软件学报 ISSN 1000-9825, CODEN RUXUEW
Journal of Software,2018,29(7):1830−1851 [doi: 10.13328/j.cnki.jos.005354]

E-mail: jos@iscas.ac.cn
http://www.jos.org.cn
Tel: +86-10-62562563

同态加密技术及其在云计算隐私保护中的应用*

李宗育[1,2], 桂小林[1,2], 顾迎捷[1,2], 李雪松[3], 戴慧珺[1,2], 张学军[4]

[1](西安交通大学 电子与信息工程学院,陕西 西安 710049)

[2](陕西省计算机网络重点实验室(西安交通大学),陕西 西安 710049)

[3](贵州大学 计算机科学与技术学院,贵州 贵阳 550025)

[4](兰州交通大学 电子与信息工程学院,甘肃 兰州 730077)

通讯作者: 桂小林, Email: xlgui@mail.xjtu.edu.cn

摘 要: 云计算技术的快速发展使得云服务模式具备了广阔的应用空间,这种模式使用户具备了过往无法比拟的计算能力和存储空间等优势.在云服务模式下用户的隐私安全问题是其推广和应用中面临的首要问题,如何在计算数据的过程中,既保证数据的隐私性,又保证其可用性,是面临的一大难题,同态加密技术作为解决这一问题的关键手段,是近年来国际国内学界的热点问题.介绍了云计算隐私安全和同态加密研究进展、同态加密算法的分类、安全理论基础、全同态加密方案的实现技术以及同态加密技术在云计算隐私保护中的应用,重点对各类同态加密方案的优缺点进行了介绍和分析,提出了未来的研究方向.

关键词: 云服务;同态加密;密文计算;隐私安全

中图法分类号: TP309

中文引用格式: 李宗育,桂小林,顾迎捷,李雪松,戴慧珺,张学军.同态加密技术及其在云计算隐私保护中的应用.软件学报, 2018,29(7):1830−1851. http://www.jos.org.cn/1000-9825/5354.htm

英文引用格式: Li ZY, Gui XL, Gu YJ, Li XS, Dai HJ, Zhang XJ. Survey on homomorphic encryption algorithm and its application in the privacy-preserving for cloud computing. Ruan Jian Xue Bao/Journal of Software, 2018,29(7):1830−1851 (in Chinese). http://www.jos.org.cn/1000-9825/5354.htm

Survey on Homomorphic Encryption Algorithm and Its Application in the Privacy-Preserving for Cloud Computing

LI Zong-Yu[1,2], GUI Xiao-Lin[1,2], GU Ying-Jie[1,2], LI Xue-Song[3], DAI Hui-Jun[1,2], ZHANG Xue-Jun[4]

[1](School of Electronics and Information Engineering, Xi'an Jiaotong University, Xi'an 710049, China)

[2](Shaanxi Province Key Laboratory of Computer Network (Xi'an Jiaotong University), Xi'an 710049, China)

[3](College of Computer Science and Technology, Guizhou University, Guiyang 550025, China)

[4](School of Electronics and Information Engineering, Lanzhou Jiaotong University, Lanzhou 730077, China)

Abstract: Cloud service mode has obtained broad application space with the rapid development of cloud computing technology. Such mode has provided users with incomparable computing power and storage space. However, privacy security of users is a primary problem in the promotion and application of the service mode. How to guarantee both the privacy and availability of data in the process of data computation remains a major challenge, and as a key means to solve this problem, homomorphic encryption technique has been a hot

* 基金项目: 国家自然科学基金(61472316, 61762058); 陕西省重大基础研究项目(2016ZDJC-05); 陕西省重点研发项目(2017ZDXM-GY-011)

Foundation item: National Natural Science Foundation of China (61472316, 61762058); Natural Science Basic Research Plan in Shaanxi Province of China (2016ZDJC-05); Key Development Program in Shaanxi Province of China (2017ZDXM-GY-011)

本文由"面向隐私保护的新型技术与密码算法"专题特约编辑薛锐研究员推荐.

收稿时间: 2017-05-18; 修改时间: 2017-07-13; 采用时间: 2017-08-22; jos 在线出版时间: 2017-10-17

CNKI 网络优先出版: 2017-10-17 13:37:57, http://kns.cnki.net/kcms/detail/11.2560.TP.20171017.1337.001.html

subject in international and domestic academic circles in recent years. In this paper, the privacy security of cloud computing, the research progress of homomorphic encryption and the application of homomorphic encryption technique in privacy protection of cloud computing are introduced. Analysis of advantages and disadvantages of various homomorphic encryption schemes is emphasized, and the future research direction is proposed.

Key words: cloud service; homomorphic encryption; cipher-text computation; privacy security

云计算技术的快速发展使得各类衍生服务得到广泛应用,通过云服务人们可以不受空间和自有终端数据处理能力的限制,完成一系列海量数据的分析、处理、存储等工作,企业将原本需要依托大型计算中心完成的任务外包给亚马逊、谷歌等运营商提供的云计算中心能够降低 30%以上硬件成本,不仅大大降低了终端开销,同时为用户带来前所未有的计算能力、几乎无限的存储空间和巨大的经济潜力.2014 年全球云计算业务所带来的营收已经达到 1 480 亿美元,2016 年全球云计算市场环比增长达到 30%,到 2020 年全球市值将达到 2 700 亿美元,然而云计算环境本身的结构特点也给安全性带来较大隐患,出于降低成本提升资源利用率上的考虑,参与计算的节点大都异构并且类型多样,物理分布稀疏,服务商难以对所有节点进行有效控制.用户往往依靠可靠性较低的网络通信和半可信的云存储服务器来传输和存储数据资源,必然存在暴露敏感信息的风险,难以确保数据的机密性、完整性和可用性,一旦敏感数据资源被窃取或者篡改,所造成的严重后果难以估计.2015 年全球近 300 多家大型公司由于数据泄露所导致的经济损失平均高达 380 万美元,JP Morgan、Home Depot 等知名公司都遭受过此类损失,有的公司面临的损失高达上亿美元,隐私安全保护已经成为云计算技术进一步发展和应用亟待解决的重大问题.为此,本文分析了当前云计算服务中面临的隐私安全问题,用户隐私保护的关键技术——同态加密技术的发展现状、不足、下一步需要研究的方向和可能的应用场景,以期为将来云服务中用户隐私安全的科研以及云计算产业发展做出探索.

本文第 1 节从总体上介绍云计算隐私安全的现状,对云计算隐私威胁和已有隐私保护手段的优劣进行分析,同时对同态加密技术的研究进展作总体概述.第 2 节介绍同态加密算法的相关理论和概念.第 3 节对同态加密算法的分类和相关技术研究进行分析.第 4 节重点介绍同态加密技术在云计算隐私保护中的应用情况.第 5 节总结当前研究现状,对未来同态加密技术在云计算隐私保护领域的可能应用场景加以展望.

1 云计算隐私安全和同态加密研究进展

1.1 云计算隐私安全

云计算的兴起无法摆脱隐私安全的问题.首先,与其他网络平台一样,攻击者有可能绕过云平台的认证机制,通过直接访问下层文件或原始数据的方式获取到用户的数据,从而引发隐私泄露问题.此外,云计算的数据外包和服务租赁的特点使得云计算还面临更严峻的数据计算时的隐私问题.如何安全、有效地在云计算环境中为用户提供隐私安全保护已成为当前学界研究的一个热点.近年来,隐私信息检索(private information retrieval)[1−3]、可搜索加密(searchable encryption)[4−8]、多方安全计算(secure multi-party computation)[9,10]技术大量地应用到了云中数据的隐私保护中,隐私信息检索和可搜索加密技术使用户可以对加密数据进行检索获取私有信息,并保证第三方数据存储端无法获取其内容,然而这些技术基本上只能满足有限的功能,诸如关键词搜索、排序搜索、区间搜索、子集搜索等.大多已有方案的计算复杂度较高,数据加密后不具备保序性,搜索服务提供方要对所有数据遍历才能寻找到目的数据,并且以这些技术为基础的隐私保护方案往往会将数据的访问模式泄露给敌手,使其能够基于搜索结果进行学习.多方安全计算协议下数个参与计算的用户可以使用自有数据联合计算,参与方的数据不需要聚合和交换,从而保证了各自的输入数据不被泄露给其他参与方,但是前提是需要按照特定的客户需求定制可以支持联合计算的软件和硬件系统,这无疑大大增加了服务实现成本.传统加密算法,如 AES、ECC 和 RSA 等,只有在密钥足够长的条件下可以对用户敏感数据起到保护作用,但是,密文数据一旦存储到云端后,当需要云服务商对这些密文数据进行计算处理时,无法实现网络中的计算资源对加密的数据进行处理,因为已有的大多数传统加密方法都不支持对密文的运算,而云环境中许多应用场景都需要对密

文数据进行操作,例如通过成千上万的患者病历数据进行药物疗效分析,统计使用搜索引擎的用户高频搜索词继而有针对性地推送广告,对加密文件进行模糊检索,对加密的公司财务信息进行统计分析等.按照传统的做法,这些数据经过加密后发送到云端需要解密再进行处理,用户本身在对数据进行处理时,也需要向服务商申请密文数据,下载到本地解密后再使用,这样不仅同样会暴露隐私,同时,当用户频繁使用数据时,需要消耗大量网络带宽和时间与服务商进行通信实现数据加密和解密以及加密数据的上传和下载等,所带来的计算和通信消耗大大降低了云计算的可用性和用户体验.除此之外,隐私安全问题在多方安全计算和数据挖掘领域也引起人们的关注.在进行数据挖掘时,通常使用传统加密方法来保护数据的隐私性,但是为了分析数据,不可避免地要对加密数据进行处理,例如进行 SUM、AVG 等运算操作,然而传统的加密算法并不支持密文域运算,因此,利用加密方式保证数据挖掘隐私性的研究面临一定的困难.同样,当多个用户利用多方安全计算协议完成某项计算任务时,一方面利用各自计算资源进行协作,另一方面又要求互不知悉各自数据内容,这样就需要一种能支持对密文域运算的加密算法,数据挖掘和多方安全计算领域的隐私保护研究取得了一定进展.在云服务环境下,无论是进行数据挖掘、分析还是多方安全计算等应用,它们都具备了共同的特征:数据拥有者的本身并不对数据进行操作,而是委托给非可信或半可信第三方服务商来处理,因此要满足支持隐私保护的外包计算,就需要既能保护数据机密性,又能按照用户需求支持密文域的某些运算操作,例如检索、算术运算等的加密算法.

云计算技术一方面为用户提供了可观的存储资源,另一方面也提供了强大的计算资源,使用传统加密算法能够确保数据外包存储的安全,却无法应对数据外包计算时的安全问题,这无疑削减了云服务模式的优势.外包计算的参与者有数据拥有者、数据使用者和服务提供者,他们之间的交互过程如图 1 所示[11],在这种典型的交互过程中,可能存在以下几种隐私威胁.

(1) 数据拥有者将数据传输到服务提供端的过程中,外部攻击者可以通过窃听的方式盗取数据;

(2) 外部攻击者可以通过钓鱼软件、木马和无授权的访问等方式来破坏服务提供者对用户数据和程序的保护,从而实现非法访问;

(3) 外部攻击者可以通过观察用户发出的请求,从而获得用户的习惯、目的等隐私信息;

(4) 由于数据拥有者的数据存放在服务提供者的存储介质上,程序运行在服务提供者的服务器中,因此内部攻击者要发起攻击更为容易.

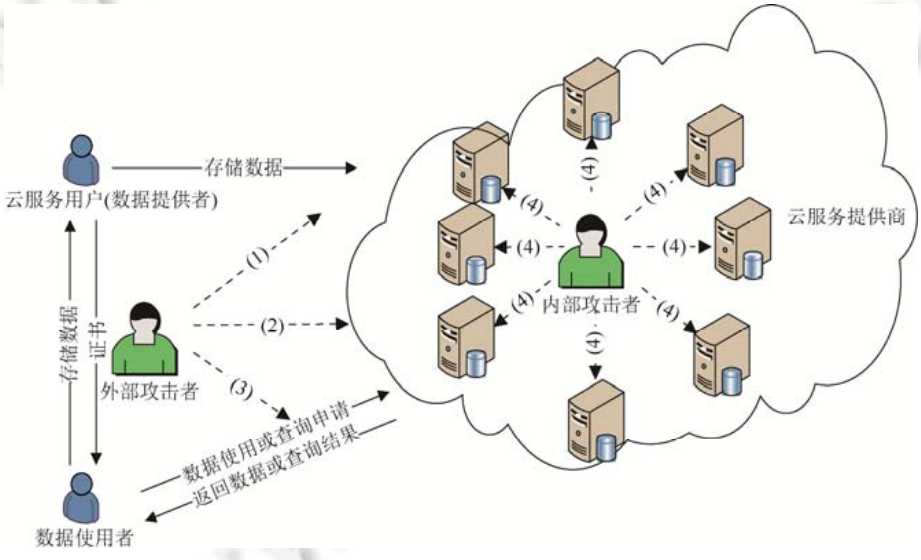

Fig.1 Privacy threat model in outsourcing computing model

图 1 外包计算模式下的隐私威胁模型

上述 4 种威胁中,前 3 种是传统网络安全中涉及的问题,人们通过访问控制机制可以有效限制攻击者的无授权访问,通过 VPN、OpenSSH 或 Tor 等方法来保证通信线路的安全;第 4 种是在云环境中外包计算模式下出现的新型隐私威胁,也是破坏性最大并且较难防御的一种安全威胁.因此,我们亟需一种技术能同时抵御以上 4 种隐私威胁.支持隐私保护的密文计算(如算数运算、检索运算)能够有效地解决这一问题,通过对外包计算模式下的隐私威胁进行分析,建立能够抵御以上 4 种攻击的计算.图 2 所示支持隐私保护的计算模型反映了数据拥有者(owner)、数据使用者(user)和服务提供者(service provider,简称 SP)之间如何实现安全的计算,可以说同态加密的问世为云计算中用户隐私安全提供了可靠、有效的保护手段.

