# 基于全同态加密的电子投票方案设计


重庆大学硕士学位论文

（专业学位）

学生姓名：刘雷燕

指导教师：张　玲　教　授

学位类别：工程硕士（电子与通信工程领域）

重庆大学通信工程学院

二〇一七年四月

# Design of E-Voting Scheme Based on Fully Homomorphic Encryption


A Thesis Submitted to Chongqing University

in Partial Fulfillment of the Requirement for the

Professional Degree

**By**

**Liu Leiyan**

**Supervisor：Prof. Zhang Ling**

**Specialty:ME (Field of Electronics and Communication Engineering)**

College of Communication Engineering of

Chongqing University, Chongqing, China

April 2017

# 摘　　要

在信息安全技术和计算机网络技术的支撑下，电子投票逐渐成为目前各种政治、娱乐活动中用于民意统计、体现活动公平性和民主性的重要手段。然而，当前大多数电子投票在选票匿名性、可验证性及完整性等方面还存在一定的不足，导致贿选、拉票等问题依旧较为普遍存在，一定程度上影响了投票活动的公平性。论文针对投票的安全性和效率问题，综合采用全同态加密、数字签名技术，设计了一个具有匿名性、可验证性和高效的电子投票方案。本文的主要研究内容如下：

① 论文从电子投票的实际应用情况出发，通过对电子投票方案的特性需求进行分析，引入全同态加密技术，最大限度的保证了选票的匿名性；同时采用数字签名技术有效保证了投票者的合法性、选票信息的完整性和选票的可验证性，最终完成了电子投票的总体方案设计。

② 电子投票方案的安全性主要依赖于全同态加密算法的同态特性，论文从基本定义、性能实现和应用三个方面对全同态加密进行研究，设计了一种基于 RLWE 问题的全同态加密方案，并基于 HElib 同态算法库对该全同态加密方案进行了验证。同时与其他全同态加密方案进行了对比分析。结果表明，基于 RLWE 问题的全同态加密能够有效地解决电子投票方案的匿名性问题，符合投票方案设计的预期目标要求。

③ 根据电子投票方案的设计目标，依据基于 RLWE 问题的全同态加密算法和 RSA 数字签名技术，从初始化、注册投票、计票和验证查票四个阶段详细阐述了电子投票方案的具体流程，并对投票方案进行了全面的特性分析，分析结果表明，该方案具有良好的匿名性、可验证性和较强的安全特性。

论文所设计的基于 RLWE 问题全同态加密的电子投票方案对解决投票的安全性问题进行了有益的探索，课题组对该方案进行了实现验证。实验结果表明，该投票方案较好地解决了投票的匿名性、完整性和可验证性，从而保证了方案的安全性，并且满足了性能要求，达到了方案设计的预期目标。

**关键词：**全同态加密，数字签名技术，电子投票，匿名性

# ABSTRACT

Under the support of the information security technology and computer network technology, electronic voting has become a way of political and recreational activities for public opinion statistics, reflecting the fairness of the activities and an important means of democracy. However, most of the current electronic voting exist some deficiencies, for example the ballot anonymity, verifiability and integrity. Bribery, canvassing and other issues are still more common, and which has great affect on the fairness of voting activities. Aiming at the problem of security and efficiency of voting, this paper designs an electronic voting scheme with anonymity, verifiability and efficiency by using fully homomorphic encryption and digital signature technology. The main results of this paper are summarized as follows:

① Based on the practical application of electronic voting, this paper analyzes the characteristics of electronic voting scheme, and introduces the fully homomorphic encryption technology to guarantee the anonymity of ballot papers to the maximum extent, and uses digital signature technology to guarantee the voters' legitimacy, the integrity of the ballot paper information and the verifiable verdict of votes. Finally, this thesis completes the overall scheme of electronic voting.

② The security of the electronic voting scheme mainly depends on the security of the fully homomorphic encryption algorithm. The fully homomorphic encryption is studied from three aspects: the basic definition, the performance realization and the application. This thesis designs a homomorphic encryption based on the RLWE problem, and validates the homomorphism scheme based on HElib homomorphic algorithm library. At the same time, it is compared with other homomorphic encryption schemes. The results show that the fully homomorphic encryption based on the RLWE problem can effectively solve the anonymity problem of the electronic voting scheme and meet the anticipated objectives requirements of the voting scheme design.

③ According to the design goal of the electronic voting scheme, the specific flow of the electronic voting scheme is elaborated from the four stages of initialization, registration and voting, counting and verification, according to the fully homomorphic encryption algorithm based on the RLWE problem and the RSA digital signature technology. And this thesis analyzes the characteristics of the voting scheme, showing that the voting scheme has good anonymity, verifiability and strong safety characteristics.

In this paper, the problem of voting security is soved by the electronic voting scheme based on FHE. The team validates the scheme in a certain network environment. The experimental results show that the voting scheme solves the anonymity, completeness and verifiability of voting, which ensures the security of the program and satisfies the performance requirements, and reaches the anticipated objectives.

**Keywords:** Fully Homomorphic Encryption, Digital Signature, E-voting, Anonymity

# 目　录

# 1 绪 论

## 1.1 课题研究背景及意义

投票是人们表达自己对某一问题想法的一种方式，这种表达方式随着社会科学技术发展水平的不同而变化，比如从古代的石头，到近代纸质投票、机械杠杆投票仪、打孔卡、光学识别投票，再到今天的直接记录电子投票系统、远程网络投票等。

传统的投票方式存在的弊端逐渐突出：第一，传统的投票方式不能有效保证投票的公正性；在一次投票活动中，活动组织者和监督者都必须完全可信，如果有一人存在作弊行为，都无法保证投票活动的公正性以及投票结果的正确性。第二，在投票过程中出现的作弊行为难以被发现；比如，如果出现合法投票者没有参加投票活动的状况，那么不可信的活动组织者可能捏造大量的选票，甚至可以用伪造的选票代替合法选票。由于一次投票活动中，参与人员较多，工作繁杂，很难找出伪造选票。第三，传统投票活动需要在特定时间段和特定地点举行，局限性很大。因此，传统投票必须要花费大量的人力和物力来保证投票活动公平的进行，防止破坏和作弊行为的发生。

电子投票是数学知识、密码学和计算机网络的综合应用。随着计算机和网络的迅猛发展，以及网络本身所具有的优势，使人们利用计算机或者各种通信设备在任何地方通过网络进行投票成为现实。比如，可以吸引更多人的来投票，方便残疾人参与投票活动，投票的人数不受天气地点等状况的影响。电子投票不仅消除了选票的运输和计票上的困难，也大大减少了投票由于日常安排原因与投票时间发生冲突而带来的不便。同时由于电子投票方式的方便性和实施成本的低廉，必将对社会经济的发展和国家民主进程产生积极而重大的影响。

尽管电子投票的方式有显著的优势，但是它在实现过程中还存在许多问题。电子投票方案不仅要考虑整个投票过程的安全性，更要考虑方案的实用性，这就对所用的加密算法的效率有一定的要求。随着密码学算法的发展，研究人员利用态加密算法的同态运算特性，对同态加密技术与电子投票方案的结合应用进行了大量的研究分析，推进了电子投票的发展。

最近的二十多年，科研人员对电子投票以及同态加密展开了深入研究，提出了许多基于同态加密的电子投票方案。但是，不管是在理论还是在实践方面，目前都没有非常完善的解决方案。因此，对基于同态加密的电子投票方案进行深入研究具有重要的现实意义。

## 1.2 国内外研究现状

由于计算机技术和通信网络的不断完善，电子投票的方式也吸引了专业人士的广泛关注。电子投票的主要的发展历程主要分为以下阶段。

① 1981 年，David Chaum 首次提出了基于 Mix-net 的电子投票协议[1]，并且证明该协议可以抵抗被动攻击。被动攻击者可以监控在混合服务器之间的所有通信，但是不能够得到混合服务器内部各个混合的排列顺序。经过混合网技术[2]处理之后，得到的最终输出结果便无法和原始输入一一对应，因此保证了投票者的秘密性。但是该方法使用的公钥密码体制算法复杂度较高，因此不适合投票人数过多的大规模投票活动。Dan Boneh，Philippe Golle 等[2]对这类算法进行了详细分析，主要是运用概率论思想查找 Mix-net 运算中的作弊服务器，并对查找成功概率进行了数学证明。高虎明等人提出了一个基于 Mix-net 的电子投票方案[3]，运用 Mix-net 协议实现计票过程的匿名性，并且给出了选票解密运算正确性的零知识证明，同时采用两组 mix 运算服务器对比计算的方法增加作弊的难度，但是该方法过度依赖可信的第三方，不能防止合谋攻击行为。

② 基于盲签名算法的电子投票方案[4~6]。盲签名方案的主要思想是，每个投票者生成自己保证过的选票数据，同时将选票数据盲签名处理之后通过匿名信道发送到可信机构，机构验证过这个签名合法后发送自己的盲签名报文，签名人接收到盲签名报文后再匿名发送投票结果以实现匿名方案。这些方案只有投票者自己可验证选票是否被计入，不具有公开可验证性。

③ 基于同态加密技术的电子投票方案。1999 年，Paillier .P 第一次提出了基于 ELGamal 加密同态性的电子投票方案[6]，利用 ELGamal 加密同态性将多张加密后的选票进行累积乘法之后，作为一个整体进行计票。文献[8]中提出了一种改进的 ELGamal 加密电子投票方案，该方案不仅规定了选票的编码格式，并通过比较两个候选人得票差值的方法进行计票。文献[9]第一次提出了一种基于 Paillier 加密同态性和门限密钥共享思想的电子投票方案，Paillier 算法的加密同态性能够实现加法同态性，所以很容易应用到电子投票方案中。文献[10]借用打孔投票中的一些思想，又重新定义了 Paillier 加密电子投票方案的选票编码格式。文献[11]针对以前的方案进行总结，对基于 ELGamal 加密同态性的电子投票方案进行优化，给出了查找作弊算法及其分析和证明。朱正阳等人提出了关于全同态加密的电子投票方案[12]，但是此方案采用的是基于整数上的全同态加密算法，此全同态加密算法效率不高，并且很难实现应用到实际的投票活动当中。

自从 1978 年由 RSA 的作者提出同态加密的思想之后，出现了许多的同态加密方案。但是这些方案只能实现单一的同态加法或同态乘法。经过 30 多年的发展，2009 年 Graig Gentry 的博士论文[13]从数学角度出发给出了全同态加密的可行性方

法，使得这项技术取得了突破性进展。首先出现的全同态加密方案基本是基于格上或者是整数近似公约数的困难问题，按照 Gentry 蓝图框架来实现的。这些全同态方案[14~29]首先构造一个部分同态加密方案，能够执行有限次数的运算；最后使用 bootsrappable 技术改造从而实现全同态加密方案，但是这些方案的执行效率不高。近几年许多密码研究者提出了新型的全同态加密方案[30]~[38]，它们的安全问题规约到 LWE(Learning With Errors，LWE)[39]或 RLWE(Learning With Errors over Ring，RLWE)[40]困难问题，打破了原有的 Gentry 构造框架，这种类型的方案用重线性化技术、模交换技术和密钥转换技术替代 bootsrappable 技术，在一定程度上提高了运行效率。近两年，国内外学者对全同态加密进行了大量的研究分析，由于全同态加密的特殊的同态特性，使得它具有一定的应用价值，所以研究人员逐渐对全同态加密的应用进行研究说明[41~46]。本文主要研究基于 RLWE 问题的全同态加密算法，将该技术引入到电子投票中，保证电子投票的匿名、安全高效性。

## 1.3 论文的主要工作

电子投票设计的基本思想主要是以密码学原理为基础，利用计算机和网络通信技术来实现投票功能。要使电子投票可以安全可靠地运行，除了要保障计算机和网络功能能够正常运行之外，最核心的是，如何利用密码学技术设计出安全的电子投票方案。随着全同态加密理论的逐渐完善，利用全同态加密的同态特性对电子投票方案进行改进，成为电子投票发展的方向。本文的主要内容就是通过对实际电子投票功能需求的分析，依据全同态加密的原理，结合 RSA 数字签名技术，设计一种匿名安全的电子投票方案。本文的主要工作如下：

① 分析了电子投票方案和全同态加密的国内外研究现状，对当前国内外基于同态加密的电子投票方案进行了总结。

② 通过对电子投票的特性需求进行分析，确定了方案的设计目标，引入全同态加密技术保证投票的匿名性，结合 RSA 数字签名技术，明确了电子投票的总体方案架构。方案主要包括投票者、认证中心、计票中心和公告板四个部分。其中，公告板是各个实体交互信息的媒介。

③ 通过对全同态加密的构造方法、性能和基础应用分析，对比常用全同态加密的安全性和运行效率，得出基于 RLWE 问题的全同态加密能够有效地满足电子投票的安全性。

1) 根据全同态加密的定义和原理以及所用到的关键技术，构造基于 RLWE 问题的全同态加密方案；

2) 在同态加密软件库 HElib 库基础上，对基于 RLWE 问题的全同态加密方案进行验证。实验结果表明，通过选择合理的安全参数和电路深度能够达到安全性和

效率的折中；

3) 对比常见的全同态加密方案，根据实际的电子投票情况，确定将基于 RLWE 问题的全同态加密方案应用到电子投票方案中，能够保证电子投票的匿名性。

④ 课题组将方案在系统上进行验证，分别对注册、投票和验票等基本功能进行测试，同时对系统的性能进行了测试，经验证设计的电子投票方案达到了预期目标。

## 1.4 论文的结构安排

本文主要包括六个章节，下面对各个章节的内容进行总结：

第一章：绪论。介绍了电子投票方案的研究背景以及现实意义，综述了电子投票方案和全同态加密技术的国内外研究状况以及发展过程，并且指出了文章的主要工作和章节安排。

第二章：密码学相关理论知识。本章介绍了文中在设计电子投票方案时所要运用到的密码学和数学理论知识，包括 Hash 函数、同态加密算法以及同态性证明等。

第三章：电子投票方案的总体设计。本章对电子投票方案的特性需求进行分析，给出电子投票方案的一般模型，对典型的电子投票方案进行分析其优缺点。最后，完成了电子投票方案的总体架构设计。

第四章：基于 RLWE 困难问题的全同态加密方案。本章分析全同态加密方案的原理、构造方法以及所用到的关键技术，构造一种基于 RLWE 困难问题的全同态加密方案（BGV 方案）。同时对方案进行了实验验证，对 BGV 方案的安全性和效率进行研究。

第五章：基于 RLWE 问题全同态加密的电子投票方案设计。结合电子投票的发展与全同态加密的性能，提出基于 RLWE 问题的全同态加密的电子投票方案，详细阐述了方案执行的具体流程。最后对电子投票系统进行了实验测试分析。

第六章：总结。对文章的工作进行全面的总结，同时指出下一步还需要改进的工作。

# 2 密码学相关理论知识

电子投票方案的安全性涉及到多种密码学技术，如同态加密、RSA 数字签名等，本章将介绍论文研究内容所需要的数学和密码学知识。

## 2.1 Hash 函数

Hash，又称作做“散列”或者“哈希”，它的主要思想是：把任意长度的输入消息，通过 Hash 函数转换成长度固定的输出数据，该输出称为散列值。一般通过压缩映射的方法来实现此转换。转换的结果表明，输出散列值的大小远远小于输入消息的大小，不同的输入消息有可能会散列成相同的输出值，但是不可能依据散列值来唯一的确定输入消息。简而言之，Hash 函数是一种将任意长度的消息压缩到固定长度的信息摘要的函数。

密码学中，Hash 函数$h(x)$必须满足下列特性：

① 压缩：对于任意大小的输入$x$，输出$y = h(x)$比$x$的长度小很多，并且输出的 $y$ 是固定长度。

② 效率：对任意给定的消息$m$，$h(m)$要满足方便计算、实际可行等特点。

③ 单向性：对任意给定的值散列值$y$，不能够找出$x$，使得$x = h(y)$成立；即求解 Hash 函数的逆运算很困难。

④ 抗弱碰撞性：根据任意给定的消息及其散列值，不能够找出另一个能映射出该散列值的消息。

⑤ 抗强碰撞性：对于任意两个不同的消息$x_1$，$x_2$，它们的散列值$h(x_1)$，$h(x_2)$必定不相等。

Hash 函数的单向运算和输出数据长度固定的特征使得它可以生成消息或者数据块的“数据指纹”（也称作消息摘要），可以被广泛应用于数据完整和数据签名等领域，在现代信息安全领域和密码学中起着重要作用。常用的 Hash 算法有很多种，比如 MD4、MD5 和 SHA-1 等。其中 MD 是 Message Digest 的缩写，MD5 是对 MD4 的改进版本，输入信息是以 512bit 分组处理，其输出是 4 个 32bit 的级联，SHA-1 是效仿 MD4 算法进行设计的，该算法对长度小于$2^{64}$bit 的输入信息，产生长度为 160bit 的散列值。

文中在数字签名的过程中，选用 MD5 算法生成散列值。MD5 算法的主要思想是：将输入的字符串分组，每组为 512bit 的消息块，且每一组又被划分为 16 个 32 位子分组，经过一系列的处理后，输出 128bit 的散列值，最后将 128bit 散列值用十六进制表示便是 32 字符的 MD5 码。

## 2.2 同态加密

### 2.2.1 同态加密概念

传统的密码体制最常见的方式是对称密码体制，也称为私钥密码体制。它是一种最快速、最简单的加密方式，采用同一个密钥对数据进行加密和解密操作，需要通信的双方共同选择和保存密钥。采用对称密码算法对信息进行处理的过程如图 2.1 所示。

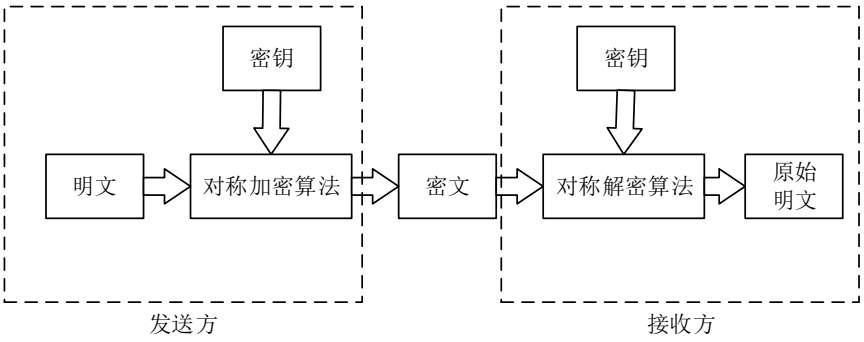


图 2.1 对称加密算法的信息处理过程

Fig.2.1 Information processing process of symmetric encryption algorithm

如果使用对称密码体制来满足 n 个用户相互通信的要求，则每个用户要和其他（n-1）个用户建立用于加解密的密钥和传输数据的秘密通道。假如有一个用户改变密钥的情况下，那么必须重新分配 n-1 个新的密钥给其他用户。因此，对称密码体制的密钥管理比较繁琐，不适合多用户之间相互通信。

