学号：E201002064
密级：

安徽大学

硕士学位论文

同态加密技术及其应用研究

Research of Homomorphic Encryption Technology and Application

学　　号	E201002064
姓名	夏超
学科专业	计算机应用技术
研究方向	网络与信息安全
指导教师	仲红
完成时间	2013 年 4 月

独创性声明

本人声明所呈交的学位论文是本人在导师指导下进行的研究工作及取得的研究成果。据我所知，除了文中特别加以标注和致谢的地方外，论文中不包含其他人已经发表或撰写过的研究成果，也不包含为获得安徽大学或其他教育机构的学位或证书而使用过的材料。与我一同工作的同志对本研究所做的任何贡献均已在论文中作了明确的说明并表示谢意。

学位论文作者签名：夏超　　签字日期：2013 年 6 月 5 日

学位论文版权使用授权书

本学位论文作者完全了解安徽大学有关保留、使用学位论文的规定，有权保留并向国家有关部门或机构送交论文的复印件和磁盘，允许论文被查阅和借阅。本人授权安徽大学可以将学位论文的全部或部分内容编入有关数据库进行检索，可以采用影印、缩印或扫描等复制手段保存、汇编学位论文。

（保密的学位论文在解密后适用本授权书）

学位论文作者签名：夏超　　导师签名：

签字日期：2013 年 6 月 5 日　　签字日期：2013 年 6 月 5 日

学位论文作者毕业去向：

工作单位：　　电话：

通讯地址：　　邮编：

摘 要

同态加密（Homomorphic Encryption）是一类具有特殊自然属性的加密方法，此概念是 Rivest 等人在上个世纪七十年代提出的。与一般加密算法相比，同态加密除了能实现基本的加密操作之外，还能实现密文间的多种计算功能，即先计算后解密可等价于先解密后计算。这个特性对于保护信息的安全具有重要意义：利用同态加密技术可以先对多个密文进行计算之后再解密，不必对每一个密文解密而花费高昂的计算代价；利用同态加密技术可以实现无密钥方对密文的计算，密文计算无须经过密钥方，既可以减少通信代价，又可以转移计算任务，由此可平衡各方的计算代价；利用同态加密技术可以实现让解密方只能获知最后的结果，而无法获得每一个密文的消息，可以提高信息的安全性。正是由于同态加密技术在计算复杂性、通信复杂性与安全性上的优势，越来越多的学者投入到其理论和应用的研究中。

频繁的网络活动使得越来越多的信息安全问题得以暴露，加剧了对安全多方计算（Secure Multi-Party Computation， SMC）需求。同态加密技术作为 SMC 的核心技术之一，其相比一般算法的优越性有助于设计高效、安全的计算协议。但目前同态加密体制的自身缺陷也限制了其应用的范围，所以从理论和应用两个方面研究同态加密具有重要的价值。本文在同态加密领域的主要工作如下：

首先，介绍分析了几种典型的同态加密方案，包括半同态和全同态方案。指出每种方案的技术特点及此类方案的研究进展。在此基础上，总结同态加密体制存在的问题，并提出进一步研究设想。

其次，提出并设计了“多对一”的同态加密方案。已有同态加密方案大多是公钥密码体制下的一方加密，一方解密的“一对一”的密码形式。随着网络应用环境的不断变化，这种方案已无法满足多用户之间的安全计算需求。在无线局域网、3G 网和有限网络等领域中，“一对多”、“多对一”和“多对多”的交互形式使得对密码形式的要求也呈现出多样性。为提高实用性，我们将同态加密的概念同“多方加密，一方解密”的密码形式相结合，提出了“多对一”的同态加密方案。针对一个“多对一”密码形式的实用场景，定义“多对一”同态加密方案的模型；以整数全同态方案的为基础，构建了我们的新方案。；并严格证明了“多

对一”同态加密方案的正确性、同态性以及安全性；分析结果表明“多对一”的同态加密方案不仅能实现“多对一”的密码形式，还可使不同密钥加密的密文呈现同态性，避免使用多密钥的情形。在此基础上对方案进行扩展，得到一个多层级的“多对一”的同态加密方案，可以实现高权限对低权限密文的同态性，扩展了方案的适用范围。

再次，提出了基于同态加密技术的安全多方乘积协议。通过对同态加密技术特点的深入分析，得知合理利用此技术可降低多方计算协议的计算复杂度与通信复杂度。安全多方乘积计算是一类特殊的安全多方计算问题，用于共享多个参与方进行乘积计算的结果。针对现有安全多方乘积协议频繁调用安全两方乘积协议造成的通信代价高、数据量大的问题，本文在半诚实模型下，利用同态加密技术，提出了适用于复杂网络环境的串行安全多方乘积协议和理想通信环境下的并行安全多方乘积协议，并从理论上证明了协议的正确性与安全性。通过已有协议的对比分析，证明了文中的两个协议在通信代价和执行效率上具有明显的优势。相比已有多方乘积协议，文中的两个协议结合了具体的网络环境，增强了协议的适应性。另外， 此协议是一个基础的安全多方计算协议，为利用同态加密技术设计其他安全多方计算协议提供了新的思路。

最后，对全文所做的工作进行系统的总结，并指出在同态加密领域需要进一步研究的问题。

关键词：同态加密；安全多方计算；多对一；安全多方乘积；串行协议；并行协议

Abstract

Homomorphic encryption, proposed by Rivest et al. in the 70s of the last century, is a class with the special nature of the encryption algorithm. Compared with the general encryption algorithm, homomorphic encryption can implement not only the basic cryptographic operations, but also specific types of computations on ciphertexts, which means the results of calculating before decrypting is same as decrypting before calculating. This property is of great significance for the protection of information security: with homomorphic encryption technology ,we can calculate multiple ciphertexts and then decrypt rather than decrypting each ciphertext at first, which spends the high price of computation; homomorphic encryption technology allows the party without secret key to calculate ciphertexts, do not have to send all the ciphertexts to key party, thus, it can not only reduce the cost of communication, but also transfer computing tasks, which can balance the computational cost of all parties; in homomorphic encryption technology, the decrypting party can only get the final results instead of every ciphertext message, this would improve the security of the information greatly. Because of the advantages of homomorphic encryption in computational complexity, communication complexity and security, a growing number of scholars involve in the study of its theory and applications.

The frequent network activity expose growing number of information security problems, which exacerbate the demand of SMC(Secure Multi-Party Computation). Homomorphic encryption, as one of the core technology of the SMC, its superiority that compared with the general algorithm contribute to the design of efficient, secure computing protocols. But the defects of homomorphic encryption system still limit the scope of its application. Therefore, research on the theory and applications of homomorphic encryption is of great significance. In this paper, the main work of the homomorphic encryption as follows:

First of all, introduce several typical homomorphic encryption schemes, including partially homomorphic encryption schemes and fully homomorphic encryption

schemes. We point out characteristics of each scheme and the application achievements relying on those characteristics in the security field. Based on these work, we summarize the existing problems of homomorphic encryption cryptosystems, and propose further ideas.

Next, introduce the "many-to-one" homomorphic encryption scheme. The present homomorphic encryption schemes are mostly in the form of "one-to-one", means one party encrypts and the other decrypts in public key cryptosystem. With the changing of network scenarios, this form of cryptography has been unable to satisfy the demand of multi-party .In the field of wireless LAN, 3G networks and limited network, the "one-to-many", "many-to-one" and "many-to-many" interactive forms ask the diversity of cryptography forms. In order to improve the practicality, we combine the concept homomorphic encryption with the cryptography form of "multi-party encryption, one party decryption" to propose the "many-to-one" homomorphic encryption scheme. Firstly, We propose a practical application scenarios in "many-to-one" cryptography form and then define the model of the "many-to-one" homomorphic encryption scheme; Secondly, build our scheme on the basis of Dijk et al.'s integer homomorphic scheme and prove the correctness, homomorphism and security of the "many-to-one" homomorphic encryption scheme under the model definition; At last, by analysis of our scheme, we show that the "many-to-one " homomorphic encryption scheme can not only achieve many-to-one form, but also has a homogeneity between the ciphertexts with different keys, which avoids appearing the case of the multiple keys. According to the way of scheme building, I extend and make a "many-to-one" homomorphic encryption scheme in multi-level, which achieves the homomorphism of high permission ciphertext to low permission ciphertext and extends the range of practicality.

Finally, introduce secure multi-party multiplication protocol based on homomorphic encryption technology. With the strict analysis of the characteristics of homomorphic encryption, we realize that the reasonable using of this technology can reduce the computational complexity and communication complexity of multi-party computation. Secure multi-party multiplication is a special problem of secure

multi-party computation, which can be used by multi-party to share the multiplication result. For the problems of high cost of communication and large amount of data which are caused by frequently using the secure two-party multiplication protocol in the present protocols, a serial secure multi-party multiplication protocol in the complex communication environment and a parallel secure multi-party multiplication protocol in the ideal communication environment are presented in this paper with the help of the semi-honest model. At last, correctness and security of those protocols are analyzed. Compared with the present protocols, the analysis shows that the proposed protocols have advantages in the communication cost and the execution efficiency. Compared with the existing multiplicative protocol of multi-party, two protocols in this paper combine the specific network environment, and enhance the practicality of the protocol. In addition, as a basic Multi-party Computation protocol, this protocol provides a new way for the study of other multi-party computation protocols using homomorphic encryption technology.

Key words: homomorphic encryption; secure multi-party computation; many to one; secure multi-party multiplication; serial protocol; parallel protocol

目 录

第一章 绪论

同态加密[1]（Homomorphic Encryption），是安全多方计算[2-3]（Secure Multi-Party Computation， SMC）的核心技术之一，在密码学理论、SMC 领域中具有重要研究价值。本章首先介绍了同态加密技术的研究背景与意义，然后对同态加密技术的研究现状进行了综述，并指出了同态加密技术在 SMC 领域取得的成就，最后介绍了本文的结构与主要内容。

1.1 研究背景与意义

当今时代，在迅猛发展的计算机和网络技术的推动下，社会无时无刻不在变化和发展，人类的生活环境已由单一的自然环境逐渐向网络环境演变。日渐便捷的互联网带给人以方便快捷的生活方式，人们不断地利用网络进行协作计算等活动。但这些网络活动可能发生在不完全信任甚至恶意的用户之间，存在严峻的安全问题，这给人们使用网络造成了一定的障碍。如何构建一个高效安全的网络环境，满足社会需求具有重要意义。安全多方计算（Secure Multi-Party Computation，简称 SMC）主要研究网络环境下多个互不信任参与方的协作计算问题，成为密码界热点研究的课题之一。

安全多方计算的诞生，为解决网络安全与应用需求之间的矛盾提供了一种新的计算方法，在电子商务、军事等领域得到广泛应用。安全多方计算中常利用同态加密（Homomorphic Encryption）、茫然传输（Oblivious Transfer）、秘密分享（Secret Sharing）、零知识证明（Zero Knowledge Proof）等技术来实现安全计算目标。近年来，网络频发隐私泄露事件，提高了人们对信息安全的保护意识。在各种加密方法中，同态加密技术（homomorphic encryption technology），由于其自身优点，成为安全多方计算核心技术之一，其在理论和应用上都得到了广泛的研究。

公钥密码体制[4]出现之后，人们对密码学的研究已经不再局限于单纯的加密、解密算法研究。一般经过加密算法进行加密的密文，在增加数据安全性的同时也带来了诸多不便。例如，对若干加密的数据进行运算，只能通过拥有密钥的一方先解密然后进行明文之间的运算。这样就会带来几个问题：一是增加了计算

的复杂度，因为每一次解密运算会带来高昂的代价；二是计算只能通过密钥拥有者，其他参与方无法对密文运算，其他参与方需要将密文数据发送给解密方，造成一定的通信代价；三是出于安全考虑，参与方只希望解密方获取最后的计算结果，若对每个密文数据都进行解密会造成一定的信息泄露。所以，密码学的研究学者试图寻找一种新的数据处理方法，使得密文之间可进行计算，同态加密应运而生。同态加密是基于数学难题的计算复杂性理论的密码学技术，对经过同态加密的数据进行处理得到一个输出，将这一输出进行解密，其结果与用同一方法处理未加密的原始数据得到的输出结果是一样的。简单的来说，就是密文操作可以等价于明文操作之后再加密。同态加密由于其特殊的性能，可以解决上述中存在的计算复杂度、通信复杂度以及安全性问题，以至于越来越受学者的关注。至今，已出现一些同态成熟的同态加密方案，有些已经广泛应用到安全协议的设计中，从中可以总结出其特殊的自然属性：

首先，同态加密技术同一般的加密技术一样对加密方消息实施加密操作，不被允许的参与方无法窃取秘密，满足了隐私保护的安全性需求。

其次，同态加密技术具有一般加密技术不具备的自然属性。一般加密状态的数据直接计算便会破坏相应明文，而利用同态加密的密文数据可直接运算而不会破坏对应明文信息的完整性和保密性。计算的中间数据也是加密的，可以寄存在任何参与方，剔除冗余数据，降低对通信要求，提高执行效率。

随着网络技术的发展，传统的单一计算模式已经不能满足用户需求，云计算[5-6]成为计算时代主题。用户希望通过云提供的服务进行一些复杂的运算，但又不想让云知道相关的隐私信息[7]，这时同态加密技术就可以发挥出重要作用。云只负责计算，而用户只需要处理计算的结果。用户数据安全需求的不断提高，现有的同态加密机制存在的问题和缺陷，也会限制其应用的范围。现有的高效率和高安全性的同态加密方案大多是半同态的，即方案只在执行单一计算操作时具备同态性。例如 RSA[8] 算法只满足乘法同态性，Paillier[9]算法只对加法同态，而 IHC[10]算法和 MRS[11] 算法也只能对加同态和标量乘同态。这些方案限制了运算种类，实用性上受到严峻的挑战。另外，也有少数几种同态加密方案同时对两种运算同态，如 Rivest 算法[11]。但这些方案要么因为安全性低，要么因为工作效率低而未能带来实际应用价值。因此，完善、发展同态加密机制，意义重大。

另外，越来越频繁的网络活动对安全多方计算也提出了一定的需求。高效、安全、覆盖范围广成为安全多方计算研究目标。但现有安全多方计算机制并不完善，有些 SMC 协议存在安全性较低、效率不高等问题；还有许多实际的网络安全问题尚未能通过安全、有效的计算方法解决。同态加密技术作为核心技术之一，研究同态加密技术有助于完善现有的安全多方计算机制。所以，如何设计高效、安全的同态加密算法既是严峻的挑战，也是安全多方计算领域中不可或缺的重要任务。这也是我们的研究目的。

1.2 研究现状

同态加密技术从诞生之日起，就得到了广泛的研究。经过国内外学者的不懈努力，已有许多成功的方案，将同态加密从单一的运算发展到多种运算。许多成熟的方案广泛应用到各个安全领域。

早在 1978 年，同态加密由 Rivest[1]等人以“隐私同态”的概念第一次提出。他们在实际的科研工作中通过一个有意思的问题引出了同态加密的概念。能不能不通过跳过解密这一步以密文操作实现对明文的相应处理？自该问题提出之后，密码界的学者就对这样一种特殊的加密方法进行了深入的研究。不仅分析已有加密方案是否具有这种性质，也试图设计新的同态加密算法。

在古典密码中，也有许多密码都具有一定的同态性。比如早期的凯撒大帝[12]在保护军情时使用的密码，即对英文字母表进行移位的一种简单密码，又称之为加法密码，具有一定的加法同态性；与凯撒密码对应的采样密码[12]，即密文由明文按照字母表每隔一定的位数取得，又称之为乘法密码，具有一定的乘法同态性。除此之外，拥有同态性质的密码还有 1929 年 Hill 提出的希尔密码等。但是，古典密码由于自身的缺陷渐渐地淡出密码界，如今的同态加密的研究主要在公钥密码体制下进行。

1976 年，W.Diffie[4]等人提出了公钥密码体制，成功使用不同的密钥将加密和解密分开实施。虽然此时还没有但是同态加密的概念，但公钥密码体制的为同态加密研究提出了模型，也加速了同态加密的诞生于发展。众多优秀的同态加密方案不断涌现。