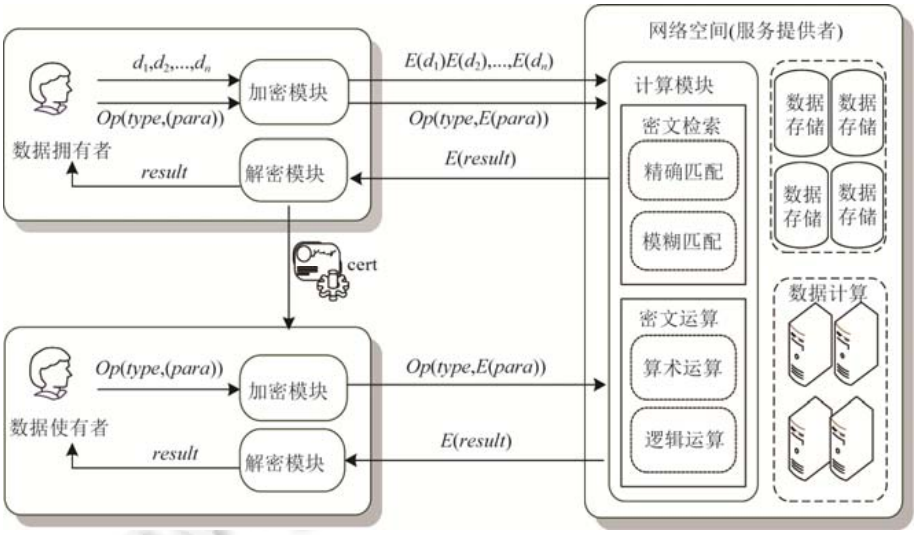

Fig.2 Privacy preserving computing model

图 2 支持隐私保护的计算模型

1.2 同态加密研究进展

同态加密(homorphic encryption)源于隐私同态,从诞生到现在经历了 30 多年,尚未有统一的分类标准,按照其发展阶段、支持密文运算的种类和次数可将其分为部分同态(partial homomorphic encryption,简称 PHE)加密、类同态加密(somewhat homomorphic encryption,简称 SHE)以及全同态加密(fully homomorphic encryption,简称 FHE).部分同态加密(PHE)仅支持单一类型的密文域同态运算(加或乘同态);类同态加密(SHE)能够支持密文域有限次数的加法和乘法同态运算;全同态加密(FHE)能够实现任意次密文的加、乘同态运算.同态加密技术对于云计算环境中的数据存储、密文检索和可信计算都有着很大的应用前景.用户隐私数据在云端始终以密文形式存储,服务商无法知悉数据内容,从而避免其在非法盗用、篡改用户数据的情况下对用户隐私进行挖掘,为用户充分利用云计算资源进行海量数据分析与处理提供了安全基础,尤其是可以与安全多方计算协议相结合较好地解决用户外包计算服务中隐私安全问题.

全同态加密是同态加密技术发展的一个新兴重要方向,使用 FHE 方案对数据加密后发送到云端,密文数据在云端可以完成安全存储、检索以及所有运算类型的操作,有效避免了明文数据在传输过程中被窃取、拦截、窜改或伪造等风险,也避免了服务商将客户的隐私数据泄露或云端服务器被恶意攻破.2009 年 Gentry[12]提出第一个真正意义上的 FHE 方案以后,全同态加密理论得到了迅速发展,基本沿着两条研究主线,一类以 Gentry 提出的 FHE 方案的构造方法为基础,Gentry 的方案本质上是一种基于理想格陪集问题构造的层次型 FHE 方案,首先构造一个对称型 SHE 方案,满足低次密文多项式在计算时的同态性,再压缩解密电路 D(D 是解密算法 Dec 的电路表示),降低解密过程中多项式次数,通过自举技术(bootstrappaping)实现全同态加密.随着量子计算机理论的

快速发展,不久的将来必然迎来量子计算机应用的大潮,量子计算机能够解决整数分解、离散对数问题等几乎现行所有的密码学方案,而格密码理论能够很好地抵御量子计算攻击.另一类是近年来同态加密技术研究的热点,基于 LWE(错误学习)和 RLWE 假设思想提出的方案,它的安全性假设可以归约到一般格上的标准困难问题,与 Gentry 构建方案的框架不同,其首先构建一个 SHE 方案,在密文计算后,通过密钥交换技术来控制密文向量的维数膨胀问题,最后使用模转换(modulus switching)技术降低密文运算过程中的噪声,不需要使用同态解密技术就能构造一个层次型 FHE 方案来执行多项式级深度的电路.2005 年 Regev 定义了 LWE 问题是"带噪声的奇偶校验学习"问题的一般化,并证明了该问题在量子规约下具有类似的最坏情况特性.2010 年 Brakerski 和 Vaikuntanathan 利用理想格构造了基于 RLWE 的 FHE 方案 BV11.2011 年 Regev[13]基于 LWE 问题提出的全同态密码方案,是现今简单程度最高的全同态加密方法.2011 年 Stehle[14]和 Smart 等人首次将 NTRU 算法引入以提高 Gentry 初始 FHE 方案的效率,其安全假设基于 RLWE(环上错误学习),通过理想格最坏情况难解性保障安全性,有许多在此基础上的改进方案也相继提出,不过,由于其在加密过程中按位进行加密,因此计算效率、传输带宽和存储效率较低的问题使得其应用有一定局限性,并且这类方案由于易受到密钥恢复攻击,因此无法有效抵御选择密文攻击方式.2012 年 Brakerski[15]和 Gentry 提出了 BGV 方案,能够支持多比特运算,计算复杂度为 $t\cdot poly\log(\lambda)$, 相比于 Gentry 的初始方案(计算复杂度为 $o(\lambda^6)$)低得多,也比 2011 年 Gentry[16]和 Halevi 实现其方案时的复杂度低两个数量级,在密文的乘法同态运算效率上也高于 Bra12 方案.基于 LWE 和 R-LWE 的 FHE 方案都享有"加性密钥同态"的属性,多个用户各自持有一对公钥私钥(pk_i,sk_i),通过所有用户的公钥相加产生的新密钥 $pk^*=\sum_{i=1}^{n}pk_i$ 加密明文 m 产生的密文 $c=Enc(pk^*,m)$, 可以使用各用户私钥相加所得的新密钥 $sk^*=\sum_{i=1}^{n}sk_i$ 来解密密文恢复明文 $m=Dec(sk^*,m)$, 即 (pk^*,sk^*) 可以构成一对新的公钥与私钥来加密解密数据.

全同态加密技术发展趋势很快,但是想获得纯粹的 FHE 方案,还需要依靠同态解密技术.总体来说,从现有研究情况来看,PHE 方案在应用中执行效率更高,但是仅能支持加法或乘法的同态运算,FHE 方案在功能性上要优于 SWHE、PHE 方案,但是由于 FHE 方案通过使用自举电路、维数归约技术即重线性化(dimension modulus reduction)等技术来降低噪声从而达到突破限制进行密文同态运算的目的,复杂的计算过程成为其实际应用的瓶颈.

2 相关概念和理论基础

密文计算(cipher-text computation)是指在密文域上所进行的计算以及具有访问权限的用户对密文域上的计算结果可确认并可解密获得对应的明文.为了确保用户隐私数据安全,需要将隐私数据进行加密处理后上传到云端存储,参与计算的密文数据主要包括两部分,分别由用户直接提供以及通过密文检索得到的数据(服务商受托方对用户交付的数据作外包计算).同态加密为云计算环境中存储与外包计算等服务的隐私安全问题提供了良好的解决方案,理论上利用全同态加密算法能够从根本上解决在第三方不可信或半可信平台上进行数据存储和数据操作时的隐私保护问题,用户将计算请求 F 和密文 $\langle c_1,...,c_t\rangle=(Enc(m_1),...,Enc(m_t))$ 发送给云端,在云端对密文直接进行任意运算,所得到的密文结果与明文运算后结果一致,即 $Y(K,F,(Enc(m_1),...,Enc(m_t)))=E(K,F(m_1,...,m_t))$, 同态的概念源于近世代数中群与环的同态,设 $\langle H_1,\circ\rangle$、$\langle H_2,*\rangle$ 为两个代数结构, $f:H_1\to H_2$ 为 H_1 到 H_2 的一个映射, $\forall a,b\in H_1$ 都有 $f(a\circ b)=f(a)*f(b)$, 则称 $f:H_1\to H_2$ 是一个同态映射.一个同态加密算法 ε包括 4 个部分,分别是密钥生成算法 Gen_ε、加密算法 Enc_ε、解密算法 Gec_ε、密文运算算法 Cal_ε.

(1) 密钥生成算法 $Gen_\varepsilon: U\to key$ 表示用户通过输入参数 U 生成密钥 key;

(2) 加密、解密算法: $Enc_\varepsilon:(key,P_\varepsilon)\to C_\varepsilon, Dec_\varepsilon:(key,C_\varepsilon)\to P_\varepsilon$, P_ε为明文空间,C_ε为密文空间;

(3) 计算算法: $Cal_\varepsilon:(P_\varepsilon,F_\varepsilon)\to(C_\varepsilon,F_\varepsilon)$, $\circ\in F_\varepsilon,(p_1,p_2,...,p_n)\in P_\varepsilon$, F_ε 是 P_ε 上的运算集合,对于 $\circ\in F_\varepsilon,(p_1,p_2,...,p_n)\in P_\varepsilon, Cal_\varepsilon$ 将 P_ε上进行的运算$\circ$转化为 C_ε上运算再进行计算,结果是等价的.

定义 1. 同态性:对于加密算法ε和明文域 P_ε上的运算$\circ$,若 $\forall p_1,p_2,...,p_n\in P_\varepsilon$ 都满足式(1):

$$Dec_{\varepsilon 1}(key,Cal_\varepsilon((c_1,...,c_n),\circ))=(p_1,...,p_n)\circ \tag{1}$$

3 同态加密算法分类及相关研究

3.1 部分同态(PHE)加密

定义 2. 对于加密算法ε和明文域 P_ε上的运算(+,×),若 $\forall p_1, p_2, ..., p_n \in P_\varepsilon$ 仅满足加法或者乘法运算在式(1)中成立,则称加密算法ε为满足部分同态的加密算法.

1978 年 Rivest 提出了基于公钥密码体制的经典加密方案 Unpadded RSA[17],并在其论文《On data banks and privacy homomorphisms》[18]中首次提出同态加密的思想,RSA 算法针对数值型数据进行加密,在加密时无需将明文扩展至与公钥一致的长度,能够支持乘法同态运算,不支持加法,密钥的产生过程也较为复杂,其安全性假设基于大数因式分解,加解密运算代价过高,由于是确定性加密算法,密钥一定的情况下加密明文会产生固定密文,难以做到一次一密,因此安全性受到影响;Elgamal[19]提出了基于离散对数困难问题的 ElGamal 算法,在加密时引入了随机数,具有语义安全性,算法满足了乘法同态的性质,但是解密过程要对离散对数进行计算,在实现上较为困难;Chen 等人[20]基于 ElGamal 的方法进行改进,提出了 NHE 方法,能够抵抗已知明文攻击(known-plaintext attack)和选择密文攻击(chosen-ciphertext attack).在对称型类同态加密体制方面,Goldwasser-Micali[21]算法于 1984 年被提出,它以合数为模的二次剩余困难性假设为基础,该方案能够实现对异或运算的同态性,但是只能逐位进行加密,效率较低;Benaloh[5]提出了第一种支持对密文进行有限次加法操作的公钥密码体制,之后许多学者相继提出了不少支持密文加法运算的同态加密方案,应用最为广泛的是 Paillier[22]加密方案,PHE 方案由于构造简单、执行效率较高,应用相对比较成熟.表 1 列出了时下的主流 PHE 方案,从密文同态运算属性、算法设计、密文膨胀、安全假设问题强度几个方面进行比较,从表 1 中可以看出,除了 RSA 和 MREA 方案,现有大部分 PHE 加密方案是基于对称加密体制和非确定性概率假设的,RSA 和 MREA 方案支持乘法同态,其他方案支持密文域的加法同态,相对来说,RSA、EGM、Paillier 方案的加解密效率相对较高,由于表 1 中几种 PHE 方案在效率上具备的良好性能,被广泛应用到现实中(Paillier 方案被大量应用到电子投票和生物计量应用中,其加解密效率可以控制在毫秒级,加密和解密每 1 024 位数据仅需要 2.33s).