1976 年，Diffie W, Hellman M E 提出了公钥密码体制的思想。通常情况下，一个完整的公钥密码体制主要由五元组{明文，密钥，加密算法，密文，解密算法}组成。公钥密码体制是非对称算法，即密钥分为公钥和私钥。其中，公钥是公开的，用于加密明文；私钥由用户秘密保存，用于解密密文。采用非对称密码算法对信息进行处理的过程如图 2.2 所示。

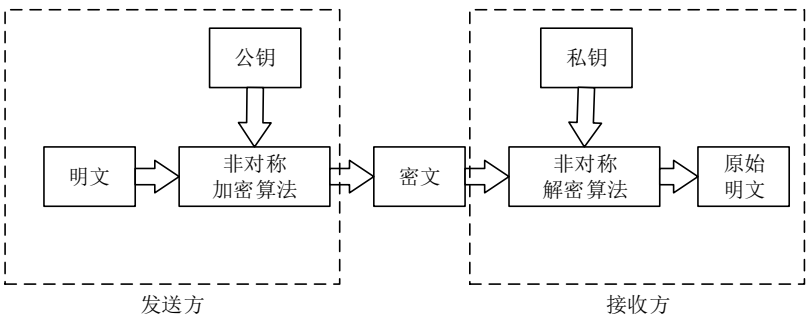


图 2.2 非对称加密算法的信息处理过程

Fig.2.2 Information processing process of asymmetric encryption algorithm

1978 年，Ron Rivest 等人首次提出了同态加密（Homomorphic Encryption）的概念。同态加密算法颠覆了传统形式下的加密模式。

传统的加密算法关注的是数据存储的安全性，它不允许用户对密文进行任何计算，否则密文解密不正确。而同态加密算法关注的是数据处理过程的安全问题，它允许第三方对密文进行特定的运算，在处理密文数据的过程中不会泄露原始的数据内容；并且用户用私钥对处理过的数据解密，得到的是处理后的数据结果。同态加密算法的加解密示意图如图 2.3 所示。

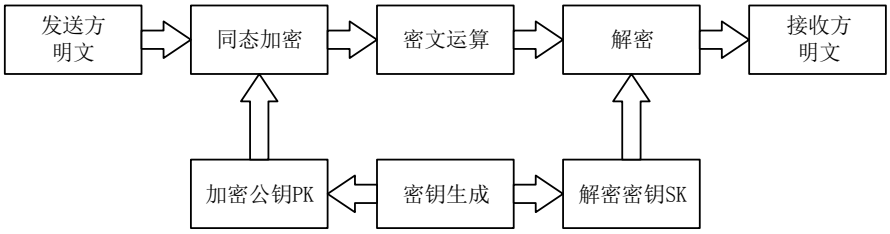


图 2.3 同态加密的信息处理过程

Fig.2.3 Information processing process of homomorphic encryption

### 2.2.2 同态加密特性

如果加密算法$Enc()$是同态，M 是明文数据集合，C 是密文数据集合；那么对于任意的$\forall m_1$，$m_2 \in M$，$Enc()$满足：

$$Enc(m_1) \odot Enc(m_2) = Enc(m_1 \odot m_2) \tag{2.1}$$

① 乘法同态

如果 $Enc(m_1)$，$Enc(m_2)$是明文$m_1$，$m_2$的密文，任何人都可以得到$m_1 \times m_2$的密文$Enc(m_1 \times m_2)$，即可以找到这样的运算符$\otimes$使得对于任意的明文信息$m_1$和$m_2$，满足：

$$Enc(m_1 \times m_2) = Enc(m_1) \otimes Enc(m_2) \tag{2.2}$$

② 加法同态

如果 $Enc(m_1)$，$Enc(m_2)$是明文$m_1$，$m_2$的密文，任何人都可以得到$m_1 + m_2$的密文$Enc(m_1 + m_2)$，即可以找到这样的运算符$\oplus$使得对于任意的明文信息$m_1$和$m_2$ 有，

$$Enc(m_1 + m_2) = Enc(m_1) \oplus Enc(m_2) \tag{2.3}$$

③ 混合乘法同态

如果$Enc(m_1)$是明文$m_1$的密文以及数据$m_2$，存在有效算法，使得$Enc(m_1 \times m_2) = Enc(m_1)m_2$，那么该算法具有混合乘法同态特性。

假如$Enc()$同时满足式（2.2）和式（2.3），则称之为代数同态，否则称之为偏同态。

## 2.3 RSA

在公钥密码加密体制中，密钥成对出现，通常情况下公钥是公开的，用于加密数据；而私钥用于解密数据则由用户自己保管，大大降低了密钥泄露的危险性。常用的公钥密码算法有 RSA 和 ElGamal 等。

### 2.3.1 RSA 加密算法

RSA 算法的实现过程为：

① 密钥生成

1) 随机选取两个大素数 p，q，|p| ≈ |q|；

2) 计算出$n = p \cdot q$；欧拉函数$\varphi(n) = (p-1)(q-1)$；

3) 任意选择一个整数 e，满足$1 < e < \varphi(n)$，$\gcd(e, \varphi(n)) = 1$；

4) 计算 d，$e \cdot d = 1 \ mod \ \varphi(n)$；

5) 公钥pk是(n,e)，私钥sk是 d。

② 加密算法

将明文分块，各个子块在模 n 下可以通过式（2.4）得到密文数据。

$$c = m^e \ mod \ n \tag{2.4}$$

③ 解密算法

解密密文 $c$，通过式（2.5）得到明文。

$$m = c^e \ mod \ n \tag{2.5}$$

### 2.3.2 RSA 的同态特性

假设公钥为(n, e)，私钥为 d。$m_1$，$m_2 \in M$，$c_1 = Enc(m_1) = m_1^e \ mod \ n$，$c_2 = Enc(m_2) = m_2^e \ mod \ n$，通过式（2.6）对$c_1$和$c_2$进行乘法运算，验证 RSA 算法是否具有乘法同态特性。

$$\begin{aligned} c_1 + c_2 &= Enc(m_1) + Enc(m_2) \\ &= (m_1^e \ mod \ n) + (m_2^e \ mod \ n) \\ &\neq (m_1 + m_2)^e \ mod \ n \\ &= Enc(m_1 + m_2) \end{aligned} \tag{2.6}$$

通过对$c_1$和$c_2$进行加法运算，验证 RSA 算法是否具有加法同态特性。结果如式（2.7）所示。

$$\begin{aligned} c_1 \times c_2 &= Enc(m_1) \times Enc(m_2) \\ &= (m_1^e \ mod \ n) \times (m_2^e \ mod \ n) \\ &= (m_1 \times m_2)^e \ mod \ n \\ &= Enc(m_1 \times m_2) \end{aligned} \tag{2.7}$$

由式（2.6）和式（2.7）的证明结果可知，RSA 算法具有乘法同态性，但是它不具有加法同态性。

### 2.3.3 基于 RSA 加密算法的数字签名系统

① 数字签名的含义

对于重要文件的传输，传统的方法是发送者在文件上手写签名来防止文件被伪造和篡改，因为计算机系统中无法使用手写签名，取而代之的是数字签名体制。数字签名（Digital Signature），主要建立在公钥加密体制基础上，附加在文件中的一组特定的符号或代码。它是利用数学方法和密码算法对该文件进行关键信息提取并进行加密而形成的，用于标识文件发送者的身份，并能被接收者用来验证该文件在传输过程中是否被篡改或伪造。

一个完整的数字签名系统主要实现以下功能：

1) 确认消息是由签名者发送的。

2) 确认消息从签名到结束，未被修改过。

3) 签名者不能采取任何方法否认信息是由自己发送的。

通常，只有消息的发送者能够产生其他人无法伪造的数字串，同时这段数字串也是对消息的发送者发送真实信息的一个有效证明。完整的数字签名有两种运算：签名和验证。其中签名是个加密的过程，而验证是个解密的过程。

② 基于 RSA 算法的数字签名系统

系统初始化生成所需的所有参数，RSA 公钥 pk=(n,e)，私钥 sk=d；Hash 函数选用 MD5 算法。RSA 签名的整个过程如图 2.4 所示。

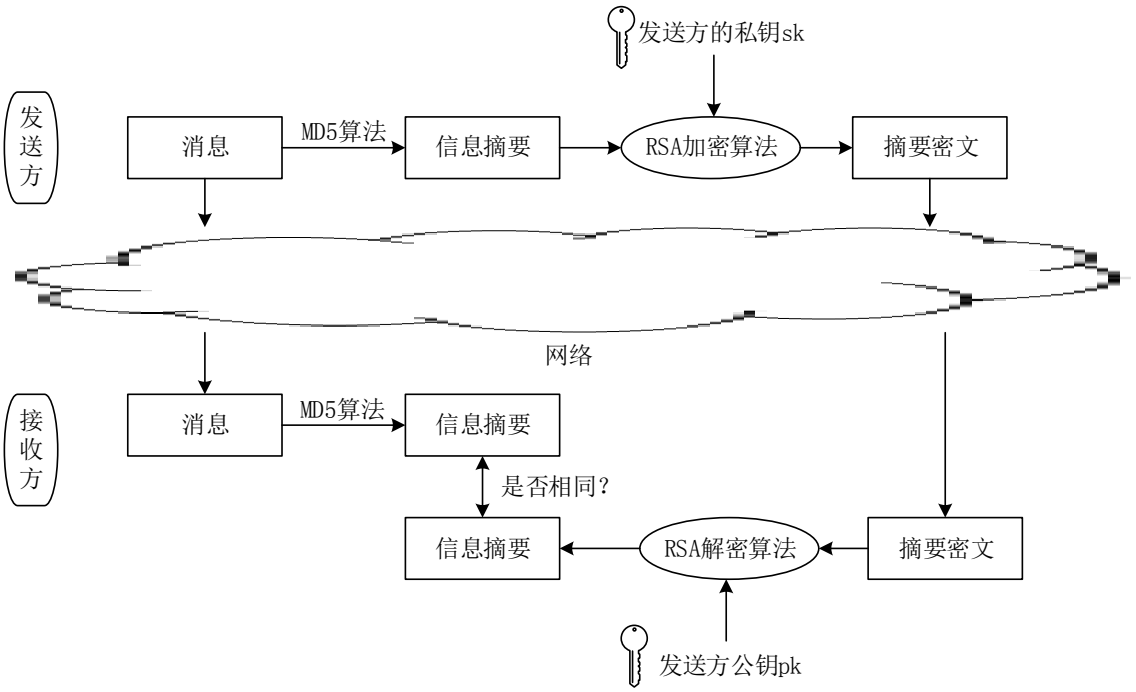


图 2.4 基于 RSA 算法的数字签名过程

Fig.2.4 Digital signature process based on RSA

RSA 签名系统的具体工作流程如下：

1) 发送方采用 MD5 算法从信息 m 中生成一个 128 位的散列值 H；

2) 发送方用私钥 *sk* 通过 RSA 加密算法对散列值 H 进行加密 *SIG*，生成一个摘要密文，通过式（2.8）发送方的数字签名。

$$SIG = H^d \ mod \ n \tag{2.8}$$

3) 将数字签名 *SIG* 作为信息 m 的附件，与信息 m 一起发送给接收方；

4) 接收方首先从原始信息 m 中，采用相同的 MD5 算法计算出 128 位的散列值$H'$；然后利用发送方的公钥 pk 采用 RSA 解密算法，对数字签名 SIG 进行解密得到明文，如式（2.9）所示。$SIG = H^d \ mod \ n$；$e \cdot d = 1 \ mod \ \varphi(n)$。

$$\begin{aligned} & SIG^e \ mod \ n = H^{ed} \ mod \ n \\ & = H^{k*(\varphi(n))+1} \ mod \ n \\ & = H * H^{k*(\varphi(n))} \ mod \\ & = H * (H^{(\varphi(n))})^k \ mod \ n \\ & = H' \end{aligned} \tag{2.9}$$

5) 最后，接收方验证两个散列值$H$和$H'$是否相等，如果相等，那么接收方确定消息 m 是由发送方签名的，否则，签名无效。

## 2.4 ElGamal

### 2.4.1 ElGamal 加密算法

① 密钥生成

1) 随机选择素数 p；

2) G 是$\mathbb{Z}_p$中的乘法群$\mathbb{Z}_p^*$的一个生成元；

3) 选择随机数α，$1 \le \alpha \le p-2$，计算$h = g^{\alpha}$；

4) 公钥是(p,g,h)，私钥是α。

② 加密算法

对于待加密的数据信息 m，随机选择一个数 k，$0 \le k \le p-2$，则密文为：

$$c = (x, y) = (g^k \ mod \ p, mh^k \ mod \ p) \tag{2.10}$$

其中$x$，$y$构成加密结果。

③ 解密算法

解密密文 c，得到明文：

$$m = \frac{y}{x^{\alpha}} \ mod \ p \tag{2.11}$$

ElGamal 算法可以在任意循环群中实现，其安全强度依赖于循环群上离散对数假设的强度。

### 2.4.2 ElGamal 的同态性

假设公钥是(G,p,g,y)，G 是群，$p$ 是群的界，g 是生成元，$y = \mathrm{g}^{z}\ mod\ p$，密钥 z，对于任意的明文信息$m_1$，$m_2 \in M$，$x_1$，$x_2$是随机数，$m_1$和$m_2$的密文分别为$c_1 = Enc_{x_1}(m_1) = (g^{x_1}\ \mathrm{mod\ p}，\ m_1 y^{x_1} \mathrm{mod\ p})$，$c_2 = Enc_{x_2}(m_2) = (g^{x_2}\ \mathrm{mod\ p}，\ m_2 y^{x_2} \mathrm{mod\ p})$，通过式（2.12）对$c_1$和$c_2$进行乘法运算，验证 ElGamal 算法是否具有加法同态特性。

$$\begin{aligned} & c_1 \times c_2 = Enc_{x_1}(m_1) \times Enc_{x_2}(m_2) \\ & = \left(g^{x_1}\ mod\ p，\ m_1 y^{x_1} mod\ p\right) \times \left(g^{x_2}\ mod\ p，\ m_2 y^{x_2} mod\ p\right) \\ & = \left(g^{x_1} g^{x_2}\ mod\ p，\ m_1 m_2 y^{x_1} y^{x_2} mod\ p\right) \\ & = \left(g^{x_1+x_2}\ mod\ p，\ y^{x_1+x_2} m_1 m_2 mod\ p\right) \\ & = Enc_{x_1 x_2}(m_1 \times m_2) \end{aligned} \tag{2.12}$$

通过对$c_1$和$c_2$进行加法运算，验证 ElGamal 算法是否具有加法同态性，验证过程如式（2.13）所示。

$$\begin{aligned} & c_1 + c_2 = Enc_{x_1}(m_1) + Enc_{x_2}(m_2) \\ & = \left(g^{x_1}\ mod\ p，\ m_1 y^{x_1} mod\ p\right) + \left(g^{x_2}\ mod\ p，\ m_2 y^{x_2} mod\ p\right) \\ & = \left((g^{x_1} + g^{x_2})\ mod\ p，\ (m_1 y^{x_1} + m_2 y^{x_2}) mod\ p\right) \\ & \neq \left(g^{x_1+x_2}\ mod\ p，\ y^{x_1+x_2}(m_1 + m_2) mod\ p\right) \\ & = Enc_{x_1+x_2}(m_1 \times m_2) \end{aligned} \tag{2.13}$$

由式（2.12）和式（2.13）可知，ELGamal 加密算法具有乘法同态性，而不具有加法同态性。

## 2.5 本章小结

本章介绍了电子投票所用到的 Hash 函数；分析了同态加密体制的基本原理，并给出了同态加法和同态乘法的定义；说明了 ElGamal 和 RSA 算法的基本步骤及其同态特性证明；最后阐述了基于 RSA 的数字签名系统，分析系统的功能和它的实现过程。

# 3 电子投票方案的总体设计

随着投票应用的日益广泛，电子投票的安全性受到了研究人员的重点关注。近年来现代密码学技术尤其是全同态加密取得了突破性进展，它能够保证选票的秘密性、完整性等问题。本章通过对电子投票进行需求分析，提出方案的设计目标，在一般电子投票模型基础上，引入全同态加密和数字签名技术，完成了电子投票的总体方案设计。

## 3.1 电子投票方案的特性需求分析

在方案的设计过程中，需求分析是一个关键的步骤与环节。在电子投票方案的设计过程中，首先要明确方案应满足哪些特性，通过对实际投票的应用情况分析进一步明确方案的具体投票流程，最终确定总体方案。

一般情况下，一个良好的电子投票方案在安全性与实用性方面，需要满足一些基本的规范和要求(即基本属性)；同时为了保证电子投票方案的安全性和高效性，还应满足一些扩展特性[47]。

① 基本属性

1) 匿名性(Anonymity)。一方面，投票者的选票内容在投票、传输、接收、收集和统计选票过程中必须是匿名的，不能被其他任何人知道。另一方面，任何个人或者组织都无法将选票信息与投票者的身份联系起来。

2) 完全性(Completeness)。计票的完全性，所有有效的选票都必须被正确计入最终结果。

3) 正确性(Soundness)。计票结果的正确性，任何无效的选票，都不能计入最终结果。

4) 不可重用性(Unreusability)。选票的唯一性，一个合法的投票者只能获得一张合法的选票，并且该选票只能进行一次投票操作，不能重复投票。

5) 公平性(Fairness)。在公布最终选举结果之前，任何人不能获知关于选票的任何信息。

6) 合法性(Eligibility)。方案要保证投票者的合法性，只有认证通过的合法投票者才能够参加投票活动。

7) 确定性(Invariableness)。结果的确定性要求最终计票的结果一定的，也就是说，不管对所有选票进行多少次重复计算，最终投票结果都是相同的。

② 扩展特性

1) 可验证性(Verifiability)。包括狭义可验证性和广义可验证性，狭义可验证，

亦即个人可验证性（Individual verifiability），是指投票者能够验证其选票是否被正确计票。广义可验证性，即是普遍可验证(Universal verifiability)，是指任何感兴趣的组织和监督者以及个人都可以验证投票结果的正确性。

2) 无收据性(Receipt-freeness)。投票者不能够得到或者构造一个收据来证明自己投票的内容。它是为了防止不合法的有心人士贿赂活动的操纵者而提出来的，主要考虑的是投票者主观上想卖票的情况。

3) 抗威胁性(Coercion-resistance)。在投票过程中，投票者不受任何人威胁，按照自己的想法进行投票，即是威胁者不可以通过各种手段获得投票者的投票数据内容。一般情况下，能够满足抗威胁性的电子投票方案同时也具有无收据性。

对电子投票方案的设计而言，无收据性和抗胁迫性比投票的匿名性更难实现，满足无收据性的方案一定满足匿名性，反之则不然。

## 3.2 一般电子投票方案及缺陷分析

在电子投票模型中，一般主要涉及到的参与实体有投票者、注册机构、计票机构、权威机构即活动的发起者。当然根据实际情况也可能有另外的机构，比如监察机构等。在电子投票过程中，各个投票参与实体之间常常涉及到数据的传输，数据传输时需要安全可靠的传输媒介，常用的通信媒介有：

