同态密码理论与应用进展

杨亚涛*①③ 赵 阳① 张卷美② 黄洁润① 高 原①

①(北京电子科技学院电子与通信工程系 北京 100070)

②(北京电子科技学院密码科学与技术系 北京 100070)

③(西安电子科技大学通信工程学院 西安 710071)

摘 要：随着云计算、云存储等各类云服务的普及应用，云环境下的隐私保护问题逐渐成为业界关注的焦点，同态密码成为解决该问题的关键手段，其中，如何构造高效的全同态加密方案是近年来同态加密研究的热点之一。首先，该文介绍了同态密码的发展情况，从不同角度对同态加密方案进行了分类分析，着重描述了可验证全同态加密方案的研究进展。通过分析近年来公开的同态加密领域知识产权文献，对同态加密在理论研究和实际应用中所取得的进展进行了归纳总结。其次，对比分析了目前主流全同态加密库Helib, SEAL以及TFHE的性能。最后，梳理了同态加密技术的典型应用场景，指出了未来可能的研究与发展方向。

关键词：同态加密；隐私保护；可验证同态加密；全同态加密；密码应用

中图分类号：TN918; TP309.7 **文献标识码**：A **文章编号**：1009-5896(2021)02-0475-13

DOI: 10.11999/JEIT191019

Recent Development of Theory and Application on Homomorphic Encryption

YANG Yatao①③ ZHAO Yang① ZHANG Juanmei②

HUANG Jierun① GAO Yuan①

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

②(*Department of Cryptography Science and Technology, Beijing Electronic Science and Technology Institute, Beijing* 100070, *China*)

③(*School of Telecommunication Engineering, Xidian University, Xi'an* 710071, *China*)

Abstract: With the popularization of various cloud services such as cloud computing and cloud storage, privacy preservation issues in the cloud environment have gradually become the focus of industrial applications. Homomorphic encryption has become an important method to solve this issue. Among them, how to construct an efficient fully homomorphic encryption scheme is one of the hotspots at present. Firstly, the development of homomorphic encryption is introduced. The homomorphic encryption schemes are analyzed and classified from different perspectives. The research progress of verifiable fully homomorphic encryption schemes is discussed in detail. By analyzing the property rights literature on homomorphic encryption that has been published in recent years, the progress in the theoretical research and application about homomorphic encryption are summarized. Secondly, the working performances of three typical homomorphic encryption libraries, Helib, SEAL and TFHE, are compared and analyzed. Finally, various application scenarios of homomorphic encryption technology are sorted out, and possible research and development directions in the future are proposed.

Key words: Homomorphic Encryption(HE); Privacy preservation; Verifiable homomorphic encryption; Fully Homomorphic Encryption(FHE); Cryptographic application

收稿日期：2019-12-23；改回日期：2020-06-09；网络出版：2020-07-17

*通信作者： 杨亚涛 yy2008@163.com

基金项目：“十三五”国家密码发展基金(MMJJ20170110)

Foundation Item: The State Cryptography Development Fund of Thirteen Five-year(MMJJ20170110)

1 前言

近年来云计算技术以及由云计算技术延伸和扩展而来的云存储技术始终热度不减，各类提供云服务的云平台也如雨后春笋般涌现。通过云计算和云存储技术，可以将海量数据的存储和复杂运算等工作外包给提供云服务的各大运营商，这实现了资源共享，减少了运算开支。然而，提供云服务的第三方无法保障用户数据的隐私安全，网络环境下的各种不可控因素对云上的用户数据隐私保护提出了挑战。使用传统加密手段可以保障数据外包时的存储安全，却难以保障其计算安全。在此背景下，同态加密(Homomorphic Encryption, HE)技术成为解决云环境下隐私保护问题的重要手段。使用同态加密技术，用户对密文进行运算后再解密得到的结果与直接对明文进行运算得到的结果一致，这一特性允许不可信第三方在没有私钥的情况下直接对密文进行运算，避免了第三方在运算过程中需要解密密文而导致的用户敏感信息泄露。

1978年Rivest等人[1]首次提出了隐私同态的概念，旨在构造一种支持密文检索的加密机制，后来发展为这样一种理念：在不解密的情况下对密文进行任意的函数变换，对变换的输出解密，所得结果与对相应的明文进行同样的函数变换所得结果一样。如何实现全同态加密(Fully Homomorphic Encryption, FHE)由此成为密码学界的开放性问题，终于在2009年Gentry[2]首次利用理想格给出了FHE方案的构造，该方案基于理想格上的有界编码问题与稀疏子集和问题，其思路如下：明文空间为{0, 1}，首先构造一个对“新鲜”密文支持有限次多项式运算的类同态加密(SomeWhat Homomorphic Encryption, SWHE)方案；然后基于稀疏子集和问题困难性假设变换私钥的形式，压缩解密电路，将其表示成关于私钥的次数足够低的多项式；最后在公钥中添加私钥的密文等辅助信息，用于对“新鲜”密文同态运算后生成的密文进行同态解密，降低其中包含的噪声，实现“自举”功能，达到对密文进行任意函数变换的目的，这一技术称为Bootstrapping(自举)技术。Gentry提出的这种构造模式被称为Gentry体制，此后全同态加密技术发展迅速，分为两条研究主线，一种是按照Gentry的思路设计的FHE方案，另一种则为基于错误学习(Learning With Errors, LWE)问题或环上错误学习(Ring-LWE, RLWE)问题实现的FHE方案[3,4]。下面，本文主要分析近年来同态加密技术的一些新进展并提出未来值得关注的几个发展方向。