Table 1 Comparison of existing classic PHE program in technical details

表 1 现有经典 PHE 方案技术细节对比

PHE 方案	加密体制				同态属性			安全假设							密文膨胀
	对称型	非对称型	确定型	概率型	加法	乘法	运算算法	IF	DL	QR	WrR	CR	SD	P-SP	SS	
RSA82[18]		√	√			√	$(M_1^e) \bmod N \times (M_2^e) \bmod N = (M_1 \times M_2)^e \bmod N$	√								1
GM84[21]		√		√	√		$\left(x^{M_1} r_1^2\right) \times \left(x^{M_2} r_2^2\right) \bmod N \equiv \left[x^{M_1+M_2} (r_1 r_2)^2\right] \bmod N$			√					√	*BitLength*(*N*)
EGM85[19]		√		√		√	$(g^{r_1}, M_1 h^{r_1}) \bmod N \times (g^{r_2}, M_2 h^{r_2}) \bmod N \equiv \left[(g^{r_1+r_2}), (M_1, M_2) h^{r_1+r_2}\right]$		√						√	2
Ben87[23]		√		√	√		$\left(g^{M_1}, r_1^\sigma\right) \bmod N \times \left(g^{M_2}, r_2^\sigma\right) \bmod N \equiv \left[\left(g^{M_1+M_2}\right), (r_1 r_2)^b\right] \bmod N$				√				√	*BitLength*(*N*)/*b*
OU98[24]		√		√	√		$\left(g^{M_1} h^{r_1}\right) \bmod N \times \left(g^{M_2} h^{r_2}\right) \bmod N \equiv \left(g^{M_1+M_2} h^{r_1+r_2}\right) \bmod N$	√						√	√	3

Table 1 Comparison of existing classic PHE program in technical details (Continued)
表 1 现有经典 PHE 方案技术细节对比(续)

PHE 方案	加密体制				同态属性			安全假设								密文膨胀
	对称型	非对称型	确定型	概率型	加法	乘法	运算算法	IF	DL	QR	WrR	CR	SD	P-SP	SS	
Pai99[22]		√		√	√		$(g^{M_1}r_1^N)\bmod N^2\times(g^{M_2}r_2^N)\bmod N^2\equiv[(g^{M_1+M_2}),(r_1r_2)^N]\bmod N$			√		√			√	2
BGN05[25]		√		√	√		$(g^{M_1}h^{r_1})\bmod N\times(g^{M_2}h^{r_2})\bmod N\equiv(g^{M_1+M_2}h^{r_1+r_2})\bmod N$			√			√		√	*BitLength*(*N*)/*BitLength*(*r*)
MREA12[26]		√	√		√		$(g^{M_1^e \bmod N}r^{M_1})\bmod N^2\times(g^{M_2^e \bmod N}r^{M_2})\bmod N^2\equiv(g^{(M_1+M_2)^e \bmod N}r^{M_1+M_2})\bmod N^2$	√				√				≥4
CEG13[27]		√		√	√		$(g^{r_1},h^{r_1}g^{m_1})\times(g^{r_2},h^{r_2}g^{m_2})\equiv[(g^{r_1+r_2}),h^{r_1+r_2}g^{M_1+M_2}]$			√					√	≥4

3.1.1 Paillier 加密方案

Paillier 是一种应用较为广泛的公钥体制 PHE 方案.方案的密钥生成过程 $Gen_{Paillier}$ 如下:

随机选取 p、q 两个大素数以及 $g\in Z_{n^2}$, 令 $n=p\cdot q,\lambda=(p-1)(q-1)$, 设函数 $l(u)=\dfrac{u-1}{n}$, 且 g、n 满足:

$$\gcd(l(g^{\lambda} \bmod n^2),n)=1 \tag{2}$$

这里,公钥为 $pk=(n,g)$, 私钥 $sk=\lambda$.

加密算法 $Enc_{Paillier}$:随机选取整数 $r\in Z_{n^2}^*$, 对于明文 $m\in Z_n$, 加密后的密文 c 为

$$c=g^m\cdot r^n \bmod n^2 \tag{3}$$

式(3)中, $c\in Z_{n^2}^*, Z_{n^2}^*$ 为小于 n^2 且与 n^2 互素的正整数集合.

解密算法 $Dec_{Paillier}$:对于密文 c,其对应的明文 m 为

$$m=\frac{l(c^{\lambda} \bmod n^2)}{l(g^{\lambda} \bmod n^2)} \bmod n \tag{4}$$

同态属性分析:

由于 $Enc(m_1)\cdot Enc(m_2)=(g^{m_1}\cdot r_1^n)\cdot(g^{m_2}\cdot r_2^n)=g^{m_1+m_2}(r_1r_2)^n=Enc(m_1+m_2)\bmod n^2$ 即明文加法运算对应密文乘法运算,所以方案具备加法同态性:

$$Dec_{Paillier}(key,Cal_{Paillier}((c_1,...,c_n),\times))=(m_1,...,m_n)+ \tag{5}$$

3.1.2 ELGaml 加密方案

ELGaml 也是一种以公钥密码体制为基础的 PHE 方案.方案的密钥生成过程为 Gen_{ELGaml}.

随机选取大素数 p,$x\in(1,p-1)$,g 为素数集 Z_p^* 的生成元,令 $y=g^x \bmod p$, 这里,$pk=y$ 为公钥,私钥 $sk=x$.

加密算法 Enc_{ELGaml}:对于明文 $m\in Z_p^*$, 随机选取 $k\in Z_p^*$, 加密后密文 c 为

$$c=Enc(m)=(c_1,c_2),c_1\equiv g^k(\bmod p),c_2\equiv m\cdot y^k(\bmod p) \tag{6}$$

解密算法 Dec_{ELGaml}:对于密文 c,其对应的明文 m 为

$$m=Dec(c)=\frac{c_2}{c_1^x}=\frac{my^k}{g^{xk}}=\frac{mg^{xk}}{g^{xk}} \bmod p \tag{7}$$

同态属性分析:

因为

$$\begin{aligned} Enc(m_1)\cdot Enc(m_2) &= (g^{x_1} \bmod p, m_1 y^{x_1} \bmod p)\cdot (g^{x_2} \bmod p, m_2 \cdot y^{x_2} \bmod p) \\ &= (g^{x_1+x_2} \bmod p, m_1 \cdot m_2 y^{x_1+x_2} \bmod p) \\ &= Enc(m_1 \cdot m_2) \bmod p, \end{aligned}$$

即密文乘法运算对应于明文乘法运算,所以方案具备乘法法同态性:

$$Dec_{ELGaml}(key, Cal_{ELGaml}((c_1,...,c_n),\times)) = (m_1,...,m_n)\times \tag{8}$$

3.2 类同态(SWHE)加密

定义 3. 对于加密算法ε和明文域P_ε上的运算(+,×),若$\forall p_1, p_2, ..., p_n \in P_\varepsilon$同时加法和乘法运算在式(1)中成立,但是仅能进行有限次的同态运算,则称加密算法ε为类同态加密算法.

一个类同态加密方案能够同时支持在密文域上进行加法和乘法的同态运算,但是由于要考虑降低密文产生时的噪声,不得不限制某一类运算的操作次数以完成解密过程,通常情况下,同态加密算法在密文计算后的新密文中会伴有随机误差向量即噪声,在解密时要尽可能地将噪声控制在安全参数允许范围内,这个限制是为了密码系统模糊同态操作后可以正确解密密文,换而言之,类同态加密方案一般只能够对特定的数据集进行密文计算,仅适用于现实中的特定应用场景,例如医学数据[28]、基因组和生物信息学数据[29−31]、无线传感器数据[32]、SQL 数据[33]以及整型数据,不少研究开始对现有类同态加密方案改进,为使其服务于自定义数据集计算,如预测分析[28]、回归分析[34]、统计分析[29,35]和其他一些运算类型.2005 年 Boneh[25]等人提出了具有语义安全的 BGN 方案,这是第一个可以同时支持不限次数的密文加法和一次乘法同态运算的方案,并且加密后密文没有发生膨胀.随后,Gentry、Halevi、Vaikuntanathan[36]对 BGN 方案进行改良提出了 GHV 方案,其安全性假设基于容错问题的困难性;Chan[37]等人基于希尔密文及 Rivest 的加密思想提出 IHC 方法和 MRS 方法,能够支持密文的加法,但乘法只支持密文与明文相乘,且这两种方法的安全性较低.Hojsík[38]等人基于 Polly Cracker 技术提出的 SymPC 方法为指数级的复杂度,通过选择合适的随机数,可以将复杂度降到多项式时间,但由于安全参数对效率的影响较大,无法同时兼顾安全性与效率.黄汝维[11]、桂小林等人提出了基于向量和矩阵运算的 CESVMC 加密方案,能够支持加密字符串的模糊检索和密文数据的加、减、乘、除法运算,但是方案仅支持一次乘法或除法运算,虽然效率较高但是密文膨胀问题依然是其瓶颈.杨攀[39]、桂小林等人提出一种对称体制的 CESIL 方案,用理想格划分多项式系数向量环的剩余类,建立商环及其代表元集合,通过代表元所在剩余类的其他元素对其进行替换完成加密,方案实现加法乘法混合同态运算,密钥及密文长度较小,并将其应用到加密图像的缩放、叠加运算,效率较为理想.应当说类同态加密技术的发展奠定了之后全同态加密研究的基础,后期许多全同态加密的方案也是由类同态加密方案改造而来.

3.2.1 BGN 加密方案

BGN 方案能够进行一次密文乘法运算和无限次加法运算.

密钥生成过程 Gen_{BGN} 如下:

设 $\lambda \in Z^+$ 为安全参数,随机选取 λ 位的大素数 q_1、q_2,令 $n = q_1 \cdot q_2$, G_1 为 q_1 阶双线性群, $e: G_1 \times G_1 \to G_2$ 为 n 阶双线性映射,随机选取 $u, g \leftarrow G_1$, 令 $h = u^{q_2}$, h 为 G_1 子群的生成元,元素 $x \in G_1$, 规定若其阶数为 q_1,则输出为 1,否则为 0.这里,公钥 $pk = (n, G_1, G_2, e, w, g)$, 私钥 $sk = q_1$.

加密算法 Enc_{BGN}:明文空间定义为整数集合 $M = \{0,1,...,T\}, T < q_2$, 随机选取整数 $r \leftarrow \{0,1,...,n-1\}$, 对于明文 m,密文为

$$c = g^m h^r \in G_1 \tag{9}$$

解密算法 Den_{GBN}:对于密文 $c = g^m h^r$, 使用私钥 $sk = q_1$ 解密,令

$$c^{q_1} = (g^m h^r)^{q_1} = (g^{q_1})^m \cdot (h^r)^{q_1},\ h^r = \underbrace{(u^{q_2})\cdot(u^{q_2})\cdot...\cdot(u^{q_2})}_{r}, (h^r)^{q_1} = \underbrace{(h^r)\cdot(h^r)\cdot...\cdot(h^r)}_{q_1} \in G_1,$$

所以,

$$c^{q_1}=(g^{q_1})^m\cdot(h^r)^{q_1}=(g^{q_1})^m\cdot 1=(g^{q_1})^m,$$

由于 q_1,c,g 都为已知,则明文为

$$m=\log_{g^{q_1}} c^{q_1} \tag{10}$$

同态属性:

很明显,由于密文 $c_1\cdot c_2=(g^{m_1}h^r)\cdot(g^{m_2}h^r)=g^{m_1+m_2}h^{2r}=Enc_{BGN}(m_1+m_2)$, 所以方案满足加法同态性质.

定义 $g_1=e(g,g),h_1=e(g,h),h=g^{\alpha q_2}(\alpha\in Z),r,r_1,r_2\in Z_n,c_1=g^{m_1}h^{r_1},c_2=g^{m_2}h^{r_2}(c_1,c_2\in G_1)$ 根据双线性对性质定义密文域乘法为

$$c_1\otimes c_2=e(c_1,c_2)h_1^r=e(g^{m_1}h^{r_1},g^{m_2}h^{r_2})h_1^r=e(g,g)^{m_1\cdot m_2}h_1^r=c_3=g_1^{m_1\cdot m_2}h_1^{r'}=Enc_{BGN}(m_1\cdot m_2) \tag{11}$$

其中, $r'=m_1r_2+r_2m_1+\alpha q_2r_1r_2+r,r'\in Z_n$, 密文乘积 $c_3\in G_1$, 可以看出方案仅支持一次同态密文乘法运算,超过一次运算时解密算法将无法对密文正确解密.