1978 年，在于同态加密概念诞生的同时， Rivest，A.Shamier 和 L.Adleman

利用数论构造了著名的 RSA 加密方案[8]，该方案具有乘法同态性，但不具备加法同态性。RSA 方案的安全性取决于大整数素分解的困难性[13-14]。但随着计算能力的增强，不少攻击者试图用迭代攻击[15]、选择明文攻击、公用模攻击[16]、低加密指数攻击[17]等手段破解 RSA。如今，RSA 密钥的越长，其安全性就越高，在银行等领域应用广泛。

由于 RSA 只对乘法同态，1978 年，Rivest 针对此缺陷又提出了一种同时满足加同态和乘同态的 Rivest 加密方法，该方案同 RSA 的安全性一样，同样取决于大整数的难分解性。但此方案存在严重的安全问题。后有学者克服了此方案的缺陷，提出了拥有更好效果的 MRS 算法[11]。

1984 年，S.Goldwasse 和 S.Micali 提出了最早概率加密方案 GM 算法[18]。同 RSA 相反，该算法仅满足加同态，而不满足乘同态。根据概率加密思想构造的加密方案大多是安全的，GM 方案安全性基于二次剩余难题[18]。由于 GM 方案每次只对一位进行加密，效率较低。随着计算能力的增加，GM 方案近年来也获得许多实际的应用。ElGamal[19]算法是另外一个比较著名的具有同态性质的概率加密方案：

1985 年，ElGamal 提出一种基于离散对数难题的公钥密码体制。ElGamal 算法即可用于加密，也可用于签名。ElGamal 算法在一个有限域[20]上施行，是典型的乘法同态加密算法。此方案的特点是密文不再完全取决于明文，也取决于随机数的选择，这就是随机化加密；缺点就是数据长度扩大了，为实现安全性需要加大有限域的选择。

1994 年，Benaloh[21]对 GM 方案进行了扩展，提出 Benaloh 密集概率加密方案，该方案同 GM 方案一样，满足加法同态性。与 GM 安全性不同的是，Benaloh 方案安全性基于数论中的高次剩余判定难题。另外一个比较著名的同态加加密算法是 Paillier[9]算法。

1999 年，Paillier 提出了一个满足加同态性质的公钥加密系统。Paillier 算法同 ElGama 算法一样具有加密的随机性，是一种概率公钥加密。其安全性是基于 DCR 假设（判定 n 阶剩余类难题）[9]。

国内的学者在同态加密方案研究上也作出了积极的贡献。2005 年，向广利[22]等人在实数域上定义了类模运算，在此基础上提出了实数范围上的同态加密机

制。该机制将普通整数范围上的加法、乘法运算扩展到加减乘除四种运算，具有一定的使用价值。但此算法并非是公钥密码体制下的同态加密算法，存在一定的安全问题，难以得到广泛的应用。

从 1978 年同态加密的概念提出的三十年时间里，许多学者不断的提出各种加密方案，但这些方案大多是半同态的（只具有一种运算的同态性），少数的几种全同态加密方案（如 Rivest 方案）由于存在一定的安全问题而未能应用到实际中。在半同态算法研究渐渐成熟以后，研究人员开始着手全同态的加密方案的思考。起初，对全同态加密算法的探索并没有明确的方向，直到 2009 年。

2009 年，就在全同态加密的研究陷入困境之时，IBM 的研究员 Craig Gentry[23] 对全同态加密做了详细的介绍并基于数学环理论中“理想”的概念第一次构造了全同态加密方案，其安全性基于离散子集求和问题。该方案是同态加密领域的重大突破，给全同态加密方案的研究提出了新的方向。但是，Craig Gentry 的方案在工作效率上仍存在一定的问题而未能实际应用。同年，在另一篇文章中，Dijk[24] 等运用简单的代数方法在整数域上先提出了安全性基于近似最大公因子难题的 Somewhat 同态加密方案[24]，并利用压缩方法可将此方案转换成了整数域上的全同态加密方案。

2010 年，Nigel P.Smart 和 Frederik Vercauteren[25]在 Craig Gentry 基础上提出了一种密钥相对较小和密文长度相对较短的全同态加密方案，并尝试对此方案的实现，但由于方案的复杂性，仅仅测试了 Somewhat 同态加密方案。2011 年，Craig Gentry 等人在欧密会上对 Nigel P.Smart 和 Frederik Vercauteren 的方案进行了一系列的优化，降低了计算复杂度，使得方案更容易理解和实施[26]。

除了上述方案之外，在 Craig Gentry 提出全同态加密方案之后，涌现了许多不同方法的全同态方案[27-29]，为全同态加密的研究作出了重要贡献。国内学者也对同态加密做出了深入的研究。2011 年，汤殿华[30]等人将重加密技术应用到整数上全同态加密方案中，更加清晰地理解了 Gentry 基于理想格同态加密框架。2012 年，汤殿华等人基于部分近似最大公因子难题（PACDP），在整数范围，又设计了一个较快速的全同态加密方案[31]。该方案与 Dijk 等人的方案相比降低了计算复杂度，提高了方案执行效率。同年，徐鹏[32]等人提出了整数环上的全同态加密算法，该算法的安全性同 Craig Gentry 理想格方案一样，基于离散子集求和

问题。

许多学者在探索同态加密算法的同时，也将同态加密技术实施到多方计算、匿名访问[33]、云计算、移动代码[34]等领域，取得了广泛的成就：2008 年，肖倩、罗守山等基于同态加密的加同态性，提出了安全两方的排序方案并将此方案直接扩展到多方排序中[35]；2009 年罗守山等人又利用 RSA 密码体制的乘法同态性，提出了安全多方数据排序方案[36]；2010 年，黄福人[37]等人利用 ElGamal 加密等技术，提出了拥有匿名性、无收据性、可验证性的电子计票方案；2011 年，张鹏[38]等人利用同态加密的相关性质，构造了一个可证签名方案，该方案具有可验证性与匿名性等特点，消除了电子计票方案中既能实现匿名性，又可验证性之间的矛盾。同态加密在当今炙手可热的云计算中，也有着丰富的应用。2012 年，李美云[39]等人基于同态加密技术的加同态和乘同态设计了一种解决云安全存储与信息管理方案。该方案可实现对密文直接检索、操作，充分享用云提供的计算服务，也保证了隐私安全性。

如何进一步完善同态加密机制，发展安全多方计算体系，有待学者们的继续研究。

1.3 研究内容与研究方法

本文的主要研究工作包括两个部分：同态加密的理论摸索与同态加密技术的应用探讨。

通过对已有同态加密方案的调研，深入研究同态加密技术的自然特性，系统分析同态加密机制中还存在的缺陷，针对缺陷提出可能的解决途径。对已有的同态加密方案的特性进行归纳总结，指出每种加密方案可能的适用场景，结合安全领域中尚未解决或有待改进的问题，设计新的实用协议。

总结同态加密技术在应用领域取得的成就，分析同态加密技术相比其他安全技术在这些协议中存在的优势。思考安全领域尚未解决的问题或者有待改善的问题是否可以用同态加密技术、用什么样特性的同态加密技术加以解决。从应用的角度明确对同态加密的需求，设计或改进已有同态加密方案，完善同态加密体制。

结合上述主要内容，本文主要按照图 1.1 所示的过程进行研究。

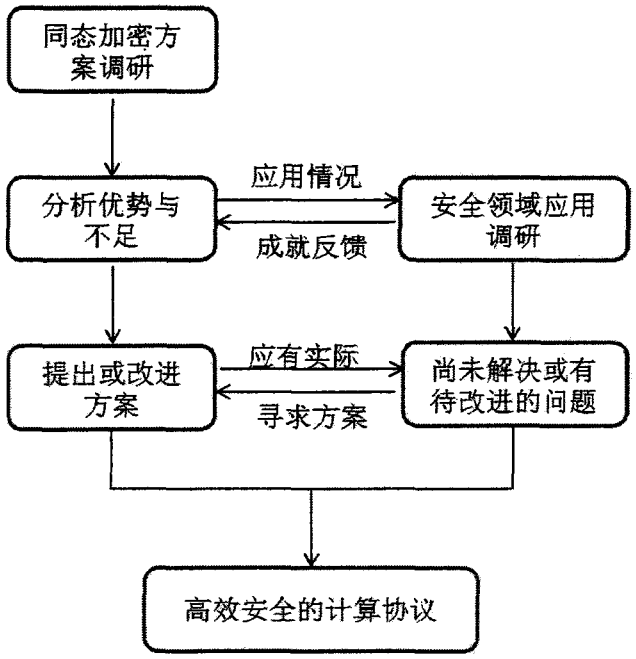

图 1.1 研究方法线路图

Fig 1.1 research methods map

根据图 1.1 所示的过程，结合实际，本文具体对以下两个问题进行了研究。

（1）多对一同态加密方案

现有的同态加密方案大多是“一对一”的密码形式，即一方加密、一方解密，无法实现多用户的应用场景。本文在 Dijk 等人提出的整数上的全同态加密基础上，由 somewhat 方案扩展得到一个“多对一”的加密方案。该方案不仅可以实现多方加密、一方解密，而且解密方可以实现对所有加密方密文加和乘的同态性。

（2）安全多方乘积协议

安全多方乘积是 SMC 领域的一个特殊问题，已有方案大多是基于茫然传输技术、频繁调用安全两方协议得到。本文结合同态加密的加密数据安全性和密文可操作性优势，提出了两个适用不同环境的多方乘积协议，降低了通信复杂度，提高了协议执行效率。

1.4 本文的内容安排

本文的章节安排如下：

第一章，绪论。主要介绍同态加密技术研究的目的和意义、国内外研究现状以及本文的主要内容。

第二章，经典同态加密算法。首先介绍了同态加密的基本概念和性质，然后介绍了同态加密方案的安全基础（数学上的一些难题假设），最后重点对现有的几个典型的同态加密算法进行了分析。

第三章，多对一同态加密方案。结合实际应用场景，在已有全同态加密方案的基础上设计了适用于多用户场景满足同态性质的加密方案，并对方案进行了相关的理论分析。

第四章，安全多方乘积协议。首先阐述了同态加密技术的优越性以及现有安全多方乘积协议存在的问题；然后在此基础上提出了适用于不同环境的串行和并行的安全多方乘积协议，随即对协议进行了正确性、安全性以及复杂度分析，并和已有方案进行了对比；最后利用安全多方乘积方案提出了一个扩展的点积协议，应用到实际工作中。

第五章，总结与展望。总结全文，指出同态加密技术理论及其应用的未来研究方向。

1.5 本章小节

本章首先介绍了网络环境所面临的信息安全问题，随即说明了研究同态加密技术的目的及意义，同时指出同态加密技术的研究是密码界也是安全多方计算领域的重要研究方向；其次介绍了同态加密技术理论研究和应用研究的一些国内外研究进展；最后介绍了本文的主要工作以及研究方法。

第二章 经典同态加密算法

本章首先以数学化方式介绍了同态加密的基本概念，洞悉了同态加密的自然特性；然后介绍同态加密算法的一些安全性基础，主要是数学上的一些难解性假设；最后重点对 1.2 节中提及的一些经典的同态加密算法进行了分类讨论。

2.1 基本概念

在第一章绪论部分，我们多次提到了同态加密，并作出了简单的描述。同态加密是满足一定性质的加密算法。公钥密码体制下的同态加密算法可描述如下：

定义 1 同态加密算法体制是满足下列条件的一个六元组 $\{M,C,K,E,D,\oplus\}$；

（1）M 是明文空间；

（2）C 是密文空间；

（3）K 是公私钥对集合；

（4）$\oplus$ 是同态运算符；

（5）对于任意的 $(pk,sk)\in K$（pk 称作公钥，sk 称作私钥），对应一个加密算法 $E_{pk}\in E$（E 是加密算法集合，$E:M\to C$）和解密算法 $D_{sk}\in D$（D 是解密算法集合，$D:C\to M$），且对任意的 $m\in M$，满足 $c=E_{pk}(m)$，$m=D_{sk}(c)=D_{sk}(E_{pk}(m))$，其中，$E_{pk}$，$D_{sk}$ 都是多项式时间内可执行的。

（6）对于所有的 $(pk,sk)\in K$，由 E_{pk} 推出 D_{sk} 是计算上不可能的。

（7）对任意的 $x,y\in M$，$E_{pk}(x)\oplus E_{pk}(y)=E_{pk}(x\oplus y)$[40]。

根据运算符 $\oplus$ 的不同，可分为加同态算法和乘同态算法。满足加同态性的算法可表述为 $E_{pk}(m_1)\oplus E_{pk}(m_2)=E_{pk}(m_1+m_2)$，而乘同态性的算法可表述为 $E_{pk}(m_1)\oplus E_{pk}(m_2)=E_{pk}(m_1m_2)$。以此，我们可以对同态加密进行分类，仅仅能实现一种同态性的算法称为半同态加密算法；满足所有同态性质的算法称为全同态加密算法。另外根据 Gentry 的定义，全同态加密算法还应具有自举性[23]，同态加密算法可以同态处理解密电路和扩展电路。

2.2 安全理论

加密算法设计的首要问题是保证安全性。计算复杂性理论[41-43]是密码系统安全理论基础，用以判断解决一个问题的难易程度。解决问题的难易程度通常根据计算复杂性决定，通常分成三类，即 P 类（易解问题）、NP（难解问题）、NPC(困难问题)。密码学的主要考虑 NP 和 NPC 问题，因为这两类问题求解在计算上是不可行的。现代密码学的算法设计主要基于数学上的一些难解性假设。

（1）整数分解难题

整数分解难题是指任意一个正整数 n，找到它所有的因子。当这个正整数很小的时候，分解可能是容易的。当 n 规模达到 1024 位的时候，分解变得非常困难。在现有计算复杂性理论中，整数分解难题是一个 NP 问题。目前有很多公钥加密算法均基于整数分解难题设计的。RSA 算法就是整数分解难题的具体特例。

（2）离散对数问题

离散对数问题[44]是除了整数分解问题之外，另一个密码界常用的难解问题。它是有限循环群上的一个问题，定义如下：

给定一个 p 阶有限循环群 G，g 为 G 上的一个生成元。如果 $x \in z_p^*$ 求 $y = g^x \bmod p$ 是容易的；当前提条件变为 y，求解 x 的时候，如果 p 是一个大素数，则计算 x 是困难。离散对数是单向函数的一种候选形式。

（3）判定 n 阶剩余类难题（DCR 假设）

$n = pq$，其中 p 和 q 都是大素数。整数 z 如果被称为模 n^2 的 n 阶剩余类，那么存在整数 $y \in z_{n^2}^*$，使得 $z = y^n \bmod n^2$。对于给定的整数 z，判定是不是模 n^2 的 n 阶剩余类是一个难解性问题。Paillier 算法是基于该难题假设的一个随机加密算法。

（4）近似最大公因子难题

给定随机选择的一组整数 $x_1, x_2, \cdots x_n$，每一个整数 x_i 都接近于它们的近似一公因子 p，其中 p 是大素数，寻找近似公因子 p 是困难的[45]。Dijk 等人提出的整数上的全同态加密方案就是基于该难题提出的。

（5）离散子集求和难题

Craig Gentry 等人基于理想格提出的全同态加密方案掀起了对同态加密研究的热潮。该方案的安全性是基于离散子集求和难题[46-48]的，描述如下：

已知整数集合 $S=\{x_1,x_2,\cdots x_n\}$ 和另一个整数 x，则，当 n 很大的时候，寻找 S 上的一个非空子集 T，满足 T 中的元素之和等于 x 是困难的。

2.3 经典同态加密算法

2.3.1 RSA 算法

密钥生成：p，q 是两个大素数，$n=pq$，根据欧拉定理，$\varphi(n)=(p-1)(q-1)$，随机选择整数 d，e，使得 $\gcd(d,\varphi(n))=1$，$ed\equiv 1(\varphi(n))$，则公钥 $pk=(n,e)$，私钥 $sk=d$。

