, Adleman L, Dertouzos M L. On data banks and privacy homomorphisms. Foundations of Secure Computation, Academic Press, 1978: 169-179

[10] Gentry C. Fully homomorphic encryption using ideal lattices//Proceedings of the 41st Annual ACM Symposium on Symposium on Theory of Computing (STOC 2009). Bethesda, USA, 2009: 169-178

[11] Dijk M, Gentry C, Halevi S, et al. Fully homomorphic encryption over the integers//Proceedings of the 29th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Riviera, France, 2010: 24-43

[12] Howgrave-Graham N. Approximate integer common divisors// Proceedings of the International Conference on Cryptography and Lattices. Providence, USA, 2001: 51-66

[13] Coron J S, Mandal A, Naccache D, et al. Fully homomorphic encryption over the integers with shorter public keys// Proceedings of the 31st Annual Cryptology Conference. Santa Barbara, USA, 2012: 487-504

[14] Coron J S, Naccache D, Tibouchi M. Public key compression

and modulus switching for fully homomorphic encryption over the integers//Proceedings of the 31st Annual International Conference on the Theory and Applications of Cryptographic Techniques. UK, 2012: 446-464

[15] Cheon J H, Coron J S, Kim J, et al. Batch fully homomorphic encryption over the integers//Proceedings of the 32nd Annual International Conference on the Theory and Applications of Cryptographic Techniques. Athens, Greece, 2013: 315-335

[16] Brakerski Z, Gentry C, Vaikuntanathan V. (Leveled) fully homomorphic encryption without bootstrapping//Proceedings of the 3rd Innovations in Theoretical Computer Science Conference. Cambridge, USA, 2012: 309-325

[17] Fan J F, Vercauteren F. Somewhat practical fully homomorphic encryption. Cryptology ePrint Archive, 2012, 2012: 144. http://eprint. iacr. org/2012/144

[18] Hacigumus H, Iyer B, Mehrotra S. Providing database as a service//Proceedings of the 18th International Conference on Data Engineering. San Jose, USA, 2002: 29-38

[19] Will M A, Nicholson B, Tiehuis M, et al. Secure voting in the cloud using homomorphic encryption and mobile agents// Proceedings of the 2015 International Conference on Cloud Computing Research and Innovation (ICCCRI 2015). Singapore, Singapore, 2015: 173-184

[20] Wang Yong-heng, Xu Chen, Chen Jing-wei, et al. Scheme on secure voting system based on HElib. Application Research of Computers, 2017, 34(7): 2167-2171. (in Chinese)
(王永恒, 徐晨, 陈经纬等. 基于HElib的安全电子投票方案. 计算机应用研究, 2017, 34(7): 2167-2171)

[21] Li Ren-jie. Design and implementation of e-voting system based on full homomorphic encryption [Master Thesis]. Chongqing University, Chongqing, 2017. (in Chinese)
(李仁杰. 全同态加密的电子投票系统设计与实现[硕士学位论文]. 重庆大学, 重庆, 2017)

[22] Peng K. An efficient shuffling based eVoting scheme. Journal of Systems and Software, 2011, 84(6): 906-922

[23] Mateu V, Sebe F, Valls M. Constructing credential-based e-voting systems from offline e-coin protocols. Journal of Network and Computer Applications, 2014, 42: 39-44

[24] Benaloh J, Fischer M J. A robust and verifiable cryptographically secure election scheme//Proceedings of the Symposium on Foundations of Computer Science. Portland, USA, 1985: 372-382

[25] Zhao Y M, Pan Y, Wang S C, et al. An anonymous voting system based on homomorphic encryption//Proceedings of the International Conference on Communications (COMM 2014). Bucharest, Romania, 2014: 1-4

[26] Baudron O, Fouque P A, Pointcheval D, et al. Practical multi-candidate election system// Proceedings of the 20th Annual ACM Symposium on Principles of Distributed Computing. Newport, USA, 2001: 274-283

[27] Damgård I, Jurik M, Nielsen J B. A generalization of paillier's public-key system with applications to electronic voting. International Journal of Information Security, 2010, 9(6): 371-385

[28] Anggriane S M, Nasution S M, Azmi F. Advanced e-voting system using paillier homomorphic encryption algorithm// Proceedings of the International Conference on Informatics & Computing. Mataram, Indonesia, 2016: 338-343

[29] Suwandi R, Nasution S M, Azmi F. Okamoto-Uchiyama homomorphic encryption algorithm implementation in e-voting system //Proceedings of the 2016 International Conference on Informatics and Computing. Mataram, Indonesia, 2016: 329-334