① 公告板（Bulletin Board）。每个参加投票的参与者都可以在公告板上发布信息。任何人都可以访问公告板。任何人都可以在公告板上自己所属的区域进行写操作，但是不能删除和修改公告板上的信息。

② 不可泄露通道（Untappable Channel）。不可泄露通道是通讯双方之间的一个秘密通道。除了通信双方，没有任何人知道通道中传输的信息内容。同时通讯参加者也不能向任何人证明自己所发送的内容。经过不可泄露通道进行信息的传输是安全可靠的。

③ 不可追踪的匿名通道或匿名通道（Untraceable anonymous channel or anonymous channel）。通过这个通道传送信息可以保证信息发送者的匿名性。信息的接收者不知道信息发送者的身份。

④ 不可泄漏的匿名通道（Untappable anonymous channel）。它既可以保证发送者的匿名性，又可以保证传输的安全。发送者和接收者不能重演发送或接收的内容。没有人能监听传输的信息。

在开始进行投票之前，投票的发起者需要对整个投票活动做一个完整的规划，事先做好前期的准备工作，方便投票者参与投票活动。需要完成以下准备工作：

① 确定候选人和投票者。在一次投票活动中，活动发起者公布候选人的相关信息，并且说明投票形式，常用的票的类型比如 1-out-of-L voting(从 L 个候选者中

选择一个)或者是 K-out-of-L voting(从 L 个候选人中选择 K 个)。根据投票活动的形式以及投票活动的范围确定哪些公民具有投票的资格，称为合法投票者。

② 给出投票者的身份凭证。一般情况下，权威机构即给合法投票者分配唯一的身份凭证（它主要是用来表明投票者的身份，证明投票者有投票的权利），比如投票编号、身份 ID 等。发起者通过安全可靠的通信渠道递交到合法者的手中。

③ 定义选票数据的形式。传统的纸质投票，大多都是将候选人的信息罗列在纸上，以便投票者选择。在电子投票方案中，投票发起者根据方案所采用的加密算法来定义选票的形式。

④ 建立投票中心。传统的投票活动中，投票地点指定在某一个特定位置，在权威人士现场控制下，投票者进行投票。投票中心可能以街道或小区为中心，进行阶段性投票。在阶段性的投票结果出来之后，每个中心将阶段性的结果报给更高级的区域中心，以此递进，直到最终投票活动的结束。

通常情况下，在完成准备工作之后，投票活动还要经过注册、投票、计票和验证四个步骤，具体的过程如图 3.1 所示。

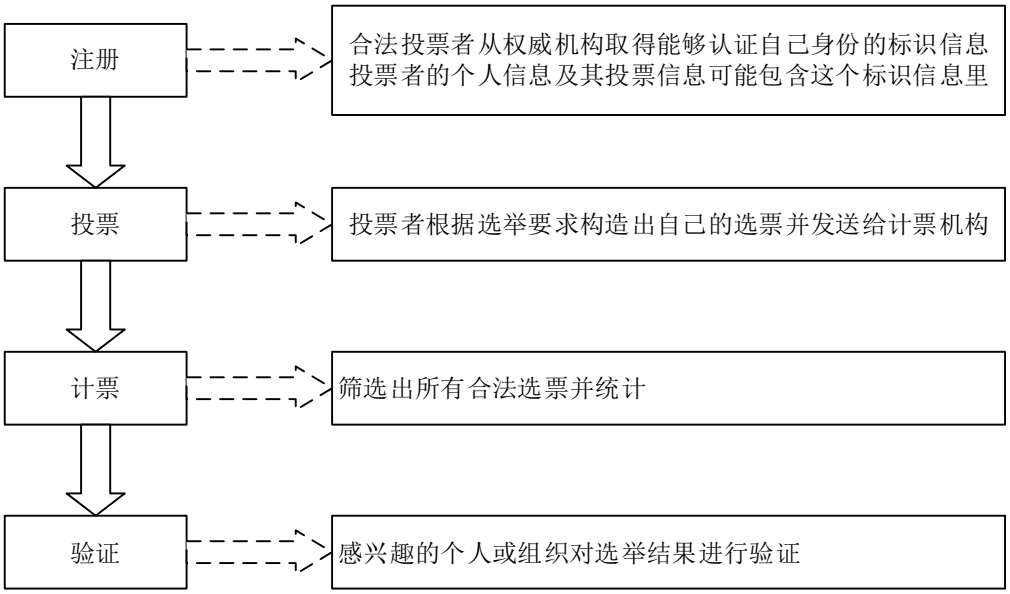


图 3.1 电子投票的过程

Fig.3.1 Process of electronic voting

① 注册阶段。投票者根据权威机构分发的身份凭证，只有通过认证的投票者才能获得投票资格。

② 投票阶段。当合法投票者验证自己的身份之后，依据规定的候选人信息，按照自己的意愿选择合适的候选人，生成选票并对其进行加密保护，防止选票信息泄露。

③ 计票阶段。在计票阶段，计票中心接收所有合法投票者的选票，当投票结束时，对所有的选票进行汇总。

④ 验票阶段。投票者根据自己的身份凭证验证自己的选票是否被正确计入；感兴趣的第三方个人或组织验证投票、计票过程是否正确。

现实生活中的大型投票活动比如国家选举，其过程一般非常复杂。本节所描述的仅仅是一般的电子投票模型，对于有特殊要求的投票活动，需要加入相关的技术进行扩展，使得投票方案能够满足具体的场景应用需求。

简而言之，设计一个电子投票方案主要的工作就是要保证它的公平性。对于投票者而言，投票者的选票要保证秘密性，并且选票应被正确地计入最终结果中。同时要投票活动的组织者是可信的。在电子投票中需要用到各种密码学技术，应用不同的密码学技术可以得到不同的结果，但最终的目的都是要实现 3.1 节所述的特性。

在电子投票方案没有引入同态加密技术之前，采用的是不支持对密文进行处理的传统加密算法。这种算法在处理选票时，存在一定的漏洞，如图 3.2 所示。计票中心计票时，首先对选票的密文进行解密得到明文，然后对明文进行相加。这种处理方式，恶意破坏者可能会对选票的明文进行篡改，导致最终计票结果不正确。

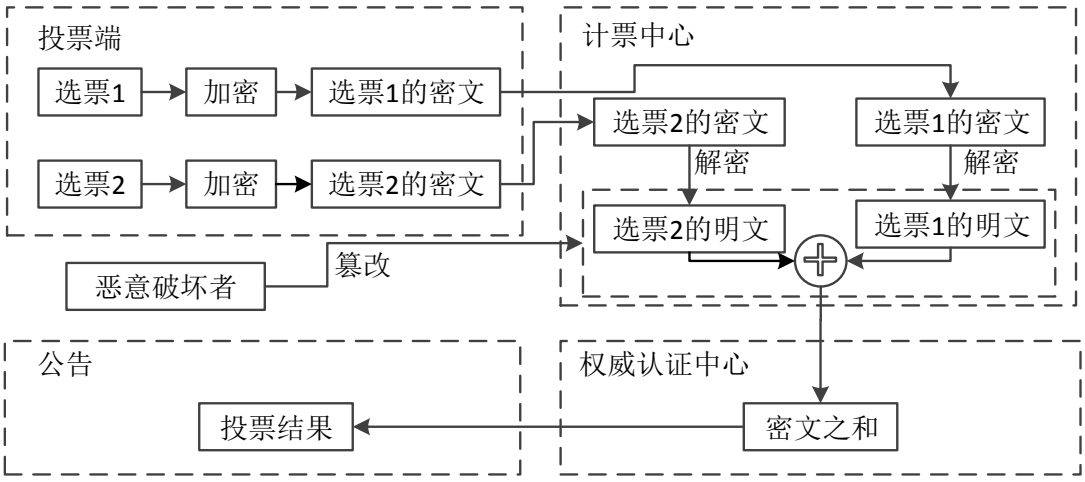


图 3.2 一般电子投票的计票漏洞示意图

Fig.3.2 Sketch map of the loopholes in general electronic voting

近年来，电子投票的研究主要以同态加密算法为基础。运用同态加密技术对投票者的选票进行加密，最后对加密的选票数据进行计算，得到最终的投票结果。常见的有基于 ElGamal 算法的电子投票方案，比如 CGS 和 KO 方案等。表 3.1 为典型电子投票方案的特性对比。

表 3.1 常见电子投票方案的对比

Table 3.1 Comparison of common e-voting schemes

| 方案 / 特性 | FOO[48] | CGS[49] | KO[50] | Moracles-Rocha[51] | 文献[12] |
|---|---|---|---|---|---|
| 秘密性 | Yes | Yes | Yes | No | Yes |
| 可验证性 | Yes | Yes | Yes | No | Yes |
| 合法性 | Yes | Yes | Yes | Yes | Yes |
| 确定性 | Yes | Yes | Yes | Yes | Yes |
| 公平性 | Yes | Yes | Yes | Yes | Yes |
| 完全性 | Yes | Yes | Yes | No | Yes |
| 不可重用性 | No | No | Yes | Yes | Yes |

其中 FOO、CGS、KO 和 Moracles-Rocha 方案，要求投票活动的发起者、计票者都可信的，而在现实的投票中，这些条件不能够得到确保。若有不诚实的投票者被威胁选取指定的候选人，那么选举结果便会失去参考价值。

文献[12]中，基于整数上的全同态加密方案应用到电子投票中，保证了整个投票方案的安全性。但是使用的是基于整数上的全同态加密该算法在实现上还不够完善，效率方面不能满足应用要求。

总的来说，当前大多电子投票方案主要存在的问题有：①大多数方案需要可信的第三方对选票进行统计。②以 1-out-of-L 投票模型为例，当前许多电子投票方案在选票密文的生成过程中，需要生成 L 个选票密文分别对应 L 个候选人。这就增加了方案的计算复杂度。③当前很多选票方案采用的是 ElGamal 和 RSA 密码算法对选票数据进行加密，这两种算法满足乘法同态特性，要想得到投票结果，需要做多次乘法运算，影响了计票的执行效率。

## 3.3 电子投票方案的总体框架

### 3.3.1 方案设计目标

目前，全同态加密方案的研究侧重于算法实现，这就为全同态加密的应用和推广奠定了基础。因此，高性能的全同态加密方案应用到电子投票中成为一种可能。本文在一般电子投票模型的基础上，通过对电子投票的特性需求进行分析，设计一个基于全同态加密的电子投票方案，实现以下几个目标。

① 匿名性。在整个投票活动要确保选票的匿名性。

② 安全性。第一，方案必须要有严格的身份验证算法。第二，投票方案要使用高强度的加密算法。第三，投票者和计票中心必须能够对选票或者是计票数据进

行验证。

③ 可验证性。在保证匿名性的前提下，投票者可以验证自己的选票是否被计入。

④ 高效性。方案使用的加密算法以及签名技术要有较高的效率，以此来保证电子投票方案的效率，只有有效率的方案才会有实现的价值。

⑤ 自计票性。只要有计算能力的第三方都可以完成计票操作，不需要可靠人员监督。

### 3.3.2 方案总体结构

同态加密技术在电子投票中起着重要的作用，全同态加密技术的突破发展，为电子投票的改进提供了可能。本文将全同态加密技术引入到电子投票方案中，对选票数据进行加密，保证其安全性；再用数字签名技术对投票者以及选票数据进行签名，保证投票者的可信度、选票数据的不可被篡改；设计了基于全同态加密的电子投票方案。该方案包括投票者、权威认证中心、计票中心和公告牌四个参与实体。

本方案的设计思想：每个投票者根据自己的意愿选择候选人生成选票，对产生的原始选票进行全同态加密、数字签名等一系列操作后发送给计票中心；计票中心对有效的选票密文进行同态加法运算，并把密文之和分阶段发送给权威认证中心；最终权威认证中心对所有选票的密文之和解密，得到明文进而找到投票的获胜者。总体方案框图如图 3.3 所示。

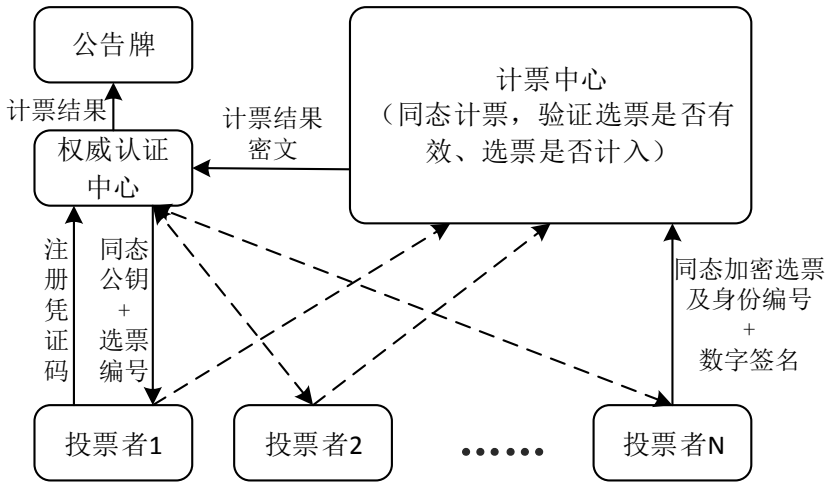


图 3.3 总体方案结构图

Fig.3.3 Structure diagram of overall scheme

① 投票者首先向权威认证中心登记注册，验证身份合格后获得投票权利。

② 投票者投票时，根据自己的意向选择候选人生成原始选票，然后对选票进行同态加密、数字签名等一系列处理之后形成最终选票，交给计票中心，完成投票。

③ 计票中心计票时，对投票者原始选票的密文进行统票获得选票的密文之和，交由权威认证中心对其进行解密获得最终的选票结果，并发布在公告板上。在这个过程中，计票中心完全不知道投票者的选票内容，保证了选票的匿名性。

各个参与实体的主要功能如表 3.2 所示。

表 3.2 方案参与者以及完成的主要功能

Table 3.2 Project participants and their main functions

| 参与实体 | 主要功能 |
| --- | --- |
| 权威认证中心<br>(Authentication Center，AC) | 规定投票模型；获得候选人信息；<br>获取预定合法投票者身份信息；<br>生成投票者身份凭证；<br>管理用于加密和签名的密钥；<br>公布最终计票结果。 |
| 投票者（Voter） | 注册验证身份；投票；<br>查询投票结果；验证投票结果。 |
| 计票中心<br>(Counting Center，CC) | 验证投票者身份；<br>接收并统计合法投票者的选票；<br>向权威中心提交选票结果。 |
| 公告牌<br>(Bulletin Board，BB) | 显示候选人信息；<br>显示当前已投票人数；<br>显示最终投票结果。 |

通过对电子投票的特性需求进行分析，根据方案的设计目标。方案预计采用全同态加密算法对投票者的选票内容进行加密，在没有同态私钥的情况下，选票信息在传输、计算与存储过程中不会被解密，因而可保证选票数据的匿名性。因此，选取一个高效的全同态加密方案是设计电子投票方案的关键。

## 3.4 本章小结

本章通过对电子投票的特性需求进行分析，提出方案的设计目标。针对投票的安全性和效率问题，在一般电子投票模型的基础之上，结合全同态加密和数字签名技术，设计了一种基于全同态加密的电子投票方案，设计了方案的总体结构。

# 4 基于 RLWE 问题的全同态加密方案

全同态加密是电子投票方案设计的核心部分。本章从全同态加密的定义和关键技术出发，研究了全同态加密的构造方法并给出基于 RLWE 问题的全同态加密方案。通过解析同态软件算法库 HElib 库，对基于 RLWE 问题的全同态加密进行实现，并对方案的性能进行分析。

## 4.1 全同态加密

在第二章中，论文给出了常用的同态加密算法以及同态特性的证明，其中典型的 RSA 和 ElGamal 公钥密码体制具有乘法同态性。全同态加密（Fully Homomorphic Encryption，FHE）算法是一类同时具有加法同态和乘法同态特性的加密算法，其主要特性是能够对密文进行任意功能的运算，运算解密之后的结果是相应于对明文做同样运算的结果。

与传统的加密算法相比，FHE 加密后的密文仍然具有较好的代数性质，密文数据无需解密即可直接参与运算。由于这一良好性质，用户要想在不泄露个人信息的情况下对数据进行处理，可以把密文存储于不可信的第三方或委托第三方对数据进行操作，得到密文的处理结果后第三方以密文的形式将处理结果返回给用户，用户收到处理结果后对其进行同态解密，便可获得已经处理好的明文数据，整个处理过程不泄露信息内容。基于全同态加密算法的数据处理过程如图 4.1 所示。

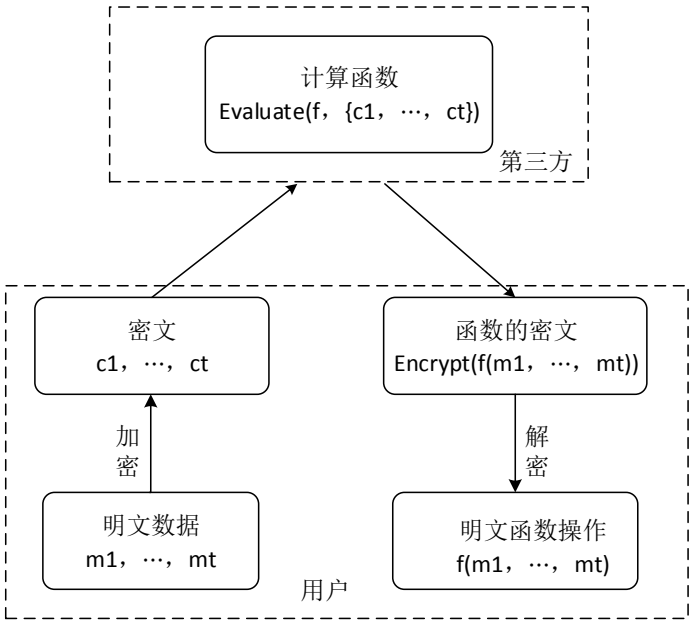


图 4.1 基于全同态加密的数据处理过程

Fig.4.1 Data processing based on fully homomorphic encryption

由于全同态加密算法的同态运算特性，使得它广泛应用于安全多方计算、云计算、图像水印等领域。对电子投票方案来说，可以从根本上解决方案的匿名性和计票时的安全性问题。

### 4.1.1 全同态加密的定义

用 E 表示一个加密方案，同时要求 E 满足以下条件：对用 E 加密的密文做任何运算之后将其进行解密操作，所得到的数据与对明文做相同的运算得到结果是一致的，对于满足上面条件的全部 E 将其称为全同态加密方案。满足条件：

$$Dec[f(c_1, c_2, \cdots, c_t)] = f\big(Dec(c_1), Dec(c_2), \cdots, Dec(c_t)\big) = f(m_1, m_2, \cdots, m_t) \quad (4.1)$$

其中$Dec()$为解密算法，$c_i$是$m_i$加密之后的密文。

### 4.1.2 全同态加密的原理

一般的加密方案主要是由 KeyGen 算法（密钥生成），Encrypt 算法（加密），Decrypt 算法（解密）三个部分构成。但是全同态加密方案的构造还需要加入 Evaluate 算法，这个算法主要是对密文进行操作，它是全同态加密方案的关键算法。