3.3 全同态加密方案(FHE)

全同态加密是当前同态加密领域研究的前沿,到目前为止,学界尚未形成统一的定义来描述全同态加密.现有的 FHE 方案主要通过电路来构造,一个 FHE 方案的核心就在于其密文计算算法 $Cal_\varepsilon(pk,C_\varepsilon,c_1,...,c_n)$, 可以用电路来理解,这里 C_ε是一个电路集合,可以等价于一个函数或功能,公钥 pk 用于密文计算,解密算法 $Dec_\varepsilon(c_1,...,c_n)=(m_1,...,m_n)$, 对密文进行运算后解密的结果要对应明文直接运算结果,所以需要有正确性保证.

定义 4. 若由密钥生成算法 Gen_ε 生成的任何一对密钥 (pk,sk), 任意电路 $C\in C_\varepsilon$, 向 Cal 输入 pk 和密文序列 $c=\langle c_1,...,c_n\rangle$、电路 C 后,输出的 $c^*=Cal(pk,C,c_1,...,c_n)$, 满足 $Dec(sk,c^*)=C(m_1,...,m_n)$, 那么称同态加密方案$\varepsilon$为正确的.

此外, $Cal_\varepsilon(pk,C_\varepsilon,c_1,...,c_n)$ 输出的新密文应保证与 $Enc_\varepsilon(m_1,...m_n)=(c_1,...,c_n)$ 过程计算量一致,即方案是紧凑的.

定义 5. 对任意的安全参数λ,始终存在一个多项式f,同态加密ε的解密过程可以表示为一个上限规模(MAX SIZE)为$f(\lambda)$的电路 W,那么称方案ε是紧凑的.

定义 6. 同态加密方案ε对某一电路 C 为正确且紧凑的,则称ε关于电路 C 为紧凑的,若上述条件满足任意一个电路 $C\in C_\varepsilon$, 则称ε是一个全同态加密方案.

Gentry 首次基于理想格构造了全同态加密方案,方案在语义上具备安全性,但是只能进行简单的密文运算,复杂密文运算经过编码之后形成较深电路深度(噪声问题),导致其解密算法无法正确得出明文.Smart 等人[40]改用整数和多项式实现全同态加密,缩短了密钥和密文长度,该方案加密解密过程实现简易,但是生成密钥的过程过于复杂.Chen[41]等人基于二元 LWE,设计了一个公钥和私钥更短的 FHE 方案,其张量密文也短于 Bra12 方案.Gentry 等人[16,42,43]对全同态加密算法中的自举技术、加密算法的解密循环分解技术、方案实现手段等方面进行了改进,在一定程度上降低了方案的复杂性,但是由于 Bootstrappaping 在实现过程方面仍然十分复杂,即使在安全性要求较低的情况下,完成一次 Bootstrappaping 也要耗时 30s 左右,因此,这些加密方法在实用性上都比较受限.2010 年 Gentry[44]与 Dijk 等人研究了整数环上的全同态加密算法,即 DGHV 方案,从同态操作与性能特性上,该方案与基于理想格的构造方案非常相似,均保持密文长度的紧凑性——密文长度完全不依赖于计算加密数据的函数的复杂性,但是,从概念性上看,DGHV 方案并非基于格理论或在 Gentry 初始方案进行改进,而是基于基本的模运算进行构造,相较于基于理想格的构造方案更简洁,DGHV 方案的安全性是基于近似最大公约(approximate greatest common divisor problem)和确定性最大公约数问题(approximate greatest common divisor problem),不过方案同样使用了 Gentry 的自举技术,最近许多研究[45−48]通过提升自举技术和减小公钥的大小来提升其执行效率,但是这些方案并没有完全解决 FHE 方案的噪声问题.之后,Brakerski 等人[49,50]基于错误学习(learning with errors)、环上错误学习 RLWE(ring-LWE)构造出不需要 Bootstrappaping 的全同态加密方法,文献[30−32]也是基于 LWE、RLWE 的同态加密方法.基于公钥全同态加密的密文计算如图 3 所示.

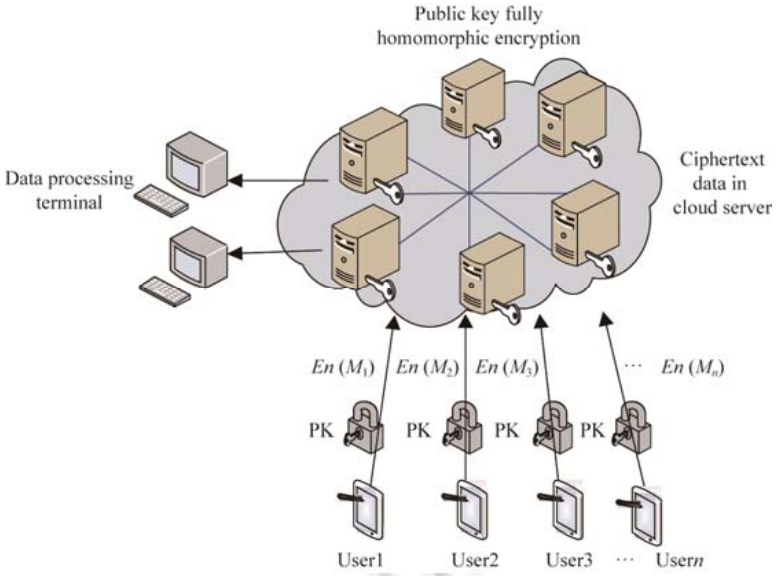

Fig.3 Ciphertext computation based on public key fully homomorphic encryption

图 3 基于公钥全同态加密的密文计算

表 2、表 3 分别是 FHE 方案在不同属性上的分类,现有的 FHE 方案大多由 SWHE 方案进行改进而来,不同之处在于 FHE 方案使用各类降噪技术使密文产生过程中的噪声不会随着密文计算过程而增加.从算法设计基础的角度来看,FHE 方案可以分为 3 个主要类别:基于格理论、基于误差校正码和基于数论,后两种是基于传统的数学方法.格密码学是近年来新兴的重要研究方向,通过使用量子规约,基于格的密码学可以从最坏情况的难题规约到一般情况难题,因而攻击基于具体格问题构造的密码系统等同于求解相应的格困难问题.事实证明,格密码能够有效地抵御量子计算攻击,同时相比于过去的 PHE 方案(EGM 方案包含幂运算),基于格的 FHE 方案具有更简约的解密电路设计,因此基于格上困难问题的全同态加密方案的构造成为了研究的焦点.

Table 2 The classification of FHE scheme in encryption system, theoretical basis and noise control technology

表 2 FHE 方案在加密体制、理论基础、噪声管控技术上的分类

FHE 方案	加密体制				方案理论基础			噪声控制技术				
	对称型	非对称型	确定型	概率型	格理论	数论	误差校正码	Bootstrapping	模转换技术	尺度不变技术	扁平化技术	无噪声方案
Gen10[12]		√		√	√			√				
SV10[13]		√		√		√		√				
DGHV10[23]		√		√		√		√				
SS10[27]		√		√	√			√				
GH11[16]		√		√	√			√				
BV11[50]		√		√	√				√			
CMT11[26]		√		√		√		√				
BL11[45]		√		√			√	√				
BGV12[15]		√		√	√				√			
Gu12[51]		√		√		√		√				
KH12[52]	√			√		√						√
GHS12a[37]		√		√	√			√				
GHS12b[53]		√		√	√				√			
GHS12c[54]		√		√	√			√				
LTV12[55]		√		√	√				√			
Bra12[56]		√		√	√					√		
CNT12[57]		√		√		√			√			
ZLX13[58]		√		√	√				√			
BLLN13[59]		√		√	√					√		
KLYC[60]		√		√		√		√				
ZY13[61]		√		√		√		√				

Table 2 The classification of FHE scheme in encryption system, theoretical basis and noise control technology (Continued)

表 2 FHE 方案在加密体制、理论基础、噪声管控技术上的分类(续)

FHE 方案	加密体制				方案理论基础			噪声控制技术				
	对称型	非对称型	确定型	概率型	格理论	数论	误差校正码	Bootstrapping	模转换技术	尺度不变技术	扁平化技术	无噪声方案
CCKM13[62]		√		√		√		√				
GSW13[63]		√		√	√						√	
DHS14[64]		√		√	√					√		
DES[65]		√		√		√						
CWS14[66]		√		√	√				√			
CLT14[67]		√		√		√				√		
ZW14[68]		√		√		√					√	
RC14[69]		√		√	√					√		

Table 3 Classification of security assumptions for FHE schemes

表 3 FHE 方案的安全假设问题分类

FHE 方案	格理论						数论					误差校验码理论
	多项式陪集问题	理想最短独立向量问题	离散子集和问题	有界距离译码问题	基于误差的学习问题	带误差环学习问题	近似最大公约数问题	近似最大确定公约数问题	整数分解问题	多元二次方程	经典离散对数问题	解码随机线性码问题
Gen10[12]			√	√								
SV10[13]	√		√									
DGHV10[23]							√					
SS10[27]			√	√								
GH11[16]		√								√		
BV11[50]			√		√							
CMT11[26]							√					
BL11[45]												
BGV12[15]								√				
Gu12[51]							√		√			
KH12[52]											√	
GHS12a[37]						√						
GHS12b[53]					√							
GHS12c[54]						√						
LTV12[55]						√						
Bra12[56]					√							
CNT12[57]							√					
ZLX13[58]						√						
BLLN13[59]						√						
KLYC[60]			√					√				
ZY13[61]							√					
CCKM13[62]						√	√					
GSW13[63]					√							
DHS14[64]						√						
DES[65]						√						
CWS14[66]					√							
CLT14[67]							√					
ZW14[68]						√						
RC14[69]						√						

3.3.1 DGHV 加密方案

DGHV 方案首先需要构造一个 SWHE 方案,再将其转换为 FHE 方案.

第 1 步.构造 SWHE 方案.

密钥生成过程 Gen'_{DGHV} 如下:

设λ为安全参数, $\tau=\lambda+\gamma,\eta=O(\lambda^2)$, 随机生成一个$\eta$位的大奇数 $p\in(2Z+1)\cap\left[2^{\eta-1},2^{\eta}\right)$, 从分布 $D_{\gamma,P}(p)$ 中选取 $\tau+1$ 个整数 $x_i\leftarrow D_{\gamma,P}(p),i\in(0,1,...,\tau),D_{r,q}(p)=\left\{x=pq+r\mid q\in Z\cap\left[0,2^{\gamma}\middle/p\right],r\in Z\cap(-2^{\rho},2^{\rho})\right\}$, 其中, $\rho=\lambda$, 从 x_i 中选取最大的数 x_0,确保其为奇数,且 $x_0 \bmod p$ 为偶数,这里,公钥为向量 $pk=X=(x_0,x_1,...,x_\tau)$, 私钥 $sk=p$.

加密算法 Enc'_{DGHV}:随机选取一个子集 $S\subseteq\{1,2,...,\tau\}$ 和整数 $r'\in(-2^{\rho'},2^{\rho'}),\rho'=2\lambda$, 对于明文 $m\in\{0,1\}$ 加密后密文 c 为

$$c=\left(m+2r'+2\sum_{i\in S}x_i\right)\bmod x_0 \tag{12}$$

解密算法 Gec'_{DGHV}:对于密文 c,其对应的明文 m 为

$$m=(c\bmod p)\bmod 2 \tag{13}$$

第 2 步.将 SWHE 转换为 FHE 方案.

DGHV 方案利用稀疏子集对解密过程简化,使构造的 SWHE 方案实现 Bootstrappaping.方案的密钥生成过程 Gen_{DGHV} 如下:

设参数 $\kappa=\gamma\eta/\rho',\Theta=\varpi(\kappa\log\lambda),\theta=\lambda$, 令 $x_p=\lceil 2^{\kappa}/p\rfloor$ 随机选择一个汉明重量为 θ 的 Θ 位二进制向量 $\vec{H}\in\{0,1\}^{\Theta}$, 定义向量 $\vec{H}$ 的元素下标集合 $H=\{i\mid h_i=1\}$, 再随机选取整数 $u_i\in Z\cap[0,2^{\kappa+1})(i=1,...,\Theta-1)$, 使其满足 $\sum_{i\in H}u_i=x_p\bmod 2^{\kappa+1}$. 令 $y_i=u_i/2^{\kappa},\vec{y}=(y_0,y_1,...,y_{\Theta-1})$, 这样便得到公钥 $pk=(\vec{x},\vec{y})$, 私钥 $sk=(\vec{H})$.

加密算法 Enc_{DGHV}:首先使用上一步构造的 SWHE 方案中的公钥对明文加密得到密文 $c=Enc'_{DGHV}(m)$, 再计算 $z_i=[c\cdot y_i]_2$, 保留 z_i 的二进制序列小数部分 $n=\log\theta+3$ 位,则新的密文为 $c'=\{c,(z_0,z_1,...,z_{\Theta-1})\}$.