加密阶段：明文空间 M 中的任意一消息 m，对应密文 $c=E_{pk}(m)=m^e(\mathrm{mod}\,n)$。

解密阶段：$m=D_{sk}(c)=c^d(\mathrm{mod}\,n)$。

图 2.1 RSA 密码体制

Fig 2.1 RSA cryptosystem

由图 2.1 不难发现 RSA 算法满足乘法同态性：

$E_{pk}(m_1m_2)=(m_1m_2)^e(\mathrm{mod}\,n)$，$E_{pk}(m_1)E_{pk}(m_2)=m_1^em_2^e(\mathrm{mod}\,n)$，

所以 $E_{pk}(m_1m_2)=E_{pk}(m_1)E_{pk}(m_2)$。

RSA 算法是目前应用比较广泛的一种同态加密算法，这也引起了对 RSA 的广泛攻击。在 2.2 节，我们已知了 RSA 算法安全性是基于大整数分解难题的。目前攻击 RSA 的方法有多种，包括分解大整数、猜测欧拉函数值、迭代攻击、选择明文攻击、定时攻击等。其中，RSA 的乘法同态性在一定程度上协助了对 RSA 的攻击（如选择明文攻击）。

为了增强 RSA 的安全性，需要对参数的选择做仔细的研究。首先，由于 RSA 的安全性基于大整数分解，因此 p，q 不仅要是大素数还要是强素数[12]，使其难

以在有限时间内分解；其次，p，q要有适当的位数差，太大或太小都可能通过尝试法分解n；私钥d应该尽可能小防止穷举，而e应稍大防止直接对密文开方运算而得到明文。随着计算能力的增强，今天要想使用 RSA 算法就需要足够大的密钥长度，比较安全密钥长度为 1024bit。

RSA 算法除了应用其加密的安全性之外，其同态性也倍受人关注。文献[36]中，选择 RSA 算法，对密钥进行了分解，利用其乘法同态性对加密的矩阵列元素进行了乘积计算，实现了对多个数据的安全排序。

RSA 算法在公私钥生成之后，加密或解密中的参数便固定下来。这会使得同一个明文加密后的密文总是相同的，这给安全性提出了挑战。下面我们介绍两种经典的随机化[49]同态加密算法。

2.3.2 Paillier 算法

密钥生成：设p，q是两个大素数，$N=pq$，$g\in Z_{N^2}^*$，记$L(x)=(x-1)/N$，公钥$pk=(N,g)$，密钥$sk=\lambda(N)=lcm(p-1,q-1)$。

加密阶段：任意明文$m\in Z_n$，随机选择$r\in Z_N^*$，那么密文$c=E_{pk}(m)=g^m r^N \bmod N^2$。

解密阶段：解密得明文$m=D_{sk}(c)=L(c^{\lambda(N)} \bmod N^2)/L(g^{\lambda(N)} \bmod N^2) \bmod N$。

图 2. 2 Paillier 密码体制

Fig 2. 2 Paillier cryptosystem

Paillier 算法是安全性基于 DCR 假设的一种概率公钥加密算法，具有加法同态性。

$E(m_1)=g^{m_1}r_1^N \bmod N^2$，$E(m_2)=g^{m_2}r_2^N \bmod N^2$，$E(m_1+m_2)=g^{m_1+m_2}r^N \bmod N^2$

$E(m_1)E(m_2)=(g^{m_1}r_1^N \bmod N^2)(g^{m_2}r_2^N \bmod N^2)=g^{m_1+m_2}r_1^N r_2^N \bmod N^2$

$D(E(m_1+m_2))=D(g^{m_1+m_2}r^N \bmod N^2)=m_1+m_2$

$=D(g^{m_1+m_2}r_1^N r_2^N \bmod N^2)=D(E(m_1)E(m_2))$

另外，显然有 $E(km)=E^k(m)$。

分析 Paillier 体制的加密过程，不难发现。与 RSA 体制不同，Paillier 体制下，每次加密都随机选择一个 $r\in Z_N^*$，这会导致即使是同一明文两次加密会产生不同密文，这给选择明文攻击带来了不小的难度，提高了加密方案的安全性。

加密算法对于保护数据安全性具有非常重要的价值，但计算复杂度也会随着算法安全性的提高而增加。在 Paillier 体制下，加密解密需要频繁地进行模乘和模幂运算，算法的实施较为困难。文献[50]中将复杂模计算转变成 MIARCL 库函数计算，提出了一种 Paillier 密码体制的一种快速实现方法，利用实验数据说明了大密钥下改进算法的效率。

Paillier 算法由于其加法同态性取得了广泛的应用。加法是最简单的运算之一，加同态性可方便参与方之间进行保密的科学计算，在秘密比较[51-53]、三角判定[54]、点积协议[55-56]等领域取得广泛应用。Paillier 算法是加同态的随机化加密算法，下面，我们介绍另外一个经典的随机化同态加密算法。

2.3.3 ElGamal 算法

密钥生成：设 p 是素数，g 是 z_p^* 的生成元。随机选择 $x\in[0,p-1]\cap Z$，计算 $y=g^x \bmod p$。公钥 $pk=y$，私钥 $sk=x$。

加密阶段：明文空间 z_p^* 上的任一消息 m，随机选择 $r\in z_{p-1}$，对应密文 $c=E_{pk}(m)=(c_1,c_2)$，其中，$c_1=g^r \bmod p$，$c_2=my^r \bmod p$。

解密阶段：解密得明文 $m=D_{sk}(c)=\dfrac{c_2}{c_1^x}=\dfrac{my^r}{g^{xr}}=\dfrac{mg^{xr}}{g^{xr}} \bmod p$

图 2.3 ElGamal 密码体制

Fig 2.3 ElGamal cryptosystem

如同 Paillier 算法，ElGamal 算法也是一种随机化的算法，密文由随机数和明文共同决定，增加了安全性同时也加大了数据长度。此算法的安全性基于离散对数难解性假设。另外，为进一步提高加密方案的安全性，应尽量选择强素数。

不难证明，ElGamal 算法是一种具有乘同态性的加密算法：

$E_{pk}(m_1)=(g^{r_1},m_1y^{r_1})$，$E_{pk}(m_2)=(g^{r_2},m_2y^{r_2})$，$E_{pk}(m_1m_2)=(g^{r_3},m_1m_2y^{r_3})$。

定义运算⊗，使得 $E_{pk}(m_1)\otimes E_{pk}(m_2)=(g^{r_1+r_2},m_1m_2y^{r_1+r_2})$，所以此算法可实现乘同态性。

ElGamal 算法是有限域上的运算，此算法的特点是密文由两部分组成，具有乘法同态性，在电子计票，多方排序等领域取得广泛应用。

从以上的介绍中不难发现，RSA、Paillier、ElGamal 算法都只是满足一种运算的同态，应用受到一定的限制。飞速发展的网络对同态加密提出了更高的要求。

2.3.4 全同态加密方案

密钥生成：R 是一个环，B_I 是 R 的一个理想[57] I 的基。由 $IdealGen(R,B_I)$ 生成理想 J 的两个基（B_J^{sk},B_J^{pk}），使得 $I+J=R$，I 和 J 互质。明文空间 M 是 R 的子集 $R \bmod B_I$。公钥 $(R,B_I,B_J^{pk},Samp)$，密钥 B_J^{sk}。$Samp(m,B_I,R,B_J^{pk})$ 表示 $x+I$。

加密阶段：对于任意 $m\in M$，密文 $c\leftarrow Samp(m,B_I,R,B_J^{pk}) \bmod B_J^{pk}$。

解密阶段：解密得明文 $m\leftarrow (c \bmod B_J^{sk}) \bmod B_I$。

图 2. 4 全同态加密方案

Fig 2. 4 Full homomorphic encryption scheme

此算法是 2009 年 Gentry 基于数学理论上环的理想概念提出。算法运用环中理想同态映射的概念，文献[23]中作者给出了正确性证明，并说明了算法的安全性基于离散子集求和问题，同时，作者证明了该方案是即满足加法又满足乘法且具有自检性的全同态加密方案。但该方案为环上的运算，实施较为困难。

Gentry 全同态加密方案是同态加密史上一个里程碑，给全同态加密的研究指出了新的方向，开启了对同态加密研究新的篇章。

2.3.5 整数上的全同态加密算法

Gentry 全同态加密方案为全同态加密方案的发展提供了一个新的方向，Dijk 等人在此基础上了基于简单的代数方案设计了整数范围的全同态加密方案：

密钥生成：η是安全系数，选择一个奇数$p\in[2^{\eta-1},2^{\eta})$作为密钥。

加密阶段：在另一个定义的范围内随机选择两个整数q,r，满足$2r$小于$q/2$。对于明文$m\in\{0,1\}$，密文即为$c=pq+2r+m$，密文同样是一个整数，模p之后等价于明文。

解密阶段：解密得明文$m=(c \bmod p) \bmod 2$。

图 2.5 简单代数同态加密方案

Fig 2.5 Simple algebraic homomorphic encryption scheme

这是利用简单的代数方法实现的一个全同态加密方案。Dijk 等人在此基础上结合 Gentry 理论，设计了一个整数范围的一个安全性基于近似最大因子难题的公钥密码体制下的 Somewhat 同态加密方案[24]。

KeyGen：选取一个η位的奇整数$p\xleftarrow{\$}[2^{\eta-1},2^{\eta})\cap(2Z+1)$作为私钥$sk$。选择$q_0,q_1,\cdots q_\tau\xleftarrow{\$}Z\cap[0,\frac{2\gamma}{p})$，使得最大的$q_i$为奇数，重新排序后使$q_0$为最大数。选择$r_0,r_1,\cdots r_\tau\xleftarrow{\$}Z\cap[-2^\rho,2^\rho]$，令$x_0\leftarrow q_0p+2r_0$，$x_i\leftarrow[q_ip+2r_i]_{x_0}$，$i\in\{1,2,\cdots,\tau\}$。公钥$pk=<x_0,x_1,\cdots x_\tau>$。

Encrypt（pk,m）：随机选取一个集合$S\subseteq\{1,2,\cdots\tau\}$和一个随机整数$r\leftarrow(-2^\rho,2^\rho)$。对于明文$m\in\{0,1\}$，输出密文$c\leftarrow[m+2r+\sum_{i\in S}x_i]_{x_0}$。

Decrypt(sk,c)：输出明文$m\leftarrow[[c]_p]_2$。

图 2.6 Somewhat 加密方案

Fig 2.6 Somewhat cryptosystem

不难证明 somewhat 加密方案满足加法和乘法的同态性。利用 Gentry 提出的压缩方法，可以将此方案扩展成全同态加密方案。

此方案的特点具有全同态性，但每次只能对{0,1}进行加密，计算代价高。此方案提出以后，国内外涌现了许多改进的算法[30-32]。

2.4 本章小节

本章以数学化的方式对同态加密进行了定义；简单介绍了现有同态加密算法的一些安全性理论；重点分析了一些著名的同态加密算法，指出半同态加密算法已趋向成熟并得到广泛应用，并结合各自特点指出其应用情况，而全同态加密算法由于其计算复杂度，目前还没有得到广泛的应用。同态加密技术，未来的发展方向是研究高效、实用的全同态加密方案。下一章中，我们将提出一个实用的同态加密算法，解决某些环境下的安全需求。

第三章 多对一同态加密方案

本章主要介绍我们设计的一个“多方加密，一方解密的”多对一同态加密方案。首先介绍了该方案的应用背景，然后在 2.3.5 节 somewhat 算法基础上提出了本文的同态加密方案，最后对方案进行了分析与扩展。

3.1 引言

密码技术是二十一世纪解决信息安全问题的重要手段，它能有效地保证信息的安全性、识别用户身份的合法性等，被广泛地应用于经济、军事等领域。密码技术历经发展，出现两大分类：安全性基于经典信息论的对称密码和安全性基于计算复杂度理论的公钥密码（非对称密码），这两类密码在现实的应用中都具有重要的意义。随着网络的发展，对密码技术的要求也更为严格，这也推动了现代密码学的不断向前发展。

密码技术的发展越来越考虑实际场景的应用。一般密码技术主要在两方之间实施，难以满足日趋发展的安全需求。面向多方的密码技术成为现代密码学研究的又一方向。在多方的环境中，我们可以通过两方密码加以扩展，但随着用户数量的增加会出现大量的密钥，造成严重的管理和安全问题。为此，文献[58]中第一次提出了广播加密的概念，即由一方加密，得到授权的其他方可以解密。广播加密在无线局域网、3G 网络、有线网络等领域具有重要价值，近年来，成为热点[59-62]。

考虑下面这种场景：一个公司有 n 个部门 $P_1, P_2, \cdots P_n$，不同部门由于业务上存在既竞争又合作的关系，需要对各自数据进行保密，但上级部门 P 为核算整个公司效益、部门工作进展，就需要获取所有部门的秘密业务数据。这就是一个“多方加密，一方解密”的应用场景。在前面提到的几种网络中，大多是需要进行数据交互的，广播加密只能解决“一方加密，多方解密”的情况，反过来却不成立。回到刚才的场景，P_i 因为工作需求往往需要对自己的数据进行加密解密，若仅仅使用 P 的公钥加密，P_i 就无法对数据解密，无法验证其正确性；如果 P 和 P_i 之间采用一对一的加密方式，那 P 需要管理大量的密钥。P_i 由于工作关系可能需要多

次发送自己的数据给 P，这样就会导致 P 都需要亲自对所有 P_i 每次发送的秘密数据解密之后才能进行统计计算，这会造成大量的计算代价；另外，上级部门 P 往往只关心最终结果，但只有 P 拥有密钥，“一对一”的方式要求只能由 P 进行计算，无法由其他部门或者云提供的服务代为计算。

同态加密的出现给加密信息之间的操作提供了新的途径，用户无须解密就能对密文进行多种计算。刚才的场景中，P 和 P_i 之间若采用同态加密技术，P 就不必对每一次接收的数据进行解密，可直接进行密文计算，由此能降低大量的计算代价。在此基础上，我们设想，倘若存在一种加密算法，P_i 能解密自己加密的密文，且 P 的密钥能解密所有 P_i 的加密的信息，P_i 和 P_j 密文在 P 面前呈现同态性（即 P 直接对全部加密方 P_i 传输过来的信息进行计算后再解密，可以得到与先解密后计算相同的结果）。这既能解决密钥管理问题，又能减少计算消耗，且 P 可将计算任务转移，自己只获取最终结果。为此，本文在 Dijk 等人提出的 somewhat 同态加密方案的基础了，基于简单的代数方法，提出了一种多方加密，一方解密的公钥同态加密方案。方案可现实“多对一”的加密模型，且多方之间的不同密文可实现同态的加、乘操作。

在第二节中，我们对一些所需要的预备知识进行简单介绍；第三节详细介绍了多对一的同态加密算法，并进行了相关分析；第四节给出了方案的一个扩展；最后一节，我们对结论进行总结。

3.2 预备知识

3.2.1 数学基础

在第二章中，我们已经介绍了整数分解问题：当正整数 n 很大的时候，找出 n 的所有因子是困难的。Dijk 等人基于 $n=pq$ 构建了 somewhat 加密方案，并通过压缩转换成全同态方案。我们利用 $n=p'pq$ 首先构建对称的同态加密方案：

KeyGen: η_1，η_2 是安全系数，选择 $p\in[2^{\eta_1-1},2^{\eta_1})$，$p'\in[2^{\eta_2-1},2^{\eta_2})$，计算 $p'p$。

Encrypt: 随机生成整数 q,r，满足 $2r<q/2$，对于需要加密的消息 $m\in\{0,1\}$，

对应密文 $c = p'pq + 2r + m$。

Decrypt: 我们可以通过 $m = (c \bmod p) \bmod 2$、$m = (c \bmod p') \bmod 2$ 和 $m = (c \bmod p'p) \bmod 2$ 三种方式解密。

