

**本科毕业设计（论文）**

|  |  |
| --- | --- |
| **题目：** | 关于隐私保护分布式统计的算法研究 |

|  |  |  |
| --- | --- | --- |
| **学号** | ： | 1800710238 |
| **姓名** | ： | 王智坚 |
| **学院** | ： | 数学与计算科学 |
| **专业** | ： | 数学与计算科学学院 |
| **指导教师** | ： | 张必山 |
| **指导教师职称** | ： | 副教授 |

2022年5月6日

摘 要

在分布式统计计算中，若自身的设备无法处理庞大的计算量，可交由第三方服务计算商代为处理.若数据为隐私、机密数据，直接发送可能会造成数据的泄露，引发不可估量的后果.所以将数据加密后，第三方服务计算商对加密后的密文进行运算，接着将结果返回这样保证了数据的隐私性、正确性和机密性.本文通过全同态加密BFV加密算法加密数据，在半诚实敌手模型下，每个计算参与方拿到密文的一部分，对密文进行同态操作，接着返回同态操作之后的密文给数据所有者.最后对BFV算法在分布式系统下的正确性，安全性，局限性进行分析.

**关键词**：同态加密；安全多方计算；半诚实敌手模型；全同态加密.

Abstract

In distributed statistical computing, if its own equipment cannot handle the huge amount of computation, it can be handled by a third-party service computing provider. If the data is private and confidential, sending it directly may result in data leakage and incalculable consequences. Therefore, after encrypting the data, the third-party service computing provider operates on the encrypted ciphertext, and then returns the result, which ensures the privacy, correctness and confidentiality of the data. In this paper, data is encrypted by fully homomorphic encryption, and two different schemes are constructed for the case of one data provider and multiple third-party computing service providers, and multiple data providers and one third-party computing service provider. The article gives the complexity, correctness and security of the scheme.

**Key words**：Homomorphic encryption; secure multi-party computation; secure computing protocol; fully homomorphic encryption

目 录

[1 绪论 1](#_Toc102046580)

[1.1 研究背景及意义 1](#_Toc102046581)

[1.2 研究现状 1](#_Toc102046582)

[2 理论与本文工作 3](#_Toc102046583)

[2.1 数据通过何种方式加密. 3](#_Toc102046584)

[2.2 本文结构 3](#_Toc102046585)

[3 理论基础 3](#_Toc102046586)

[3.1 背景知识 3](#_Toc102046587)

[3.2 加密算法原理 4](#_Toc102046588)

[3.2.1 背景介绍 4](#_Toc102046589)

[3.2.2 使用环上的多项式加密 7](#_Toc102046590)

[3.3 半诚实敌手模型 11](#_Toc102046591)

[4 实验概述 11](#_Toc102046592)

[4.1 实验环境 12](#_Toc102046593)

[4.1.1 环境要求和配置 12](#_Toc102046594)

[4.1.2 实验数据参数 12](#_Toc102046595)

[4.1.3 分析依据 12](#_Toc102046596)

[5 算法的分析 12](#_Toc102046597)

[5.1 同态加法 12](#_Toc102046598)

[5.2 正确性 13](#_Toc102046599)

[5.3 安全性 14](#_Toc102046600)

[5.4 局限性 14](#_Toc102046601)

[6 结束语 18](#_Toc102046602)

[谢 辞 19](#_Toc102046603)

[参考文献 20](#_Toc102046604)

# 绪论

## 研究背景及意义

信息大爆炸的今天，海量的数据扑面而来.面对这些激增的数据，如果自己的设备无法处理，那么就可以交由有能力的第三方代行计算，这时就涉及到了数据的隐私与机密的问题.例如，一款软件若要在本地处理数据，若用户设备性能低，在本地处理会大大消耗设备资源，造成使用卡顿，用户体验性极差.而将这些数据提交到云服务器上去计算，则能大大解决这一问题.这时迎来了有一个问题，若将用户的隐私数据直接提交给云服务器，就会造成数据的泄露，这就是大数据下的隐私问题.而将数据进行加密，再安全传输协议发送至云服务器，由云服务器代为处理，这也许是一个好的办法.

## 研究现状

针对密文计算问题，如果能将数据进行加密，并且对加密后的数据执行同样的加减乘除操作，若是此时将结果进行解密仍能得到相同的结果，那么这就叫做同态加密，一种先计算后解密等同于先解密后计算的方案——同态加密，是由Rivest等人[1]在上世纪七十年代提出的。这使得数据能由多方提供给云服务器进行密文计算，对数据的机密性，完整性和隐私性得到了有效的保护。同态加密方案支持对密文的计算，并能由密文的计算结果解密得到正确的明文计算结果。在后来的同态加密方案中，有些只支持加法同态，如Paillier方案[2]和Goldwasser-Micali方案[3]；有些只支持乘法同态，如Unpadded-RSA方案[4]和ElGamal方案[5]。而能同时支持加法和乘法运算的加密方案则较少。Boneh[6]等人提出了Boneh-Goh-Nissim加密方案，能够支持任意次的加法操作，但只能支持一次乘法操作。Centry[7,8]提出了一种基于理想格的加密方案，并利用提提出的“Bootstrappable”技术，通过对密文的重加密使密文支持任意次数的同态运算，是真正意义上的全同态加密，也称为全同态加密的研究奠定重要基础。后续的很多同态加密方案[7~13]也都基于Centry的“Bootsrappable”技术，这些方案对文献[7]都有不同程度的改进。如Smart等人[9]改用整数和多项式实现全同态加密，减少了密文和密钥的长度，Dijk等人[10]使用整数进行加密，更利于理解。但由于“Bootstrappable”技术本身的复杂性，即使具有较低安全性时，一次“Bootstrappable”操作也需要大约30s的时间[13]，因此，这些加密方案都较难应用到实际中，后来，Centry等人[14,15]从加强全同态算法中的自展技术、全同态加密算法的解密循环的分解技术、实现方法等方面展开了研究，虽然降低了同态加密的复杂性，但仍较难于实际应用。黄汝维等人[16]针对云计算环境的隐私保护问题提出了基于向量和矩阵运算的加密可计算方案（CESVMC），算法运行效率较高，但其算术运算方案不支持加法和乘法的混合匀速那，且仅支持一次乘法和除法匀速那，运算后的密文长度会增大，而且需要记录密文经过的运算类型以完成解密。