[30] Cramer R, Gennaro R, Schoenmakers B. A secure and optimally efficient multi-authority election scheme. European Trans on Telecommunications, 1997, 8(5): 481-490

[31] Yang X C, Yi X, Nepal S, et al. A secure verifiable ranked choice online voting system based on homomorphic encryption. IEEE Access, 2018, 6(2): 506-519

[32] Azougaghe A, Hedabou M, Belkasmi M. An electronic voting system based on homomorphic encryption and prime numbers//Proceedings of the 2015 11th International Conference on Information Assurance and Security. Marrakech, Morocco, 2015: 140-145

[33] Saadeh I A, Abandah G A. Investigating parallel implementations of electronic voting verification and tallying processes//Proceedings of the 2017 European Conference on Electrical Engineering and Computer Science (EECS 2017). Bern, Switzerland, 2017: 70-75

[34] Abandah G A, Darabkh K A, Ammari T, et al. Secure national electronic voting system. Information Science and Engineering, 2014, 30(5): 1339-1364

[35] Víctor M, Josep M, Francesc S. A hybrid approach to vector-based homomorphic tallying remote voting. International Journal of Information Security, 2016, 15(2): 211-221

[36] Tsoutsos N G, Maniatakos M. Cryptographic vote-stealing attacks against a partially homomorphic e-voting architecture// Proceedings of the International Conference on Computer Design. Scottsdale, USA, 2016: 157-160

[37] Wu C, Tang S H, Yan X F. A homomorphic LWE-based verifiable electronic voting system//Proceedings of the 2018 IEEE Conference on Dependable and Secure Computing (DSC 2018). Kaohsiung, Taiwan, 2018: 1-8

[38] Bajard J C, Eynard J, Hasan A, et al. A full RNS variant of FV like somewhat homomorphic encryption schemes// Proceedings of the Selected Areas in Cryptography-SAC 2016. Newfoundland, Canada, 2016: 423-442

[39] Cheon J H, Kim A, Kim M, et al. Homomorphic encryption for arithmetic of approximate numbers//Proceedings of the 23rd International Conference on the Theory and Applications of Cryptology and Information Security. Hong Kong, China, 2017: 409-437

[40] Burrows M, Abadi M, Needham R M. A logic of authentication. ACM Transactions on Computer Systems, 1990, 8(1): 18-36

Yang Ya-Tao, Ph. D. Associate professor. His current research interests include information security, homomorphic encryption, cryptographic protocol and algorithm.

Zhao Yang, M. S candidate. His current research interests include homomorphic encryption and information security.

Zhang Qi-Lin, M. S candidate. His current research interests include information security.

Ma Ying-Jie, Ph. D. Associate professor, her current research interests include information security and cryptographic algorithms.

Gao Yuan, Ph. D. Lecturer, her current research interests include information security and algorithms.

Background

Electronic voting, as an alternative to the traditional voting schemes, has become a popular research topic in recent years.

A weighted electronic voting system with homomorphic encryption is proposed based on SEAL. The main contributions include:

(1) A weighted electronic voting scheme is proposed. Based on the homomorphic encryption technology, the homomorphic ciphertext calculating is adopted, which is able to avoid the risk of privacy leakage in traditional plaintext tallying, and to prevent inside personnel from maliciously tampering with the ballot data during the tallying stage. Homomorphic multiplication operations were used to achieve weighted voting, at the same time, this scheme could support multiple-candidate-voting, which is applicable to many kinds of voting scenarios. In proposed solution, the ballot's secrets were stored in the cloud database, the counting center is deployed on the third-party computing platform, which could achieve efficient data processing by using cloud storage and cloud computing technologies.

(2) The scheme is implemented by using SEAL. Based on SEAL library, homomorphic computing operations in electronic voting system were implemented. The evaluation of performance showed that our system's efficiency in tallying process is much higher than other electronic voting systems based on homomorphic encryption technology. Compared with the electronic voting system based on Paillier proposed by Will et al. at ICCCR I2015, the runtime of homomorphic tallying is reduced by 32.73%. Compared with the electronic voting system based on Helib proposed by Wang et al. in 2017, the runtime is reduced by 96.26%. Compared with the electronic voting system based on Helib proposed by Li in 2017, the runtime is reduced by 91.81%. The working efficiency in our scheme could meet the requirements of practical applications in large-scale election. The core encryption scheme in our e-voting system is BFV, and its security is based on the hardness of RLWE problem on the lattice, which is able to resist quantum computing attacks.