根据数论中的一般知识，方案的正确性是显然的。另外不难证明此方案满足加法同态性和乘法同态性。

因为模运算的特殊性，此方案中共有三种解密方法，随着因子数量的改变，解密的方法也呈现多样性。这种模运算的特殊性对于设计多方加密，一方解密的加密方案具有重要价值。

3.2.2 多对一同态加密模型

定义 2 多对一同态加密算法可描述为：一个解密方 P 和多个加密方 P_i。明文空间 M，P 生成公私钥对（pk, sk），P_i 生成公私钥对（pk_i, sk_i）。除了拥有一般公钥加密算法的性质外，对于加密算法 $E(\cdot)$ 和对应的解密算法 $D(\cdot)$，对任意的明文 $m \in M$，$m_1, m_2 \in M$，满足如下性质，其中 $\oplus$ 表示某一运算符，$i \neq j$：

$$D_{sk_i}(E_{pk_i}(m)) = m，（2\text{-}1）$$

$$D_{sk}(E_{pk}(m)) = m，（2\text{-}2）$$

$$D_{sk_i}(E_{pk_j}(m)) \neq m，（2\text{-}3）$$

$$D_{sk}(E_{pk_i}(m)) = m，（2\text{-}4）$$

$$D_{sk}(E_{pk}(m_1 \oplus m_2)) = D_{sk}(E_{pk}(m_1) \oplus E_{pk}(m_2))，（2\text{-}5）$$

$$D_{sk_i}(E_{pk_i}(m_1 \oplus m_2)) = D_{sk_i}(E_{pk_i}(m_1) \oplus E_{pk_i}(m_2))，（2\text{-}6）$$

$$D_{sk}(E_{pk_i}(m_1 \oplus m_2)) = D_{sk}(E_{pk_i}(m_1) \oplus E_{pk_i}(m_2))，（2\text{-}7）$$

$$D_{sk}(E_{pk}(m_1 \oplus m_2)) = D_{sk}(E_{pk_i}(m_1) \oplus E_{pk_j}(m_2))，（2\text{-}8）$$

式 2-1、2-2 和 2-3 主要是指自己的私钥可以解密用自己公钥加密的信息，而无法解密其他加密方信息；式 2-4 解释多对一的性质，即多个加密方 P_i 加密的密

文可由 P 的私钥进行解密；式 2-5、2-6 说明算法对同一组密钥的同态性；式 2-7 表面 P_i 加密的数据同态性可由 P 解密；而多对一加密的另外一个重要性质由式 2-8 给出，P_i 和 P_j 加密的密文在 P 面前呈现同态性质。

满足以上条件的一个加密算法称为“多对一”的同态加密算法。如何构建这一算法，我们将在后面一节介绍。

3.3 具体方案

3.3.1 参数选择

方案中有许多参数，包括公私钥长度、安全整数等，所有参与由一个安全系数 λ 决定。

γ 是 P 的公钥尺寸，γ_i 是 P_i 的公钥尺寸；

η 是 P 的私钥尺寸，η_i 是 P_i 的私钥尺寸；

ρ 是 P 的干扰尺寸，ρ_i 是 P_i 的干扰尺寸；

τ 是 P 的公钥组成元数量，τ_i 是 P_i 的公钥组成元数量；

为保证协议安全性，各个参数的选择是 $\gamma = O(\lambda^6)$，$\gamma_i = O(\lambda^6)$，$\eta = O(\lambda^5)$，$\eta_i = O(\lambda^2)$，$\rho = \lambda$，$\rho_i = \lambda$，$\tau = \lambda + \gamma$，$\tau_i = \lambda + \gamma$。此参数下本文的计算复杂度 $O(\lambda^{12})$

3.3.2 方案的构建

KeyGen：加密系统由一个解密方 P 和多个加密方 P_i（$i = 1,2\cdots,n$）组成。P 根据 Dijk 等人 somewhat 方案生成公钥 $pk = < x_0, x_1, \cdots x_\tau >$，$sk = p$，（参数大小按照 3.1 节定义）；$P_i$（$i = 1,2\cdots,n$）选择一个整数 $p_i \xleftarrow{\$} [2^{\eta_i - 1}, 2^{\eta_i}) \cap (2Z+1)$ 作为自己的密钥 sk_i。P_i 对 P 的公钥进行随机置换得到 $\overline{pk} = < \overline{x_0}, \overline{x_1}, \cdots \overline{x_\tau} >$，选择 $q_{i,0}, q_{i,1}, \cdots q_{i\tau} \xleftarrow{\$} Z \cap [0, \frac{2^{\gamma_i}}{p_i})$，$r_{i,0}, r_{i,1}, \cdots r_{i,\tau} \xleftarrow{\$} Z \cap [-2^{\rho_i}, 2^{\rho_i}]$，使得 $x_{i,0} \leftarrow q_{i,0} \overline{p_i} p_i^2 x$，$x_{i,j} \leftarrow q_{i,j} p_i \overline{x_j} + 2r_{i,j}$，$j \in \{1,2,\cdots,\tau_i\}$，且 $x_{i,0}$ 最大，重新计算

$x_{i,j} \leftarrow [x_{i,j}]_{x_{i,0}}$ （$[x_{i,j}]_{x_{i,0}} = x_{i,j} \bmod x_{i,0}$），$P_i$ 公钥 $pk_i = < x_{i,0}, x_{i,1}, \cdots x_{i,\tau_i} >$。

Encrypt（pk_i, m_i）：P_i 随机选取一个集合 $S_i \subseteq \{1,2,\cdots\tau_i\}$ 和一个随机整数 $t_i \leftarrow (-2^{\rho_i}, 2^{\rho_i})$。对于明文 $m_i \in \{0,1\}$，输出密文 $c_i \leftarrow [m_i + 2t_i + \sum_{j \in S} x_{i,j}]_{x_{i,0}}$。

Decrypt(sk_i, c_i, sk)：P_i 可根据密钥 $sk_i = p_i$ 解密得 $m_i \leftarrow [[c_i]_{p_i}]_2$，或者 P 根据密钥 $sk = p$，解密得 $m_i \leftarrow [[c_i]_p]_2$。

另外，根据 Dijk 等人的压缩方法，本方案可扩展为一个全同态的加密方案。

3.3.3 正确性分析

引理 1 (pk, sk) 是 P 按照 Dijk 等人 somewhat 方案生产的密钥对，选择 Dijk 方案能够成功实现加密解密。

定理 1 (pk_i, sk_i) 是 P_i 的密钥对。密文 $c_i \xleftarrow{R} Encrypt(pk_i, m_i)$，$m_i \in \{0,1\}$。$P_i$ 使用解密算法 $Decrypt(sk_i, c_i)$ 能成功解密 m_i。

证明 $c_i \leftarrow [m_i + 2t_i + \sum_{j \in S} x_{i,j}]_{x_{i,0}}$，由于 $|x_{i,0}| \geq |x_{i,j}|$，$j \in \{1,\cdots,\tau_i\}$。所以

$$c_i = (m_i + 2t_i + \sum_{j \in S} x_{i,j}) + k_i \cdot x_{i,0}，\ |k_i| \leq \tau_i。$$

对任何一个 j，存在 $q_{i,j}$ 和 $r_{i,j}$，使得 $x_{i,0} \leftarrow q_{i,0} p_i \overline{x_0} + 2r_{i,0}$，$x_{i,j} \leftarrow q_{i,j} p_i \overline{x_j} + 2r_{i,j}$，

整理得：$c_i = p_i(k_i q_{i,0} \overline{x_0} + \sum_{j \in S} q_{i,j} \overline{x_j}) + (m_i + 2t_i + 2k_i r_{i,0} + \sum_{j \in S} 2r_{i,j})$

由 3.1，$|(m_i + 2r_i + 2k_i r_{i,0} + \sum_{j \in S} 2r_{i,j})| < p_i$，令 $a_i = (k_i q_{i,0} \overline{x_0} + \sum_{j \in S} q_{i,j} \overline{x_j})$，$b_i = r_i + k_i r_{i,0} + \sum_{j \in S} r_{i,j}$，有 $c_i = p_i a_i + 2b_i + m_i$，所以 $m_i = [[c_i]_{p_i}]_2$。

综上所述，P_i 使用解密算法 $Decrypt(sk_i, c_i)$ 能成功解密 m_i。

定理 2 (pk_i, sk_i) 是 P_i 的密钥对。密文 $c_i \xleftarrow{R} Encrypt(pk_i, m_i)$，$m_i \in \{0,1\}$。$P$ 使用解密算法 $Decrypt(sk, c_i)$ 能成功解密 m_i。

证明 由定理 1，$c_i = p_i(k_i q_{i,0} \overline{x_0} + \sum_{j \in S} q_{i,j} \overline{x_j}) + (m_i + 2t_i + 2k_i r_{i,0} + \sum_{j \in S} 2r_{i,j})$。因为 $\overline{pk} = < \overline{x_0}, \overline{x_1}, \cdots \overline{x_\tau} >$，根据 Dijk 方案密钥生成 $x_i = q_i p + 2r_i$。所以：

$$c_i = p_i(k_i q_{i,0}(\overline{q_0}p + 2\overline{r_0}) + \sum_{j\in S} q_{i,j}(\overline{q_i}p + 2\overline{r_i})) + (m_i + 2t_i + 2k_i r_{i,0} + \sum_{j\in S} 2r_{i,j})$$

$$c_i = p(p_i k_i q_{i,0}\overline{q_0} + \sum_{j\in S} q_{i,j}\overline{q_i}) + 2(p_i\overline{r_0} + \sum_{j\in S} q_{i,j}\overline{r_i} + t_i + k_i r_{i,0} + \sum_{j\in S} r_{i,j}) + m_i$$

根据 3.1，$|2(p_i\overline{r_0} + \sum_{j\in S} q_{i,j}\overline{r_i} + t_i + k_i r_{i,0} + \sum_{j\in S} r_{i,j}) + m| < p$，令

$a_i = p_i k_i q_{i,0}\overline{q_0} + \sum_{j\in S} q_{i,j}\overline{q_i}$，$b_i = p_i\overline{r_0} + \sum_{j\in S} q_{i,j}\overline{r_i} + t_i + k_i r_{i,0} + \sum_{j\in S} r_{i,j}$，则

$c_i = pa_i + 2b_i + m_i$，所以 $m_i = [[c_i]_p]_2$。

综上所述，P 使用解密算法 $Decrypt(sk, c_i)$ 能成功解密 m_i。

在 3.2.2 节中，我们定义了多对一同态加密的模型，由引理 1、定理 1、定理 2 可知，式 2-1，2-2，2-4 成立。

3.3.4 同态性分析

引理 2 (pk, sk) 是 P 的密钥对，选择 Dijk 方案可现实加法和乘法的同态性

定理 3 (pk_i, sk_i) 是 P_i 的密钥对，P_i 在 3.3.2 节的算法中可实现对密文加法与乘法的同态性。

证明 对任意的明文 $m_{i,1}, m_{i,2} \in \{0,1\}$，密文 $c_{i,1} \xleftarrow{R} Encry(pt_i, pk_{i,1})$ 和 $c_{i,2} \xleftarrow{R} Encrypt(pk_i, m_{i,2})$。由定理 1 可知：存在 $a_{i,1}, b_{i,1}, a_{i,2}, b_{i,2}$ 使得：

$$c_{i,1} = p_i a_{i,1} + 2b_{i,1} + m_{i,1}，\quad c_{i,2} = p_i a_{i,2} + 2b_{i,2} + m_{i,2}。$$

$m_{i,1}, m_{i,2} \in \{0,1\}$，则 $m_{i,1} + m_{i,2} \in \{0,1\}$，$m_{i,1} m_{i,2} \in \{0,1\}$，加密得密文：

$c_{i,3} \xleftarrow{R} Encrypt(pk_i, (m_{i,1} + m_{i,2}))$，$c_{i,3} \xleftarrow{R} Encrypt(pk_i, (m_{i,1} m_{i,2}))$。

由定理 1：存在 $a_{i,3}, b_{i,3}, a_{i,4}, b_{i,4}$ 使得：

$c_{i,3} = p_i a_{i,3} + 2b_{i,3} + m_{i,1} + m_{i,2}$，$c_{i,4} = p_i a_{i,4} + 2b_{i,4} + m_{i,3} m_{i,4}$。

$$c_{i,1} + c_{i,2} = p_i a_{i,1} + 2b_{i,1} + m_{i,1} + p_i a_{i,2} + 2b_{i,2} + m_{i,2}$$

$$= p_i(a_{i,1} + a_{i,2}) + 2(b_{i,1} + b_{i,1}) + m_{i,1} + m_{i,2}$$

$$c_{i,1} c_{i,2} = (p_i a_{i,1} + 2b_{i,1} + m_{i,1})(p_i a_{i,2} + 2b_{i,2} + m_{i,2})$$

$= p_i((p_i a_{i,2} + 2b_{i,2} + m_{i,2})a_{i,1} + (p_i a_{i,1} + 2b_{i,1} + m_{i,1})a_{i,2}) + 2(b_{i,1}b_{i,2} + b_{i,1}m_{i,2} + m_{i,1}b_{i,2}) + m_{i,1}m_{i,2}$

不难证明，$2(b_{i,1} + b_{i,1}) + m_{i,1} + m_{i,2} < p_i$，$2(b_{i,1}b_{i,2} + b_{i,1}m_{i,2} + m_{i,1}b_{i,2}) + m_{i,1}m_{i,2} < p_i$。

P_i 根据 3.2 节解密算法，解密 $D_{sk_i}(c_{i,3}) = m_{i,1} + m_{i,2}$，$D_{sk_i}(c_{i,4}) = m_{i,1}m_{i,2}$，

$D_{sk_i}(c_{i,1} + c_{i,2}) = m_{i,1} + m_{i,2}$，$D_{sk_i}(c_{i,1}c_{i,2}) = m_{i,1}m_{i,2}$。

所以 $D_{sk_i}(c_{i,3}) = D_{sk_i}(c_{i,1} + c_{i,2})$，即 $D_{sk_i}(E_{pk_i}(m_{i,1} + m_{i,2})) = D_{sk_i}(E_{pk_i}(m_{i,1}) + E_{pk_i}(m_{i,2}))$，

$D_{sk_i}(c_{i,4}) = D_{sk_i}(c_{i,1}c_{i,2})$，即 $D_{sk_i}(E_{pk_i}(m_{i,1}m_{i,2})) = D_{sk_i}(E_{pk_i}(m_{i,1})E_{pk_i}(m_{i,2}))$。

综上所述：P_i 在 3.2 节的算法中可实现对密文加与乘的同态性。

定理 4 (pk_i, sk_i) 是 P_i 的密钥对，P 在 3.3.2 节的算法可实现对 P_i 密文的加法与乘法的同态性。

证明 对任意的明文 $m_{i,1}, m_{i,2} \in \{0,1\}$，密文 $c_{i,1} \xleftarrow{R} Encrypt(pk_i, m_{i,1})$ 和 $c_{i,2} \xleftarrow{R} Encrypt(pk_i, m_{i,2})$。由定理 2 可知：存在 $a_{i,1}, b_{i,1}, a_{i,2}, b_{i,2}$ 使得：

$$c_{i,1} = pa_{i,1} + 2b_{i,1} + m_{i,1}，\quad c_{i,2} = pa_{i,2} + 2b_{i,2} + m_{i,2}。$$

$m_{i,1}, m_{i,2} \in \{0,1\}$，则 $m_{i,1} + m_{i,2} \in \{0,1\}$，$m_{i,1}m_{i,2} \in \{0,1\}$，加密得密文：

$c_{i,3} \xleftarrow{R} Encrypt(pk_i, (m_{i,1} + m_{i,2}))$，$c_{i,3} \xleftarrow{R} Encrypt(pk_i, (m_{i,1}m_{i,2}))$。

由定理 2：存在 $a_{i,3}, b_{i,3}, a_{i,4}, b_{i,4}$ 使得：

$c_{i,3} = pa_{i,3} + 2b_{i,3} + m_{i,1} + m_{i,2}$，$c_{i,4} = pa_{i,4} + 2b_{i,4} + m_{i,3}m_{i,4}$。

结合定理 3：

$c_{i,1} + c_{i,2} = p(a_{i,1} + a_{i,2}) + 2(b_{i,1} + b_{i,1}) + m_{i,1} + m_{i,2}$

$c_{i,1}c_{i,2} = (pa_{i,1} + 2b_{i,1} + m_{i,1})(pa_{i,2} + 2b_{i,2} + m_{i,2})$