对于同态加法的安全性来说，满足选择明文不可区分(IND-CPA)安全是十分重要的。上述的ElGamal和作为应用最广的Pailler加密系统满足此安全性，但EliGamal的密文会成倍扩张，这是它的不足之处。Goldwasser-Micali在二次剩余困难问题上也同样满足此安全，但作为异或同态加密系统，每次操作只能为单比特，由此加密效率大打折扣。渐渐的，后续在安全的基础上出现了许多的浅同态加密方案，作为代表的Boneh在理想成员判定困难假设下设计的加密方案，能执行若干次加法运算和解决2NF问题，但只能进行一次乘法运算，且解密时需要搜索解密，由此基于2NF的计算协议效率可以说是很低。时间往后接着推移，身处IBM的研究员Craig Gentry[22]发表一篇论文于STOC，他解决了一项棘手的数学问题，该问题自几十年前公钥加密发明以来，一致困扰着科学家们。他基于“理想格idea lattice”的数学对象，使人们可以充分操作加密状态的数据，即可以在不解密的情况下对加密数据进行任何可以在明文上的计算，对加密后的信息仍能深入和无限的分析，保证数据的隐私性、完整性和保密性。这个加密技术被称为全同态加密(full homomorphic encryption)。

目前对密文计算在分布式统计方面研究较少，马飞，蒋建国[23]在分布式计算的基础上，运用Pailier同态加密提出了在SMH模式下，采用CClient，KClient，SServer的拓扑结构进行统计分析的计算方案.本文想运用BFV全同态加密算法在分布式统计情况下，研究其算法的正确性，安全性和局限性.

# 理论与本文工作

## 数据通过何种方式加密.

BFV算法加密方案来源于文章 "Somewhat Practical Fully Homomorphic Encryption"，它是基于 RLWE (Ring-Learning With Errors)难题的全同态加密方案.密文形式为两个模为的多项式，依据多项式相同幂级项相加的特性，可应用于分布式系统，交由多个计算参与方计算，且计算参与方之间互不干扰.

## 本文结构

第三章部分本文的相关理论基础.第二部分分析计算协议对数据的安全.第三部分对方案正确性，安全性，复杂性以及局限性进行分析.

对于本文工作.介绍了在分布式情况下，基于半诚实模型，数据所有者于计算参与方之间时如何完成委托计算的过程，以及数据所有者在保护数据隐私的情况下，如何对数据进行加密，以至于保证数据不被泄露的BFV全同态加密算法.最后模拟在多个计算参与方进行多次同态加法之后，对算法进行正确性，安全性，局限性分析.

# 理论基础

## 背景知识

同态加密是一种加密形式，具有额外的评估能力，可以在不访问密钥的情况下计算加密数据.这种计算的结果仍然是加密的.同态加密可以看作是公钥密码学的扩展.同态是指代数中的同态，加密和解密函数可以被认为是明文空间和密文空间之间的同态.同态加密的方案中，有密钥生成算法，加密算法，解密算法

1）密钥生成算法.根据明文空间的随机数生成密钥.

2）加密算法.表示明文空间，表示密文空间，利用密钥加密明文，返回密文.

3）解密算法.利用密钥解密密文，返回明文

对于明文空间上的多项式

|  |  |  |
| --- | --- | --- |
|  |  | (3-1) |

及数据，使用密钥生成算法，数据经过加密算法加密后，得到密文.这时候第三方对密文进行计算处理，得到加密后的结果，第三方将结果返回给数据拥有者，数据拥有者通过私钥，结合解密算法就可以将结果还原为明文形式，即

|  |  |  |
| --- | --- | --- |
|  |  | (3-2) |

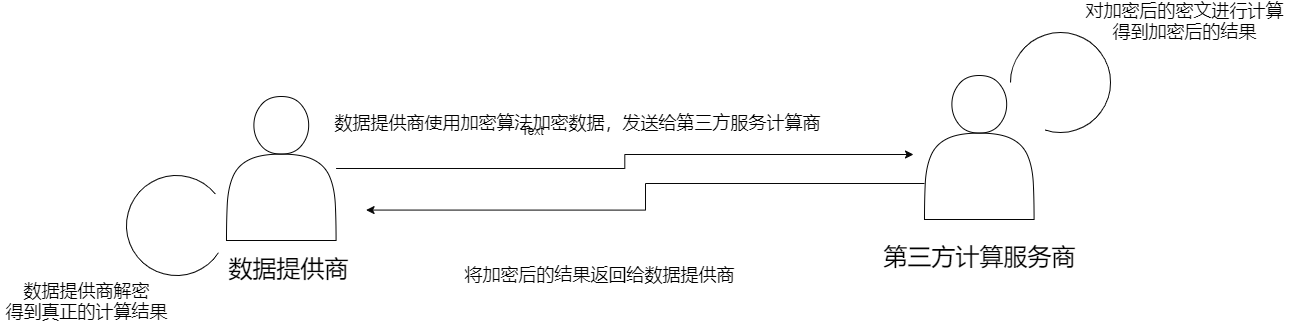


图 3‑1加密解密操作流程图

加密后进行加法运算得到的结果解密后与明文运算的一致，称为加法同态加密.同理满足减法、乘法的称为减法同态加密，乘法同态加密，而能够对密文进行任意计算的称为全同态加密.