解密算法 Dec_{DGHV}:对于密文 c,其对应的明文 m 为

$$m=\left(c-\sum_{i=0}^{\Theta-1}z_iH_i\right)\bmod 2 \tag{14}$$

3.3.2 BV11 加密方案

BV11 是一种高效的层次型 FHE 方案,采用密钥交换技术与模交换技术来控制密文膨胀(关于密钥交换技术与模交换技术将在后面详细介绍).BV11 首先使用密钥交换技术将经过乘法运算后膨胀的密文乘积 $c=c_1\cdot c_2$ 转化成与 c_1,c_2 维数相同的新密文 c', 进入下一层电路后使用模交换技术控制噪声.

$Step(1^{\lambda},1^{\mu})$: 设安全参数为 λ,j 层解密电路为 $L=\{L_0,L_1,...,L_j\}$, 模 $q_L(L=0,1,...,j)$ 为一个递减序列,由随机选取的 μ 位奇数 q 生成. $f(x)=x^n+1,n=n(\lambda,\mu)\in 2^k(k\in N)$, 由 q 生成 n 维多项式 $R_q^n=Z[x]/f(x)$, 随机选取 μ 位奇数 q 生成多项式环 $R_q^n=Z_q[x]/f(x)$, χ 是 R_q^n 上离散高斯分布.

密钥生成过程 Den_{BV11} 如下:

从 L_j 到 L_0 层电路,随机选取向量 $s\leftarrow\chi,e\leftarrow R_q^n,a\leftarrow R_q^n$, 令 $b=as+2e$. 每层生成公钥、私钥分别为 sk_L=$s_L\leftarrow(1,-s)\in R_q^n\times R_q^n,pk_L$=$(a,b)\in R_q^n\times R_q^n$, 这里,向量乘法定义为向量间内积运算.

加密算法 Enc_{BV11}:对于二进制明文 $m\in\{0,1\}$, 将其明文序列转换为多项式 R_2^n,m 的二进制序列即为多项式 R_2 常数项的系数.随机选取 $\sigma\leftarrow\chi,\varsigma\leftarrow\chi,\upsilon\leftarrow\chi$, 用公钥 pk_L=(a,b) 加密明文 m 得到第 j 层密文 c':

$$c'=(c_0,c_1),c_0=a\sigma+2\varsigma+m,c_1=b\sigma+2\upsilon \tag{15}$$

进入第 j–1 层电路,计算 $s'=s\times s\in(R_q\times R_q\times R_q),SwitchKeyGen(s',s'_{i-1})\rightarrow\tau_{j-1}$ 表示由 s',s_{i-1} 通过密钥交换算法得到参数 τ_{j-1}, 以此类推直到第 0 层,因此各层对应的私钥集合 sk=$\{s_L\}$, 公钥集合 pk=$\{pk_L,\tau_L\}$.

解密算法 Dec_{BV11}:对于密文 c,其对应的明文 m 为

$$m=((c_0+c_1\times s)\bmod q)2 \tag{16}$$

只要保证 $\|c_0+c_1\times s\|<q/2$, 就能正确解密出明文 m 密文加法运算 Cal^{+}_{BV11}: 对于两个密文 $c_{j,1},c_{j,2}$, 若二者同属第 j 层,所对应的密钥为 $s'_j\leftarrow(1,-s_j)$, 则直接按照多项式向量加法运算法则计算 $c_{j,1}+c_{j,2}=c_{j,3}$; 若密文 $c_{j,1},c_{k,1}$ 不同属一层,先使用密钥交换算法将较高层的密文 $c_{\max\{j,k\},1}$ 转换成底层密文 $c_{\min\{j,k\},1}$, 再进行加法运算得到密文 $c_{\min\{j,k\},2}$, 再使用模转换技术降低其噪声,最终得到与执行加法运算前的密文维数相同的密文 $c'_{\min\{j,k\},2}$.

密文乘法运算 $Cal^{\times}_{BV11}$: 与加法运算相同,若两个密文同属一层,则直接执行密文乘法运算,若不属一层,则按

照上述操作方法完成计算.

目前现有的 FHE 方案在实现上仍然较为复杂且计算模型复杂度较高.构造一个 FHE 方案时 Bootstrappaping 过程的耗时较长,在计算模型中,程序需要以布尔电路形式编码,由于要进行乘法运算,一般的应用程序编码后对应层数很深的布尔电路,为了保证语义安全阻止敌手获取任何明文数据相关信息,方案所基于的安全假设问题带来的计算开销也很可观.另外,表 2 中的 FHE 方案都不能直接进行浮点数的运算,需要转换为两个整数相除的形式.这些问题是现有 FHE 方案还无法适用于大型云服务应用的主要原因.尽管大部分现行 FHE 方案在执行效率上还无法满足大范围实际应用的需求,但是全同态加密算法的研究从理论上使得在密文域进行各种运算操作成为可能,这也是密码学研究领域的一个重大突破.

3.4 对称与非对称同态加密算法

与传统加密方法类似,同态加密算法也通过使用相同的一对密钥(对称加密方案)或不同的一对密钥(非对称加密方案)来加密数据,现有大多数的同态加密算法都基于非对称密码体制(公钥加密系统),少数是对称 HE 方案,主要是由于现行对称型方案的实现效率不高,而且密钥管理较为复杂,在实际应用中部署并不现实.此外,大多数对称同态加密方案由于算法设计[45−48]还存在安全漏洞,从理论上还不能完全证明其安全性,不过,基于公钥加密体制的 HE 方案也存在明显的瓶颈,由于方案的实现往往需要巨大的计算开销,因而不能满足云环境中诸如外包计算这样的服务要求,有的文献[70−72]通过减小加密方案的计算开销来构造轻量化的密文计算方案,但是仍无法满足云中海量数据的外包计算要求.

3.5 确定性与非确定性同态加密算法

大部分现有的同态加密算法通过概率特性而保证其语义安全[17−19,21−26,73],如果敌手无法从密文中获得任何有用的信息来恢复明文,则可以认为加密方案在语义上是安全的,少数是确定性 HE 方案.在确定性 HE 方案中,使用同一密钥对明文加密后始终得到同样的密文,若同一明文经过同样的密钥加密后可以得到不同的密文,则可以归类为概率性 HE 方案.

3.6 全同态加密的实现技术

3.6.1 同态解密技术

在一个 FHE 方案中密文计算后产生的噪声是面临的首要困难,同态解密计算技术正是为了解决这一问题而提出的.以 DGHV 方案来说,在第 1 步构造的 SWHE 方案中,密钥 $sk=p$ 是 w bit 的大奇数,随机选取整数 q,对明文进行加密 $c=m+2r+pq$,这里,$m+2r$ 即为噪声,只有当 $c \bmod p=m+2r<P/2$ 时才能确保解密得到正确明文即 $(m+2r) \bmod 2=m$,为了将 SWHE 方案转换成对电路深度没有要求的全同态加密方案,在第 2 步中需要使用 Gentry 提出的自举技术,选取大奇数 p 作为私钥 sk,公钥 $pk_i=\{x_i | pq_i+2r_i, 0 \leqslant i \leqslant \eta\}$, r_i(较小)、q_i 为随机选取的整数,这实际上是一个刷新密文(recryption)过程:用公钥 pk_2 加密明文 m,公钥 pk_1 对私钥 sk 的二进制数逐位加密得到密钥向量 SK,将二者作为输入后输出 pk_2 加密的密文,即 $Dec_{enc_{pk_2}}(En_{pk_2}(En_{pk_1}(m)))=Enc_{pk_2}(Dec(sk, En_{pk_1}(m)))=Enc_{pk_2}(m)$,反复刷新密文以降低噪声,使密文能够正确计算直到完成所有运算,从而突破 SWHE 方案中密文计算次数的限制,不过,在解密过程中存在密钥多项式函数次数过高的问题,为此,Gentry 使用 Squash 技术,给公钥向量 $1/p$ 一个提示信息(CLUE),引入稀疏子集,集合 $S=\{x_i | i=1,2,...,N\}$ 存在一个子集 $T=\{b_i | b_i=\sigma_i x_i,\ \sigma_i \in \{0,1\}\}$ 使得集合 T 中所有元素相加之和为公钥向量 $1/p$,将 $\sigma=[\sigma_1,...,\sigma_N]$ 作为新密钥,对集合 S 中元素做变换得到 $z_i=x_i \times c$,这样,解密过程由 $m=c-[\omega \times c] \bmod 2$ 变为 $m=c-\sum_i \sigma_i z_i \bmod 2$,可以将转换后的解密函数写成次数为集合 T 中的元素个数的 σ_i 的多项式表达式,这样的话,只要控制 T 中元素数目为较小的数就可以解决解密函数中多项式次数太高的难题.后续的很多同态加密方案[13,16,41−43,74,75]也都使用 Gentry 的 Bootstrappaping 技术,这些方案对文献[12]中所提方案都有不同程度的改进,2010 年 Stehle 和 Sheinfeld[27]提出了一种快速刷新密文的算法来提升 Bootstrappaping 技术表现;Gentry 和 Halevi[27]通过减小公钥大小以及使用

批处理技术来提高这项技术的性能,但是这些改进仍然没有显著提升其效率.例如在一台处理器配置为 Intel Xeon E5450 64 位 4 核的终端上对大小为 380bit 密文重加密(re-encryption)过程中,按照最低安全要求也要超过 1.5 分钟来运算[43],除了存在计算效率的问题外,Gentry 和 Halevi 的方案需要超过 78 万位的密文来加密一位二进制明文,过大的密文体量在传输密文的带宽方面也造成瓶颈,2011 年 Gentry、Halevi[16]又提出了一种无需 Squash 技术来实现解密电路的方案,但是这些对 Bootstrappaping 技术的改进方法由于 Gentry 的初始方案存在的内在瓶颈与现实商用还有距离.

3.6.2 模交换技术

模交换技术是为了降低密文运算后噪声呈数量级增加的问题而提出来的,源自以下引理:对于奇数 p、q 和向量 $C, C' \approx (p/q)C$, 且 $C' = C \bmod 2$, 如果对某个 S 有式(17)成立,则有式(18)及式(19)成立,具体如下:

$$\forall S, \left\| \langle C, S \rangle \bmod q \right\| < q/2 - (p/q)l(S) \tag{17}$$

$$\langle C', S \rangle \bmod p = \langle C, S \rangle \bmod q \bmod 2 \tag{18}$$

$$\left\| \langle C', S \rangle \bmod p \right\| < (p/q) \left\| \langle C, S \rangle \bmod q \right\| + l(S) \tag{19}$$

其中,$l(S)$为 S 的范数,$\langle C,S \rangle$为向量内积运算.

通过上述引理可知,当密钥 S 未知时,只要知道其长度边界,就能将密文从模 p 下转换为模 q,并且 $\langle C', S \rangle \bmod p = \langle C, S \rangle \bmod q \bmod 2$ 仍然成立,即解密正确.

例如两个噪声为 x 的密文,经过一轮相乘后噪声达到 x^2,若取模 $p = x^n$, 密文经过 lbn 轮相乘就达到了噪声上限从而使解密算法无法正确解密,如果在第 1 轮密文相乘后对噪声除以 x,噪声则恢复为原来大小,模降为 $p = x^{n-1}$, 经过 k 轮操作,模为 p/x^k,模形成一个递减系列,如式(20)所示:

$$p_i = \left\{ x_i \left| x^k \middle/ x^i, 0 \leqslant i \leqslant k \right. \right\} \tag{20}$$

其中,噪声始终控制为 x,这样,密文可以进行 n 轮相乘才会达到噪声上限,比未使用模转换的 lbn 轮达到噪声上限时可以做到数量级上的提升,通过降噪和模递减使方案可以对最高次数为任意的多项式密文做计算并保持同态性,不需要使用 Bootstrappaping 来实现,提升了方案的可用性和效率,BGV 方案是应用此项技术的典型方案,也是目前效率最理想的 FHE 方案.

3.6.3 密钥交换技术

在所有基于 LWE 的 FHE 方案中,密文 C 和密钥 S 都是向量,密文在计算时乘法定义为张量积形式 $C_1 \otimes C_2$, 相应密钥为 $S_1 \otimes S_2$, 因此密文在计算后维数将极速上升,很快达到计算边界,通过密钥交换技术来降低维数膨胀的问题,其本质是将一个矩阵 B 和密文 C_1 相乘得到新的密文,即 $C_1^T \times B \to C_2$ (B 行数是 S_1 的维数,列数是 S_2 的维数,S_2 的维数小于 S_1),通过密钥交换可将维数是 h_1 的密文转换为维数 h_2 的密文,即 $\langle C_1, S_1 \rangle \to \langle C_2, S_2 \rangle (h_2 < h_1)$, 模 p 保持不变,达到降低密文维数的目的,对较小的密文明文 C_2 执行解密算法 $m = ((\langle C_2, S_2 \rangle \bmod q) \bmod 2)$, 这样既可省去 Squash 操作也能正确完成脱密.但是这种方法的缺陷是每次密钥交换时密文都需要乘以一个矩阵,这会影响到 FHE 方案的执行效率.此外,新的密文 C_2 在计算后的噪声也略高于 C_1.