$= p((pa_{i,2} + 2b_{i,2} + m_{i,2})a_{i,1} + (pa_{i,1} + 2b_{i,1} + m_{i,1})a_{i,2}) + 2(b_{i,1}b_{i,2} + b_{i,1}m_{i,2} + m_{i,1}b_{i,2}) + m_{i,1}m_{i,2}$

又，$2(b_{i,1} + b_{i,1}) + m_{i,1} + m_{i,2} < p$，$2(b_{i,1}b_{i,2} + b_{i,1}m_{i,2} + m_{i,1}b_{i,2}) + m_{i,1}m_{i,2} < p$。

P 根据 3.2 节解密算法，解密 $D_{sk}(c_{i,3}) = m_{i,1} + m_{i,2}$，$D_{sk}(c_{i,4}) = m_{i,1}m_{i,2}$，

$D_{sk}(c_{i,1} + c_{i,2}) = m_{i,1} + m_{i,2}$，$D_{sk}(c_{i,1}c_{i,2}) = m_{i,1}m_{i,2}$。

所以 $D_{sk}(c_{i,3})=D_{sk}(c_{i,1}+c_{i,2})$，即 $D_{sk}(E_{pk_i}(m_{i,1}+m_{i,2}))=D_{sk}(E_{pk_i}(m_{i,1})+E_{pk_i}(m_{i,2}))$，

$D_{sk}(c_{i,4})=D_{sk}(c_{i,1}c_{i,2})$，即 $D_{sk}(E_{pk_i}(m_{i,1}m_{i,2}))=D_{sk}(E_{pk_i}(m_{i,1})E_{pk_i}(m_{i,2}))$。

由此可知：P 在 3.3.2 节的算法可实现对 P_i 密文的加与乘的同态性。

定理 5 (pk_i,sk_i) 是 P_i 的密钥对，(pk_j,sk_j) 是 P_j 的密钥对，P_i 在 3.3.2 节的算法中可实现对 P_i 和 P_j 密文的加法与乘法的同态性。

证明 对任意的明文 $m_i,m_j\in\{0,1\}$，密文 $c_i\xleftarrow{R}Encrypt(pk_i,m_i)$ 和 $c_j\xleftarrow{R}Encrypt(pk_j,m_j)$。由定理 2 可知：存在 a_i,b_i,a_j,b_j 使得：

$$c_i=pa_i+2b_i+m_i,\quad c_j=pa_j+2b_j+m_j。$$

$m_i,m_j\in\{0,1\}$，则 $m_i+m_j\in\{0,1\}$，$m_im_j\in\{0,1\}$。

$c_i+c_j=p(a_i+a_j)+2(b_i+b_j)+m_i+m_j$

$c_ic_j=(pa_i+2b_i+m_i)(pa_j+2b_j+m_j)$

$=p((pa_j+2b_j+m_j)a_i+(pa_i+2b_i+m_i)a_j)+2(b_ib_j+b_im_j+m_ib_j)+m_im_j$ 又，

$2(b_i+b_j)+m_j+m_i<p$，$2(b_ib_j+b_im_j+m_ib_j)+m_im_j<p$。

P 根据 3.2 节解密算法，$D_{sk}(c_i+c_j)=m_i+m_j$，$D_{sk}(c_ic_j)=m_im_j$。

$D_{sk}(E_{pk}(m_i+m_j))=D_{sk}(E_{pk_i}(m_i)+E_{pk_i}(m_j))$

$D_{sk}(E_{pk}(m_im_j))=D_{sk}(E_{pk_i}(m_i)E_{pk_i}(m_j))$。

综上所述：P_i 在 3.3.2 节的算法中可实现对 P_i 和 P_j 密文的加与乘的同态性。

由引理 2、定理 3、定理 4、定理 5 可知，3.2 节加密方案满足式 2-5、2-6、2-7、2-8。结合 3.1 节的正确性证明，本方案是多方加密，一方解密的具有加法和乘法同态性的算法。

在 3.2.2 节中，式子 2-3 还没有满足，即方案的安全性。下一节，我们分析本方案的安全性。

3.3.5 安全性分析

定理 6 本方案的安全性同文献[24]的 somewhat 同态加密方案，基于近似最大公因子难题。

证明 文献[25]中，作者对 somewhat 同态加密方案的正确性、安全性做出了分析，somewhat 同态加密方案的安全性基于近似最大公因子难题。本方案与 somewhat 方案相比，由一对一加密扩展到多对一加密，扩展了加密方的密钥选择方式，加密与解密计算方法不变。

解密方 P 的公私钥同文献[24]somewhat 同态加密方案相同，公私钥的安全性基于近似最大公因子难题。加密方 P_i 随机选择一个大奇数 p_i 作为公钥，随机置换 P_i 的公钥 $\overline{pk}=<\overline{x_0},\overline{x_1},\cdots\overline{x_\tau}>$，并计算 $x_{i,0}\leftarrow q_{i,0}p_i\overline{x_0}+2r_{i,0}$，$x_{i,j}\leftarrow q_{i,j}p_i\overline{x_j}+2r_{i,j}$，$j\in\{1,2,\cdots,\tau_i\}$，由于置换后的 $\overline{x_i}$ 和 $q_{i,j}$ 的随机性，$x_{i,0}$，$x_{i,j}$ 的计算方案可等价于 $x_{i,0}\leftarrow q'_{i,0}p_i+2r_{i,0}$，$x_{i,j}\leftarrow q'_{i,j}p_i+2r_{i,j}$，$j\in\{1,2,\cdots,\tau_i\}$，由此 P_i 得到公钥 $pk_i=<x_{i,0},x_{i,1},\cdots x_{i,\tau_i}>$。可见 P_i 公钥生成与文献[24]somewhat 方案相同，基于近似最大公因子难题假设，P 和其他 P_j（$i\neq j$）无法通过 $pk_i=<x_{i,0},x_{i,1},\cdots x_{i,\tau_i}>$ 获取 P_i 的私钥。

综上所述，3.3.2 节的多方加密、一方解密的同态加密算法是安全的，安全性基于最大公因子难题假设。

3.3.6 实例介绍

前面我们具体介绍了多对一同态加密方案，下面我们通过一个实例进一步理解该方案，为此，我们简化了参数的选择：

假设此多对一同态加密系统由一个解密方 P 和三个加密方 P_i（$i=1,2,3$）组成。P 根据 2.1 节 Dijk 等人 somewhat 方案生成公私钥。令 $sk=9999$，$x_1=9999\times3+2=29999$，$x_2=9999+2=10001$，$x_3=9999\times2+2\times0=19998$，则公钥 $pk=<29999,10001,19998>$。P_1 置换 P 公钥 $\overline{pk}=<10001,19998,29999>$，选

择私钥 sk_1=19，$x_{1,1}=10001\times3\times19+2=570059$，$x_{1,2}=19998\times19+2\times0=379962$，$x_{1,3}=29999\times19+2=569983$，公钥 $pk_1=<570059,379962,569983>$。同样 P_2 选择私钥 sk_2=21，生成公钥 $pk_2=<629981,420044,419958>$，$P_3$ 选择私钥 sk_3=23，生成公钥 $pk_3=<690071,459954,689977>$。下面我们对照 2.2 节多对一同态加密方案模型定义验证本文方案。

1 正确性

对于明文 $m=1$，P 的公钥加密得密文 $c=E_{pk}(m)=(29999+10001)+2\times2+1=40005$，$P$ 根据其私钥解密得 $m=(40005 \bmod 9999) \bmod 2=1$，即 P 可以正确解密其公钥加密的明文。

对于明文 $m=1$，P_1 的公钥加密得密文 $c_1=E_{pk_1}(m)=(570059+379962+569983)+2\times1+1=1520007$，$P_1$ 根据其私钥解密得 $m=(1520007 \bmod 19) \bmod 2=1$，$P$ 根据其密钥解密 $m=(1520007 \bmod 9999) \bmod 2=1$。即 P_1 可以正确解密其公钥加密的明文，P 可以正确解密 P_1 公钥加密的密文。

同样方法可验证 P_2,P_3 加解密的正确性以及 P 对 P_2,P_3 公钥加密密文解密的正确性，体现“多方加密，一方加密”的性质。

2 同态性

明文 $m_1=0,m_2=1$，P 的公钥分别加密得 $c_1=40002,c_2=49998$，$D_{sk}(c_1+c_2)=((40002+49998) \bmod 9999) \bmod 2=1$，$D_{sk}(c_1\times c_2)=((40002\times49998) \bmod 9999) \bmod 2=0$，即 P 的公钥加密的密文在 P 前满足加法与乘法的同态性。

明文 $m_1=0,m_2=1$，P_1 的公钥分别加密得 $c_1=950023,c_2=949950$，$D_{sk_1}(c_1+c_2)=((950023+949950) \bmod 19) \bmod 2=1$，$D_{sk_1}(c_1\times c_2)=((950023\times949950) \bmod 19) \bmod 2=0$，即 P_1 的公钥加密的密文在 P_1 前

满足加法与乘法的同态性。$D_{sk}(c_1+c_2)=((950023+949950)\bmod 9999)\bmod 2=1$，$D_{sk}(c_1\times c_2)=((950023\times 949950)\bmod 9999)\bmod 2=0$，即 P_1 的公钥加密的密文在 P 前满足加法与乘法的同态性。同样 P_2,P_3 的公钥加密的密文在 P 前满足加法与乘法的同态性。

明文 $m_1=0,m_2=1,m_3=1$，P_1 公钥加密 m_1 得 $c_1=1140044$，P_2 公钥加密 m_2 得 $c_2=840003$，P_3 公钥加密 m_3 得 $c_3=1149932$。P 可先对密文计算，再解密。

$$D_{sk}(c_1+c_2)=((1140044+840003)\bmod 9999)\bmod 2=1$$

$$D_{sk}(c_1+c_3)=((1140044+1149932)\bmod 9999)\bmod 2=1$$

$$D_{sk}(c_2+c_3)=((840003+1149932)\bmod 9999)\bmod 2=0$$

$$D_{sk}(c_1+c_2+c_3)=((1140044+840003+1149932)\bmod 9999)\bmod 2=0$$

$$D_{sk}(c_1\times c_2)=((1140044\times 840003)\bmod 9999)\bmod 2=0$$

$$D_{sk}(c_1\times c_3)=((1140044\times 1149932)\bmod 9999)\bmod 2=0$$

$$D_{sk}(c_2\times c_3)=((840003\times 1149932)\bmod 9999)\bmod 2=1$$

即不同公钥加密的密文在 P 前呈现加法与乘法同态性。

3.4 方案扩展

上一节，我们介绍了本文的多方加密、一方解密的同态加密算法，并验证了其正确性与安全性，方案的计算复杂度由 3.3.1 节的参数选择决定。

3.4.1 多层次的“多对一”同态加密算法

本文方案是 Dijk 等人方案的一个扩展，将普通“一对一”的同态加密算法扩展到“多对一”的同态加密算法。如图 3.1：

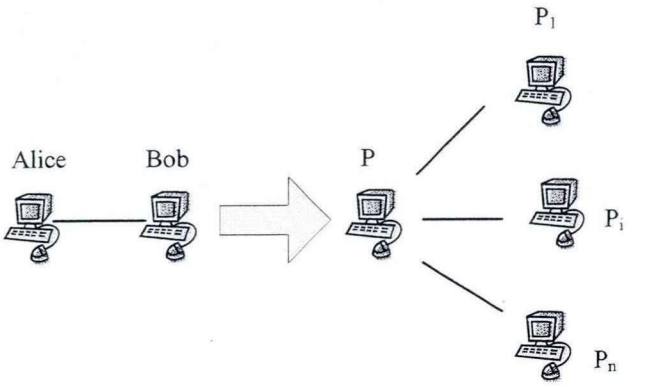

图 3.1 多对一模型

Fig 3. 1 Many-to-one model

从 3.3.5 节的安全性分析中，我们获知扩展的一个基本方法：合理选择参数，将一方的公钥作为计算自己公钥的随机生成元素，即可同样方法生成自己公钥。这是一个可递归的方案。根据需要我们可以进一步扩展为多层次的多对一同态加密方案，如图 3.2：

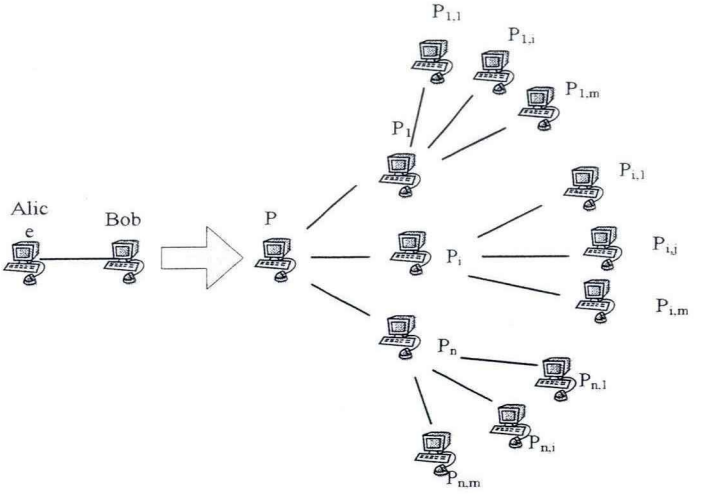

图 3.2 多层次同态加密方案

Fig 3. 2 Multi-level homomorphic encryption scheme

在此多层次的多对一同态加密方案中，处在较高层级的参与方可以实现对其子层的密文解密，且具有同态性。图 3.2 中，P_i 可解密所有 $P_{i,j}$ 的密文，且可对密文直接计算，而 P 可解密图中所有参与方的密文，具有最高权限。这是一个递归的方案，本文不再具体实现该算法。

但这并非是一个可无限扩展的方案，当层数变多的时候，为实现其正确性与

安全性不得不增大参数的选择范围，这会带来巨大的计算代价，方案的效率就会降低。

3.4.2 数据扩展

本文加密解密运算主要是模运算，明文空间{0,1}，实际应用场景的明文往往是较大的整数。利用模运算的特殊性，可对方案进行简单的扩展。我们知道模2运算的结果是0或1，而模q计算结果是$\{0,1\cdots,q-1\}$。我们有一个简单的加密算法：

KeyGen: p大素数为密钥，q素数，$q \ll p$。

Encrypt: 随机生成整数t,r，$m \in \{0,1,\cdots,q-1\}$，密文$c = pt + qr + m$。

Decrypt: $m = (c \bmod p) \bmod q$。

方案的正确性显然，将明文空间由{0,1}扩展到$\{0,1\cdots,q-1\}$。此算法为一个基础的算法，结合3.3节方案，同样的方法可扩展为明文空间为$\{0,1\cdots,q-1\}$的多对一同态加密方案，本文不再介绍。

3.5 本章小节

密码技术是二十一世纪实现信息安全的重要手段，应用场景的多样化使得各种密码技术层出不穷。密码形式也由传统的“一对一”发展到“一对多”、“多对一”、“多对多”的形式，而密码的性质也由单纯的实现加密解密发展到了具有密文可计算性的同态加密技术。本文将“多对一”的思想与同态加密的概念相结合，基于简单的代数理论，在Dijk等人的somewhat方案的基础了提出了一个“多方加密，一方解密”的同态加密方案。方案不仅可以实现“多对一”的密码形式，还同时具有加法和乘法的同态性，即保证了加密方之间信息的安全，又能实现解密方上密文的同态性。方案在军事、经济等领域具有重要价值。最后，在此基础上，本文归纳了一个多层次的“多对一”同态加密方案，可在多层次的环境中应用。此外，本文基于整数分解思想提出的是“多对一”的同态加密方案，如何设计“多对多”的同态加密方案有待进一步研究。

第四章 基于同态加密的安全多方乘积协议

4.1 引言

安全多方计算主要探讨网络环境下多个未知参与方之间的合作计算问题。通常有多个成员参与合作计算，但目前安全多方计算问题多数局限在两方安全计算问题[63-64]的研究中。文献[65]总结了部分特殊的安全两方计算问题，包括安全两方科学计算、安全两方几何计算、安全两方统计分析等，并指出了多方计算协议由两方协议推广得到的方法。虽然安全多方计算问题的研究取得了一定的成果[35-36, 66]，但是特殊的安全多方计算协议距离应用需求还有很大的差距。安全多方乘积（Secure Multi-Party Multiplication）正是这样的一类特殊安全多方计算问题。