## 加密算法原理

BFV加密是主流的基于容错学习问题的全同态加密方案之一，其主要思想是将明文放在密文的高位，通过整除的方式，去除低位的噪声.比如有一个BFV的密文，私钥，则BFV的解密为，其中是解密噪声，显然，当噪声足够小的时候，我们可以通过除以取整获得明文.

### 背景介绍

对于一个简单整系数多项式

|  |  |  |
| --- | --- | --- |
|  |  | (3-3) |

对系数取模.假设，如9加6得到3，这就好比一个12月份的日历，经过一年，但观察其月份仍在12月之中.之后多项式中的所有系数都是这样处理的.

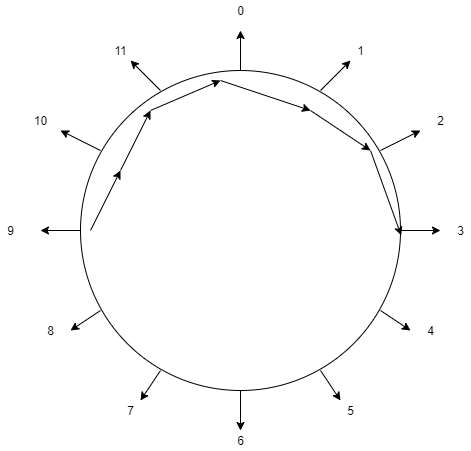


图 3‑2的多项式环

由于计算机取模的特性，一个负数-3对取模，得到的是9，若我们想拥有负数的系数空间，那么可以自行定义其取模方法，将数字处于-5到6之间，那么我们就可以对负数进行求解。但是这只是一个方便系数，对于余数-1和余数11之间是没有区别的。同时，若两个多项式相乘，那么多项式的最高次的次数将会增加，若进行多次相乘，则多项式的规模想不断增大，对此，余数的思想也同样可以使用到多项式本身。

这时，由BFV加密方案，定义一个多项式模，它是由一个特殊多项式组成，如同多项式的系数模一般，次数为4的多项式与次数为14的多项式相乘，对次数为16的多项式取模，得到了一个次数为2的多项式。而定义的多项式模的形式为，那么对于上述的多项式模可知取，并且规定了，因此多项式为。

接下来讨论对于多项式模之后得到的余数，若多项式存在幂为16或更高次的幂，那么将其对多项式模取模之后都会消去，那么我们讨论的幂也就只有从到的多项式.运用数学公式可以表示为，这说明将多项式的幂归约到了幂之间，而可以被替换。

所以接下来考虑的多项式都是这种形式的

|  |  |  |
| --- | --- | --- |
|  |  | (3-4) |

其中这16系数（即）中的每一个范围都是从0到，我们可以用系数的环面来说明，如下所示

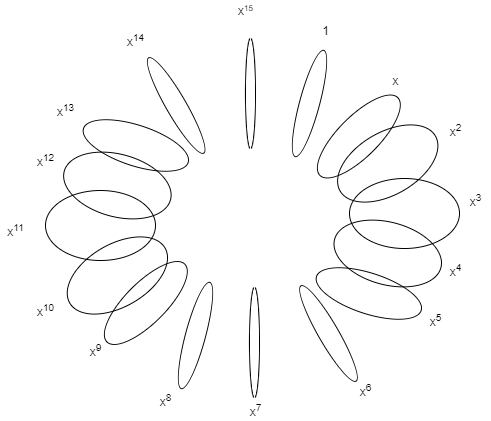


图 3‑3系数环面

当我们执行加密方案时，涉及到多项式的乘法计算，会将两个的幂次相乘，例如将与相乘会得到结果。由BFV加密方案规定，需要将得到的多项式对多项式模进行取模，若多项式模定义为，那么余数只需要在系数环面上从转过直到即可。但是根据BFV加密方案，定义的多项式模——如上所示，常数项1使得余数的系数发生了变化，这有助于进一步干扰乘法得到的结果。

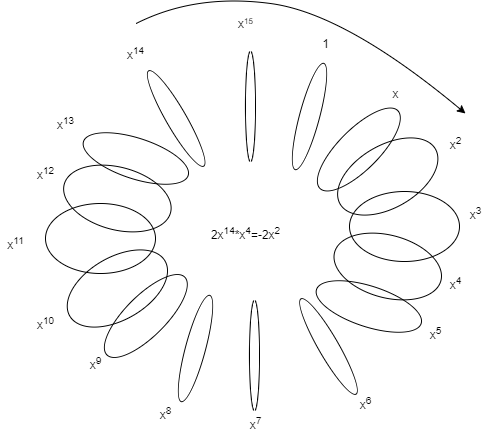


图 3‑4环面变化

由图 3‑4可知，因其幂次加上4，环面由此向前旋转四个到达，此时我们得到结果，又因为系数模，则最后的结果为（若我们想得到存在负数的结果，那么取值范围可以是-12到11，也就是说也是成立的），