3.6.4 并行计算技术

密文打包技术、批处理技术、单指令流多数据流(SIMD)技术都被用于提升 FHE 方案的执行效率.2010 年 Smart 和 Vercauteren[13]首次提出了密文打包技术,并由 Gentry 和 Halevi 应用到 FHE 方案中[16],不同于以往逐位对明文进行加密的方式,利用这种方法可以将二进制明文的多位打包成向量元素,通过中国剩余定理来加密成一个新的单个密文.单指令流多数据流技术可以将密文重加密过程并行处理,能够显著提升速度并且降低所需带宽和通信成本,在 Coron[57]等人的方案中,原本加密 4MB 的明文数据需要在网络中传输 74TB 的密文数据,通过并行计算技术[62]改进 FHE 方案,利用 SIMD 技术对 AES 十轮操作并行处理,这样,每个操作平均耗时 12min,最终可以将通信成本降低到接近 280GB[76],Smart[77]等人通过中国剩余定理对明文序列进行批处理,然后利用 SIMD 技术实现了明文序列的并行计算,在文献[53]中采用密文打包技术对 FHE 方案进行优化,将 AES 的十轮

操作并行化处理,平均每个操作花费 40min,比 Gentry、Halevi[16]的方案在速率上高出几个数量级,文献[42,53,54]的 FHE 方案都使用了并行计算技术来优化以提升方案的效率.

4 同态加密技术在云计算隐私保护中的应用

4.1 云计算中保护隐私的检索(privacy-preserving search)

随着云计算技术深入拓展到各个领域,云端数据的存储和使用呈几何爆炸式增长,对加密数据的检索成为一个亟待解决的难点问题,目前已有的研究工作通常都是采用一种数据结构来存储明文对应的多个可能的模糊关键字的密文,通过精确匹配来实现模糊检索,但是它们只适用于小规模数据的检索,且代价高效率低.基于全同态加密的数据检索技术能够直接在加密的数据上直接检索,避免检索数据被统计分析,不仅能做到保序检索,还能对检索的数据进行比较、异或等简单运算.Gopal[78]和 Singh 基于 Gentry 的 FHE 方案提出了一个 PPS 方案,利用密钥加密文件中每个关键字和查询,这样,云端在不知道密钥的情况下,只能对密文数据进行操作返回密文结果.Cao[79]等人提出了一种多关键字排序搜索技术,方案的思想是使用密钥加密向量时添加虚假关键字,进行分割或相乘操作(密钥由一个向量和两个矩阵组成),用户端也将应用相同的操作(作少许更改)对查询向量使用相同的密钥加密然后发送到云端,云端接收后对加密的向量(查询和索引)进行处理再生成相似向量.Li[80]等人提出了一种用于对加密数据进行模糊关键字检索的技术,数据所有者通过构造一个模糊关键字集合来构建一个索引,然后通过数据所有者和授权用户之间共享的密钥计算门陷集,数据所有者再将此索引发送到云端,检索数据集时,授权用户使用与数据所有者间共享的密钥计算查询关键字的门陷集,然后将其发送到云端,云端接收查询后,与索引表进行比较,根据模糊关键字返回所有可能的加密文件标识.

4.2 多方安全计算中的应用

在现实中,某个应用场景中需要多方参与计算,但是各方互相可能为可信也可能为不可信,当需要对私有数据进行检索、分析、处理时,大家都不希望数据内容被其他参与方掌握,所有参与方将自有数据以密文形式进行联合计算,使用全同态加密算法,可以使除用户和授权者外的第三方利用其同态特性在密文上直接操作,将结果返回后得到明文计算相同的结果,从而完成用户的需求.Bendlin 等人[81]对多方安全计算和同态加密技术的关系进行了系统论述,文献[82]基于同态加密算法来解决了“百万富翁”难题,Goethals 等人[83]在向量点积多方安全计算问题中同样借助了同态加密算法.现实中,很多应用场景需要通过多方安全计算协议来实现,例如电子投票、多人参与的网上棋牌游戏等,密钥分配协议、不经意传输协议等都是多方安全计算协议的特例,而同态加密算法则是构建多方安全计算协议的重要基础.

4.3 密文数据库

CryptDB 是麻省理工计算机科学和人工智能实验室(CSAIL)以 PHE 方案为基础实现商用化的应用实例,它能够实现用户对存储在 SQL 数据库的数据进行多种查询操作,通过 SQL 能够“识别”的 4 种操作(order comparison、equality checks、join、aggregate)来分解所有原始查询语句以对数据按列进行加密,从内到外层层采用不同加密方案来加密不同查询功能,其安全性由内层的低强度到最外层满足语义安全.另外,CryptDB 系统对用户身份密码和加密算法密钥进行捆绑,这样用户如果不使用正确的身份密码将无法登录对数据项进行解密,连数据库管理员也无法对密文数据解密,即使服务器被攻破,只要用户没有登录,攻击者也无法解密用户的密文数据,并且 CryptDB 主要采用对称型 HE 方案,因此所有操作对系统效率影响较小.Tu 等人[84]提出 Monomi 算法,对 CryptDB 进行改进使其能处理更复杂的查询.近期,国外研究者在 CryptDB 基础上提出了 MrCrypt[85]、Crypsis[86],MrCrypt 应用于云计算系统的开源系统 Hadoop 中的并行计算模型 MapReduce、Crypsis 用于支持如 Pig Latin 这样的高级数据流语言,Crypsis 和 MrCrypt 都使用 Pai、EGM 方案分别来实现密文数据的加法和乘法同态运算,为了支持多种类型的查询服务,CryptDB 中的每一条数据和变量都需要使用不同的同态加密方案进行加密(例如,Paillier 加密方案支持统计查询,EGM 方案支持关键词搜索),这导致额外的存储消耗,当外包数据频繁进行传输时也会增加与第三方云服务商的通信开销.

4.4 其他应用研究

Brenner 等人[87]针对云计算环境中的数据隐私问题,采用全同态加密技术实现了机密程序在第三方服务器上的安全执行.Hsu 等人[88]针对云计算环境中的多媒体信息检索问题,提出了一个基于 Paillier 的安全尺度不变特征变换(SIFT),从而实现隐私保护的特征抽取和表示,并基于量子的安全比较策略实现了同态比较.Ren 等人[89]针对无人值守的无线传感器网络(unattended wireless sensor networks,简称 UWSN),基于同态密钥共享和同态加密机制设计了一个数据传输方案 H2S,提高了数据传输效率,并为数据的机密性和完整性提供了保障.Zhu 等人[90]针对分布式计算模 Map-Reduce 中的隐私保护问题,基于 BloomFilter 和加法同态算法实现了隐私保护的密文检索.Zhu 等人[91]描述了同态加密算法在加密的声音信息检索中的应用.Igor 等人[92]描述了同态加密技术在移动设备的隐私保护中的应用.Liu 等人[93]针对无线传感器网络中的隐私安全问题,采用同态密钥共享和同态加密的方法来保证数据的安全和检索.Upmanyu 等人[94]基于安全的多方计算和同态加密算法 Paillier 实现了隐私保护的分布式 k-均值聚类.Yi 等人[95]针对 UWSN 中安全和高效的存储问题,提出了基于同态加密和密钥推导的方案.Lipmaa[96]基于全同态加密技术实现了外包数据的安全更新.马进等人[97]提出了分布式环境下的基于随机数值片拆分统计机制的匿名均值统计和匿名方差统计方法,并结合加法同态加密算法 Paillier,设计了分布式环境下的随机数据交换方法,实现了分布式环境中匿名数据交换机制.方炜炜等人[98]针对分布式决策树挖掘的隐私保护问题,提出一种基于同态加密技术的决策树挖掘算法,使各参与方在不共享其隐私信息的前提下达到集中式挖掘的效果.Jaideep 等人[99]基于同态加密技术改进了贝叶斯分类方法,保证了分类过程中的数据隐私安全.Vaidya 等人[100]也是基于同态加密技术实现了支持向量机的分类.应当说,加强同态加密技术在云计算隐私保护领域中的应用,不仅能够利用同态加密算法的优势来解决云计算安全问题,同时还可以帮助同态加密自身发展,从而达到互利双赢的目的.

5 总结与研究展望

目前,同态加密技术在云计算隐私安全的应用领域不断扩展,这同时也加速了同态加密技术本身的改进与发展,虽然不少研究者提出了新的 FHE 方案,但当前基于各种传统数学难题假设的方案在运算效率上还比较低,所要求的计算量和密文膨胀率都不理想,许多已有方案往往要求数据拥有者在数据外包的过程中做大量的协助工作,例如建立并维护目录,或者要求通过一个第三方才能实现对密文的运算,前者会使用户的使用体验大打折扣,后者增加了接触数据的参与者,即增加了数据泄露的风险,大范围商用还不现实.此外,密文空间膨胀是现有同态加密算法所面临的共同问题,大部分建立在公钥体制上语义安全的同态加密算法都有这个问题,这也是概率性加密算法固有的问题,密文过大也使用户从客户端上传加密数据到云端以及从云端下载加密到客户端会面临传输带宽瓶颈.现阶段从技术上彻底解决密文膨胀的问题还不现实,还需要从减小密文空间大小的角度进行改进和探索,现有 FHE 方案主要通过同态解密技术来降低密文膨胀问题,这样确实从理论上看能够克服计算边界的问题,但从实现角度上看非常复杂.此外,安全性与适用性问题也必须加以考虑.首先,大部分同态加密算法无法有效抵抗自适应选择密文的攻击,最高安全级别只能达到抵抗选择明文攻击;其次,由于可关联性是同态加密算法的内在属性,导致其不能应用在需要不可关联方案支持的场景中.掌握同态加密方案的适用范围,可以明确在什么场景下应用,什么情况下要避免使用同态加密算法而使用传统加密算法,以免误用造成安全隐患;最后,现有大多数 FHE 方案都是以 Gentry 的 FHE 方案为原型,这类方案在构造过程中一般分两个阶段,首先设计一个 SWHE 方案,然后通过噪声管控技术将其转换为一个 FHE 方案,因此,如何不经过 SWHE 方案阶段直接构造一个 FHE 方案仍然是一个开放问题.以上都是需要进行研究的重点问题.本文对云计算隐私安全面临的威胁和同态加密技术的研究进展进行了介绍,对现有同态加密方案作了分类和总结,分析了各种方案的优缺点,重点对全同态加密算法的构造、实现技术、安全基础作了分析.全同态加密技术是未来云计算隐私保护的重要依托,现有方案在加、解密效率上较低,构造方式和实现技术也很复杂,这些问题都有待解决,需要研究者持续而有创造性地进行工作,我们认为,未来可以在以下几个方面作进一步研究.

(1) 对称密码体制同态加密方案.

在大多数公钥同态加密算法中,都面临公钥尺寸过大、加密后明文对应密文过大问题,如在 Dijk 等人的整数 FHE 加密方案中,1Bit 明文加密后产生λ^5 Bit(λ为安全参数)的密文,当前的同态加密算法,无论是电路同态加密算法还是代数同态加密大多基于公钥私钥体制来构建,使用公钥压缩技术减小公钥大小,同时扩大明文空间,缩小密文空间是有效降低密文计算复杂度的方法,但是以这种方法为构建基础的一个明显缺点是算法的计算复杂度较高,明文的加密速度很慢.因此一般情况下,非对称公钥加密算法并不适用于用户在云服务器上进行外包计算这类需要对大量数据进行加密的场景,要实现云环境中密文的快速稳定存储等应用,就迫切需要研究计算复杂度低的对称类同态加密算法.

(2) 可验证的同态加密方案.

若用户将计算函数也外包存放在网络空间中,也会带来用户无法对返回的计算结果予以正确性验证的问题.尽管同态加密方案用来保证云环境中用户数据外包给半可信或不可信云服务商进行运算的安全性,但用户更加关注计算结果的准确性,以及这些不可信的服务供应商是否正确执行用户提出的计算要求或只是将近似的结果返回给用户,要解决这个问题,需要将同态加密技术与可验证计算技术一起使用,以保证用户外包计算数据的完整性,而现有的同态加密算法均未对计算结果的正确性予以考虑.因此,研究一种可验证的同态加密方案成为当前迫切需要解决的问题,即设计一种支持高效且安全性高的同态加密方案,并研究出针对该算法的验证方案,用以满足云计算存储服务中对于安全性、可靠性、可用性的需求.

(3) 无噪声 FHE 方案.

无噪声(没有密文膨胀)FHE 方案是近期的另一个热点研究方向,在加密方案中并不使用任何噪声管理技术,这些无噪声是基于经典的数理论概念构建的对称加密方案,如基于八进制代数、交换环和非交换环.现有的无噪声 FHE 方案中除了 Nuida[101]提出的方案是基于非对称密码体制的以外,大部分都是对称型,但是大部分现行的无噪声 FHE 方案在安全性上并不可靠,Kipnis[74]等人基于交换环的方案无法抵御选择明文恢复密钥的攻击,Yagisawa[102]等人基于离散对数问题的方案无法抵御量子攻击,未来无噪声 FHE 方案需要在安全性分析上进行更深入的探索,以求构建真正安全可靠的加密方案.