首先定义一个全同态加密方案$FHE = \{KeyGen, Encrypt, Decrypt, Evalute\}$，然后对其各个算法进行详细讲解。

① 密钥生成算法$KeyGen()$

在执行该算法之前，确定方案的安全参数λ，根据此算法产生用于加密明文数据所用的公钥 *pk* 和用于解密密文数据的私钥 *sk*，同时还有用于密文运算的公钥 Evk。Evk 主要是在执行密文计算时用到，而且 Evk 的形式与构造的全同态方案直接相关。

1) 如果使用 Bootstrapping 技术构造全同态加密方案，即每次对密文操作之后要用同态解密减少密文的噪声大小，这时密文公钥 Evk 就是对私钥的每一位加密后生成的密文。密文运算公钥 Evk 中每个公钥的大小就是私钥使用加密函数 Encrypt()加密后产生密文的大小。

2) 如果使用密钥转换技术和模交换技术得到全同态加密方案，例如 BGV 方案。在这种情况下，Evk 包含 L-1 个矩阵，称为密钥转换矩阵(KeySwitching Matrix)，该矩阵主要用于密钥转换，其中 L 是方案中电路的深度。每次密文计算后，需要用 Evk 将维数增加的密文向量转换成初始维数的密文向量。

3) 还有一种情况是不需要密文计算公钥 Evk，在 Crypto13 会议的论文 GSW13 中，Gentry 使用的密文是矩阵形式，因此密文进行相乘或相加运算不会产生密文维数的改变，所以在密文运算过程中也就不需要密文计算公钥 Evk。

② 加密算法$Encrypt()$

加密函数$Encrypt(pk，m)$，用公钥 *pk* 对明文数据 *m* 进行加密获得密文数据 *ctxt*(*Ciphertxt*)，一般称为新鲜密文，即是初始密文，没有对其进行任何计算操作。

③ *Evaluate* 算法

该算法通过函数$Evaluate(Evk, f, \{c_1, c_2, c_3, \cdots, c_t\})$来实现，第一个输入密文公钥 *Evk* 根据全同态加密方案的形式判定它的存在形式；第二个输入是函数$f$，即是 Evaluate()算法要执行的函数，理论上可以是任意函数，因为全同态加密的目标就是对密文能够进行任意计算；第三个输入是任意 t 个密文$\{c_1, c_2, \cdots, c_t\}$，其中$c_i \leftarrow Encrypt(pk, m_i)$，理论上可以是无穷多个密文。该函数的输出结果为处理后的密文数据 *C*。

④ 解密算法$Decrypt()$

解密函数为 Decrypt(sk，*C*)，采用同态私钥 *sk* 对密文数据 *C* 进行解密得到明文信息 $m$。这里解密算法不仅能对初始密文解密，同时还能够对进行代数运算后的密文解密，并且解密的结果与对应明文数据做相同运算的计算结果相等。

### 4.1.3 全同态加密的关键技术

在全同态加密方案的构造过程中，密文计算时产生的噪声对解密产生了很大的影响，如果密文噪声的大小大于密文空间，便不能得到正确的解密结果。假设两个密文噪声都为 *B*，那么两个密文进行加法后，密文噪声变为 2*B*；而进行乘法计算后，密文噪声增加到了$B^2$，同时也增大了密文的维数。为了解决这些问题，一方面利用模交换技术，将密文计算增加的噪声约减到原本的噪声大小；另一方面，采用密钥交换技术，把密文的维数缩减到原来的维数之后，再进行下一次的密文运算。

① 模交换技术

模交换技术的作用是减少密文中的噪声。假设$q \approx x^k$，有两个模$q$的密文，且每个密文噪声为$x$，两个密文相乘，那么密文噪声大小变为$x^2$，而经过四次乘法后噪声大小变为$x^{16}$，那么经过$log_2^k$层乘法后，密文噪声大小就会达到上限$x^k$，此时继续进行密文计算则可能导致解密不正确。

利用模交换技术可以解决噪声增大问题，提高密文乘法运算次数，即如果在每次密文相乘之后，密文噪声乘以$1/x$，则第一次密文相乘后，新密文的噪声就会从$x^2$缩减到$x$，而此时模缩减为$q/x$。以此类推，选择依次递减的模$\{q_i = q/x^i\}$，其中$i < k$，这样每次密文相乘后，噪声缩减到和初始密文一样的大小，增加了密文运算的次数。

② 密钥交换技术

密钥交换技术对基于 LWE(或 RLWE)[39]的全同态加密方案的发展有着至关重要的作用。基于 LWE(或 RLWE)的全同态加密方案的密文和密钥采用向量形式来表示，所以密文乘积使得密文维数急速膨胀，所以只能进行有限次数的密文乘法运算，密钥交换技术主要是将维数增长的密文缩减为原始的维数。

密钥交换技术的思想：用密钥转换矩阵$M$乘密文$\overrightarrow{c_1}$得到密文$\overrightarrow{c_2}$，即$\overrightarrow{c_2} \leftarrow c_1^T \times M$，

其中$M$的行数是$\overrightarrow{sk_1}$的维数，$M$的列数是$\overrightarrow{sk_2}$的维数，$M$形式上可以看成是用密钥$\overrightarrow{sk_2}$对$\overrightarrow{sk_1}$加密的 LWE 实例构成。这项技术的主要功能，一方面，将一个密文(对应密钥$sk_1$)变换成一个新的密文(对应密钥$sk_2$)；另一方面可以约减密文的维数。

全同态加密方案要把模交换技术和密钥转换技术结合起来使用，每次乘法计算后，首先使用密钥转换技术将密文的维数降低为原来的大小，再通过模交换技术降低密文的噪声，从而可以进行下一次乘法操作。

### 4.1.4 常见全同态加密方案对比

每个公钥密码系统都依赖于数学困难问题。同样地全同态加密方案的构造也主要依赖于数学困难问题。根据不同的数学困难问题可以构造出不同的全同态加密方案。

全同态加密从 2009 年发展至今经历了三代，第一代是 Gentry 所提出的基于理想格的全同态加密方案，比如 DGHV、CAFED 等；第二代是 2011 年 Brakershi 等人提出的基于 LWE[39]（或 RLWE[40]）问题，使用密钥交换技术、重线性化技术与模交换技术构造的 FHE，比如 BGV 方案[33]、Bra12 方案等；第三代是 GSW13 使用近似特征向量方法构造的 FHE。常见的全同态加密方案对比如表 4.1 所示。

表 4.1 全同态加密方案的对比

Table 4.1 Fully homomorphic encryption schemes comparison

| FHE 方案 | 主要思想 |
|---|---|
| DGHV | 理想格；BootStrapping 技术 |
| BV | 基于 LWE 问题；重线性化和模转换技术 |
| BGV | 基于 RLWE 问题；密钥转换和模交换技术 |
| Bra12 | 基于 LWE 问题；密钥转换技术 |
| GSW13 | 近似特征向量 |

从表 4.1 中可知，基于 LWE(或 RLWE)问题的全同态加密方案，称之为 BGV 方案。LWE(或 RLWE)问题对提高全同态加密的运行效率做出了很大的贡献，而且使用模交换技术而非 BootStrapping 技术获得全同态方案，从而提高了该方案的效率。2013 年 Gentry 和 Halevi 等人针对 BGV 方案开发了同态加密开源库 HElib；使得 BGV 方案得以实现。

## 4.2 基于 RLWE 问题的全同态加密方案构造

### 4.2.1 LWE 问题与 RLWE 问题

2005 年，Regev 首次提出了 LWE 问题并证明在适当假设的情况下，LWE 问

题是难解的。LWE 问题主要是区分有小量的随机“噪音”干扰的线性方程组和均衡干扰的问题。2010 年，Lyubashevsky、Peikert 和 Regev 等人提出了环的误差学习问题（RLWE）以及该问题的代数变式。它们已经成为全同态加密方案的主要应用基础，利用 LWE(或 RLWE)困难问题，可以构造出很多种密码体制。

为了更好地描述 LWE 问题与 RLWE 问题，首先给出用到的数学符号描述表，如表 4.2 所示。

表 4.2 数学符号及其含义描述

Table 4.2 Description of mathematical symbols and its meanings

| 符号 | 符号含义 |
|---|---|
| $\mathbb{Z}^n$ | 由整数组成的$n$维向量 |
| $\mathbb{Z}_q$ | 整数模$q$ |
| $\mathbb{Z}_q^n$ | 由模$q$的整数组成的$n$维向量 |
| $\mathbb{Z}_q[x]$ | 多项式集合$\mathbb{Z}_q[x]=\{\sum_{i=0}^{*}\alpha_i x^i \mid \alpha_i \in \mathbb{Z}_q\}$ |
| $R$ | 多项式环$R=\mathbb{Z}[x]/f(x)$ |
| $R_q$ | 模$q$的$R_q=\mathbb{Z}_q[x]/f(x)$ |

① LWE 困难问题(Learning With Errors，LWE)：对于给定的安全参数 λ，设定$n=n(\lambda)$、$q=q(\lambda)\geq 2$为正整数，$\chi=\chi(\lambda)$为$\mathbb{Z}$上的一个随机分布，一般情况下，$\chi$选取满足标准差为$\alpha q$的离散高斯分布，其中$\alpha<1$。$LWE_{n,q,\chi}$问题即是：

随机选取分布$a_i\leftarrow\mathbb{Z}_q^n$，$b_i\leftarrow\mathbb{Z}_q$，$\boldsymbol{s}\in\mathbb{Z}_q^n$，$e_i\leftarrow\chi$，则$(a_i,b_i=<a_i,s>+e_i)$与随机均匀选取的$(a_i,b_i)\leftarrow\mathbb{Z}_q^n\times\mathbb{Z}_q$是计算不可区分的。也就是说，从分布$\chi$中取出一些样本，不能够估算出$\boldsymbol{s}$的值。

② RLWE 困难问题(Learning With Errors over Ring，RLWE)：设定安全参数 λ，$f(x)=x^n+1$，其中整数$n=n(\lambda)$是 2 的幂次方；同时令$q=q(\lambda)\geq 2$ 是素数，$R_q=\mathbb{Z}_q[x]/f(x)$，其中$R_q=R/Rq$；最后给出环$R$上的一个随机误差分布$\chi=\chi(\lambda)$。$RLWE_{n,q,\chi}$困难问题即是：

随机均匀地在环$R_q$上选取出，$a_i\leftarrow R_q$，$s\leftarrow R_q$，$e\leftarrow\chi$，则$(a,b)=(a,<a,s>+e)$与随机均匀选取的$(a,b)\leftarrow R_q\times R_q$是计算不可区分的。

LWE 是更加标准化的假设，但是它的计算困难度远远超过 RLWE，所以 RLWE 更加有效。LWE 问题是在$\mathbb{Z}_q^n\times\mathbb{Z}_q$上进行数据元素选择，而 RLWE 只是在$R_q^2$上进行数据元素选取，因此，基于 RLWE 困难问题的全同态加密方案的密钥尺寸相对来说较小，并且算法在$R_q$更加有效率。

### 4.2.2 基于 RLWE 问题的部分同态加密方案

近年来，越来越多的密码学者相继提出了许多新的全同态加密方案，安全性规约到 LWE(或 RLWE)困难问题的全同态加密方案构造方法打破了原有的 Gentry 蓝图框架。

采用 RLWE 困难问题可以构造出部分同态加密方案（Somewhat Homomorphic Encryption，SWHE），该方案同时具有同态加法和同态乘法特性，但是它仅支持有限次数的密文计算。该方案的具体构造过程：

① 参数设置$params$

1) $n$是 2 的幂次方，多项式环$R = \mathbb{Z}[x]/f(x)$，其中$f(x) = x^n + 1$；

2) $q$是和 n 有一定关系的素数，满足等式$q \equiv 1\ mod\ 2n$；

3) 密文数据的空间选择多项式环$R_q = \mathbb{Z}_q[x]/f(x)$；

4) 设定$p \ll q$，那么明文数据的空间取多项式环上$R_p = \mathbb{Z}_p[x]/f(x)$；

5) σ是离散高斯分布$\chi = D_{Z^n,\sigma}$的标准差。

特殊地，在 BGV 方案中，明文空间设置为$R_p = \mathbb{Z}_p[x]/\Phi_m(x)$，其中分圆多项式$\Phi_m(x) = \prod_{1\le k\le m,\ \gcd(k,m)=1}(x - e^{2i\pi\frac{k}{m}})$。

② 密钥生成算法

通过密钥生成函数$KeyGen(params)$，根据 RLWE 困难问题获得方案的公钥和私钥。从分布$\chi$中随机选择$s \leftarrow \chi^n$，从密文空间均匀选择$a_1 \leftarrow R_q$，$e \leftarrow \chi^n$；通过计算得到$a_0 = -(a_1 \cdot s + e \cdot p)$，则私钥$sk = s$，公钥$pk = (a_0, a_1)$。

③ 加密算法

首先从明文空间$R_p$中选取出$M \leftarrow R_p$，然后从分布$\chi$中随机选择三个样本$u, f, g \leftarrow \chi^n$，通过式（4.2）可以得到密文$ctxt$。

$$\overrightarrow{ctxt} = Encrypt(pk, M) = (c_0, c_1) = (a_0 \cdot u + gp + M, a_1 u + fp) \quad (4.2)$$

④ 解密算法

通过解密函数$Decrypt(sk,\ ctxt)$并采用私钥$sk = s$对密文$ctxt$进行解密。因为$\overrightarrow{ctxt} = (\boldsymbol{c_0}, \boldsymbol{c_1})$，通过式（4.3）得到解密结果。

$$Decrypt(sk,\ ctxt) = M' = (c_0 + c_1\, s)\ mod\ q\ mod\ \Phi_m(x) \quad (4.3)$$

如果密文$\overrightarrow{ctxt} = (c_0, c_1, \cdots, c_k)$是多维向量时，私钥向量$\overrightarrow{sk} = (1, s, s^2, \ldots, s^k)$，解密计算如公式（4.4）所示。

$$Decrypt(sk,\ ctxt) = M' = \sum_{i=0}^{k} \boldsymbol{c}_i \boldsymbol{s}^i\ mod\ q\ mod\ \Phi_m(x) \quad (4.4)$$

其中$\Phi_m(x)$表示关于$x$的$m$阶分圆多项式。

⑤ 同态加法

对于任意两个密文向量$\overrightarrow{ctxt_1} = (c_0, c_1, \cdots, c_\gamma)$，$\overrightarrow{ctxt_2} = (c'_0, c'_1, \cdots, c'_\eta)$进行同态加密运算，如果$\overrightarrow{ctxt_1}$与$\overrightarrow{ctxt_2}$的维数相同，通过式（4.5）完成同态加密运算。

$$\overrightarrow{ctxt_{add}} = \overrightarrow{ctxt_1} + \overrightarrow{ctxt_2} = (c_0 + c_0', c_1 + c_1', \cdots, c_\gamma + c_\eta') \quad (4.5)$$

如果维数不同，则高位补 0，通过式（4.5）得出同态密文和。

$$\overrightarrow{ctxt_{add}} = \overrightarrow{ctxt_1} + \overrightarrow{ctxt_2} = (c_0 + c_0',\ c_1 + c_1',\ \cdots,\ c_{max(\gamma,\eta)} + c'_{max(\gamma,\eta)}) \quad (4.6)$$

⑥ 同态乘法

对于两个密文向量$\overrightarrow{ctxt_1} = (c_0, c_1, \cdots, c_\gamma)$，$\overrightarrow{ctxt_2} = (c_0', c_1', \cdots, c_\eta')$进行同态乘法运算，$\overrightarrow{ctxt_{mult}} = \overrightarrow{ctxt_1} \times \overrightarrow{ctxt_2}$计算方式如下：

因为该方案是在多项式环上执行的，所以引入变量$x$，那么$\sum_{i=0}^{\gamma} c_i\, x^i$，$\sum_{i=0}^{\eta} c_i'\, x^i$分别表示变量$x$的一元多项式；这两个多项式相乘得到$\sum_{i=0}^{\gamma+\eta} \tilde{c}_i\, x^i = \sum_{i=0}^{\boldsymbol{\gamma}} \boldsymbol{c_i}\, x^i \times \sum_{i=0}^{\boldsymbol{\eta}} \boldsymbol{c_i'}\, x^i$，得到相应项系数，并且使得系数值$\tilde{c}_i$，$\cdots$，$\tilde{c}_{\gamma+\eta} \in R_q$，则两密文乘积$\overrightarrow{ctxt_{mult}} = (\tilde{c}_i,\ \cdots,\ \tilde{c}_{\gamma+\eta})$。

### 4.2.3 基于 RLWE 问题的全同态加密方案

全同态加密方案，是能够对密文进行任何计算，但是在密文乘法计算的过程中使得密文的维数增加，便会导致解密不正确。为了解决此问题，利用密钥交换和模交换技术来实现部分同态加密到全同态加密的转化。在 4.1.3 节中已进行了详细阐述，密钥交换技术将密文乘积$ctxt_{mult}$及其私钥$\overrightarrow{sk'}$转换成另外一个与$\overrightarrow{sk}$维数相同的密钥$\overrightarrow{sk''}$和新的密文$\overrightarrow{ctxt''_{mult}}$，目的是为了减少密文和密钥维数；模交换技术利用一系列递减的模量$q_i$，将$\overrightarrow{ctxt_{mult}}$的模$q$转换为$q_i = q/x^i$，有效地控制噪声和密文空间的增长。因此，不需要 bootstrapping 技术就可以成功构造全同态加密方案，效率得到了提升。

## 4.3 基于 RLWE 问题的全同态加密方案分析

2013 年，IBM 研究员基于 BGV 方案设计了 HElib 库，它是在 NTL 数论库和 GMP 大数库的基础上使用 C++语言编写而成的同态加密算法软件库。HElib 软件库可以在 Visual Studio 2010 平台下运行。

### 4.3.1 方案的解析与评估

在 4.2 节中，给出了基于 RLWE 问题的全同态加密方案，该方案的算法流程如图 4.2 所示。

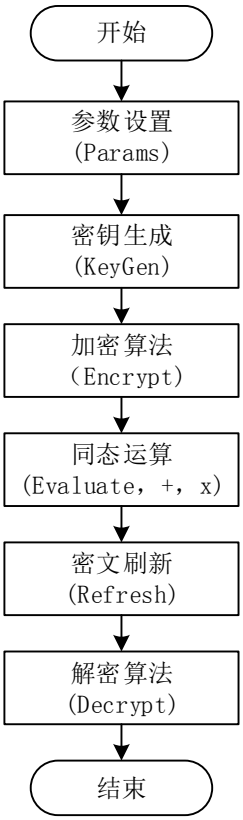


图 4.2 基于 RLWE 问题的全同态加密算法流程图

Fig.4.2 Flow chart of FHE algorithm based on RLWE problem

基于 RLWE 问题的全同态加密算法主要包括 Params、KeyGen、Encrypt、Evaluate、Refresh、Decrypt 六个子算法。其中密文刷新算法 Refresh 功能是：通过密钥转换和模交换技术对密文进行刷新，完成多次加法和乘法的同态运算。下面主要分析它们的具体实现过程。