### 使用环上的多项式加密

由前文所述，我们了解了BFV加密方案中的多项式系数环面的定义，接下来了解加密方案中的加密与解密的原理。由密码学基础知识可知，加密解密需要一对密钥（公钥和私钥），那么我们先了解其是如何生成私钥与公钥的，接着能更好的理解其加密与解密过程。

1)私钥和公钥

若将明文进行加密使其转换为密文，那么需要生成一个私钥，接着利用私钥派生出一个公钥，最后使用公钥将明文进行加密。

对于明文空间的多项式，其经过多项式模的取模，且其系数在系数模之中。明文通过私钥生成的公钥加密之后，得到两个环上的多项式，且具有相同的多项式模，得到的两密文多项式与明文不相同的是，其系数模为，且远大于。

如果我们假设，无论是明文还是密文，那么就会存在个系数，为了计算的安全，需要系数模取得大，令，同时，密文多项式的系数就需要比系数模还要大，如或更大。

为了表述直观但又保证一定的安全性，我们使、和。

对于私钥，它是由系数为-1、0和1组成的多项式，接下来我们随机生成一个私钥，用表示。

|  |  |  |
| --- | --- | --- |
|  |  | (3-5) |

为了接下来生成公钥，还需生成一个随机多项式，但其系数模需仍为 ，生成的多项式用表示。

|  |  |  |
| --- | --- | --- |
|  |  | (3-6) |

此外，为了加密的安全，引入了一个“小”的噪声多项式来扰乱其密文系数分布。噪声多项式的系数将从离散的高斯分布中提取，但是此多项式仅使用一次，不必保存。

|  |  |  |
| --- | --- | --- |
|  |  | (3-7) |

由BFV加密方案的规定，生成的公钥由两个多项式组成，且具有多项式模和系数模q的.

对于上面给出的示例，公钥的第一个多项式被构造为

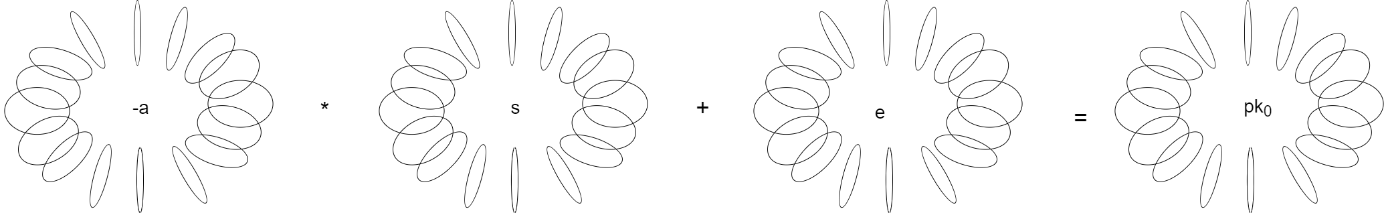


图 3‑5公钥生成

|  |  |  |
| --- | --- | --- |
|  |  | (3-8) |

由上图可知，将随机多项式取负号，接着与系数为-1，0和1的私钥相乘，同时执行加密方案的取模操作，接着再与噪声多项式相加，同理，一样需要取模。而取模操作有效的打乱了的所有系数，由由于噪声多项式的加入，使得公钥的中的私钥得到有效的隐藏，保护。

对于公钥中噪声多项式的加入，让的系数得到有效的保护，此时若从公钥中找的私钥的可能性将很难。若选择去掉噪声多项式，就会很容易计算出私钥，而噪声多项式系数的大小又是一个难题，太大使得通过私钥解密出错误的结果，太小不能保护，所以噪声多项式的系数选择是十分关键的。

2)加密

将明文加密为密文，这个过程如同生成公钥一般，将一个系数模为的多项式通过引入噪声多项式扰乱系数的分布，最后得出一对系数模为的多项式。接下来，我们尝试使用一个简单的多项式作为明文（称为消息）——。

同样的，这次我们引入三个“小”的多项式，两个噪声多项式的系数都取自离散高斯分布，另一个多项式同私钥一般，系数只有-1、0和1，我们将其称为。

|  |  |  |
| --- | --- | --- |
|  |  | (3-9) |
|  |  | (3-10) |

和

|  |  |  |
| --- | --- | --- |
|  |  | (3-11) |

这些多项式只在加密过程中使用，然后丢弃.

密文是由两个多项式组成的，通过如下计算得到

|  |  |  |
| --- | --- | --- |
|  |  | (3-12) |

通过观察密文的第一个多项式可以发现，上述给定的消息其系数模为t，而在密文的计算中，将其缩放为了(即1280)，让其处于的范围之中，对于后续的同态加法，同态减法能保持一致性，同时又能将消息进行掩盖。与公钥的第一个多项式相乘，而的随机性又增加了密文的安全性，使得每此加密后都能产生不同的密文。