(4) 基于人工智能技术的 FHE 方案.

近期微软公司将人工智能技术引入到同态加密中,按照 CryotoNets[103]的报道,一家公司利用基于 RLWE 和 LWE 的 FHE 方案对数据进行加密上传到云端,云服务提供商使用人工前馈神经网络可以基于密文进行预测分析,但是所使用的神经网络模型需要提前用密文数据进行训练,并且训练神经网络所消耗的时间较为可观,将来是否有其他人工智能技术与同态加密技术相结合也值得研究.

(5) 支持“多对一”模式的同态加密方案.

现有的同态加密方案大多采用“一对一”部署模式,一方使用公钥对明文进行加密,另一方使用私钥对密文解密,这种形式的加密方式在“一对多”“多对一”和“多对多”的应用场景下效率很低.在现实中,存在不少“多对一”的应用场景,尤其是在云服务模式下,作为数据接收者的服务提供商数量远远小于作为服务请求者的用户数量,一个服务提供者常常要求为数以万计的数据发送者提供服务.传统的“一对一”同态加密方案在这种“多对一”的应用要求下是低效的.因此研究支持“多方加密、一方解密”应用场景的同态加密方案对于云服务模式下隐私保护非常有意义,设 S 为数据接收方,拥有一对公钥与私钥(pk,sk),P_i(i=1,…,n)为多个数据发送者或服务请求者,各自拥有一对公钥私钥(pk_i,sk_i).“多对一”模式同态加密方案除了要满足典型公钥加密系统的特性外,对于明文空间 M 内任意 $m\in M$,m_1,$m_2\in M$ 应满足以下特性:

$$D_{sk}(E_{pk}(m))=m \tag{21}$$

$$D_{sk_i}(E_{pk_i}(m))=m \tag{22}$$

$$D_{sk_i}(E_{pk_j}(m))\neq m \tag{23}$$

$$D_{sk}(E_{pk_i}(m))=m \tag{24}$$

$$D_{sk}(E_{pk}(m_1\circ m_2))=D_{sk}(E_{pk}(m_1)\circ E_{pk}(m_2)) \tag{25}$$

$$D_{sk_i}(E_{pk_i}(m_1\circ m_2))=D_{sk_i}(E_{pk_i}(m_1)\circ E_{pk_i}(m_2)) \tag{26}$$

$$D_{sk}(E_{pk_i}(m_1 \circ m_2)) = D_{sk}(E_{pk_i}(m_1) \circ E_{pk_i}(m_2)) \quad (27)$$

$$D_{sk}(E_{pk}(m_1 \circ m_2)) = D_{sk}(E_{pk_i}(m_1) \circ E_{pk_j}(m_2)) \quad (28)$$

∘为密文运算符号,式(21)~式(23)表示不同用户仅能够使用各自的一对公钥私钥对进行加解密,式(24)体现了“多对一”加密方式的特性,不同的用户用各自私钥加密数据发送给同一数据接收者 S 后,S 能够使用自有私钥 sk 进行解密,式(25)、式(26)表示 $P_i(i=1,\ldots,n)$、S 在密钥对(pk_i,sk_i),(pk,sk)下各自支持关于∘的同态运算,式(27)表示 P_i 与 S 在密钥对(pk_i,sk)下支持关于∘的同态运算,式(28)表示 P_i、P_j、S 在$(PK(pk_i,pk_j),sk)$下支持关于∘的同态运算.

References:

[1] Goldreich O, Kushilevitz E, Sudan M. Private information retrieval. Journal of the ACM, 1998,45(6):965–981.

[2] Dan B, Kushilevitz E, Ostrovsky R, *et al*. Public key encryption that allows PIR queries. In: Advances in Cryptology CRYPTO 2007. 2007. 50–67.

[3] Avni H, Dolev S, Gilboa N, *et al*. SSSDB: Database with private information search. In: Algorithmic Aspects of Cloud Computing. Springer Int’l Publishing, 2016.

[4] Song DX, Wagner D, Perrig A. Practical techniques for searches on encrypted data. In: Proc. of the IEEE Symp. on Security and Privacy. 2000. 44–55.

[5] Benaloh J, Chase M, Horvitz E, *et al*. Patient controlled encryption: Ensuring privacy of electronic medical records. In: Proc. of the ACM Cloud Computing Security Workshop, CCSW 2009. Chicago, 2009. 103–114.

[6] Liu Q, Wang G, Wu J. Secure and privacy preserving keyword searching for cloud storage services. Journal of Network & Computer Applications, 2012,35(3):927–933.

[7] Pasupuleti SK, Ramalingam S, Buyya R. An efficient and secure privacy-preserving approach for outsourced data of resource constrained mobile devices in cloud computing. Journal of Network & Computer Applications, 2016,64(C):12–22.

[8] Gajek S. Dynamic symmetric searchable encryption from constrained functional encryption. In: Proc. of the Cryptographers’ Track at the RSA Conf. Cham: Springer-Verlag, 2016. 75–89.

[9] Lindell Y, Pinkas B. Secure multiparty computation for privacy-preserving data mining. Journal of Privacy & Confidentiality, 2012,25(2):761–766.

[10] Damgard I, Polychroniadou A, Rao V. Adaptively secure multi-party computation from LWE (via equivocal FHE). In: Proc. of the Public-Key Cryptography—PKC 2016. Berlin, Heidelberg: Springer-Verlag, 2016.

[11] Huang WR, Gui XL, Yu S, Zhuang W. Privacy-Preserving computable encryption scheme of cloud computing. Chinese Journal of Computers, 2011,(12):2391–2402 (in Chinese with English abstract).

[12] Gentry C. A fully homomorphic encryption scheme [Ph.D. Thesis]. Stanford University, 2009.

[13] Regev O. On lattices, learning with errors, random linear codes, and cryptography. Journal of the ACM, 2009,56(6):1–40.

[14] Stehlé D, Steinfeld R. Making NTRU as secure as worst-case problems over ideal lattices. In: Proc. of the Int’l Conf. on Theory and Applications of Cryptographic Techniques: Advances in Cryptology. Springer-Verlag, 2011. 27–47.

[15] Brakerski Z, Gentry C, Vaikuntanathan V. (Leveled) Fully homomorphic encryption without bootstrapping. In: Proc. of the Innovations in Theoretical Computer Science Conf. ACM, 2012. 309–325.

[16] Gentry C, Halevi S. Fully homomorphic encryption without squashing using depth-3 arithmetic circuits. In: Proc. of the 52nd IEEE Annual Symp. on Foundations of Computer Science, FOCS 2011. Palm Springs: IEEE, 2011. 107–116.

[17] Rivest RL, Shamir A, Adleman L. A method for obtaining digital signatures and public-key cryptosystems. Communications of the ACM, 1978,26(2):96–99.

[18] Rivest RL, Adleman L, Dertouzos ML. On data banks and privacy homomorphisms. In: Foundations of Secure Computation. 1978. 169–179.

[19] Elgamal T. A public key cryptosystem and a signature scheme based on discrete logarithms. In: Advances in Cryptology. Berlin, Heidelberg: Springer-Verlag, 1984. 469–472.

[20] Chen L, Xu Y, Fang W, *et al*. A new ElGamal-based algebraic homomorphism and its applications. In: Proc. of the ISECS Int'l Colloquium on Computing, Communication, Control, and Management, CCCM 2008. Guangzhou: IEEE, 2008. 643–648.

[21] Goldwasser S, Micali S. Probabilistic encryption. Journal of Computer Security, 1984,28(2):270–299.

[22] Paillier P. Public-Key cryptosystems based on composite degree residuosity classes. In: Proc. of the Int'l Conf. on Theory and Application of Cryptographic Techniques. Springer-Verlag, 1999. 223–238.

[23] Benaloh J. Verifiable secret-ballot elections [Ph.D. Thesis]. Yale University, 1987.

[24] Okamoto T, Uchiyama S. A new public-key cryptosystem as secure as factoring. In: Proc. of the Int'l Conf. on the Theory and Applications of Cryptographic Techniques. Berlin, Heidelberg: Springer-Verlag, 1998. 308–318.

[25] Boneh D, Goh EJ, Nissim K. Evaluating 2-DNF formulas on ciphertexts. In: Theory of Cryptography. Berlin: Springer-Verlag, 2005. 325–341.

[26] Dhakar RS, Gupta AK, Sharma P. ModifiedRSA encryption algorithm (MREA). In: Proc. of the 2nd Int'l Conf. on Advanced Computing & Communication Technologies. IEEE, 2012. 426–429.

[27] Stehlé D, Steinfeld R. Faster fully homomorphic encryption. In: Advances in Cryptology-ASIACRYPT 2010, Proc. of the Int'l Conf. on the Theory and Application of Cryptology and Information Security. Singapore, 2010. 377–394.

[28] Bos JW, Lauter K, Naehrig M. Private predictive analysis on encrypted medical data. Journal of Biomedical Informatics, 2014, 50(8):234–243.

[29] Lauter K, López-Alt A, Naehrig M. Private computation on encrypted genomic data. In: Progress in Cryptology-LATINCRYPT 2014. Springer Int'l Publishing, 2014. 3–27.

[30] Dowlin N, Ran GB, Laine K, *et al*. Manual for using homomorphic encryption for bioinformatics. Proc. of the IEEE, 2017,105(3): 552–567.

[31] Miran K, Kristin L. Private genome analysis through homomorphic encryption. BMC Medical Informatics & Decision Making, 2015,15(S5):1–12.

[32] Castelluccia C, Mykletun E, Mykletun E, *et al*. Efficient and provably secure aggregation of encrypted data in wireless sensor networks. ACM Trans. on Sensor Networks, 2009,5(3):20.

[33] Boneh D, Gentry C, Halevi S, Wang F, Wu DJ. Private database queries using somewhat homomorphic encryption. In: Proc. of the ACNS 2013: Applied Cryptography and Network Security. 2013. 102–118.

[34] Hall R, Fienberg S, Nardi Y. Secure multiple linear regression based on homomorphic encryption. Official Statistics, 2011,27(4): 669–691.

[35] Yasuda M, Shimoyama T, Kogure J, *et al*. Secure statistical analysis using RLWE-based homomorphic encryption. Lecture Notes in Computer Science, 2015,9144:471–487.

[36] Gentry C, Halevi S, Vaikuntanathan V. A simple BGN-type cryptosystem from LWE. In: Proc. of the Int'l Conf. on the Theory and Applications of Cryptographic Techniques. Berlin, Heidelberg: Springer-Verlag, 2010. 506–522.

[37] Chan CF. Symmetric-Key homomorphic encryption for encrypted data processing. In: Proc. of the IEEE Int'l Conf. on Communications. IEEE, 2009. 1–5.

[38] Hojsík M, Plapanova V. A fully homomorphic cryptosystem with approximate perfect secrecy. In: Dawson E, ed. Topics in Cryptology—CT-RSA 2013. Berlin, Heidelberg: Springer-Verlag, 2013. 375–388.

[39] Yang P, Gui XL, Yu J, Lin JC, Tian F, Zhang XJ. Research on algorithms of data encryption scheme that supports homomorphic arithmetical operations. Journal on Communications, 2015,36(1):171–182 (in Chinese with English abstract).

[40] Smart NP, Vercauteren F. Fully homomorphic encryption with relatively small key and ciphertext sizes. In: Proc. of the Int'l Conf. on Practice and Theory in Public Key Cryptography. Springer-Verlag, 2010. 420–443.

[41] Chen, ZG, Wang J, Zhang ZN, *et al*. A fully homomorphic encryption scheme with better key size. China Communications, 2014,11(9):82–92.

[42] Gentry C, Halevi S, Smart N. Better bootstrapping in fully homomorphic encryption. In: Fischlin M, Buchmann J, Manulis M, eds. Public Key Cryptography–PKC 2012. Berlin, Heidelberg: Springer-Verlag, 2012. 1–16.

[43] Gentry C, Halev Si. Implementing Gentry's fully-homomorphic encryption scheme. In: Proc. of the Int'l Conf. on Theory and Applications of Cryptographic Techniques: Advances in Cryptology. Springer-Verlag, 2014. 129–148.

[44] Dijk MV, Gentry C, Halevi S, *et al*. Fully homomorphic encryption over the integers. In: Proc. of the Int'l Conf. on Theory and Applications of Cryptographic Techniques. Springer-Verlag, 2010. 24–43.

[45] Bogdanov A, Lee CH. Homomorphic encryption from codes. Eprint Arxiv, 2011.

[46] Chillotti I, Gama N, Georgieva M, *et al*. Faster fully homomorphic encryption: Bootstrapping in less than 0.1 seconds. In: Advances in Cryptology—ASIACRYPT 2016. Berlin, Heidelberg: Springer-Verlag, 2016.