安全多方乘积作为SMC最基本的运算之一，近年来得到了广泛的关注。在文献[67]中，作者将一般的乘积问题转换成简单求和问题;借与此种思想,文献[68]给出一个安全两方乘积协议并应用到除法计算中；文献[69]提出基于签名技术的安全多方乘积协议，可有效的防止非法人员对信息的篡改；文献[70]将普通的数量乘扩展到矩阵乘，提出了多方安全矩阵乘积协议并用以到求解线性方程组、矩阵特征值的SMC协议中。现有这些协议因采用茫然传输技术，协议无须第三方的参与，安全性高，在秘密分享、科学计算等安全多方计算领域中具有重要意义。但是，这些多方乘积协议都是由两方协议的扩展得到，参与方两两之间需要频繁通信，造成协议的通信代价高；而利用茫然传输技术的数据量大，造成了网络带宽消耗大、协议的执行效率低等问题。

多方参与的协作计算中，通信代价是衡量协议性能的重要因素。本文利用同态加密技术，在半诚实模型下，设计了适用于不同通信环境下的串行和并行的安全多方乘积协议。比如，在这样的复杂通信环境中：参与方Alice计算一个中间数据时间为1，而Alice与其他参与方通信一次的时间要远远超过1。此时，参与方之间如果频繁的通信会造成较高的通信代价，不利于协议执行。选择通信轮次少的串行协议可有效的降低通信代价；相反，如果参与方之间通信一次的时间接近或小于1，通信环境较为理想的时候，并行协议能有效的减少参与方的等待时间，提高乘积协议的效率。

4.2 预备知识

4.2.1 计算模型

在多方参与的计算环境中，参与者的行为会决定协议的设计难度。按照参与者行为，可分为三种：

（1）诚实参与者。此类参与者在协议执行过程中，严格按照协议要求进行自己的行为，保密自己的所有输入和输出，且不与其他参与方合谋，但可能会根据自己得到的中间数据推算其他参与方的秘密。

（2）半诚实参与者。这类参与方与诚实参与方唯一不同的是，他们可以在参与协议的过程中记录下中间数据、参与方相互联合起来推断其他参与方数据信息、可能将中间结果泄露给恶意参与者。

（3）恶意参与者：恶意者在协议的执行过程中的行为是不确定的。他们会根据自己的攻击意图破坏协议步骤、泄露数据、篡改数据、甚至会终止协议的执行。

本章节提出的安全多方乘积协议主要是在半诚实模型下进行的。

4.2.2 半诚实模型下的安全性

本协议的各参与方是半诚实的，即 n 个参与方 $P_1,P_2,\cdots P_n$，他们各自拥有 x_i，在不暴露各自任何信息的情况下合作计算多项式时间函数：

$$f(x_1,x_2,\cdots x_n)$$

$$=(f_1(x_1,x_2,\cdots x_n),f_2(x_1,x_2,\cdots x_n),\cdots,f_n(x_1,x_2,\cdots x_n))。$$

其中 $f_i(x_1,x_2,\cdots x_n)$ 表示第 i 个分量。设计算 f 的协议标记为 π，那么 $P_i(i=1,2,\cdots n)$ 在执行协议 π 后得到的视图 $\mathrm{VIEW}_i^{\pi}(x_1,x_2,\cdots x_n)=(x_i,r_i,v_{i,1},v_{i,2},\cdots,v_{i,m})$，其中 r_i 是 P_i 随机选择的结果，$v_{i,j}$ 表示 P_i 接收到的第 j 个消息。协议执行后，P_i 得到的输出序列为 $\mathrm{OUTPUT}_i^{\pi}(x_1,x_2,\cdots x_n)$。

上述各方 $P_i(i=1,2,\cdots,n)$ 执行协议 π 能够安全地计算出 f，当且仅当下面的多项式时间算法 $S_i(i=1,2,\cdots,n)$ 成立，即：

$$\{S_i(x_i,f_i),f_1,f_2,\cdots f_{i-1},f_{i+1},\cdots,f_n\}_{x_1,x_2,\cdots x_n}$$

$$\overset{C}{\equiv}\{\mathrm{VIEW}_i^{\pi}(x_1,x_2,\cdots x_n),\mathrm{OUTPUT}_i^{\pi}(x_1,x_2,\cdots x_n)\}_{x_1,x_2,\cdots x_n}$$

其中 $\overset{C}{\equiv}$ 表示计算不可区分，S_i 也称为模拟器。

4.2.3 茫然传输协议

茫然传输（Oblivious Transfer Protocol，OT 协议）的概念最早在 1981 年由 MRabin 在文献[71]提出：Alice 发送给 Bob 两个秘密，Bob 根据自己需求获取其中一个秘密。Alice 不知道 Bob 获取哪个秘密，而 Bob 也无法获取另一个秘密。这样的协议称为 OT_2^1 协议。OT_2^1 协议是在两个秘密中获取一个信息，文献[72]将茫然传输的概念扩展到 OT_n^1，即一个参与方从另一个参与方中的 n 个消息中秘密地获取且只能获取一个信息。茫然传输协议已发展到 $OT_n^m(0<m<n)$，从 n 个消息中秘密地获取 m 个消息。

茫然传输方案实现方法有很多种，文献[73]、[74]给出了 OT_2^1 协议的具体实现过程，频繁的调用 OT_2^1 协议便可以将茫然传输协议扩展到 OT_n^1。而 OT_n^m 协议实现也涌现多种方案[75-76]。

4.2.4 安全两方乘积协议

安全两方乘积协议是计算两方乘积并共享结果的协议。双方各有一个秘密 x 和 y，而计算的结果双方分别得到 u 和 v，使得 $xy=u+v$，协议要求双方不暴露各自的秘密而又能得到正确的计算结果。文献[68]、[69]、[70]中分别基于不同茫然传输设计了安全两方乘积方案。两方乘积协议作为最基本的安全多方计算协议之一，在设计其他复杂科学计算协议等领域得到广泛的应用。

已有安全多方乘积协议大多为两方协议的推广，而两方协议可以是文献[68]和文献[69]等提出的方案，也可由 4.2.1 节的 Paillier 算法的加法同态性质得到。由于乘积具有分配率，即 $x(y+z)=xy+xz$，根据文献[67]提到的一般方法，容易由两方扩展得到一个多方的乘积协议：

输入：P_1 有一个秘密 x_1，…，P_n 有一个秘密 x_n。

输出：P_1 得到 y_1，…，P_n 得到 y_n，且满足 $\sum_{i=1}^{n} y_i = \prod_{i=1}^{n} x_i$。

（1）参与方 P_1，…，P_{n-1} 分别调用两方乘积协议。P_1，…，P_{n-1} 各自获得 y_1 …，

y_{n-1}'，满足$\sum_{i=1}^{n-1} y_i' = \prod_{i=1}^{n-1} x_i$。

（2）$P_1(y_1')$与$P_n(x_n)$执行两方协议，P_1获得y_1，P_n获得$y_{n,1}$。

$P_2(y_2')$与$P_n(x_n)$执行两方协议，P_2获得y_2，P_n获得$y_{n,2}$。

……

$P_{n-1}(y_{n-1}')$与$P_n(x_n)$执行两方协议，P_{n-1}获得y_{n-1}，P_n获得$y_{n,n-1}$。

（3）P_n计算$y_n = \sum_{i=1}^{n-1} y_{n,i}$，协议执行完毕

此扩展协议需要执行$\binom{n}{2} = \frac{n(n-1)}{2}$次安全两方乘积协议，其正确性及安全性由安全两方乘积协议保证。由协议的执行过程可见其复杂性，下面我们介绍本文的安全多方乘积协议。

4.3 基于同态加密的安全多方乘积协议

4.3.1 问题描述及符号说明

（1）问题描述

假设有n个参与方$P_i\ (i=1,\cdots,n)$，每个参与方P_i拥有一个秘密整数x_i。所有参与方希望在不泄露各自秘密的前提下，计算出所有x_i的乘积并且由参与方共享计算结果。

（2）相关符号说明

RANDOM SELECT $r_1, r_2, ..., r_n$，代表选择随机n个数$r_1, r_2, ..., r_n$；

$x \to y$，代表将变量x值赋给变量y；

SEND(Alice, Bob, $s_1, s_2, s_3, ..., s_n$*)*，表示 Alice 将信息$s_1, s_2, ..., s_n$发送给 Bob；

Alice *COMPUTE*，表示 Alice 进行计算；

Alice *GET* s，表示 Alice 获得信息s。

4.3.2 串行的安全多方乘积方案

以下给出串行和并行安全多方乘积协议的详细步骤，数据传输流程分别如图 4.1、图 4.2 所示。

$$P_1 \xrightarrow{z_{1,1}} P_2 - - \to P_i \xrightarrow{z_{i,1}, z_{i,2}, \cdots, z_{i,i}} P_{i+1} - - \to P_n \xrightarrow{z_{n,1}, z_{n,2}, \cdots, z_{n,n}} P_1$$

图 4.1 串行协议数据传输流程

Fig 4. 1 Serial protocol data transfer process

注：$P_A \xrightarrow{z_{i,j}} P_B$，图中表示 P_A 将数据 $z_{i,j}$ 发送给 P_B.

输入：参与方 $P_i\ (i=1,\cdots,n)$ 拥有整数 x_i，P_i 选择 2.2 节 *Paillier* 算法并产生公私钥 (pk_i, sk_i)。

输出：P_i 获得整数 y_i，使得 $\sum_{i=1}^{n} y_i = \prod_{i=1}^{n} x_i$。

协议步骤如下：

Step1 *For* $i=1 to n$

P_i *RANDOM SELECT* $r_{i,1}, r_{i,2}, \ldots, r_{i,i-1}$

/* P_i 选择 $i-1$ 个整数，P_1 不选择*/

P_i *COMPUTE* $\sum_{j=1}^{i-1} r_{i,j} \to r_i$

/*例如，$r_3 = r_{3,1} + r_{3,2}$，令 $r_1 = x_1$*/

end For

Step2 *For* $i=1 to n$

/*如图 4.1 所示 n 个参与方依次进行计算*/

P_i *COMPUTE* /* P_i 计算 i 个中间数据*/

For $j=1 to i$

if $j=i$ $E_{pk_i}(r_i) \to z_{i,i}$

else $z_{i-1,j}^{x_i} E_{pk_j}(-r_{i,j}) \to z_{i,j}$

end if

end For

$SEND(P_i, P_{i+1}, z_{i,1}, z_{i,2}, \ldots, z_{i,i})$ /* P_{n+1} 即 P_1*/

end For

Step3 *For* $i=1 to n$

P_i *GET* $z_{n,i}$

/* P_i 从 P_{i-1} 传来的数据中获得 $z_{n,i}$*/

$SEND(P_i, P_{i+1}, z_{n,i+1}, z_{n,i+2}, \cdots, z_{n,n})$

/*当P_n获得$z_{n,n}$后，无数据可发*/

end For

Step4 *For* $i=1$ *to* n

P_i *COMPUTE* $D_{sk_i}(z_{n,i}) \rightarrow y_i$

end For /*协议执行完毕*/

串行协议中，参与方P_i存在等待时间，我们改变协议的执行规则，得到并行协议。

4.3.3 并行的安全多方乘积方案

输入：参与方P_i $(i=1,\cdots,n)$拥有整数x_i，P_i选择 2.2 节 *Paillier* 算法并产生公私钥(pk_i, sk_i)。

输出：P_i获得整数y_i，使得$\sum_{i=1}^{n} y_i = \prod_{i=1}^{n} x_i$。

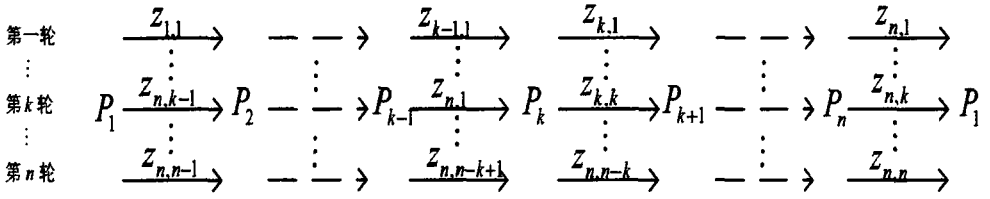

图 4.2 并行协议数据传输流程

Fig 4. 2 Parallel protocol data transfer process

协议步骤如下：

Step1 *For* $i=1$ *to* n

P_i *RANDOM SELECT* $r_{i,1}, r_{i,2}, \ldots, r_{i,i-1}$

/*P_i选择$i-1$个整数，P_1不选择*/

P_i *COMPUTE* $\sum_{j=1}^{i-1} r_{i,j} \rightarrow r_i$

/*例如，$r_3 = r_{3,1} + r_{3,2}$，令$r_1 = x_1$*/

end For

Step2 *For* $k=1$ *to* n /*如图 4.2 每个参与方执行n轮计算或数据传送*/

if $k=1$ /*第一轮*/

For $i=1$ *to* n /*同一轮下，参与方同时进行*/

P_i *COMPUTE* $E_{pk_i}(r_i)\rightarrow z_{i,1}$

$SEND(P_i,P_{i+1},z_{i,1})$

end For

else /*第 k 轮*/

For $i=1$ *to* n

if $i<k$ /*编号小于计算轮次的参与方只进行数据传递，如图 4.2*/

$SEND(P_i,P_{i+1},z_{n,k-i})$

else /*编号大于计算轮次的参与方进行计算和数据传递*/

P_i *COMPUTE* $z_{i-1,k-1}^{x_i}E_{pk_{i+1-k}}(-r_{i,k-1})\rightarrow z_{i,k}$

$SEND(P_i,P_{i+1},z_{i,k})$

end if

end For

end if

end For

Step3 *For* $i=1$ *to* n

P_i *COMPUTE* $D_{sk_i}(z_{n,n-i+1})\rightarrow y_i$

end For /*协议执行完毕*/。

4.4 方案分析

4.4.1 串行方案分析

定理 7 在半诚实模型下，串行多方乘积协议能够使参与方 P_i 得到整数 y_i，满足 $\sum_{i=1}^{n}y_i=\prod_{i=1}^{n}x_i$。

证明 在串行协议 Step2 中：

$$z_{n,i}=z_{n-1,i}^{x_n}E_{pk_i}(-r_{n,i})=(z_{n-2,i}^{x_{n-1}}E_{pk_i}(-r_{n-1,i}))^{x_n}E_{pk_i}(-r_{n,i})$$

$$=\cdots=((\cdots(E_{pk_i}^{x_{i+1}}(r_i)E_{pk_i}(-r_{i+1,i}))^{x_{i+2}}\cdots)^{x_{n-1}}E_{pk_i}(-r_{n-1,i}))^{x_n}E_{pk_i}(-r_{n,i})$$

根据 2.1 节加同态性质，P_i 解密 $z_{n,i}$ 得到：

$$y_i = D_{sk_i}(z_{n,i}) = r_i x_{i+1} \cdots x_n - r_{i+1,i} x_{i+2} \cdots x_n - \cdots - r_{n-1,i} x_n - r_{n,i}$$

所以：

$$y_1 = x_1 x_2 \cdots x_n - r_{2,1} x_3 x_4 \cdots x_n - \cdots - r_{n-1,1} x_n - r_{n,1}$$

$$y_2 = r_2 x_3 \cdots x_n - r_{3,2} x_4 \cdots x_n - \cdots - r_{n-1,2} x_n - r_{n,2}$$

$$\cdots$$

$$y_i = r_i x_{i+1} \cdots x_n - r_{i+1,i} x_{i+2} \cdots x_n - \cdots - r_{n-1,i} x_n - r_{n,i}$$

$$\cdots$$

$$y_{n-1} = r_{n-1} x_n - r_{n,n-1}$$

$$y_n = r_n$$

结合 Step1 中，$\sum_{j=1}^{i-1} r_{i,j} \to r_i$，所以 $\sum_{i=1}^{n} y_i = \prod_{i=1}^{n} x_i$。