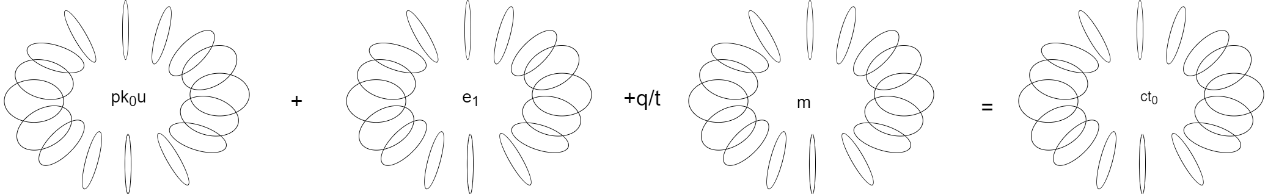


图 3‑6通过公钥加密明文为密文

由于消息只与系数模和相乘，以比例的形式存在于密文之中，噪声多项式掩盖了其系数分布，使得同态加法与同态乘法得以实现。

使用上面给出的多项式显式地计算密文的第一个元素

|  |  |  |
| --- | --- | --- |
|  |  | (3-13) |

将密文中的公钥展开，我们可以看到密文的第一个元素为

|  |  |  |
| --- | --- | --- |
|  |  | (3-14) |

由公式(3-14)可知，是“大”的多项式，能将消息进行有效的隐藏

密文的第二个元素是这样计算的:

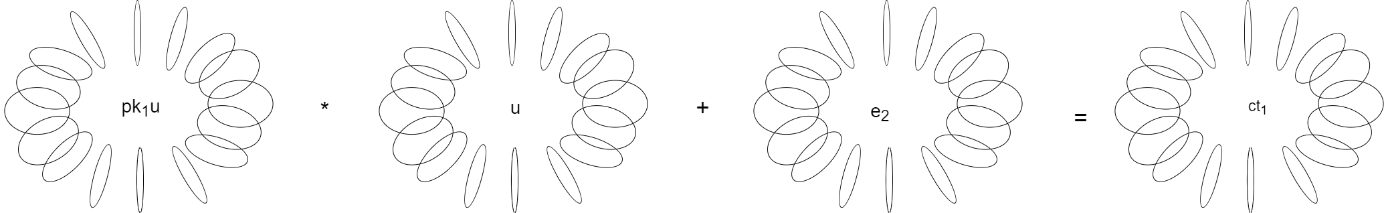


图 3‑7密文多项式的第二项

|  |  |  |
| --- | --- | --- |
|  |  | (3-15) |

将密文中的公钥展开，观察密文的第二个多项式可知，若其乘以私钥，那么我们就可以得到，其中的与密文中的第一个多项式相似，所以当我们解密时，可以消去这一干扰因素。

综上所述，密文可以用公钥(public key)、私钥(private key)、掩码(mask)、噪音(noise) 和消息(message)表示为

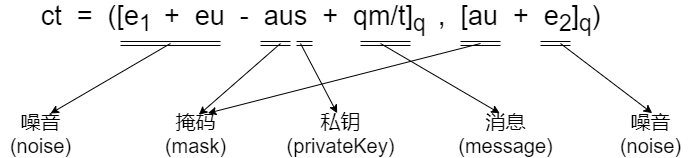


图 3‑8密文的组成

3)解密

如上所述，将密文中的第二个多项式乘以私钥我们可以得到与第一个多项式相同的项，所以，在解密时，我们计算，消除“大”的多项式的影响，只剩下了，此时若噪声多项式的系数不太大，我们就可以通过缩放系数将消息还原。

明确地，

|  |  |  |
| --- | --- | --- |
|  |  | (3-16) |

通过观察多项式可以发现，除了我们给定的消息的系数外，其余的所有系数都小于与，此时我们将多项式系数缩放至范围内，那么我们就得到

|  |  |  |
| --- | --- | --- |
|  |  | (3-17) |

将系数进行四舍五入取整，多项式就会变为我们的明文消息，由此来恢复我们的信息。

把它们放在一起，我们通过如下计算来解密密文

|  |  |  |
| --- | --- | --- |
|  |  | (3-18) |

⌊⌉表示舍入到接近的整数(四舍五入).

可以发现，当我们对系数进行缩放操作的时候，如果噪声多项式的系数过大，缩放之后导致解出一个与正确值不同的整数，接着解密就会悄无声息的失败了。在本次例子中，最大的噪音为，所有本次将会正确的解密出消息

## 半诚实敌手模型

半诚实敌手模型应用于多方安全计算中，而对于安全多方计算拥有两种安全模型，一是半诚实敌手模型(The Semi-Honest Model)，二是恶意敌手模型(The Malicious Model).

按照协议的规定并诚实的执行下去的计算参与方，这就是半诚实敌手模型。但是，执行协议的过程中计算参与方的输入输出和运行过程中得到的信息可能会被窃取，被恶意攻击者监听到。在生活中，往往被动攻击是占攻击的大部分，根据成本和开销，主动攻击相对来说更复杂和困难，由此，很多协议都是基于半诚实敌手模型下的安全而建立的，且满足半诚实敌手模型是安全多方计算的基础条件。

# 实验概述

通过matlab软件编写私钥、随机噪声多项式、公钥、加密、解密函数代码，接着通过matlab的deploy命令讲编写的函数打成jar包，最后在Java语言平台上运用apache开源的mina框架中的ServerSocket与ClientSocket模拟分布式情况，观察分析其同态操作效果.

## 实验环境

### 环境要求和配置

硬件配置：Dell笔记本电脑；Windows 10 家庭中文版；Intel(R) Core(TM) i5-9300H CPU @ 2.40GHz 2.40GHz.

代码语言：matlab，Java.

编译工具：matlab2017R，IntelliJ IDEA 2021.2.

### 实验数据参数

模多项式次数，模系数以及系数模

### 分析依据

通过数百次的模拟，统计计算出其在分布式情况下的加密后的密文在多次同态操作后的解密成功率，之后分析其正确性，安全性以及局限性.