[47] Yagisawa M. Fully homomorphic encryption without bootstrapping. ACM Trans. on Computation Theory, 2015,6(3):1–36.

[48] Chan CF. Symmetric-Key homomorphic encryption for encrypted data processing. In: Proc. of the IEEE Int'l Conf. on Communications. IEEE, 2009. 1–5.

[49] Brakerski Z, Gentry C, Vaikuntanathan V. (Leveled) fully homomorphic encryption without bootstrapping. In: Proc. of the 3rd Innovations in Theoretical Computer Science Conf., ITCS 2012. Cambridge: ACM, 2012. 309–325.

[50] Brakerski Z, Vaikuntanathan V. Fully homomorphic encryption from ring-LWE and security for key dependent messages. In: Proc. of the Cryptology Conf. Berlin, Heidelberg: Springer-Verlag, 2011. 505–524.

[51] Gu C. More practical fully homomorphic encryption. Int'l Journal of Cloud Computing and Services Science, 2012, 1–17.

[52] Kipnis A, Hibshoosh E. Efficient methods for practical fully homomorphic symmetric-key encrypton, randomization and verification. Uiban Research & Practice, 2012,7(3):255–257.

[53] Gentry C, Halevi S, Smart NP. Homomorphic evaluation of the AES circuit. In: Advances in Cryptology–CRYPTO 2012. Berlin, Heidelberg: Springer-Verlag, 2012. 850–867.

[54] Gentry C, Halevi S, Smart N. Fully homomorphic encryption with polylog overhead. In: Advanced in Cryptology–EUROCRYPT. LNCS 7237, 2012. 465–482.

[55] Tromer E, Vaikuntanathan V. On-the-Fly multiparty computation on the cloud via multikey fully homomorphic encryption. In: Proc. of the 44th ACM Symp. on Theory of Computing. ACM, 2012. 1219–1234.

[56] Brakerski Z. Fully homomorphic encryption without modulus switching from classical GapSVP. In: Advances in Cryptology –CRYPTO 2012. Berlin, Heidelberg: Springer-Verlag, 2012. 868–886.

[57] Naccache D, Tibouchi M. Public key compression and modulus switching for fully homomorphic encryption over the integers. In: Proc. of the Int'l Conf. on Theory and Applications of Cryptographic Techniques. Springer-Verlag, 2012. 446–464.

[58] Zhang W, Liu S, Yang X. RLWE-Based homomorphic encryption and private information retrieval. In: Proc. of the Int'l Conf. on Intelligent NETWORKING and Collaborative Systems. IEEE, 2013. 535–540.

[59] Bos JW, Lauter K, Loftus J, *et al*. Improved security for a ring-based fully homomorphic encryption scheme. In: Cryptography and Coding. Berlin, Heidelberg: Springer-Verlag, 2013. 45–64.

[60] Cheon JH, Kim J, Lee MS, *et al*. CRT-Based fully homomorphic encryption over the integers. Information Sciences, 2015, 310(C):149–162.

[61] Zhang L, Yue Q. A fast integer-based batch full-homomorphic encryption scheme over finite field. IACR Cryptology ePrint Archive, 2013.

[62] Cheon JH, Coron JS, Kim J, *et al*. Batch fully homomorphic encryption over the integers. In: Proc. of the Int'l Conf. on the Theory and Applications of Cryptographic Techniques. Berlin, Heidelberg: Springer-Verlag, 2013. 315–335.

[63] Pisa PS, Abdalla M, Duarte OCMB. Somewhat homomorphic encryption scheme for arithmetic operations on large integers. In: Proc. of the Global Information Infrastructure & Networking Symp. IEEE, 2013. 1–8.

[64] Doroz Y, Hu Y, Sunar B. Homomorphic AES evaluation using NTRU. IACR Cryptology ePrint Archive, 2014. 1–16.

[65] Doröz Y, Shahverdi A, Eisenbarth T, *et al*. Toward practical homomorphic evaluation of block ciphers using prince. In: Proc. of the Int'l Conf. on Financial Cryptography and Data Security. Berlin, Heidelberg: Springer-Verlag, 2014. 208–220.

[66] Chen Z, Wang J, Song X. A regev-type fully homomorphic encryption scheme using modulus switching. The Scientific World Journal, 2014,17(21):331–342.

[67] Coron J, Lepoint T, Tibouchi M. Scale-Invariant fully homomorphic encryption over the integers. LLAR Journal, 2014,50(4): 361–372.

[68] Zhou H, Wornell G. Efficient homomorphic encryption on integer vectors and its applications. In: Proc. of the Information Theory and Applications Workshop. 2014. 1–9.

[69] Rohloff K, Cousins DB. A scalable implementation of fully homomorphic encryption built on NTRU. In: Proc. of the WAHC 2014 Workshop on Applied Homomorphic Cryptography and Encrypted Computing. 2014. 221–234.

[70] Wang C, Ren K, Wang J. Secure optimization computation outsourcing in cloud computing: A case study of linear programming. IEEE Trans. on Computers, 2016,65(1):216–229.

[71] Chen X, Huang X, Li J, *et al*. New algorithms for secure outsourcing of large-scale systems of linear equations. IEEE Trans. on Information Forensics and Security, 2015,10(1):69–78.

[72] Alderman J, Janson C, Cid C, *et al*. Hybrid publicly verifiable computation. In: Topics in Cryptology-CT-RSA 2016. Springer Int'l Publishing, 2016.

[73] Hu Y. Improving the efficiency of homomorphic encryption schemes [Ph.D. Thesis]. Worcester: Department of Electrical and Computer Engineering, Worcester Polytechnic Institute, 2013.

[74] Clear M, Mcgoldrick C. Bootstrappable identity-based fully homomorphic encryption. In: Proc. of the Cryptology and Network Security. Springer Int'l Publishing, 2014. 1–19.

[75] Coron JS, Mandal A, Naccache D, *et al*. Fully homomorphic encryption over the integers with shorter public keys. In: Rogaway P, ed. Advances in Cryptology–CRYPTO 2011. Berlin, Heidelberg: Springer-Verlag, 2011. 487–504.

[76] Lepoint T, Naehrig M. A comparison of the homomorphic encryption schemes FV and YASHE. In: Proc. of the Int'l Conf. on Cryptology in Africa. Springer Int'l Publishing, 2014. 318–335.

[77] Smart NP, Vercauteren F. Fully homomorphic SIMD operations. Designs Codes & Cryptography, 2014,71(1):57–81.

[78] Gopal GN, Singh MP. Secure similarity based document retrieval system incloud. In: Proc. of the 2012 Int'l Conf. on Data Science Engineering (ICDSE). 2012. 154–159.

[79] Wang CN, Li C, Ren M, Lou WK. Privacy-Preserving multi-keyword ranked search over encrypted cloud data. IEEE Trans. on Parallel and Distributed Systems, 2014,25(1):222–233.

[80] Li J, Wang Q, Wang C, *et al*. Fuzzy keyword search over encrypted data in cloud computing. In: Proc. of the Conf. on Information Communications. IEEE Press, 2010. 441–445.

[81] Bendlin R, Damgard I, Orlandi C, *et al*. Semi-Homomorphic encryption and multiparty computation. Lecture Notes in Computer Science, 2011,6632(2010):169–188.

[82] Lin HY, Tzeng WG. An efficient solution to the millionaires' problem based on homomorphic encryption. In: Proc. of the Int'l Conf. on Applied Cryptography and Network Security. Springer-Verlag, 2005. 456–466.

[83] Goethals B, Laur S, Lipmaa H, *et al*. On private scalar product computation for privacy-preserving data mining. In: Proc. of the Int'l Conf. on Information Security and Cryptology. Springer-Verlag, 2004. 104–120.

[84] Tu S, Kaashoek M, Madden S, Zeldovich N. Processing analytical queries over encrypted data. Int'l Conf. on Very Large Data Bases, 2013,6(5):289–300.

[85] Tetali SD, Lesani M, Majumdar R, *et al*. MrCrypt: Static analysis for secure cloud computations. In: Proc. of the ACM Sigplan Int'l Conf. on Object Oriented Programming Systems Languages & Applications. ACM, 2013. 271–286.

[86] Stephen JJ, Savvides S, Seidel R, *et al*. Practical confidentiality preserving big data analysis. In: Proc. of the Usenix Conf. on Hot Topics in Cloud Computing. USENIX Association, 2014. 10.

[87] Brenner M, Wiebelitz J, Voigt GV, *et al*. Secret program execution in the cloud applying homomorphic encryption. In: Proc. of the IEEE Int'l Conf. on Digital Ecosystems and Technologies. IEEE, 2011. 114–119.

[88] Lu CS. Homomorphic encryption-based secure SIFT for privacy-preserving feature extraction. In: Proc. of the SPIE-The Int'l Society for Optical Engineering, 2011,7880(2):788005-788005-17.

[89] Ren W, Ren Y, Zhang H. H2S: A secure and efficient data aggregative retrieval scheme in unattended wireless sensor networks. In: Proc. of the 5th Int'l Conf. on Information Assurance and Security. IEEE Computer Society, 2009. 450–453.

[90] Zhu H, Bao F. Private searching on MapReduce. In: Proc. of the Int'l Conf. on Trust, Privacy and Security in Digital Business, Trustbus 2010. Bilbao, 2010. 93–101.

[91] Zhu HH, He QH, Zhu HH, *et al*. Voiceprint-Biometric template design and authentication based on cloud computing security. In: Proc. of the Int'l Conf. on Cloud and Service Computing. IEEE Computer Society, 2011. 302–308.

[92] Bilogrevic I, Jadliwala M, Kumar P, *et al*. Meetings through the cloud: Privacy-Preserving scheduling on mobile devices. Journal of Systems & Software, 2011,84(11):1910–1927.

[93] Liu Y, Ren W. Robust and secure yet simple data collection in WSNs applying to marine gas turbine. In: Proc. of the Int'l Conf. on Multimedia Information NETWORKING and Security. IEEE Computer Society, 2009. 360–364.

[94] Upmanyu M, Namboodiri AM, Srinathan K, *et al*. Efficient privacy preserving *K*-means clustering. In: Intelligence and Security Informatics. Berlin, Heidelberg: Springer-Verlag, 2010. 154–166.

[95] Ren Y, Oleshchuk V, Li FY. Secure and efficient data storage in unattended wireless sensor networks. In: Proc. of the Int'l Conf. on New Technologies, Mobility and Security. IEEE Press, 2009. 244–248.

[96] Lipmaa H, Zhang B. Two new efficient PIR-writing protocols. Lecture Notes in Computer Science, 2010,6123:438–455.

[97] Ma J, Li F, Li JH. Perturbation method for distributed privacy-preserving data mining. Journal of Zhejiang University, 2010, 44(2):276–282 (in Chinese with English abstract).

[98] Fang WW, Hu J, Yang BR, Zhou CS. Research of privacy-preserving in distributed decision-tree mining. Coputer Science, 2009,36(4):239–242 (in Chinese with English abstract).

[99] Jaideep V, Murat K, Chris C. Privacy-Preserving Naïve Bayes classification. The VLDB Journal, 2008,17:879–898.

[100] Vaidya J, Yu H, Jiang X. Privacy-Preserving SVM classification. Knowledge & Information Systems, 2008,14(2):161–178.

[101] Nuida K. Candidate constructions of fully homomorphic encryption on finite simple groups without ciphertext noise. Technical Report, 2014/97, 2015.

[102] Yagisawa M. Fully homomorphic public-key encryption based on discrete logarithm problem. Technical Report, 2016/054, 2016.

[103] Downlin N, Bachrach RG, Laine K, Lauter K, Naehrig M, Wernsing J. CryptoNets: Applying neural networks to encrypted data with high throughput and accuracy. Microsoft Research Technical Report, MSR-TR-2016-3, 2016.

附中文参考文献:

[11] 黄汝维,桂小林,余思,庄威.云环境中支持隐私保护的可计算加密方法.计算机学报,2011,(12):2391–2402.

[39] 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法算法研究.通信学报,2015,36(1):171–182.

[97] 马进,李锋,李建华.分布式数据挖掘中基于扰乱的隐私保护方法.浙江大学学报,2010,44(2):276–282.

[98] 方炜炜,胡健,杨炳儒,周长胜.分布式决策树挖掘的隐私保护研究.计算机科学,2009,36(4):239–242.

李宗育(1985－),男,江西上饶人,博士生,CCF 学生会员,主要研究领域为云计算隐私保护,密码学.

李雪松(1992－),男,硕士,CCF 学生会员,主要研究领域为密码学,区块链.

桂小林(1966－),男,博士,教授,博士生导师,CCF 高级会员,主要研究领域为云计算隐私保护,网络安全,可信计算.

戴慧珺(1979－),女,博士,工程师,CCF 专业会员,主要研究领域为隐私保护,加密计算.

顾迎捷(1992－),男,博士生,主要研究领域为信息安全,区块链技术.

张学军(1977－),男,博士,副教授,CCF 专业会员,主要研究领域为位置隐私保护与度量,云安全.