由上可知，串行协议是正确的。

定理 8 在半诚实模型下，串行多方乘积协议参与方除了得到 y_i，无法得到其它参与方秘密。

证明 设串行多方乘积协议标记为 π，我们通过构造模拟器的方式对 π 进行安全性证明：

对 $P_i(i=1,2,\cdots,n)$ 的视图：P_i 通过协议 π 在 Step2 中得到由 P_{i-1} 发送的数据 $z_{i-1,1}, z_{i-1,2} \cdots z_{i-1,i-1}$。对 P_i 产生视图可记为：

$\mathrm{VIEW}_i^{\pi}(x_1, x_2, \cdots x_n) = (x_i, r_i, (z_{i-1,1}, z_{i-1,2}, ..., z_{i-1,i-1}))$，其中 $E_{pk_{i-1}}(r_{i-1}) \to z_{i-1,i-1}$，$z_{i-2,j}^{x_{i-1}} E_{pk_j}(-r_{i-1,j}) \to z_{i-1,j}$ $(i \neq j)$。

P_i 模拟器 S_i 产生过程如下：$S_i(x_i, f_i(x_1, x_2, \cdots x_n)) = (x_i, r_i, (z_{i,1}, z_{i,2}, ..., z_{i,i}))$，其中 $E_{pk}(r_i) \to z_{i,i}$，$z_{i-1,j}^{x_i} E_{pk_j}(-r_{i,j}) \to z_{i,j}$ $(i \neq j)$。由于 x_i 是 P_i 私有的，且 $r_{i,j}$ 是随机的，基于 Paillier 的语义安全性，所以 $(z_{i-1,1}, z_{i-1,2}, ..., z_{i-1,i-1})$ 和 $(z_{i,1}, z_{i,2}, ..., z_{i,i-1})$ 计算不可区分；另外，$E_{pk}(r_i) \to z_{i,i}$ 由 P_i 的公钥加密的，无密钥的参与方无法解密，所以 P_i 视图与模拟器输出是计算不可区分的，P_i 的信息没有泄露。

综上所述，串行多方乘积协议的安全的，参与方除了得到 y_i，无法得到其它参与方秘密。

效率分析：

（1）计算复杂度：假设本协议的数据长度为m bit，Paillier加密方案的模为M，那么一次加密或者加密需要$2\log M$次模乘，一次模指运算$E(x)^k$最多$2m+1$次模乘。Step2中，P_i加密计算i个中间数据，需要$i-1$次模指运算和i次加密运算，Step4中进行一次解密运算。所以总计算复杂度为$O(n^2(m+\log M))$次比特模乘运算。

（2）通信复杂度：由Step2中$SEND(P_i,P_{i+1},z_{i,1},z_{i,2},...,z_{i,i})$和Step3中$SEND(P_i,P_{i+1},z_{n,i+1},z_{n,i+2},...,z_{n,n})$可知，串行协议的参与方$P_i$只与$P_{i+1}$进行两次通信，发送$n$个数据。所以总的通信轮次是线性的，带宽$O(mn^2)$。

4.4.2 并行方案分析

定理9 在半诚实模型下，并行多方乘积协议能够使参与方P_i得到整数y_i，满足$\sum_{i=1}^{n} y_i = \prod_{i=1}^{n} x_i$。

证明：在并行方案的Step2中可知，当参与方编号小于计算轮次的参与方只进行数据传递，而编号大于计算轮次的参与方进行计算和数据传递。每个中间数据$z_{i,k}$都只采用同一个用户的公钥pk_{i+1-k}进行加密等运算，Step2执行完毕之后，参与方P_i得到采用pk_i加密的$z_{n,n-i+1}$。根据同态机密的性质，Step3中由P_i解密得到$y_i = r_i x_{i+1}\cdots x_n - r_{i+1,1}x_{i+2}\cdots x_n - \cdots - r_{n-1,n-1-i}x_n - r_{n,n-i}$。结合定理7可知：$\sum_{i=1}^{n} y_i = \prod_{i=1}^{n} x_i$。所以方案是正确的。

定理10 在半诚实模型下，并行多方乘积协议参与方除了得到y_i，无法得到其它参与方秘密。

证明：Step2中，每一轮计算：

当参与方编号小于计算轮次时，参与方只进行数据传递。此时，由$SEND(P_i,P_{i+1},z_{n,k-i})$可知，参与方$P_i$知道$z_{n,k-i}$。有定理8可知$z_{n,k-i}$是由$pk_{k-i}$加密的，$P_i$无法从$z_{n,k-i}$获取任何有价值的信息。

当参与方编号大于计算轮次的时候，参与者P_i计算$z_{i-1,k-1}^{x_i}E_{pk_{i+1-k}}(-r_{i,k-1})\rightarrow z_{i,k}$并将

计算结果发送给 P_{i+1}。$z_{i-1,k-1}^{x_i} E_{pk_{i+1,k}}(-r_{i,k-1}) \to z_{i,k}$ 中使用 x_i 和 $r_{i,k-1}$ 两个保密参数，根据 Paillier 算法的安全性可知，并结合串行方案的安全性证明，即使其他参与方合谋也无法获取 x_i 和 $r_{i,k-1}$ 的信息。

由上可知，并行协议是安全的。

定理 11 并行方案的计算复杂度同串行方案，通信轮次 $O(n^2)$，带宽 $O(mn^2)$。

证明：比较并行方案和串行方案可知，两个方案仅仅是数据流的不同，数据量以及计算方法没有发生变化，所以计算复杂度同方案。

另外，并行方案总数据量没有变化，所以总带宽为 $O(mn^2)$。由 Step2 中的 $SEND(P_i, P_{i+1}, z_{i,k})$ 可知参与方之间每次只实时发送一个数据，因此增加了参与方之间的通信轮次，总通信轮次为 $O(n^2)$。

4.4.3 协议比较

在前两节，我们具体的介绍了本文提出的安全多方乘积协议，并分析了协议的正确性、安全性以及复杂度。单从这些分析来看，很难体现本文优势之处。为了突出本文优势，这一节我们将本文的两个协议同现有安全多方乘积协议相比较，结果如表 4.1 所示。

表 4.1 安全多方乘积协议比较

Table 4.1 The secure multiparty multiplied protocol comparison

协议	安全性	计算复杂度	通信代价		理想通信环境下协议执行时间
			通信轮次	带宽	
文献[69]	OT_1^2 安全性	$O(lmn^2)$	$O(ln^2)$	$O(lmn^2)$	$O(ln^2)$
文献[70]	OT_1^p 安全性	$O(plmn^2)$	$O(ln^2)$	$O(plmn^2)$	$O(pln^2)$
串行协议（本文）	Paillier 算法安全性	$O(n^2(m+\log M))$	$O(n)$	$O(mn^2)$	$O(n^2)$

并行协议（本文）	Paillier 算法安全性	$O(n^2(m+\log M))$	$O(n^2)$	$O(mn^2)$	$O(n)$

注：l，p 为茫然传输安全系数，n 为参与方个数，m 为数据长度。文献[70]提出的多方矩阵乘积协议，当矩阵维数是 1 的时候就退化为数量乘积。假设在理想通信环境下，计算一个中间数据的时间为 1。

由表 4.1 可知，本文利用同态加密技术，在保证安全性的同时，减少了数据量，避免了文献[69]和文献[70]中所有参与方两两之间都需要频繁通信的情况，降低了通信代价。在计算代价相当的情况下，串行协议和并行协议各有优势，串行协议通信轮次少，适用于通信较为复杂的网络环境；当网络环境较为理想或者参与方数量较多时，并行协议参与方无须等待，可以减少协议的执行时间。

此外，本文的通信模型为环形，此模型可进一步优化。根据参与方之间的通信代价，设计一个通信代价最低的环，提高协议执行效率；也可以结合信任评估模型[77]设计一个通信方之间信任度最高的环，提高协议的安全性。与文献[69]和文献[70]中的复杂网状模型相比，本文降低了对通信环境的要求，无需所有参与方之间都存在通信关系，只要能形成一个通信环，协议便能正确执行，减少了被攻击的途径。

4.5 扩展的点积协议

4.5.1 点积协议

点积协议是另一个比较实用的安全协议，与安全两方乘积协议有相似的地方。只是点积协议主要计算两个向量的乘积，并共享向量的计算结果。可理解为对安全两方乘积协议的扩展。Alice 有一个秘密向量 $X=(x_1,x_2,\cdots,x_n)$，Bob 有一个秘密向量 $Y=(y_1,y_2,\cdots,y_n)$，协议执行之后 Alice 得到 u，Bob 得到 v，使得 $u+v=\sum_{i=1}^{n}x_iy_i$。执行过程中不泄露各自向量的任何信息也无法获得另一方的最终结果。

同安全两方乘积协议相同，点积协议也可利用茫然传输协议来设计，安全性高。另外，随着点积协议应用领域的扩展，不同思想的点积协议不断涌现，文献[50]对常用的点积协议构造方法进行了总结。

4.5.2 扩展的点积协议

前面我们提出了基于同态加密技术的安全多方乘积方案，并验证了其正确性与安全性。乘积作为一个基本的运算存在着广泛的应用，我们利用 4.3 节的安全多方乘积协议提出了一个扩展的点积协议。

生活中可能存在这样的场景：产品从生产到销售可能要经历很多环节，生产商，供应商，中间商，销售商都要获取一定的利润，如表 4.2。由于存在即竞争又合作的关系，他们在实施合作之前要对自己在每种产品中获取的利润保密。为了评估整个合作中产生的总效益，他们之间需要进行安全的多方计算。

表 4.2 商品利润率

Table 4. 2 Commodity interest

	成本	生产商利润率	供应商利润率	中间商利润率	销售商利润率
商品 A	W	a_1	b_1	c_1	d_1
商品 B	X	a_2	b_2	c_2	d_2
商品 C	Y	a_3	b_3	c_3	d_3
商品 D	Z	a_4	b_4	c_4	d_4

从表不难发现，他们在四种商品之间的合作产生总利润为 $a_1b_1c_1d_1W+a_2b_2c_2d_3X+a_3b_3c_3d_3Y+a_4b_4c_4d_4Z$，为了实现安全计算的目的，此时需要一个扩展的点积协议。

在第二章中，我们给出了点积协议的定义。而扩展的点积协议可以描述为：参与方 P_1 有一个私有的向量 $X_1=(x_{11},x_{12},\cdots,x_{1m})$，$P_2$ 有一个私有的向量 $X_2=(x_{21},x_{22},\cdots,x_{2m})$，…，$P_n$ 有一个私有的向量 $X_n=(x_{n1},x_{n2},\cdots,x_{nm})$。所有参与方希望计算 $\sum_{i=1}^{n}\prod_{j=1}^{m}x_{ij}$ 的结果并由所有参与方共享，在此过程中不泄露参与方任何信息。具体协议如下：

输入：参与方 $P_i\ (i=1,\cdots,n)$ 输入秘密向量 $X_i=(x_{i1},x_{i2},\cdots,x_{im})$。

输出：参与方 $P_i\ (i=1,\cdots,n)$ 获得 y_i，使得 $\sum_{i=1}^{n}y_i=\sum_{i=1}^{n}\prod_{j=1}^{m}x_{ij}$。

协议步骤如下：

Step1 参与方 $P_i\ (i=1,\cdots,n)$ 输入 x_{i1} 执行 4.3 节的安全多方乘积方案（根据具体环境选择并行或者串行方案），P_i 得到 y_{i1}。

Step2 每次改变参与方 P_i 的输入 $x_{ij}\ (i=2,\cdots,m)$ 重复执行 Step1，P_i 得到 $y_{ij}\ (i=2,\cdots,m)$。

Step3 P_i 计算 $y_i=\sum_{j=1}^{m} y_{i,j}$，协议执行完毕。

此协议根据具体的环境选择适用的多方乘积方案。协议的正确性显然，安全性由多方乘积的安全性保证。结合表 1，生产商拥有向量 $\vec{a}=(a_1,a_2,a_3,a_4)$，供应商拥有向量 $\vec{b}=(b_1,b_2,b_3,b_4)$，中间商拥有向量 $\vec{c}=(c_1,c_2,c_3,c_4)$，销售商拥有向量 $\vec{d}=(d_1,d_2,d_3,d_4)$，运用扩展的点积协议即可安全的计算出总的利益。

4.6 本章小节

安全多方计算在信息和通信安全中都占有重要的地位，而同态加密技术是安全多方计算中的关键技术之一。结合实际，本文提出了两个适用不同环境的安全多方乘积协议，协议无须第三份的参与，保证安全性的同时降低了通信代价，提高了协议的执行效率。此外，现有的安全多方计算协议多为两方协议的扩展，本文提出一个 SMC 基础协议，为研究安全多方计算其他问题提供了新思路，在此基础上设计了一个扩展的点积协议。本文是基于半诚实模型下的协议，恶意模型下参与方可能不完全遵守协议，如何对参与方的行为进行验证，构建安全的多方计算协议有待进一步的研究。

第五章 总结与展望

本章将对全文在同态加密领域所做的工作进行系统的梳理，对文中主要解决的问题进行分析，并讨论其中的不足，由此指出在同态加密领域进一步的研究方向。

5.1 文章总结

同态加密技术是二十一世纪信息安全领域热门的研究课题之一。同态加密由于其特殊的自然属性，在电子商务、云服务、物联网等领域具有广泛应用。本文主要针对同态加密的算法设计问题和其在安全领域的应用情况进行了研究。本文主要工作有以下三点：

（1）系统总结了同态加密的发展状况，详细介绍了几个较为典型的同态加密方案，分析每个同态加密方案的技术特点和其在安全领域取得的成就。以此提出进一步的设想。

（2）多对一同态加密方案。安全应用场景的多样性，使得对密码技术的要求越来越多。传统的一对一的密码形式已经不能满足多用户场景的安全需求。“多对一”，“一对多”，“多对多”的加密技术成为密码界研究又一方向。本文指出了一个“多对一”加密技术的应用场景，并运用简单的代数理论，在安全性基于近似最大公因子难题的整数全同态加密方案基础上，设计了一个多方加密，一方解密的“多对一”同态加密方案，使得加密技术不仅有“多对一”的特点，还具有加法与乘法的同态性。此方案可进一步扩展成一个多层次的加密方案。

（3）基于同态加密技术的安全多方乘积协议。安全多方计算是同态加密的一个重要的应用领域。多方乘积计算问题是一个基础的安全多方计算问题，但现有多方乘积协议多为两方扩展，没有考虑通信环境，通信复杂度高、效率低。针对此问题，结合同态加密技术的特点，在半诚实模型下，基于 Paillier 算法提出了适用于不同环境的串行和并行的安全多方乘积协议。协议考虑具体环境，大大提高了执行效率，为研究其他多方计算协议提供了新的思路。

5.2 进一步研究展望

同态加密技术是一个热门的研究领域，在信息安全领域具有很多的实际应用。对同态加密的研究也不仅限于此，本文提出的“多对一”具有加法和乘法同态性的加密方案和基于同态加密的安全多方乘积协议都具有一定的局限性，我们还需进一步研究：

（1）深入研究全同态的加密方案。目前较为成熟的同态加密技术多为半同态方案，全同态的方案由于其复杂性和安全性等因素暂未得到广泛的应用。随着云计算的快速发展，迫切需求这种具有全同态性质的高效、安全的加密算法。对于加密算法而言，高效、安全、全同态性三者之间本身就是一种矛盾。我们需要进一步研究全同态加密技术，结合特定的适用场景，平衡三者之间的矛盾。

（2）深入研究高效、安全的“多对多”同态加密方案。本文提出了“多对一”的同态加密方案，此方案是对整数上全同态加密方案的扩展，但目前全同态加密技术的不成熟，本文的方案还有待进一步提高效率。另外，本方案是“多对一”的方案，未能达到“多对多”的需求。但我们在文中已经的知道“多对多”模型的迫切性，如果设计“多对多”同态加密方法是下一步的研究工作

（3）扩展同态加密技术的应用领域，突破半诚实模型。本文设计的适用不同环境的两个多方乘积协议是在半诚实模型下的协议，协议不能抵抗恶意攻击者的破坏。为使多方乘积协议更具有适用性，我们需要进一步研究，设计一个可在恶意模型下执行的多方乘积协议。另外，乘积协议仅仅是同态加密技术应用的一个方面，我们需要扩展同态加密技术的应用领域，不仅在半诚实模型下，也在恶意模型下，设计多款高效、实用的安全协议。

参考文献

[1] R.Rivest,L.Adleman,and M.Dertouzos.On data banks and privacy homomorphisms[C].In Foundations of Secure Computation,pages 169-180,1978

[2] A.C.Yao, "Protocols for secure computations," In:Proc.23rd Annual IEEE Symposium on Foundations of Computer Science.Los Alamitos:IEEE Computer Society Press, pp.160- 164,1982

[3] O.Goldreich, Silvio Micali, and Avi Wigderson, "How to Play any Mental Game," The 19th Annual ACM Conference on Theory of Computing,NewYork, pp.218-229,1987

[4] Diffie,W. and Hellman,M.E, "New directions in cryptography,"IEEE Trans. On Information Theory, Vol.IT-22,No.6,pp.644-654.Nov.1976

[5] Above the clouds: a berkeley view of cloud computing. http://www.eecs.berkeley.edu/Pubs/TechRpts/2009/EECS-2009-28.html

[6] 司品超, 董超群, 吴利, 等. 云计算: 概念, 现状及关键技术[J]. 2008 年全国高性能计算学术年会论文集, 2008.