# 算法的分析

## 同态加法

在分布式系统下，将一个明文输入数据加密后得到一个多项式的密文.可以根据计算参与方的数量，决定BFV加密算法的多项式模中参数的选择.例如，拥有16个计算参与方，此时取，则生成的密文产生了两个最高次次数不超过16的多项式，将两个多项式写成一个2行16列的向量，例如密文

|  |  |  |
| --- | --- | --- |
|  |  | (5-1) |

|  |  |  |
| --- | --- | --- |
|  |  | (5-2) |

将其转换为矩阵形式

(5-3)

将得到的矩阵对同一列的进行拆分，保留行数，结果得到

|  |  |  |
| --- | --- | --- |
|  |  | (5-4) |

的密文对.将每个密文对分发给每个计算参与方，参与方拿到密文对后，对其进行同态加法操作.

由于这是单个数据加密得到的密文，若有个数据进行加密，那么就能得到个密文，那么就会有个2行列的矩阵，也将其对应的拆分，发送给参与方.那么此时的计算参与方拥有个2行1列的向量

|  |  |  |
| --- | --- | --- |
|  |  | (5-5) |

当计算参与方对每一个进行相加，得到一个2行1列的列向量

|  |  |  |
| --- | --- | --- |
|  |  | (5-6) |

将此向量返回给数据所有者，即可完成同态加法的操作.

## 正确性

对于同态加法.数据所有者加密得到的多项式密文可以看作一个维的矩阵，对多项式密文的加法操作，等同于对矩阵的加法操作，再将其细分，观察其内部，可以发现：

1)计算参与方拿到的个维向量数据对其进行加法操作，在矩阵计算中，属于不同矩阵中同一位置元素进行相加得到结果.所以对于计算参与方通过加法操作密文数据，得到的结果是正确的.

2)对于将密文多项式看作维的矩阵.多项式的加法中，幂次相等的项相加与矩阵的同一位置元素相加的操作是一致的.那么此过程是保证了同态加法的正确性.

而BFV加密算法方案是拥有同态乘法的全同态加密，对于同态乘法包括两个步骤：第一步很简单，基本上是将多项式和 相乘，然后按 缩放.但问题是我们最终得到的密文是由3个环元素组成的，而不是2个.且由于多项式乘法的性质，一个计算参与方拥有的数据只是这一幂级的系数，无法拥有另一个幂级的系数，这就需要计算参与方之间的通信.若要完成乘法操作，那么获得其他幂级的系数就相当于获取了整个密文的所有系数，那么对于分布式系统来说，这就南辕北辙了.

## 安全性

为所有参与方都是半诚实的，且使用的加密体制是安全的，计算参与方获取到的为加密数据的一部分，此时计算参与方是无法推算出原始数据，保证其安全性.

## 局限性

对BFV加密算法而言，其本质是通过对多项式取模，对系数取模，接着添加噪声多项式来掩盖真实的消息，最后对密文多项式缩放，四舍五入取整确定系数.那么，由于添加噪声多项式的关系，且加法具有加法交换律，那么密文

|  |  |  |
| --- | --- | --- |
|  |  | (5-7) |

相加，得到新密文

|  |  |  |
| --- | --- | --- |
|  |  | (5-8) |

而根据解密算法，解密的多项式为

|  |  |  |
| --- | --- | --- |
|  |  | (5-9) |

随着同态加法操作的不断增加，噪声多项式的系数不断累积，当对解密多项式乘以消去消息的系数，噪音多项式的系数可能会出现有一个介于的值，那么对系数四舍五入取整时，会将噪音多项式的系数给加上，那么解密就会解出错误的结果.

针对此问题，将噪音分为三类

|  |  |  |
| --- | --- | --- |
|  |  | (5-10) |

为了直观感受与分析，分别取对这三种噪音多项式类型分别添加了1，5和30个噪音多项式，观察其系数分布

1) 类型噪音多项式

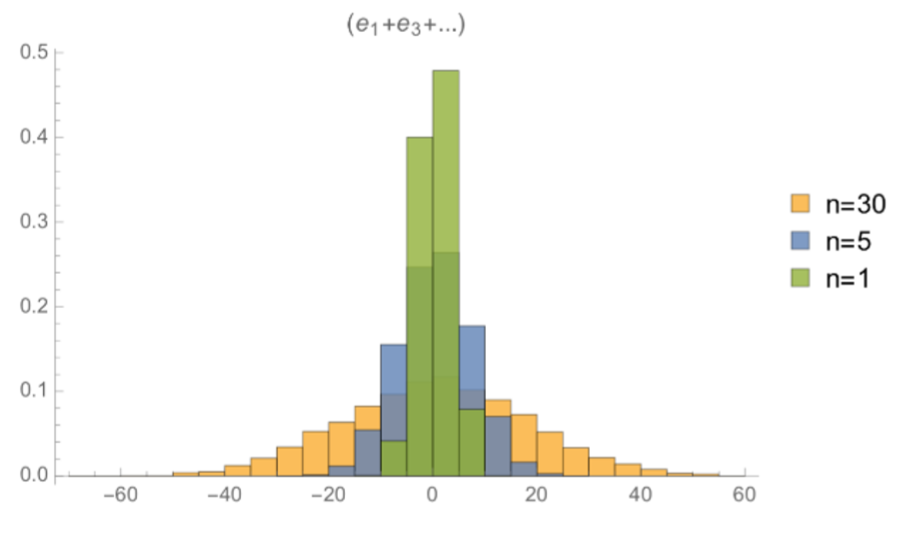


图 5‑1类型各噪声多项式系数分布

当我们添加30个噪音多项式时，某些系数有可能会大于64，即超过了的一半，所以解密不会产生正确的结果.