算法实现的软件测试环境为：

CPU：Intel(R) Xeon(R) E5-2630 v2 @ 2.60GHz

内存：24GB

操作系统：Ubuntu 12.04 Server LTS

① 参数设置

从安全性方面考虑，方案的安全参数 k 必须足够大才能满足安全性；但从性能角度考虑，选择的安全参数值应较小以满足方案的效率需求。为了能够保证全同态加密方案的性能和安全性的平衡，选择合适的参数是关键。根据输入的安全参数以及明文空间等值，生成其他所需的参数。具体参数的选择如表 4.3 所示。使用 HElib 库的 FindM()函数来完成方案参数设置的工作。

表 4.3 基于 RLWE 问题的全同态加密方案的参数设置

Table 4.3 Setting of parameters of FHE scheme based on FHE

| 参数 | 取值 |
|---|---|
| P 是明文空间基数 | 根据加密方案情况而定 |
| m 是模数 | 根据方案情况而定 |
| R 密文运算的轮数 | 默认值为 1 |
| L 电路深度(密文计算的次数) | 根据密文计算复杂度而定 |
| w 生成密钥所需要的权重 | 取值为 64 |
| k 安全参数 | 取值为 80 |
| c 密钥转换矩阵的列数 | 默认值为 2 |
| d 是扩展度 | 默认值为 1 |

整个参数设置过程，根据全同态加密方案的实际应用情况，给定初始化参数 k，L，c，p，d 和 s，建立方案的参数环境。其中 FindM()函数的具体流程如图 4.3 所示。

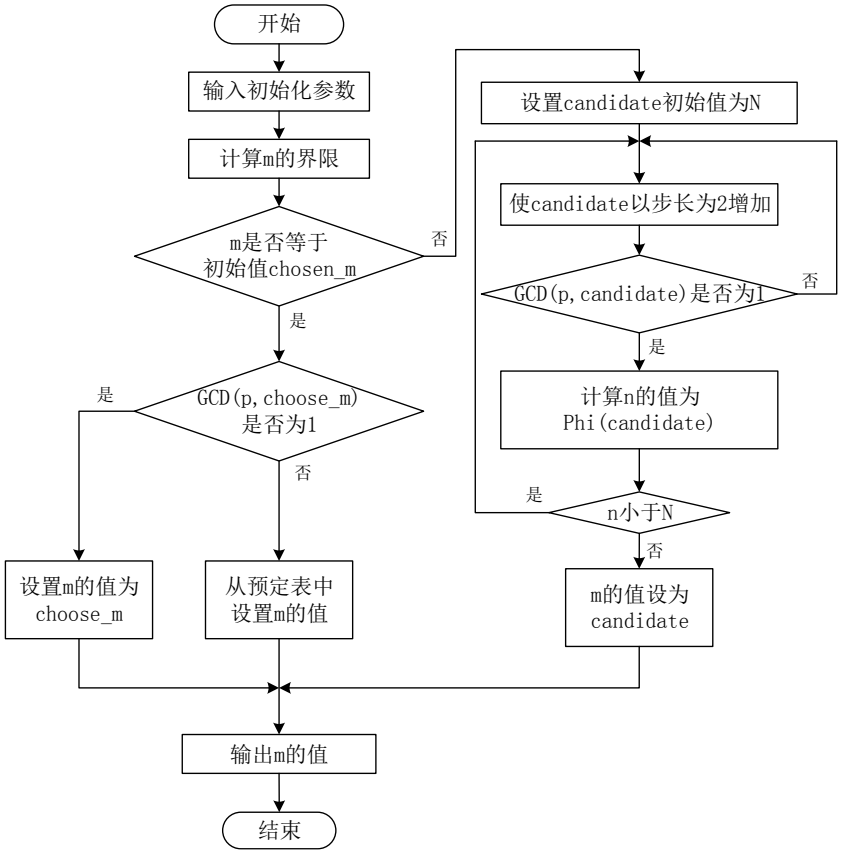


图 4.3 参数设置流程图

Figure 4.3 Flow chart of setting parameters

参数设置的主要目的是：根据输入的参数 k，L，c，p，d 和 s，找出满足方案安全性和正确性的模值 m，使得整个方案能够有效地实现。

② 密钥生成算法

根据生成的方案参数，通过密钥生成算法产生方案的密钥。整个密钥生成算法的详细流程图如图 4.4 所示。

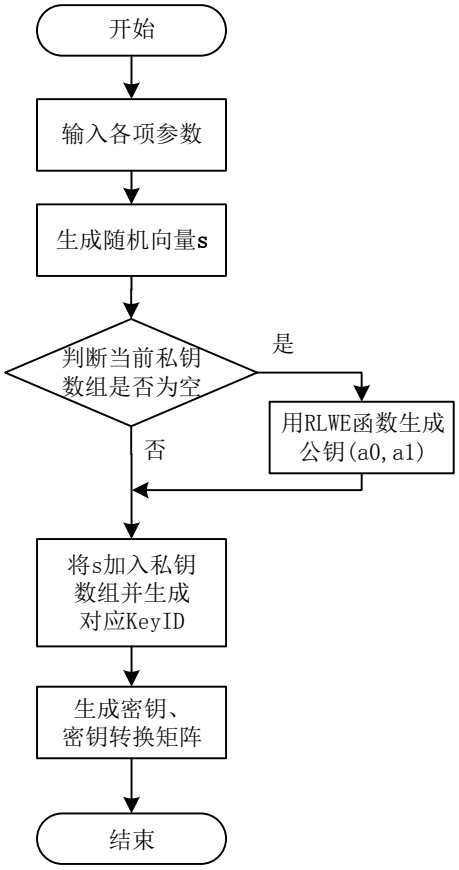


图 4.4 密钥生成算法流程图

Fig.4.4 Flow chart of key generation algorithm

密钥生成是基于 RLWE 困难问题的。首先根据生成的安全参数，取得随机向量 s，然后判断已存在私钥数据，若不存在则基于 RLWE 困难问题生成公钥(a0,a1)，私钥 sk=s。假如私钥数据存在则直接将 s=sk。

③ 加密算法

通过加密函数输入明文 ptxt 和公钥 pk，采用 pk.Encrypt(ctxt，ptxt)函数对明文进行加密得到密文 ctxt。加密算法 Encrypt()的具体实现流程图如图 4.5 所示。

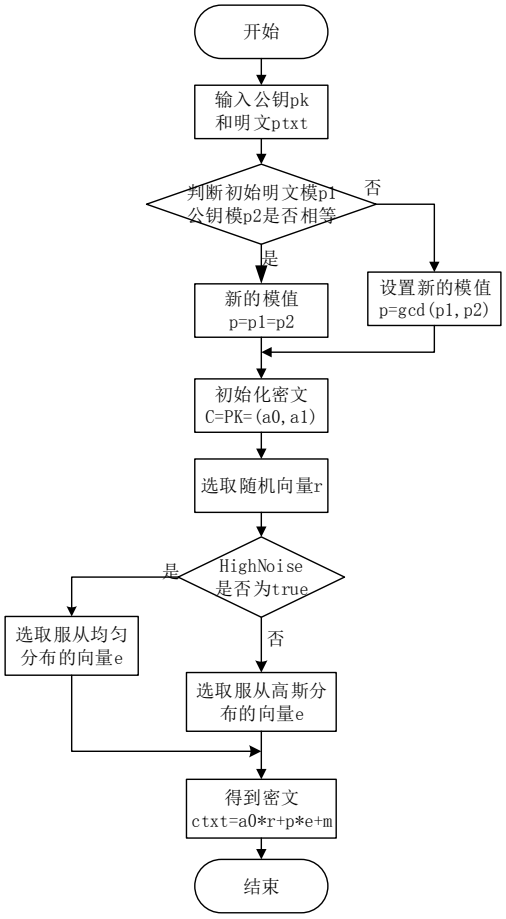


图 4.5 加密算法的流程图

Fig.4.5 Flow chart of encryption process

加密公式为：

$$ctxt = r * (a_0, a_1) + p * e + (ptxt, 0) = (a_0 * r + e * p + ptxt, a_1 * r + 0) \quad (4.7)$$

其中 $r$ 和 $e$ 为随机向量，向量 $r$ 中的每一个元素都从集合{-1,0,1}中取值，其中 0 出现的概率为 0.5，$e$ 服从高斯分布。

④ 同态运算算法

对两个密文进行同态加法或乘法运算之后，先调用密钥转换函数刷新密文，再通过模交换技术减少密文的噪声，经过上述两步操作后的密文才能够继续参与运算。公式（4.8）给出两密文之和的计算函数 *addCtxt*()。

$$add_{ctxt} = ctxt_1.addCtxt(ctxt_2) \quad (4.8)$$

⑤ 解密算法

通过式（4.9）用私钥 sk 通过解密函数 *Decrypt*()对密文$ctxt$进行解密正确得到明文数据。

$$pctxt = sk.Decrypt(ptxt, ctxt) \quad (4.9)$$

### 4.3.2 方案的性能分析

全同态加密方案主要从两方面着手研究：一方面是如何确保方案的安全性；另一方面是如何在保证解密正确性的情况下提高全同态加密方案的效率。其中，影响全同态加密的安全性和运行效率的主要因素为密文噪声 *noise*、电路深度 L 以及安全参数 *k*。本小节主要测试分析噪声 *noise* 与电路深度 L 的关系、电路深度 L 对 BGV 方案效率的影响，并对实验结果进行分析说明。

① 噪声 noise 与电路深度 L 的关系。

编写测试程序，主要功能是可以实现密文的同态乘法、同态加法、左移、取反、乘以常数等基本运算。其中输入数据为不同的电路深度 L、固定的模值 m，输出数据为 log(noise/modulus)的值。方案的参数设置如表 4.3 所示。L=3 时输出结果情况如图 4.6 所示。

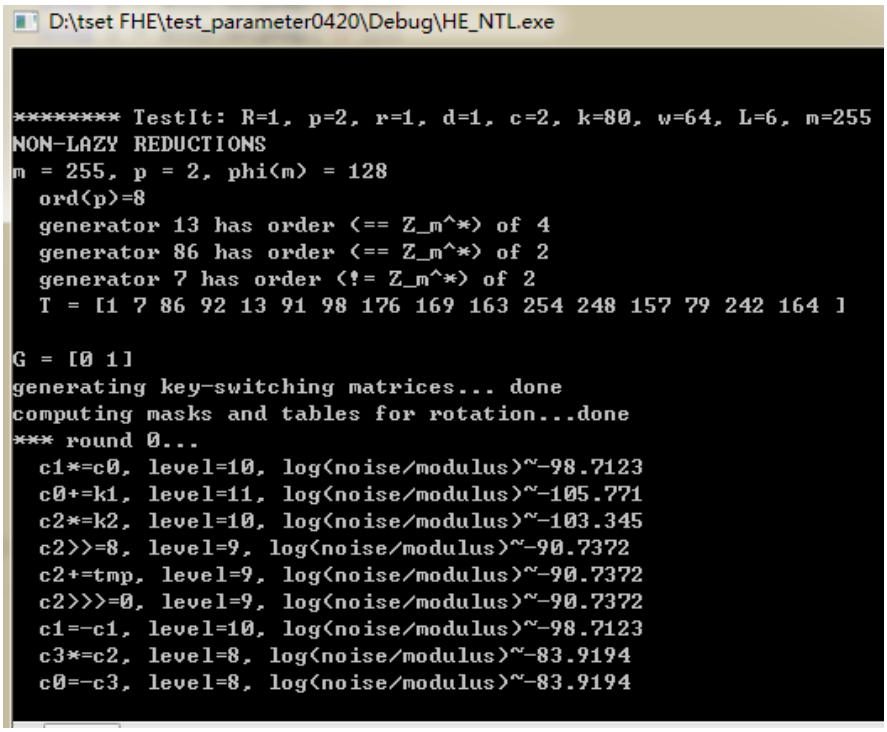


图 4.6 L=3 时的运行情况

Fig.4.6 Running status when L value is 3

1) 首先固定模值 m=255，安全参数 k=80，改变电路深度 L 的值，密文进行取反、相加、相乘运算时，log(noise/modulus)的数值大小。测试数据如表 4.3 所示。将测试数据绘制成图像，观察值 log(noise/modulus)的变化规律，如图 4.7 所示。其中 c0，c1，c3 为密文数据。

表 4.4 L 值不同情况下的实验结果

Table 4.4 Result of experiment test when L changes

| log(noise/modulus) 的值 / L 值 | c1=~c1 时， | c0=-c3 时， | c1*=c0 时， |
|---|---|---|---|
| 6 | -52.683 | -36.7567 | -52.683 |
| 9 | -113.093 | -97.4433 | -113.093 |
| 12 | -143.012 | -127.449 | -143.012 |
| 15 | -202.309 | -186.927 | -202.309 |
| 18 | -231.864 | -216.658 | -231.864 |
| 21 | -288.784 | -260.502 | -288.784 |
| 24 | -316.506 | -288.784 | -316.506 |
| 27 | -377.131 | -361.343 | -377.131 |
| 30 | -407.306 | -391.565 | -407.306 |
| 33 | -466.931 | -451.484 | -466.931 |
| 36 | -496.38 | -481.238 | -496.38 |
| 39 | -554.458 | -525.519 | -554.458 |
| 42 | -581.710 | -554.458 | -581.710 |
| 45 | -642.619 | -626.704 | -642.619 |
| 48 | -672.93 | -657.085 | -672.93 |

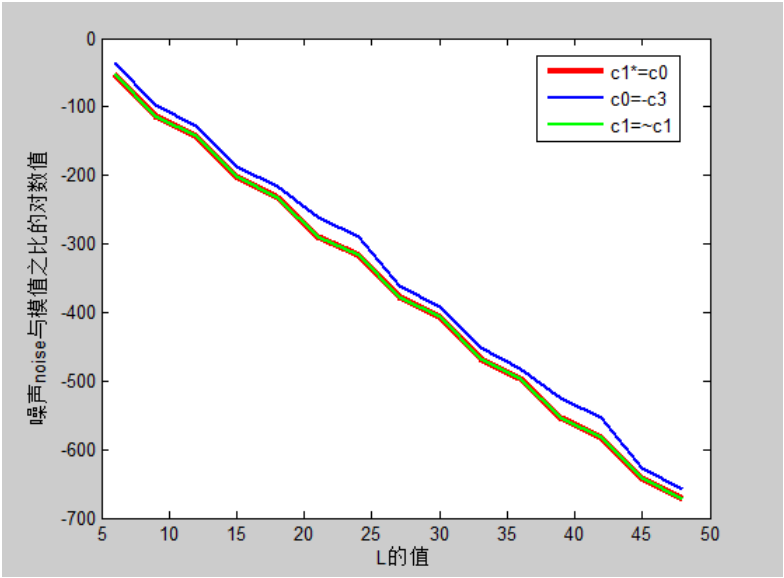


图 4.7 L 与 log(noise/modulus)的关系

Fig.4.7 Relationship between L value and log(noise/modulus)

由图 4.7 可知，随着 L 的不断增大，噪声与模数之比的对数值减小，并且呈现出近似线性关系。因此，噪声与模数的比呈指数形式减小。

2) 当 L=48 时，每一个密文运算都要重复进行多次计算，每一次运算情况下，log(noise/modulus)值的大小如表 4.5 所示。分析每一轮的值 log(noise/modulus)的变化情况，如图 4.8 所示。

表 4.5 L=48 时，实验测试结果

Table 4.5 Result of experiment test when L value is 48

| log(noise/modulus)的值 / 轮数 | c1=~c1 时, | c0=-c3 时， | c1*=c0 时， |
|---|---|---|---|
| 1 | -672.93 | -657.085 | -672.93 |
| 2 | -642.619 | -626.661 | -642.619 |
| 3 | -612.168 | -596.246 | -612.168 |
| 4 | -581.71 | -554.458 | -581.71 |
| 5 | -540.102 | -525.102 | -540.102 |
| 6 | -510.963 | -481.514 | -510.963 |
| 7 | -466.931 | -451.484 | -466.931 |
| 8 | -437.211 | - 421.889 | -437.211 |
| 9 | -407.306 | -391.565 | -407.306 |
| 10 | -377.131 | -361.343 | -377.131 |
| 11 | -346.893 | -330.987 | -346.893 |
| 12 | -316.506 | -288.784 | -316.506 |
| 13 | -275.085 | -246.447 | -275.085 |
| 14 | -231.864 | -216.499 | -231.864 |
| 15 | -202.309 | -187.078 | -202.309 |

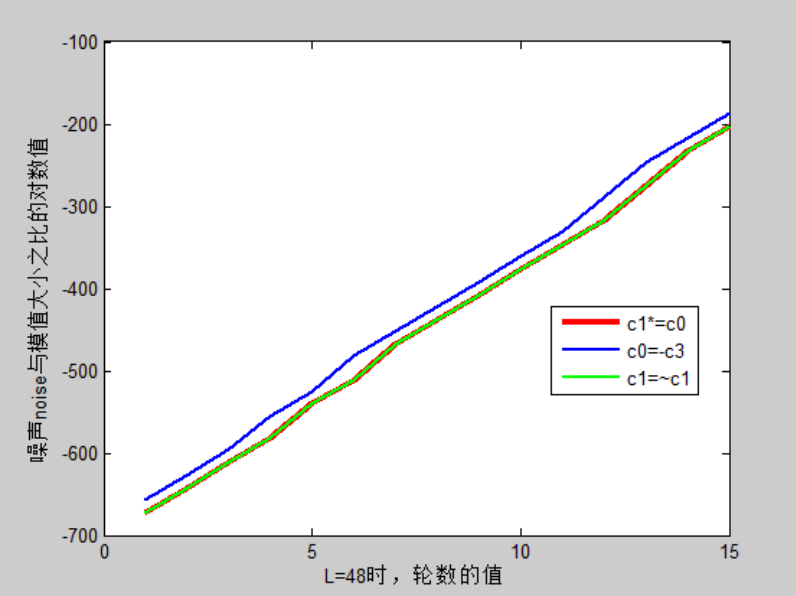


图 4.8 L=48 时，每一轮的 log(noise/modulus)的变化情况

Fig.4.8 Changes in each round of the log(noise/modulus) when L value is 48

由图 4.8 可知，随着计算轮数的不断增加，log(noise/modulus)的值呈线性增长的趋势，所以 noise/modulus 呈指数形式增长。

由图 4.7 和图 4.8 可知，在全同态加密方案中，用户可以通过增加模数 modulus 降低噪声，保证解密的正确性。当模数 modulus 增大，noise/modulus 的值就会减小，那么噪声对密文刷新产生的影响就减小了。但模数的增加降低了加密过程的效率。如果用户要求解密结果的准确性较高，那么通过增加模数来实现；如果用户对方案效率要求严格，那么可以通过降低电路深度 L 来实现。