[7] 冯登国, 张敏, 张妍, 等. 云计算安全研究[J]. 软件学报, 2011, 22(1).

[8] R. L. Rivest, A. Shamir, and L. Adleman. "A method for obtaining digital signatures and public-key cryptosystems,"Communications of ACM,Vol.21,No.2, pp.120-126,Feb.1978

[9] Paillier P. Public-key crytosystems based on composite degree residuosity classes[C].Advances in cryptology-EUROCRYPT 99，LNCS1592. Berlin: Springer-Verlag，1999：223. 238

[10] D. R. Stinson. Cryptography: Theory and Practice. CRC Press, Inc.,Boca Raton, FL, USA, 1995.

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

[12] 王育民,刘建伟.通信网的安全——理论与技术[M].西安电子科技大学出版社，2005,35-36.

[13] Leonard M.Adleman. "Factoring numbers using singular integers," Proceedings of the twenty-third annual ACM symposium on Theory of computing Pages 64-71,1991

[14] J Buhler, H Lenstra, C Pomerance. "Factoring integers with the number field sieve,"A.K.Lenstra and H.W.Lenstra Jr.(Eds),The Development of the Number Field Sieve volume 1554 of Lecture notes in Mathematics, pp.50-94, Springer-Verlag,1993.

[15] Simmons,G.J.and Norris,M.J. "Prelimimary comments on MIT public key cryptosystem,"Cryptologia,Vol.2,406-417,1977.

[16] Moore,J.H. "Protocol failures in cryptosystems,"Proceedings of the IEEE,Vol.76,No.5,pp594-602,May 1988.

[17] Wiener,M.J. "Cryptanalysis of short RSA secret exponents,"IEEE Trans.on Information Theory,Vol.36,NO,3,pp.553-558.May 1990.

[18] Goldwasser S，Micali S．Probabilistic encryption[J]．Journal of Computer and System Sciences，1984，28(2)：270-299.

[19] 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.

[20] 章照止.现代密码学基础[M].北京邮电大学出版社，2008，256-263.

[21] Benaloh J．Dense probabilistic encryption[C].Proc of theworkshop on selected areas of cryptography(SAC' 94)．Kingston，Canada，1994：120-128.

[22] 向广利, 陈莘萌, 马捷, 等. 实数范围上的同态加密机制[J]. 计算机工程与应用, 2005, 41(20): 12-14.

[23] Craig Gentry. A fully homomorphic encryption scheme[M]. Stanford University, 2009.

[24] van Dijk M，Gentry C，Halevi S，et al.Fully homomorphic encryption over the integers[C]//Volume 6110 of LNCS：Proc of Eurocrypt，2010：24-43.

[25] Smart N P，Vercauteren F.Fully homomorphic encryption with relatively small key and ciphertext sizes[C]// Volume 6056 of Lecture Notes in Computer

Science：Public Key Cryptography-PKC’10，Springer，2010.

[26] GENTRY Craig，HALEVI Shai. Implementing Gentry's Fully-homomorphic Encryption Scheme[C]//EUROCRYPT.[s.l.]：Springer，2011：129-148.

[27] Zvika Brakerski, Vinod Vaikuntanathan. Efficient Fully Homomorphic Encryption from (Standard) LWE[J]. IEEE Symposium on Foundations of Computer Science,2011.

[28]Craig Gentry ,Shai Halevi.Fully Homomorphic Encryption without SquashingUsing Depth-3 Arithmetic Circuits[J]. IEEE Symposium on Foundations of Computer Science,2011.

[29] Craig Gentry, Shai Halevi, and Vinod Vaikuntanathan. A Simple BGN-Type Cryptosystem from LWE. Lecture Notes in Computer Science Volume 6110, 2010, pp 506-522

[30] 汤殿华, 祝世雄, 曹云飞. 整数上全同态加密方案的重加密技术[J]. 信息安全与通信保密, 2012, 1: 037.

[31] 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.

[32] 徐鹏, 刘超, 斯雪明. 基于整数多项式环的全同态加密算法[J]. Computer Engineering, 2012, 38(24).

[33] Ying Luo, Sen-ching S. Cheung, Shuiming Ye. Anonymous Biometric Access Control Based on Homomorphic Encryption[J]. IEEE International Conference on Multimedia and Expo,2009.

[34] 陈良. 基于同态加密的移动代码安全技术研究 [D] 华南理工大学, 2009.

[35] 肖倩, 罗守山, 陈萍, 等. 半诚实模型下安全多方排序问题的研究[J]. 电子学报, 2008, 36(4): 709-714.

[36] 邱梅, 罗守山, 刘文, 等. 利用 RSA 密码体制解决安全多方多数据排序问题[J]. 电子学报, 2009, 37(5): 1119-1123.

[37] 黄福人. 电子投票的研究与设计[D]. 中国科学技术大学, 2010.

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

[39] 李美云, 李剑, 黄超. 基于同态加密的可信云存储平台[J]. 信息网络安全, 2012, 9: 015.

[40] H.Y.Lin and W.G.Tzeng. An efficient solution to the millionaires problem based on hormomorphic encryption. ACNS 2005,Vol.35 31 of LNCS, 2005:456–466.

[41] Cormen T H, Leiserson C E, Rivest R L, et al. Introduction to algorithms[M]. MIT press, 2001.

[42] Rawlins G J E. Compared to what?: an introduction to the analysis of algorithms[M]. Computer Science Press, 1992.

[43] Papadimitriou C H. Computational complexity[M]. John Wiley and Sons Ltd., 2003.

[44] Rueppel R A. Security models and notions for stream ciphers[J]. Cryptography and Coding, 1992, 11: 213-230.

[45] Howgrave-Graham N. Approximate integer common divisors[J]. Cryptography and Lattices, 2001: 51-66.

[46] Martello S, Toth P. Knapsack problems: Algorithms and computer interpretations[J]. Hoboken, NJ: Wiley-Interscience, 1990.

[47] Pfitzmann B, Waidner M. Attacks on protocols for server-aided RSA computation[C]//Advances in Cryptology—EUROCRYPT'92. Springer Berlin/Heidelberg, 1993: 153-162.

[48] Nguyen P, Shparlinski I. On the insecurity of a server-aided RSA protocol[J]. Advances in Cryptology—ASIACRYPT 2001, 2001: 21-35.

[49] William Stallings,孟庆树,王丽娜等译.密码编码学与网络安全：原理与实践（第四版）[M]，电子工业出版社,2008

[50] 周青婷. 基于 Paillier 密码体制的点积协议研究[D]. 云南大学, 2012.

[51] I Ioannidis, A Grama. An efficient protocol for Yao's millionaire's problem [A]. In Proceedings of the 36th Annual Hawaii International Conference on System Sciences [C]. Los Alamitos: IEEE Computer Society Press, 2003. 205.

[52] 秦波, 秦慧, 周克复, 等. 常数复杂性的百万富翁协议[J]. 西安理工大学学报, 2005, 21(2): 149-152.

[53]Shundong Li, Daoshun Wang, Yiqi Dai, Ping Luo. Symmetric cryptographic

solution to yao's millionaires problem and an evaluation of secure multiparty computations [J]. Information Sciences.2008, 178(1):245-255.

[54] 程文娟, 董莹莹, 汪庆. 有关保护私有信息的三角不等式判定问题研究[J]. 合肥工业大学学报: 自然科学版, 2012, 35(5): 625-628.

[55] M. J. Atallah, Du Wenliang. "Secure Multi-Party Computational geometry". In:Lecture Notes in Computer Seience 2125.Berlin:Springer,165-179,2001.

[56]Zhiqiang Yang. Rebecca N. Wright. Hiranmayee Subrmaniam. Experimental Analysis of a Privacy-Preserving Scalar Product Protocol[J]. International Journal of Computer Systems Science and Engineering. Vol. 21, No. 1, 2006, pp. 47-52.

[57] http://baike.baidu.com/view/144821.htm#6

[58] Fiat A and Naor M. Broadcast Encryption [C]. Advances in Cryptology: CRYPTO 1993, LNCS vol. 773, pp. 480-491, 1993.

[59]Dodis Y, Fazio N. Public key broadcast encryption secure against adaptive chosen ciphertext attack [C]. Public Key Cryptography 2003, LNCS, vol. 2567, pp. 100–115, 2003.

[60]Boneh D, Gentry C and Waters B. Collusion resistant broadcast encryption with short ciphertexts and private keys [C]. Advances in Cryptology: CRYPTO 2005, LNCS, vol. 3621, pp. 258–275, 2005.

[61]Zhang Leyou, Hu Yupu and Wu Qing. Adaptively secure identity-based broadcast encryption with constant size private keys and ciphertexts from the subgroups [J]. Mathematical and Computer Modelling, vol. 55, no. 1-2, p. 12-18, 2012.

[62]Park C, Hur J, Hwang S and Yoon H. Authenticated public key broadcast encryption scheme secure against insider's attack [J]. Mathematical and Computer Modelling, vol. 55, no. 1-2, p. 113-122, 2012.

[63] 刘文，罗守山,王永滨.安全两方向量优势统计协议及其应用[J].电子学报,2010,38(11):2573-2577.

[64] 秦静,张振峰,冯登国,李宝.一个特殊的安全双方计算协议[J].通信学报,2004,25(11):35-42.

[65] Du Wenliang. A study of several specific secure two-party computation problems

[Ph.D.dissertation].Purdue University,USA,2000

[66] 刘文,王永滨.安全多方信息比较相等协议及其应用[J].电子学报, 2012, 40(5):871-876.

[67] Maurer U. Secure multi-party computation made simple[C]. //Proceedings of the 3rd international conference on Security in communication networks. 2003:14-28.

[68] 李禾,王述洋.关于除法的安全两方计算协议[J].计算机工程与应用, 2010,46(6):86-88.

[69] 张华.陈智雄.肖国镇.一个基于签密技术的安全多方乘积协议[J].计算机科学, 2005,32(2):50-52.

[70] 罗文俊,李祥.多方安全矩阵乘积协议及应用[J].计算机学报. 2005,28(7): 1230-1235.

[71] Rabin M O. How to exchange secrets by oblivious transfer[R]. Technical Report TR-81, Harvard Aiken Computation Laboratory, 1981.

[72] Brassard G, Crépeau C, Robert J M. All-or-nothing disclosure of secrets[C]//Advances in Cryptology—CRYPTO'86. Springer Berlin/Heidelberg, 1987: 234-238.

[73] Naor M, Pinkas B. Oblivious transfer and polynomial evaluation[C]//Proceedings of the thirty-first annual ACM symposium on Theory of computing. ACM, 1999: 245-254.

[74] Brassard G, Crépeau C, Santha M. Oblivious transfers and intersecting codes[J]. Information Theory, IEEE Transactions on, 1996, 42(6): 1769-1780.

[75] Mu Y, Zhang J, Varadharajan V. m out of n Oblivious Transfer[C]//Information Security and Privacy. Springer Berlin/Heidelberg, 2002: 243-265.

[76] 陈志德, 朱洪. n 取 m 不经意传输协议构造研究[J]. 小型微型计算机系统, 2006, 27(003): 466-468.

[77] Duma C, Shahmehri N, Caronni G. Dynamic trust metrics for peer-to-peer systems[C]//Database and Expert Systems Applications, 2005. Proceedings. Sixteenth International Workshop on. IEEE, 2005: 776-781.

附录 A 图索引

Figure Index

附录 B 表索引

Table Index

致谢

岁月如梭，三年时光悄然而逝！随着论文的即将完成，研究生生涯也将画上圆满的句号。在此，请允许我向所有关心、帮助和支持我的人表示衷心的感谢！

首先我要感谢我的老师仲红教授，感谢她在这三年里给予我学业上的指导、生活上的照顾、思想上的引领。在学习上，仲老师治学严谨、耐心倾心，为我们创造了积极的学术氛围，每周定时召开学术会议，耐心地听我们的研究进展，倾心地给予我们学习上的指导；在生活上，仲老师和蔼可亲、平易近人，她像母亲一样对我们无微不至的关怀，我们在她的呵护下不断的成长；在思想上，仲老师劳心劳力、认真负责的人生态度深深的感染着我，我清晰地记得她在各个方面对我们的教诲，犹如指南针一般，引领我们走向正确、夯实的道路。正是在仲老师这样的指导、关心、引领下，我们才能找到工作，顺利的毕业。再次对您说一声“谢谢”。

其次，我要感谢同一个课题组的石润华教授、崔杰老师和许艳老师。石老师治学严谨、平易近人，每当我遇到难题疑惑，石老师都会耐心地给我讲解，在学术上给我提出了许多宝贵的意见和建议让我受益匪浅，使我攻克了一个又一个难关。感谢崔杰老师和许艳老师，在每周的学术研讨会上对我的报告的指点和建议，感谢二位老师论文和其他学习上的帮助。

再次，我要感谢我的学长易磊、韦小东、吴军、刘亚峰和学姐李文娟、花常琪、孙苏。从步入研究生校门的那一刻起，学长学姐们就给我们提供了很多学习资料和宝贵的学习经验。每当我不知所措的时候，学长学姐们总能给我们指明方向，他们增长了我的学识、丰富了我的生活、陶冶了我的情操。谢谢你们！我要感谢我的同门郭松矗、田立超、钱小强、吴芬、周玲玲，我们如兄弟姐妹一般，相互学习、相互关心、相互进步，在仲老师、石老师的引领下，我们不断成长，不断进步，不断向着人生的理想前进。

我还要感谢我的家人。我能顺利的大学毕业离不开他们的支持，我能顺利的研究生毕业更离不开他们的支持。虽然他们无法给予我学业上的帮助，但我知道他们总是默默地支持着我。家里条件不好，他们总是不辞辛苦地想尽一切办法支持我完成学业，不让我有任何的后顾之忧。正是在这样的支持和鼓励下，我奋勇

前进，以后用实际行动报答他们。感谢我的朋友马琼，总是在我最需要的时候给予我心灵上的慰藉，不断的鼓励着我前进。

最后，我向所有关心过我、帮助过我的人表示感谢！你们的关心让我感觉这个世界很温暖，让我感觉三年的时光是幸福的，祝福你们。同时我要感谢各位评审老师，感谢百忙之中，你们给予我论文的宝贵意见，我为此感到荣幸，向您的辛苦工作表示敬意。

谢谢！

攻读学位期间发表的学术论文目录

[1] 夏超，仲红，石润华：基于同态加密技术的安全多方乘积协议：计算机工程与应用，2013 年 7 月（已录用）

攻读硕士学位期间参加的科研项目

[1]国家自然基金项目(61173188)：

“面向 MANET 的密钥管理关键技术研究”

[2]国家自然基金项目(61173187)：

“量子秘密共享若干关键问题研究”

[3]安徽省自然基金项目（11040606M141)：

“移动自组织网密钥管理的关键技术”

[4]安徽高校省级重点自然科学研究项目(KJ2010A009)：

“基于秘密共享的移动 Ad hoc 网络若干安全问题研究”