另外两项表示不同的情况——第二项是一个噪音多项式乘以一些“小的多项式”(系数为-1、 0或1)的总和.这种乘法会产生更大的噪音.这意味着这个噪音与多项式的最高次的平方根一致.

对这一项绘制与上面相同的分布可以看出，它比第一项大得多，而且即使对于我们示例中的参数，也存在错误解密的危险，即使只是添加了几个参数.

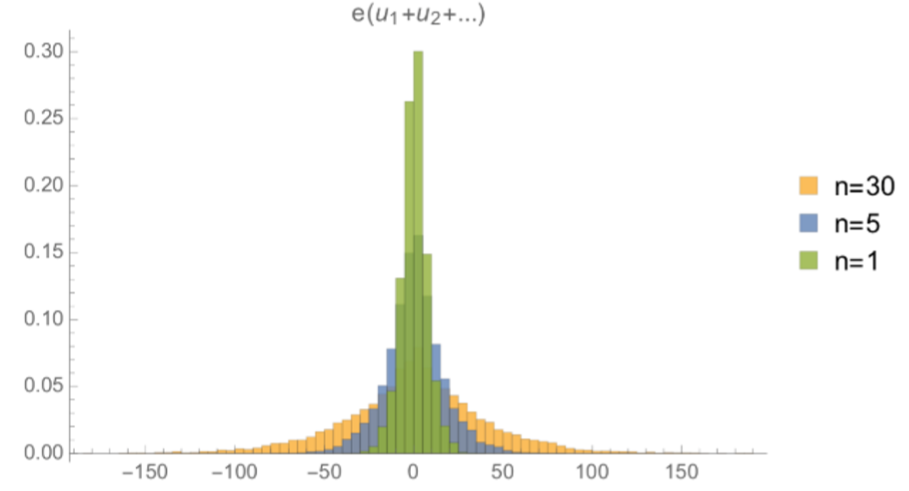


图 5‑2类型各噪声多项式系数分布

第三项是类似的——一组噪音多项式之和，乘以一个“小的多项式”.它的噪音分布是这样的:

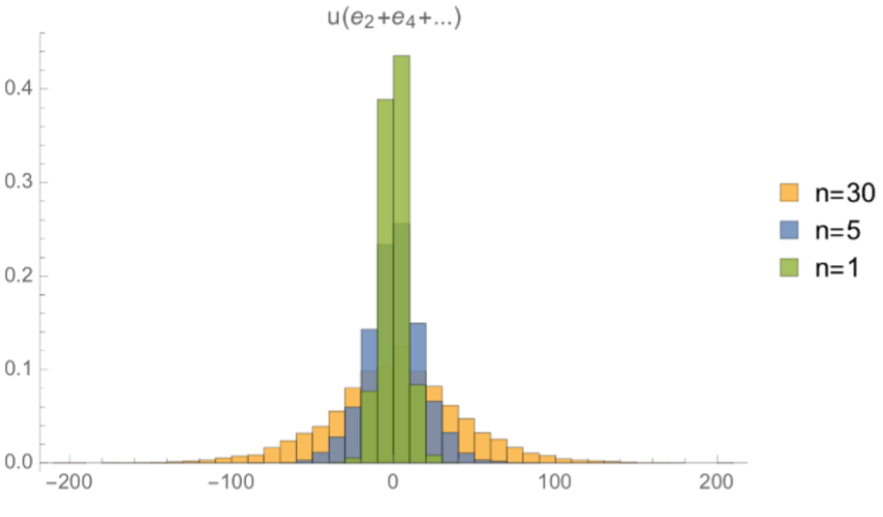


图 5‑3类型各噪声多项式系数分布

这表明，对于我们所选择的参数，由两个以上加法产生的密文，解码错误的概率很高，而且两次加法失败的概率也很高.这是因为有时最大错误大于64，当q/t = 128时，会导致不正确的解密，就像这里一样.为了给这样的操作提供更多的空间，我们需要使用更大的q/t比值， 这可以应对通常由所执行的操作数量引入的噪音量.

# 结束语

本文在半诚实模型下，关于数据在分布式计算下的隐私性对全同态加密的BFV方案进行分析，对方案进行了正确性，安全性与局限性的分析.能支持对数据的加密与解密， 保证数据的隐私不被泄露.

通过仿真模拟发现，当同态操作达到一定次数时，由于噪声多项式的累加影响，会对最后的解密成功率产生影响，使得解密失败，这也就导致了BFV方案不能进行任意次数的同态加法操作.而又由于分布式特点，使得BFV算法本具有的同态乘法操作与分布式概念相冲突.同时，由于解密算法对的系数进行四舍五入化简，使得同态计算只能进行整数类型的加密，运算和解密操作.这对于分布式统计来说是远远不够的.

所以对未来的展望是，加入CKKS算法，让其能拓展明文空间范围，能计算浮点数类型，最好是能进行任意此的同态操作.