② 测试电路深度 L 对 BGV 方案的效率影响

编写程序实现两个密文进行同态乘法的功能，其中方案的参数设置如表 4.3 所示。具体的测试数据如表 4.6 所示。为了方便分析，用 MATLAB 将数据绘制成图。

表 4.6 L 值对方案的效率影响

Table 4.6 Effect of the L value on the efficiency of the scheme

| L 值 | 2 | 5 | 10 | 20 | 40 | 60 | 80 | 100 |
|---|---|---|---|---|---|---|---|---|
| 乘法耗时(ms) | 10 | 30 | 80 | 330 | 1260 | 3050 | 4870 | 6940 |
| 总耗时(ms) | 1100 | 2040 | 6420 | 21730 | 79690 | 164670 | 269960 | 368820 |

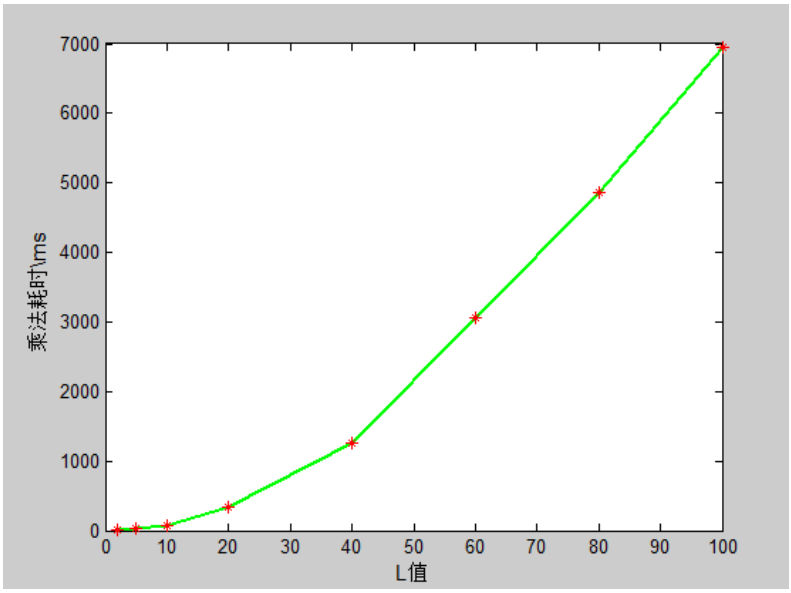


图 4.9 L 值与密文乘法运算时间的关系

Fig.4.9 Relation between L value and ciphertext multiplication time

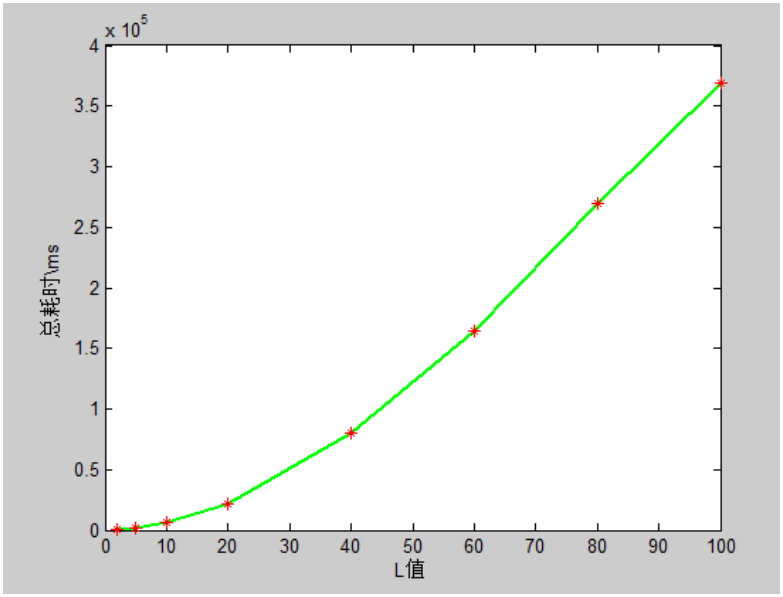


图 4.10 L 值与方案总运行时间的关系

Fig.4.10 Relationship between the L value and the total run time of the scheme

从上面的实验结果中，可以看出方案总的运行时间与 L 值的大小有关。由表 4.6 和图 4.10 可知，随着电路深度 L 的不断增加，方案总运行时间和乘法运算时间逐渐增大。可见，电路深度 L 对方案的效率影响显著。k 和 L 分别反映方案的抗攻击能力和密文计算复杂度，因此，在实际应用过程中，选定合适的 k 和 L 来保证安全性和有效性。

### 4.3.3 与其他它方案的对比分析

文献[17]中给出了基于整数的全同态加密方案（Gentry 方案）及其实现过程。我们利用 FHE-code 代码库可以对该方案进行动态分析，FHE-code 代码库主要包括密钥生成、加密、解密和密文刷新等算法。两种方案的安全性都是基于数学困难问题的，表 4.7 给出两种方案的安全性和实现方式的对比。

表 4.7 Gentry 方案和 BGV 方案对比

Table 4.7 Comparison between Gentry scheme and BGV scheme

| 方案 | 基于的数学难题 | 实现方式 | 程序 |
|---|---|---|---|
| Gentry 方案 | 近似 GCD | “自举”技术和解密电路压缩 | FHE-code |
| BGV 方案 | RLWE 困难问题 | 模交换和密钥转换技术 | HElib |

接下来主要从程序本身出发对两个方案实现程序的动态分析、安全性和有效性等方面进行对比分析。软件测试环境为：

操作系统：Windows7　　内存：4G

CPU：　Intel(R) Core(TM) i3-2350M@2.3GHz

首先，设定明文$m_1 = 2$，$m_2 = 3$，分别对两者进行同态加法和同态乘法运算，在相同测试平台下，测试 Gentry 方案和 BGV 方案在不同的安全参数下所需要的时间。如表 4.8 和 4.9 所示。

表 4.8 加法运算时间对比

Table 4.8 Comparison about the time of additive operation

| 安全参数的值 / 耗时(ms) | 8 | 16 | 32 | 64 | 80 | 100 | 128 |
|---|---|---|---|---|---|---|---|
| Gentry 方案 | 46789 | 74312 | 82415 | 91256 | 101253 | 113247 | 185329 |
| BGV 方案 | 35756 | 63920 | 78835 | 84413 | 86845 | 105629 | 178548 |

表 4.9 乘法运算时间对比

Table 4.9 Comparison about the time of additive operation

| 安全参数的值 / 耗时(ms) | 8 | 16 | 32 | 64 | 80 | 100 | 128 |
|---|---|---|---|---|---|---|---|
| Gentry 方案 | 50431 | 87961 | 94742 | 97452 | 99431 | 106772 | 198219 |
| BGV 方案 | 41920 | 72291 | 85887 | 86705 | 87458 | 104439 | 191925 |

从表 4.8 和 4.109 可以看出，①当给定相同的安全参数，BGV 方案相对于 Gentry 方案在效率上有明显的提高，主要与其基于的困难问题、实现方式有一定的联系。基于 RLWE 问题的 BGV 方案性能优势显著，主要是因为采用的模交换和密钥转换技术能够有效地控制密文噪声和空间的增长。②对于 BGV 方案而言，乘法计算的效率远远高于加法计算，主要是因为在密文乘法计算过程中增大了密文噪声和空间，而为了保证解密结果的正确性，需要增加电路深度 L 的值，因此，效率上有所降低。

BGV 方案在安全性和效率上都有明显的优势，本文将 BGV 方案运用到电子投票中，能够同时满足方案安全性和性能方面的需求。

## 4.4 本章小结

本章主要研究了全同态加密方案，构造并实现了基于 RLWE 问题的全同态加密方案。①首先根据全同态加密的定义、原理以及所用到的关键技术构造一个部分全同态加密方案；再根据模转化技术和密钥交换技术把它转化成基于 RLWE 问题的全同态加密方案。②基于软件同态算法库 HELib 库，验证了基于 RLWE 问题的全同态加密方案（BGV 方案），并对其性能进行分析。③通过与 Gentry 方案对比，说明 BGV 方案适合运用到电子投票方案中，保证投票的安全性。

# 5 基于 RLWE 问题全同态加密的电子投票方案设计

在文中第三章明确了电子投票方案的总体架构。第四章中对基于 RLWE 问题的全同态加密进行了研究分析。本章依据整体方案框架，结合基于 RLWE 问题的全同态加密和数字签名技术，详细阐述注册、投票、计票和查票验证阶段投票方案的具体流程。最后对方案的安全性、可行性和实用性进行分析，验证方案是否完成了设计目标。

## 5.1 方案的实施步骤

根据 3.3 节的总体方案设计可知，本方案主要包括四个参与实体：投票者、计票中心、权威认证中心以及公告牌。根据各个参与实体的主要功能要求。给出整个投票过程的具体流程如图 5.1 所示。

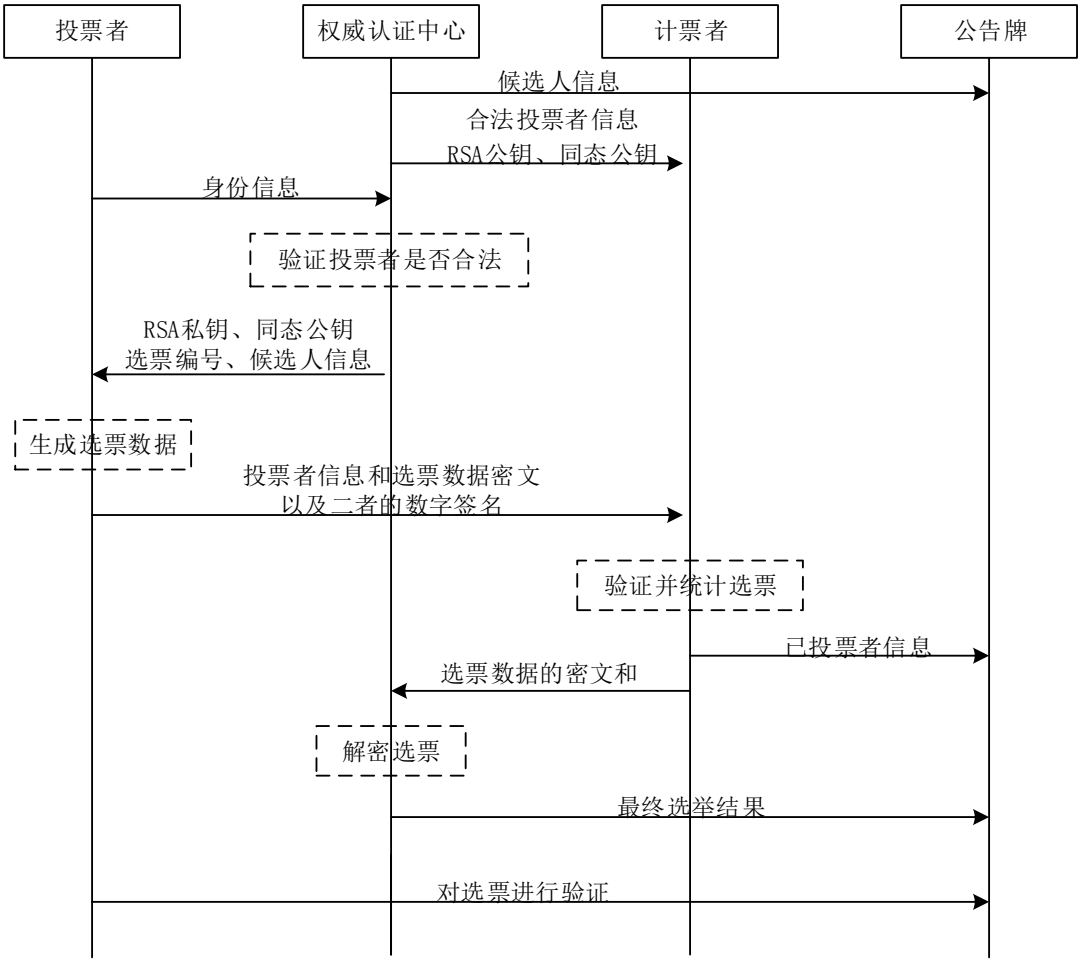


图 5.1 基于 RLWE 问题的全同态加密方案的电子投票方案流程

Fig.5.1 Flow chart of e-voting scheme based on FHE

投票和计票阶段是电子投票过程的主要环节。投票者在投票时，使用同态公钥将选票数据进行加密，并用数字签名算法对选票数据进行签名，保证选票信息的真实可靠性，最后发送给计票方，计票中心收到所有的选票密文之后，首先验证其是否可信，然后再进行计票，这样便匿名安全地完成了一次投票。为了更好地描述方案，首先给出一些符号定义如表 5.1 所示。

表 5.1 方案所使用的符号以其含义

Table 5.1 Symbols used by the scheme

| 符号 | 所表示的含义 |
|---|---|
| $voter_i$ | 投票者$i$ |
| $C_i$ | 候选人$i$ |
| $W_i$ | 获胜者$i$ |
| $ID_i$ | $voter_i$的身份编号 |
| $Pro_i$ | 合法投票者注册凭证 |
| $BN_i$ | 投票者 i 的选票编号 |
| $CI_i$ | 候选人$i$的基本信息 |
| $PK_{FHE}$ | BGV 方案的同态公钥 |
| $SK_{FHE}$ | BGV 方案同态私钥 |
| $pk_i$ | $voter_i$的 RSA 数字签名公钥 |
| $sk_i$ | $voter_i$的 RSA 数字签名私钥 |
| $Ballot\_data_i$ | $voter_i$生成的未经处理的选票 |
| $Ballot\_ctxt_i$ | 原始选票$Ballot_data_i$同态加密密文 |

一般情况下，在投票活动启动之前活动的发起者（权威认证中心）需要做准备工作。①规定投票的活动形式：本方案投票场景采用 K-out-of-M 投票类型，从 M 个候选人$\{C_1,\cdots,C_i,\cdots,C_M\}$中选择 K 获胜者$\{W_1,\cdots,W_i,\cdots,W_K\}$，并把候选人基本信息发布于公告板上。 ②定义选票数据的形式：对于基于 RLWE 问题的全同态加密方案而言，明文空间是建立在多项式环上的，将明文转换成多项式的系数（向量的形式），然后再对其进行加密。所以，投票者根据候选人的个数生成 M 维的明文向量，其中向量的每一位对应一个候选人，保证整个投票过程的单人单票性。

投票方案包括以下实体结构：M 个候选人$\{C_1,\cdots,C_i,\cdots,C_M\}$，L 个投票者$\{voter_1,\cdots,voter_L\}$，一个计票中心，一个权威认证中心。

根据实际投票活动的情况，方案将整个投票过程分为四个阶段：初始化阶段、投票者注册投票阶段、计票公布阶段、查询认证阶段。

### 5.1.1 初始化阶段

权威认证中心完成以下四部分的初始化工作。

① 根据投票活动的实际情况，获得 M 个候选人的信息$\{CI_1,\cdots,CI_i,\cdots,CI_M\}$，并发布到公告板上；同时为每个合法投票者分派唯一的注册凭证，那么 L 个合法者即是$\{Pro_1,\cdots,Pro_i,\cdots,Pro_L\}$。该注册凭证除了合法投票者自己和权威认证中心之外，无人可以获得它的内容。

② 采用 RSA 公钥加密算法，生成 L 个投票者用于数字签名的公钥$\{pk_1,\cdots,pk_i,\cdots,pk_L\}$和私钥$\{sk_1,\cdots,sk_i,\cdots,sk_L\}$。

投票者$voter_i$的 RSA 密钥生成过程如下：

1) 随机选择两个大素数$p_i$，$q_i$，满足$|p_i|\approx|q_i|$；

2) 设定$\varphi(n_i)=(p_i-1)(q_i-1)$；

3) 任意选择一个整数$e_i$，满足$1<e<\varphi(n_i)$，$\gcd(e,\varphi(n_i))=1$；

4) 根据等式$e_i\cdot d_i=1\bmod\varphi(n_i)$，求得$d_i$；

5) 公钥$pk_i$为$(n_i,e_i)$，私钥$sk_i$为$d_i$。

③ 根据第四章中介绍的基于 RLWE 问题的全同态加密方案，为所有的选票数据生成一对密钥，选票的密钥即是 4.2.2 节的公钥$PK_{FHE}=(a_0,a_1)$，$SK_{FHE}=s$，其中公钥$PK_{FHE}$用于对选票进行加密，所有投票者共享这个公钥，私钥$SK_{FHE}$用于对最终计票结果进行解密，由权威认证中心保管。

④ 随机生成投票者对应的唯一选票编号(Ballot Number，BN) 以及合法投票者的身份编号(Identity Number)，分别用符号$\{BN_1,\cdots,BN_i,\cdots,BN_L\}$和$\{ID_1,\cdots,ID_i,\cdots,ID_L\}$来表示。

### 5.1.2 注册投票阶段

① 注册阶段

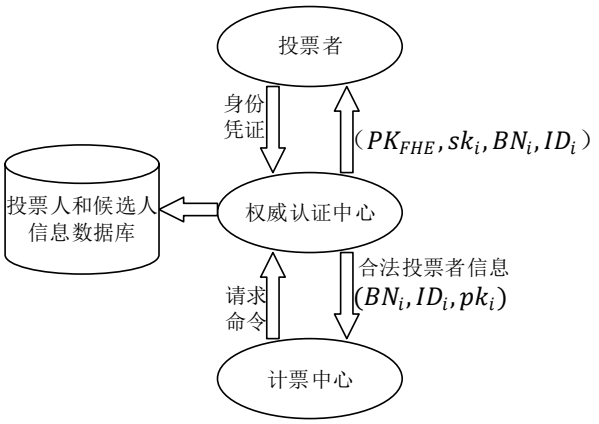


图 5.2 注册阶段过程图

Fig.5.2 Flow chart of registration process

图 5.2 为注册阶段的具体过程图。投票者$voter_i$在注册阶段主要的工作是：使用自己的注册凭证$Pro_i$，去权威认证中心 AC 进行注册，权威认证中心给合法投票者唯一的选票编号$BN_i$，具体过程如下。权威认证中心通过对比$Pro_i$验证该投票者是否合法，若合法，那么便向投票者$voter_i$分发五部分信息：用于加密选票的同态加密公钥$PK_{FHE}$、用于数字签名的 RSA 私钥$sk_i$、所有候选人信息、唯一的选票编号$BN_i$和身份编号$ID_i$；若不合法，则驳回投票者的注册请求并记录该投票者的$ID_i$，防止该投票者再次注册。

计票中心在注册阶段主要的工作是：向权威认证中心发送请求，权威认证中心将全同态加密公钥$PK_{FHE}$、投票者 RSA 公钥$\{pk_1,\cdots,pk_i,\cdots,pk_L\}$以及所有合法投票者的身份编号 ID 和选票编号 BN 共享给计票中心。