# 谢 辞

经过此次毕业论文设计，让我领略了学术的魅力， 完整的逻辑框架搭建，数据处理，结果的分析，一步一个脚印的走下去，最后直到成果的完成，这是自豪的，这是有成就感的。

这次的过程中，困难是必不可少的，但我们要迎难而上，要有“千淘万漉虽辛苦，吹尽狂沙始到金”的精神，打倒路上的纸老虎。但一个人的力量终究是弱小的，幸而我们在学校中，有同学的陪伴，有老师的支持，以及家中父母给予的鼓励。同学之间相互帮助，拥有的信息互相交流，基础算法的相互帮助，这让我们的毕设进度都能得到前进。遇到难题，进入死胡同时，父母发来的鼓励让我心中产生一丝慰藉，我不是一个人在战斗，父母永远是我身后最有力的后盾。

其中感受最深的是张必山老师，让我体会到了“山重水复疑无路，柳暗花明又一村”，给予了我建议，给了我论文指导了方向，以至于不用走太多的弯路。他的博学多才，一眼看出我论文的问题所在，非常认真负责，真诚地提出批评和指正，在此由衷的感谢张必山老师。对老师的感激，我将铭记于心。

大学时光就随着论文的结束而匆匆离去，路上我遇到了很多可爱的同学，敬业的老师，感谢你们的一路陪伴，大学的时光有你们而璀璨。

# 参考文献

* + - 1. RIVEST R L, ADLEMAN L, DERTOUZOS M L.On data banks and privacy homomorphisms[A]. DeMillo RA Foundations of Secure Computation[C]. NY, USA: Academic Press, 1978.169-180.
      2. PAILLIER P. Public-key cryptosystems based on composite degree residuosity classes[A]. Proc of the Advances in Cryptology(EUROCRYPT99)[C]. Prague, Czech Republic, 1999.233-238
      3. GOLDWASSER S, MICALI S. Probabilistic encryption[J]. Journal of Computer and System Sciences, 1984,28(2): 270-299.
      4. RIVEST R L, SHAMIR A, ADLEMAN L. A method for obtaining digital signatures and public-key cryptosystems[J]. Communications of the ACM, 1978,21(2):120-126.
      5. ELGAMAL T. A public-key cryptosystem and a signature scheme based on discrete logarithms[J]. IEEE Transactions on Information Theory, 1985,31(4):469-472.
      6. BONEH D, GOH E J, NISSIM K. Evaluating 2-DNF formulas on ciphertexts[A]. Second Theory of Cryptography Conference (TTC 2005)[C]. Cambridge, MA, USA, 2005.325-341.
      7. GENTRY C. A Fully Homomorphic Encryption Scheme[D]. California, USA: Stanford University, 2009.
      8. GENTRY C. Fully homomorphic encryption using ideal lattices[A]. Proc of the 41st ACM Symposium on Theory of Computing(STOC 09)[C]. Bethesda, Maryland, USA, 2009.169-178.
      9. SMART P N, VERCAUTEREN F. Fully homomorphic encryption with relatively small key and ciphertext sizes[A]. Proc of the Public Key Cryptography (PKC 2010)[C]. Paris, France, 2010.420-443.
      10. DIJK V M, GENTRY C, HALEVI S, et al. Fully homomorphic encryption over the integers[A]. Proc of the Advances in Cryptology (EUROCRYPT 2010)[C]. Riviera, France, 2010.24 43.
      11. CORON J, MANDAL A, NACCACHE D, et al, Fully homomorphic encryption over the integers with shorter public keys[A]. Proc of the Advances in Cryptology (CRYPTO 201 1)[C]. Santa Barbara, California, USA, 2011.487-504.
      12. BRAKERSKI Z, VAIKUNTANATHAN V. Fully homomorphic encryption from ring-lwe and security for key dependent messages[A]. Proc of the Advances in Cryptology (CRYPTO 201 1)[C]. Santa Barbara, Califomia, USA, 2011.505 -524.
      13. GENTRY C, HALEVI S. Implementing Gentry's fully-bomomorphic encryption scheme[A]. Proc of the Advances in Cryptology(EUROCRYPT 2011)[C]. Tallinn, Estonia, 2011.129-148.
      14. BRAKERSKI Z，GENTRY C，VAIKUNTANATHAN V. Fully homomorphic encryption without bootstrapping[]. Computer and Information Science, 2011, 111(111): 1-12.
      15. GENTRY C, HALEVI S. Fully homomorphic encryption without squashing using depth-3 arithmetic circuits[A]. Proc of the 2011 IEEE 52nd Annual Symposium on Foundations of Computer Science[C]. Palm Springs, CA, USA, 201 1.107-109.
      16. 黄汝维，桂小林，余思等.云环境中支持隐私保护的可计算加密方法[J].计算机学报, 2011, 34(12): 2391-2402.
      17. T. Elgamal, "A public key cryptosystem and a signature scheme based on discrete logarithms," in IEEE Transactions on Information Theory, vol. 31, no. 4, pp. 469-472, July 1985, doi: 10.1109/TIT.1985.1057074.
      18. Paillier P . Public-key cryptosystems based on composite degree residuosity classes[J]. Advances in Cryptology Leurocrypt, 2004.
      19. Goldwasser, S.; Micali, S.; Rivest, R. L. (1988). "A Digital Signature Scheme Secure Against Adaptive Chosen-Message Attacks". SIAM Journal on Computing. 17 (2): 281.
      20. D Boneh, EJ Goh, K Nissim (April 2006). "Evaluating 2-DNF Formulas on Ciphertexts"
      21. STOC '09: Proceedings of the forty-first annual ACM symposium on Theory of computingMay 2009 Pages 169–178https://doi.org/10.1145/1536414.1536440
      22. 杨攀,桂小林,姚婧,林建财,田丰,张学军.支持同态算术运算的数据加密方案算法研究[J].通信学报,2015,36(01):171-182.