② 投票阶段

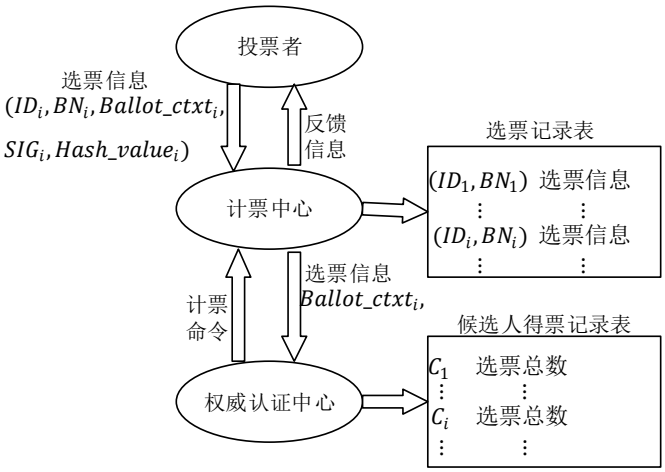


图 5.3 投票阶段过程图

Fig.5.3 Flow chart of voting process

投票阶段，合法投票者$voter_i$根据权威认证中心分发的候选人信息、同态公钥$PK_{FHE}$、签名私钥$sk_i$和选票编号$BN_i$，生成表明自己身份的唯一选票，具体过程如下。

1) 首先投票者$voter_i$，根据所有候选人信息选取出合适的候选人，以及所定义的选票数据形式，生成向量形式的初始选票数据$Ballot_data_i = (voter_{i1}, voter_{i2},\cdots, voter_{iM})$，其中$voter_{ij}$表示投票者$voter_i$对候选人$C_j$的意愿。

$$voter_{ij} = \begin{cases} 0，\text{不同意} \\ 1，\text{同意} \end{cases}，\ \mathrm{i} = 1,2,\cdots,\mathrm{L};\ \mathrm{j} = 1,2,\cdots \mathrm{M} \tag{5.1}$$

采用同态加密公钥$PK_{FHE}$，基于 RLWE 的全同态加密算法对初始选票数据$Ballot_data_i$进行加密，通过式（5.2）

$$Ballot\_ctxt_i = Enc(PK_{FHE}, Ballot\_data_i) \tag{5.2}$$

获得初始选票的密文数据$Ballot_ctxt_i$。

2) 接着对该投票者的身份编号$ID_i$、选票编号$BN_i$和选票数据的同态密文$Ballot_ctxt_i$进行数字签名。采用 2.3.3 节中所述的基于 RSA 加密算法的数字签名系统，具体实施步骤如下：

通过 Hash 函数$H$计算得到该投票者相关信息的信息摘要，如式（5.3）所示。

$$MD_i = H(ID_i \parallel BN_i \parallel Ballot\_ctxt_i) \tag{5.3}$$

其中 Hash 函数选用 MD5 算法。

该投票者使用 RSA 私钥$d_i$，采用 RSA 加密算法，通过式（5.4）对报文摘要信息$MD_i$进行加密，得到该投票者的签名信息(Signature Information，SIG)。

$$SIG_i = (MD_i)^{d_i} \, mod \, n_i \tag{5.4}$$

为了防止签名信息被伪造，使得投票者身份及其选票信息被泄露，再次采用 MD5 算法对$(ID_i \parallel BN_i \parallel Ballot_ctxt_i)$以及签名信息$SIG_i$进行 Hash 运算，通过式（5.5）生成最终散列值$Hash_value_i$：

$$Hash\_value_i = H((ID_i \parallel BN_i \parallel Ballot\_ctxt_i),\ SIG_i) \tag{5.5}$$

3) 最后投票者$voter_i$将最终的投票信息$((ID_i \parallel BN_i \parallel Ballot_ctxt_i),\ SIG_i,\ Hash_value_i)$发送给计票中心，计票中心对其进行验证并计票。

### 5.1.3 计票公布阶段

计票中心的计票过程主要工作：对投票者经同态加密、数字签名一系列处理之后的选票信息进行计票。当接收到投票者的投票信息时，首先对信息内容进行判断筛选，判定选票是否合法，若选票是合法的则把该选票计入最终结果，否则放弃该选票。整体的计票过程如图 5.4 所示。

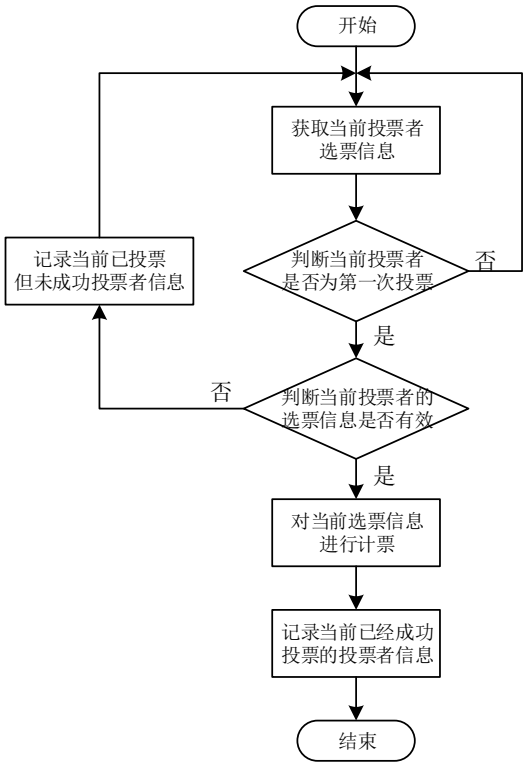


图 5.4 计票过程图

Fig.5.4 Flow chart of counting process

假如计票中心接收到投票者$voter_i$的投票信息$((ID_i \parallel BN_i \parallel Ballot_ctxt_i)$，$SIG_i$，$Hash\_value_i)$，对整个计票阶段的过程进行阐述。

① 首先，计票中心检验收到的投票信息是否被篡改，即是验证$((ID_i \parallel BN_i \parallel Ballot_ctxt_i)$，$SIG_i$，$Hash_value_i)$是否有效。

$$Hash\_value_i = H(ID_i \parallel BN_i \parallel Ballot_{ctxt_i} || SIG_i) \tag{5.6}$$

如果上式中两者相等，那么收到的信息是完整的，否则信息不完整，反馈给投票者$voter_i$，然后让其重新发送投票信息。

② 计票中心根据投票者的身份编号$ID_i$和唯一的选票编号$BN_i$判断该投票者是否为第一次投票，如果不是第一次投票，则终止当前选票信息的验证，并丢弃该选票，防止一票多投的情况发生。如果是第一次投票，则继续判断当前投票者$voter_i$的选票信息是否有效。

③ 选票信息是否有效的判定主要包括当前投票者的身份是否已经被权威认证中心认证、当前投票者选票信息的数字签名是否正确即是选票信息是否被篡改。具体过程如下：

1) 首先，判断当前投票人的身份信息$ID_i$和唯一的选票编号$BN_i$是否已经认证通过，防止重复投票。若未通过验证则直接放弃该选票，否则继续选票信息的验证。

2) 其次，计票中心用与当前投票者在投票阶段提取报文摘要时相同的 Hash 函数 H，从原始选票信息$(ID_i \parallel BN_i \parallel Ballot_ctxt_i)$中计算出新的报文摘要$H(ID_i \parallel BN_i \parallel Ballot_ctxt_i)$；RSA 公钥$(n_i, e_i)$来对选票信息的数字签名$SIG_i$进行解密，获得原始的报文摘要$(SIG_i)^{e_i} \ mod \ n_i$，判断式（5.7）左右两边是否相等。

$$H\left(ID_i \parallel BN_i \parallel Ballot_{ctxt_i}\right) = (SIG_i)^{e_i} \ mod \ n_i \tag{5.7}$$

如果两者相同，那么计票中心接收的选票信息是完整的，没有被篡改。

3) 最后，通过以上认证之后，表示该投票者以及投票者的选票是合法的，筛选出选票信息中的选票密文$Ballot_ctxt_i$，并对其进行计票。同时把当前投票者的信息(身份信息$ID_i$和唯一的选票编号$BN_i$)保存并记录，防止合法投票者重复投票。当投票结束之后，公告牌显示成功投票总人数和投票者信息，以便投票者查证选票结果。

④ 统计所有加密过的合法选票数据。计票中心统计所有投票者$\{voter_1, voter_2, \cdots, voter_L\}$的合法选票信息$\{((ID_1 \parallel BN_1 \parallel Ballot_ctxt_1), SIG_1), ((ID_2 \parallel BN_2 \parallel Ballot_ctxt_2), SIG_2), \cdots, ((ID_\mu \parallel BN_\mu \parallel Ballot_ctxt_\mu), SIG_\mu)\}$ 其中$\mu$小于等于投票人数$L$，筛选出合法选票数据的同态密文$\{Ballot_ctxt_1, Ballot_ctxt_2, \cdots, Ballot_ctxt_\mu\}$，使其密文相加得到密文和

$$ctxt\_sum = \sum_{i=0}^{\mu} Ballot\_ctxt_i \tag{5.8}$$

计票中心将选票数据的同态密文之和发送给权威的认证中心。

⑤ 权威认证中心对选票密文之和解密。认证中心用同态加密私钥$SK_{FHE}$，对密文之和$ctxt_sum$进行解密。根据基于 RLWE 全同态加密算法的实现方式得知最终解密结果是以向量的形式呈现的。所以，权威认证中心对所有选票的密文之和$ctxt_sum$解密之后得到明文向量，如公式（5.9）所示。

$$Decrypt\left(SK_{FHE}, ctxt\_sum\right) = (sum_1, sum_2, \cdots, sum_M) \tag{5.9}$$

其中$sum_i$表示候选人第$i$的选票结果。权威认证中心统计出每一个候选人的选票总数，得到投票活动的最终选举结果。

⑥ 公布结果。权威认证中心将所有候选人最终得票数公布到公告板上，如表 5.2 所示；同时计票中心会统计成功投票者的信息和未成功投票者的信息，以便投票者对计票结果进行验证。

权威认证中心向公告板发送的信息如表 5.2 所示。

表 5.2 计票中心向公告板发送的信息

Table 5.2 Central counting send information to the bulletion board

| 候选人 | 候选人信息 | 候选人票数 |
|---|---|---|
| $C_1$ | $CI_1$ | xxx |
| …… | …… | …… |
| $C_i$ | $CI_i$ | xxx |
| …… | …… | …… |
| $C_M$ | $CI_M$ | xxx |

### 5.1.4 验证查票阶段

验证查票阶段主要的工作：如果对计票结果的正确性存有质疑的个人、组织或者第三方，提出申请后，选举活动的权威认证机构给出投票过程中保存的记录用以证明结果的正确性。

因为计票中心对已成功投票的合法投票者和未成功投票的投票者的身份编号和选票编号，都有明确的记录，所以投票者$voter_i$可以使用自己的$ID_i$和唯一的选票编号$BN_i$去验证自己的选票是否被计入最终结果。

基于 RLWE 全同态加密方案的电子投票方案，结合基于 RLWE 困难问题的全同态加密、数字签名技术等，在保证满足匿名性、不可重用性、合法性、公平性等基本基本特性的同时，重点解决了方案的公开可验证性、自计票性、高效性和实用性。

## 5.2 方案的实现与验证

### 5.2.1 方案实现

整个电子投票系统主要有投票者客户端、计票中心服务端和权威认证中心服务端。由于选票的数据是在加密的情况下进行计算的，编码工作主要是建立在同态加密库 HElib 库基础上进行展开的。根据实际电子投票系统的应用需求，系统建立在 TCP/IP 网络上，采用 Client/Server 结构来对系统进行设计，最后通过计算网络完成投票活动。电子投票系统的模型如图 5.5 所示。

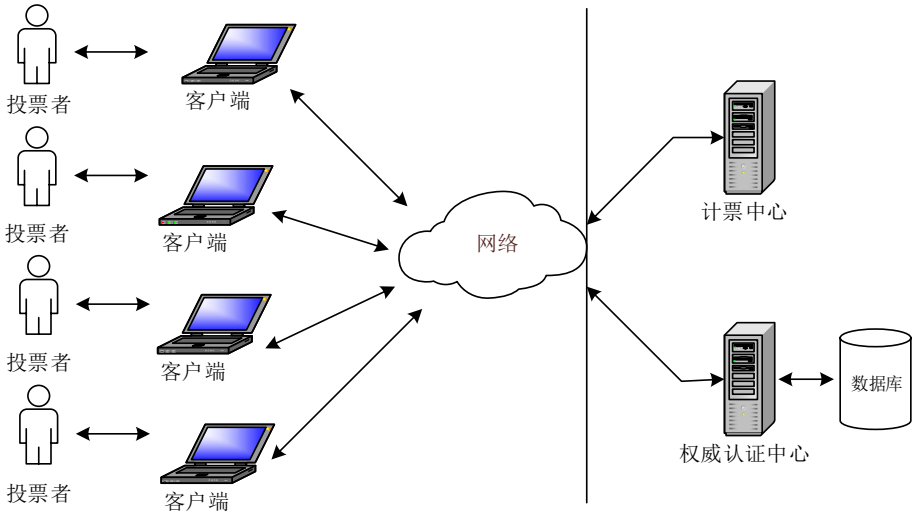


图 5.5 电子投票系统的模型图

Fig.5.5 Electronic voting system model

课题组根据方案的设计要求，采用计算机和网络技术对其进行实现，验证该方案是否可行。系统结构主要包括可信的认证中心、公告牌、计票中心和投票客户端四个部分，它们之间主要是通过以太网完成数据交互。具体的系统实物图如图 5.6 所示。

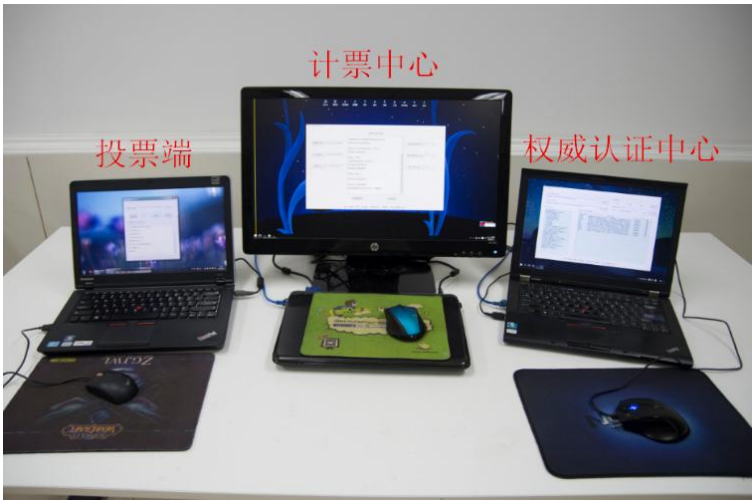


图 5.6 系统实物图

Fig.5.6 Physical map of the system

① 投票者使用智能手机、平板电脑和便携式电脑等设备通过网络访问投票系统进行注册、投票、查验结果等操作。

② 权威认证中心主要完成的工作：开始和终止投票活动、设定候选人信息、规定投票者的范围、生成投票凭证并通过安全的方式交由投票者手中；同时向计票

中心提供投票者身份认证服务。它是整个系统中唯一持有同态加密私钥的部门，为最终的结果提供解密服务，保证整个投票过程的匿名性。

③ 计票中心往往设置在具有强大的计算功能的第三方云平台上，利用第三方的计算资源，对选票数据进行阶段性统票。

### 5.2.2 方案测试

① 系统测试环境

首先对系统的网络环境进行搭建：权威认证中心和计票中心各使用一台 64 位 Windows7 操作系统的 PC 机，用作服务器端。投票客户端可以采用智能手机或者 PC 机。

测试场景的要求如下：票选唐朝最有影响力的诗人。

② 系统功能测试

初始化阶段，权威认证中心导入候选人名单，设置可选候选人人数，点击“启动投票”按钮，开启投票，发送开始注册命令。如图 5.7 所示。

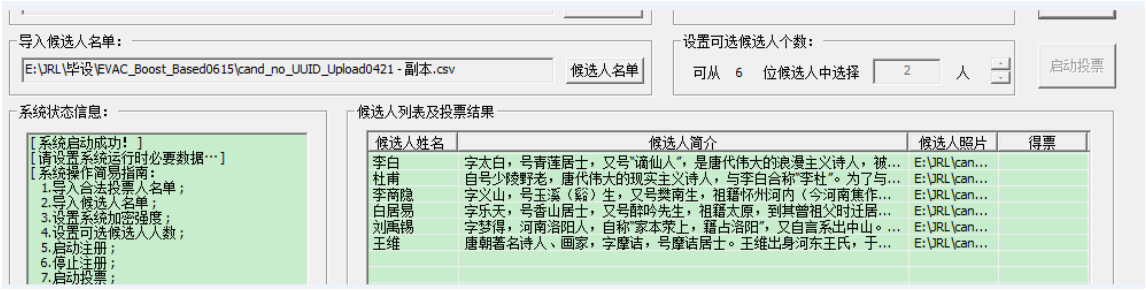


图 5.7 初始化阶段测试图

Fig.5.7 Test chart the stage of initialization

投票者接收到注册命令后，输入唯一的投票凭证，点击“注册”按钮，开启注册工作。当权威认证中心反馈注册成功消息后，点击“投票”按钮，进入投票界面，根据候选人信息选出候选人；点击否则无法进入投票界面进行投票操作。如图 5.8 所示。


(a)投票者注册成功　　(b)获取候选人列表

(c)查看候选人信息　　(d)选择候选人

图 5.8 注册和投票的测试图

Fig.5.8 System test charts of registration and voting

在投票过程中，计票中心对选票进行统计，并记录当前已成功投票人数和未成功投票人数。当投票结束后，计票中心将加密的选票发送给权威认证中心，最后，权威认证中心对选票密文进行处理，给出候选人的得票情况。结果显示如图 5.9 所示。

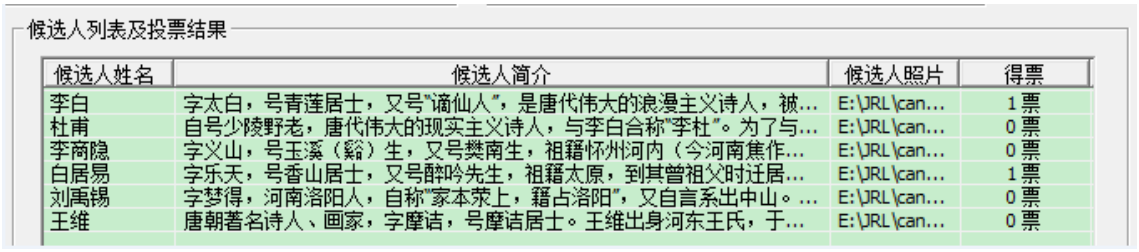


图 5.9 投票结果显示图

Fig.5.9 Show graph of the result of voting

当投票结束后，合法投票者可以验证自己的选票是否被计入。检测结果如图 5.10 所示。


图 5.10 查票结果测试图

Fig.5.10 Test figure of the result of checking a ticket

系统功能测试的结果表明，各个参与实体均能完成相应的工作，满足电子投票方案设计的目标。下面对系统的性能进行测试。

对于一个完善的系统来说，除了满足基本功能要求之外，性能测试是必不可少的一部分。下面分别从整个系统的稳定性和效率等方面做一系列测试。

① 数据传输效率测试

系统分别对客户端和服务器的数据通信速率进行了测试，同时有 100 个投票用户连接服务器，客户端的选票数据传输时间为 0.05s，在系统可接受的范围内。

② 同态加法和乘法的运算开销

因为整个系统是基于 HElib 来实现的，表 5.3 给出 HElib 基础的加法和乘法运算的性能测试。

表 5.3 同态加法和乘法运算开销测试表

Table 5.3 Overhead test table of homomorphic addition and multiplication

| 电路深 L | 模值 m | 加法运算耗时(ms) | 乘法运算耗时(ms) |
|---|---|---|---|
| 35 | 43691 | 0 | 630 |
| 20 | 27305 | 0 | 190 |
| 10 | 11441 | 0 | 50 |
| 5 | 7781 | 0 | 30 |
| 3 | 4051 | 0 | 10 |
| 2 | 4051 | 0 | 0 |

从表中数据可以看出，电路深度 L 对乘法运算效率影响颇大，但是同态加法运算几乎不耗时，这样便为电子投票系统中选票数据密文相加提供了便利。

综上，经过用户的多次测试，反映系统体验度高，系统反应速度较好，具有较好的稳定性。另外，整个系统在整个运行过程中所消耗系统资源都在预期可接受的范围内，达到了电子投票方案的设计目标。

## 5.3 方案总结分析

### 5.3.1 安全性分析

① 选票的秘密性

该方案采用基于 RLWE 问题的全同态加密算法对选票数据进行加密，它的主要优点就是对选票数据密文直接进行加法运算。投票者$voter_i$的选票数据$Ballot_data_i$一直是加密的，即使在计票阶段也没有对单一的选票数据进行解密。投票者在生成选票信息$((ID_i \parallel BN_i \parallel Ballot_data_i)，SIG_i)$的过程中，使用了基于 RSA 公钥密码体制的数字签名技术，这样能够验证选票数据是否合法有效，防止选票数据在传输过程中被攻击或者篡改。而且在统票过程中，利用全同态加密方案 BGV 方案的同态私钥对所有选票密文之和进行解密，因此，整个投票过程中不会泄露任何一张选票的信息。同时无法将该加密的选票无法与某个投票者联系起来，保证了投票者的匿名性。

② 选票的唯一性

投票者$voter_i$在向权威认证中心注册时，权威机构发放的是唯一的选票编号$BN_i$；并且在向计票中心提交选票信息时，计票中心首先判断该投票者是否为第一次提交选票，若不是第一次投票则放弃该选票，而且不合法的投票者提交的选票，计票中心不会对其进行统计；若是第一次投票，则计票中心把它计入合法投票列表，防止合法投票者重复投票。因此该方案具有选票的唯一性。

③ 投票的公平性

投票者在整个投票过程中，并没有向权威认证中心和计票中心泄露有关选票的任何信息。在计票最终结果公布之前，无人知道具体的投票结果，因此方案满足投票的公平性。

④ 投票的完整性

在注册阶段，权威认证中心首先对合法投票者唯一的身份凭证$Pro_i$进行验证，只有认证通过之后，才会分发唯一的选票编号$(ID_i \parallel BN_i)$。同时权威认证中心也会把合法投票者的信息$(ID_i \parallel BN_i)$发送给计票中心，计票中心在进行统票之前，会检查投票者的身份；同时在统计选票时实时地统计成功投票人数和未成功投票人数。所以不会出现作假的投票者投票或者合法投票者被漏掉等问题，保证所有合法投票者的选票都能够被正确计入选票结果，因此方案具有完整性。

⑤ 投票的合法性

每一个投票者都会去注册，并且合法的投票者拥有唯一的选票编号$BN_i$和身份信息$ID_i$，在任何一个环节，机构都会投票者的身份进行验证确保所有的投票者都是合法的，所以不会出现不合法的选票。因此方案满足投票的合法性。

⑥ 投票的可验证性

即是投票者可以验证自己的选票是否被统计。每一个投票者$voter_i$都具有自己的身份信息$ID_i$和用于数字签名公钥 $pk_i$和私钥$sk_i$，并且拥有唯一的选票编号$BN_i$。在投票过程中，投票者独特的信息$(ID_i \parallel BN_i)$，有利于对投票者的身份与签名进行验证；而在验证查票阶段，可以跟踪到该投票者的投票情况，验证选票是否被统计。

⑦ 自计票性

该方案采用基于 RLWE 的全同态加密方案，每个投票者的选票数据都经过了同态公钥 PK 加密，任何一个具有计算功能的第三方都可以统计出最终选票结果$\{sum_1，sum_2，\cdots，sum_M\}$，但又无法得知选票的详细内容。

### 5.3.2 实用性分析

① 方便性

投票者只需从权威认证中心获取所有候选人的信息，然后直接选择候选人生成选票，并发送给计票中心即完成了投票，投票操作非常简单，对投票这段的专业

知识和技能没有要求。另外，一个投票者不需要等待其他投票者完成投票过程，因此方案具有很好的方便性。

② 高效性

方案的投票步骤简单，不要求投票者到指定地点完成投票，同时具有自计票性，不需要对选票进行逐一解密，利用全同态加密的加法同态性对所有选票相加，完成计票操作。

## 5.4 本章小结

本章设计了一个基于 RLWE 问题的全同态加密的电子投票方案，详细分析了各个参与实体在注册、投票、计票和查票验证阶段的具体工作流程。课题组在一定的网络环境中对该方案进行了实现验证，并详细地对方案的安全性和实用性进行分析，分析结果表明，本文所设计的基于 RLWE 全同态加密的电子投票方案完成了预期设计目标。

# 6 总结与展望

## 6.1 本文工作总结

由于在电子投票过程中需要保证选票的匿名性，所以电子投票方案的发展离不开现代密码学技术，而电子投票的发展也推动了密码学的应用，二者是相辅相成的。全同态加密技术的突破性进展，为电子投票方案的改进提供了更多的方法。为了设计更加使用的电子投票方案，本文对全同态加密方案进行研究分析，将基于 RLWE 问题的全同态加密引入到电子投票方案中，设计了一种安全的电子投票方案。

① 分析了电子投票方案和全同态加密的国内外研究现状，对当前国内外基于同态加密的电子投票方案进行了总结。

② 通过对电子投票的特性需求进行分析，确定了方案的设计目标，针对电子投票的安全不高和效率较低等问题，引入全同态加密技术保证投票的匿名性，结合 RSA 数字签名技术，明确了电子投票的总体方案架构。方案主要包括投票者、认证中心、计票中心和公告板四个部分。其中，公告板是各个实体交互信息的媒介。

③ 通过对全同态加密的构造方法、性能和基础应用分析，对比常用全同态加密的安全性和运行效率，分析结果表明基于 RLWE 问题的全同态加密能够有效地满足电子投票的匿名性。

1) 根据全同态加密的定义和原理以及所用到的关键技术，设计基于 RLWE 问题的全同态加密方案；

2) 在同态加密库 HElib 库基础上，对基于 RLWE 问题的全同态加密方案方案进行验证。根据实验结果表明通过选择合理的安全参数和电路深度能够达到安全性和效率的折中。

3) 对比常见的全同态加密方案，根据实际的电子投票情况，确定将基于 RLWE 问题的全同态加密方案应用到电子投票方案中，能够保证电子投票的匿名性。

④ 课题组将方案在系统上进行验证，分别对注册、投票和验票等基本功能进行测试，同时对系统的性能进行了测试，经验证设计的电子投票方案达到了预期目标。

## 6.2 下一步研究方向

设计一个高效安全并且实用强的电子投票方案是一项繁琐的工作，虽然本文最终实现了一个匿名可验证的电子投票，但是有些问题仍然有待改进，它们主要表现在以下几个方面：

① 文中采用新型的 BGV 方案和 RSA 数字签名来满足整个系统的匿名性和安全性；但是二者运算量较大且计算复杂，对于大型投票活动，不能够满足其效率要求；需要算法进行加速，是接下来要重点研究的内容。

② 本文对电子投票的安全性都是从理论知识角度来说的，没有给出严格的证明。对电子投票方案的安全特性进行形式化分析给出严谨的科学证明，是下一步研究的重点。

# 致　谢

时光蹉跎，三年的研究生生活很快地拉下了帷幕，回顾这三年的学习生活，收获颇丰。其中，基于同态加密的电子投票方案设计与实现这个项目，无论是技术层面还是心理方面，都是我得到了飞速的成长。我将这个项目的开发经历视为人生重要的财富，因为这个项目，我的专业知识和理论实践技术水平日益成熟，项目开发以及参加比赛的紧迫感也增加了自己对于工作的责任感，同时在项目开发过程中增加了面对困难与挫折的勇气。

在此，首先，感谢何伟教授、张玲教授和林英撑老师为我提供了参与这个项目开发的机会。在我的研究生学习期间，三位老师给我提供了许多科研上的指导性建议和意见，使得我克服了许多困难，并且三位老师严谨的工作态度也为我树立了好的榜样。其次，感谢项目组的李仁杰、杜志洲和孟庆瑞同学，本项目的成功离不开大家的共同努力，团队的合作使得我们解决了很多的难题。最后，感谢我亲爱的父母，你们二十多年来悉心的教导，诚挚的关爱给了我不断前进的动力，你们面对自己事业的专注与成就让我树立了人生的目标，也激励我在面对繁重的科研任务的时候，保持责任感、恒心与毅力。深深感谢所有帮助和关心我的老师、家人和朋友。

刘雷燕

二〇一七年四月　于重庆

# 参考文献


[1] Chaum D L . Untraceable electronic mail , return addresses and digital pseudonyms[J]. Communications of the ACM，1981，24(2)：84-88.

[2] Dan B，Golle P. Almost entirely correct mixing with applications to voting[C]. ACM Conference on Computer and Communications Security，CCS 2002，Washington，Dc，Usa，November. DBLP，2002：68-77.

[3] 高虎明，王继林，王育民. 一个基于 Mix net 的电子投票方案[J]. 电子学报，2004，32(6)：1047-1049.

[4] Yun S H，Lee S J. An electronic voting scheme based on undeniable blind signature scheme[C]. IEEE，2003 International Carnahan Conference on Security Technology，2003. Proceedings. IEEE，2003：163-167.

[5] Wang S，Fan H，Cui G. A proxy blind signature schemes based DLP and applying in e-voting[C]. International Conference on Electronic Commerce，Icec 2005，Xi'an，China，August. DBLP，2005：641-645.

[6] 胡海燕. 基于盲签名的电子投票方案的研究与实现[J]. 科教导刊：电子版，2016(9)：138-138.

[7] Paillier P. Public-Key cryptosystems based on discrete logarithms Residues[J]. Eurocrypt ’99 Lncs，1999.

[8] Wang C， Leung H F . A secure voter-resolved approval voting protocol over internet[C]. International Conference on Electronic Commerce，Icec 2005，Xi'an，China，August. DBLP，2005：646-652.

[9] Baudron O，Fouque P A，Pointcheval D，et al. Practical Multi-candidate election system[J]. In PODC，2001:274-283.

[10] Parkes D C，Rabin M O，Shieber S M，et al. Practical secrecy-preserving，verifiably correct and trustworthy auctions[C]. International Conference on Electronic Commerce：Imitations to Conducting Successful Business on the Internet，2006，Fredericton，New Brunswick，Canada，August. DBLP，2006：70-81.

[11] 张虎强. 基于 ElGamal 加密同态性的电子投票系统研究[D]. 中国科学技术大学，2007.

[12] 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.

[13] Gentry C. A fully homomorphic encryption scheme[C]. Stanford University. 2009.

[14] Smart N P，Vercauteren F. Fully homomorphic encryption with relatively small key and ciphertext sizes[J]. Lecture Notes in Computer Science，2010，2009：420-443.

[15] Van Dijk M，Gentry C，Halevi S，et al．Fully homomorphic encryption over the integers[C]．EUROCRYPT．Springer-Verlag，2010：24-43．

[16] Stehl éD，Steinfeld R．Faster Fully Homomorphic Encryption[M]．Advances in Cryptology - ASIACRYPT 2010．Springer Berlin Heidelberg，2010：377-394．

[17] Gentry，Craig，Halevi，Shai．Implementing Gentry's fully-homomorphic encryption scheme[C]．International Conference on Theory and Applications of Cryptographic Techniques：Advances in Cryptology．Springer-Verlag，2011：129-148．

[18] Gentry C，Halevi S．Fully homomorphic encryption without squashing using Depth-3 Arithmetic Circuits[C]．Foundations of Computer Science．IEEE，2011：107-109．

[19] Han J L，Ming Y，Wang Z L．Fully homomorphic encryption scheme extended to large message space[C]．First International Conference on Instrumentation，Measurement，Computer，Communication and Control．IEEE，2011：533-536．

[20] Coron J S，bastien，Naccache D，et al．Public key compression and modulus switching for fully homomorphic encryption over the integers[C]．International Conference on Theory and Applications of Cryptographic Techniques．Springer-Verlag，2012：446-464．

[21] Chen Y，Nguyen P Q．Faster algorithms for approximate common divisors：breaking fully-homomorphic-encryption challenges over the integers[C]．International Conference on Theory and Applications of Cryptographic Techniques．Springer-Verlag，2012：502-519．

[22] 汤殿华，祝世雄，曹云飞．一个较快速的整数上的全同态加密方案[J]．计算机工程与应用，2012，48(28)：117-122．

[23] Goldwasser S，Kalai Y T，Popa R A，et al．How to Run Turing Machines on Encrypted Data[M]．Advances in Cryptology – CRYPTO 2013．Springer Berlin Heidelberg，2013：536-553．

[24] Goldwasser，Shafi，Kalai，et al．Reusable garbled circuits and succinct functional encryption[J]．Proceedings of the Annual Acm Symposium on Theory of Computing，2013：555-564．

[25] Cheon J H，Kim J，Lee M S，et al．CRT-based fully homomorphic encryption over the integers[J]．Information Sciences An International Journal，2015，310(C)：149-162．

[26] 熊婉君，韦永壮，王会勇．一个基于整数的全同态加密改进方案[J]．密码学报，2016，3(1)：67-78．

[27] 李子臣，张峰娟，王培东．一种短密钥高效全同态加密方案[J]．计算机应用研究，2017(2)：487-489．

[28] Ho T P T，Chang C H．Accelerating residue-to-binary conversion of very high cardinality moduli set for fully homomorphic encryption[C]．Circuits and Systems．IEEE，2017．

[29] 代洪艳，丁勇，吕海峰，等．一种较快速的基于整数的全同态加密方案[J]．计算机应用研究，2015(11)：3448-3451．

[30] Brakerski Z，Vaikuntanathan V．Efficient Fully homomorphic encryption from (standard) LWE[C]．Foundations of Computer Science．IEEE，2011：97-106．

[31] Regev O．On Lattices，Learning with errors，random linear codes，and cryptography[J]．Journal of the ACM，2009，56(6)：34．

[32] Brakerski Z，Vaikuntanathan V．Fully homomorphic encryption from Ring-LWE and security for key dependent messages[J]．2011，6841：505-524．

[33] Brakerski Z，Gentry C，Vaikuntanathan V．(Leveled) fully homomorphic encryption without bootstrapping[C]．Innovations in Theoretical Computer Science Conference．ACM，2012：309-325．

[34] Brakerski Z．Fully Homomorphic Encryption without modulus switching from classical GapSVP[C]．Cryptology Conference on Advances in Cryptology --- CRYPTO．Springer-Verlag New York，Inc．2012：868-886．

[35] Pez-Alt A，Tromer E，Vaikuntanathan V．On-the-fly multiparty computation on the cloud via multikey fully homomorphic encryption[C]．Forty-Fourth ACM Symposium on Theory of Computing．ACM，2012：1219-1234．

[36] Gentry C B，Halevi S．Efficient implementation of fully homomorphic encryption：US，US8565435[P]．2013．

[37] Brakerski Z，Gentry C，Halevi S．Packed Ciphertexts in LWE-Based Homomorphic Encryption[M]．Public-Key Cryptography – PKC 2013．Springer Berlin Heidelberg，2013：1-13．

[38] 陈智罡，石亚峰，宋新霞．全同态加密具体安全参数分析[J]. 密码学报，2016，3(5)．

[39] Duc M A．The learning with error problem[J]．General Information，2012．

[40] Lyubashevsky V，Peikert C，Regev O．On ideal lattices and learning with errors over rings[J]．Journal of the ACM (JACM)，2010，60(6)：43．

[41] Sun X，Zhang P，Sookhak M，et al．Utilizing fully homomorphic encryption to implement secure medical computation in smart cities[J]．2016．

[42] Bonnoron G，Fontaine C，Gogniat G，et al．Somewhat/Fully homomorphic encryption: implementation progresses and challenges[J]．2017．

[43] Ran C，Raghuraman S，Richelson S，et al．Chosen-Ciphertext secure fully homomorphic encryption[J]．2017．

[44] 李顺东，窦家维，王道顺. 同态加密算法及其在云安全中的应用[J]. 计算机研究与发展，2015，52(6)：1378-1388．

[45] 项世军，罗欣荣，石书协．一种同态加密域图像可逆水印算法[J]．计算机学报，2016，39(3)：571-581．

[46] Demirel D，Schabhüser L，Buchmann J．Verifiable Computing from Fully Homomorphic Encryption[M]．Privately and Publicly Verifiable Computing Techniques．Springer International Publishing，2017．

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

[48] A．Fujioka，T．Okamoto，K．Ohata．A practical secret voting scheme for large scale election [A]．J．Seberry(Eds.)．AUSCRYPT'92 [C]，Berlin Heidelberg：Springer-Verlag，1993：244-251．

[49] Cramer R，Gennaro R，Schoenmakers B．A secure and optimally efficient multi-authority election scheme[C]．International Conference on Theory and Application of Cryptographic Techniques. Springer-Verlag，1997：103-118．

[50] Kim S，Oh H．A new universally verifiable and receipt-free electronic voting scheme using One-Way untappable channels[C]．The Workshop on Content Computing．DBLP，2004：337-345．

[51] Morales-Rocha V，Soriano M，Puiggalí J．New voter verification scheme using pre-encrypted ballots[J]．Computer Communications，2009，32(7–10)：1219-1227．

# 附　录

## A．作者在攻读硕士学位期间参与课题及成果

[1] 汽车驾驶员疲劳检测系统设计，纵向课题，该项目由“重庆市研究生科研创新项目”资助，项目编号为 CYS14026，参与时间为 2015.01-2015.12；

[2] 一种基于同态加密的匿名可验证电子投票方案设计，纵向课题，该项目由“重庆市研究生科研创新项目”资助，项目编号为 CYS185，参与时间为 2016.04-2017.03。

## B．作者在攻读硕士学位期间参与的竞赛及获奖情况

[1] 汽车驾驶员疲劳检测系统设计，荣获“华为杯”第十届中国研究生电子设计竞赛西南赛区二等奖、商业专项赛全国二等奖；

[2] 一种基于同态加密的匿名可验证电子投票方案设计，荣获“华为杯”第十一届中国研究生电子设计竞赛西南赛区二等奖；

[3] 一种基于同态加密的匿名可验证电子投票方案设计，荣获“Altera 亚洲创新大赛”优胜奖。