2 相关概念及理论基础

电路观点是指用电路模型来理解同态加密方案的密文计算(Ciphertext computation)算法，电路模型必须接触到所有的输入数据，不会泄露任何信息，因此可以将一个函数或功能f等效为一个电路模型$C(c_1,c_2,\cdots,c_k)\in C_\lambda$，其中$C_\lambda$为电路集合，$\lambda$为安全系数。电路模型下可以通过门电路数量、乘法电路深度等来衡量算法的计算复杂度。

通常一个公钥加密方案包含3个算法：密钥生成算法(KeyGen)、加密算法(Enc)和解密算法(Dec)。但是在同态加密中，除了上述3个算法之外，还包含第4个算法即密文计算算法(Eval)。密文计算是指在密文域上进行的运算，它通常需要满足正确性以及可验证性。

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

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

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

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

以上4个算法都是概率多项式时间(Probabilistic Polynomial Time, PPT)算法。

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

$$\begin{aligned}&\mathrm{Dec}(\mathrm{sk},\mathrm{Eval}(\mathrm{ek},(c_1,c_2,\cdots,c_k),^\circ))\\&=(m_1,m_2,\cdots,m_k)^\circ\end{aligned}\tag{1}$$

定义2 正确性：对于KeyGen(λ)生成的公私钥对(pk, sk)，电路集合C_λ中的任意电路C，明文域M中的任意明文$m_1,m_2,\cdots,m_k$以及加密得到的密文$(c_1,c_2,\cdots,c_k)$，其中$\mathrm{Enc}(\mathrm{pk},m_i)\to c_i$，如果对输出的$c^*=\mathrm{Eval}(\mathrm{ek},(c_1,c_2,\cdots,c_k),C)$，都有$\mathrm{Dec}(\mathrm{pk},c^*)=C(m_1,m_2,\cdots,m_k)$，则认为同态加密方案$\alpha$关于电路集合$C_\lambda$中的电路是正确的。

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

通俗来讲，满足紧凑性意味着算法的解密电路不依赖于密文或密文运算函数。

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

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

其中，$(\mathrm{pk},\mathrm{sk})\leftarrow \mathrm{KeyGen}(1^{\lambda})$。

3　同态加密类型及研究动态

3.1　同态加密算法的分类

同态加密技术虽然还没有统一的分类标准，但是其发展历史仍是具有阶段性特征的。按照各同态加密方案允许密文计算的种类和次数，可以将其分为3类：部分同态加密(Partial Homomorphic Encryption, PHE)方案、类同态加密方案和全同态加密方案。PHE仅满足加法或乘法的密文同态运算；SWHE可同时满足加法和乘法有限次的密文同态运算；FHE可同时满足加法和乘法无限次的密文同态运算。

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

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

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

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

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

目前很多PHE方案已经取得了比较可观的加解密效率，并且已经被切实应用到了现实生活中(例如Paillier[5]加法同态加密方案被频繁应用在电子投票、医疗计量等场景下，其加解密耗时仅为毫秒级)，但是FHE方案由于管理密文计算中持续增长的噪声需要投入大量的计算资源，效率仍然较低，还不能满足实际应用的需求，此外由于同态性与延展性之间的相互矛盾，全同态加密无法实现IND-CCA2安全。因此，对全同态加密的研究仍然任重道远，且相应的主要聚焦于两个方面：一是提高FHE方案的效率；二是提高FHE方案的安全性。全同态加密近十年来的研究进程可大致划分为3个阶段[6]：第1阶段是以Gentry的突破性工作为基础构造的各类FHE方案，首先构造一个SWHE方案，然后通过Bootstrapping技术控制噪声增长实现全同态；第2阶段是以Brakerski和Vaikuntanathan的工作为基础构造的基于LWE和RLWE的FHE方案，通过密钥交换(key switching)技术来解决维数膨胀的问题，通过模交换(Modulus Switching)技术来控制噪声，一定程度上摆脱了对Bootstrapping技术的依赖；第3阶段是由Gentry等人[7]构造的基于近似特征向量的GSW方案，该方案的同态运算全部为简单的矩阵运算，故不会出现维数膨胀的问题，该方案提供了一种构造FHE方案的新思路，将原先复杂的密文运算过程简化为了较为单纯的代数运算，更加便于理解。宋新霞等人[8]对密文矩阵的本质及构造方法进行了研究，提出抽象解密结构的概念，并以此为基础揭示了密文矩阵FHE与其它FHE之间的包含关系。总而言之，近年来对全同态加密技术的研究进展迅速，但是其实现效率问题仍是亟需解决的主要难题。

除了上述按照发展阶段进行划分以外，FHE还可以依照所基于的困难问题来分类[9]，主要有两种，一种是基于传统数论中的困难问题，如整数上近似最大公约数(Approximate Greatest Common Divisor, AGCD)问题，另一种是基于格密码学中的困难问题，如格上LWE问题和RLWE问题。另外，近年还出现了基于NTRU(Number Theory Research Unit)的FHE方案、基于身份和属性的FHE方案以及无噪声的FHE方案等诸多其他类型的FHE方案，李子臣等人[10]通过格上的高斯抽象算法生成密钥对，然后利用Flattening技术构造了基于NTRU选择明文攻击可证明安全的全同态加密方案。为了解决NTRU在实现过程中的侧信道攻击安全隐患，杨亚涛等人[11]对NTRU算法所有系数执行掩码操作，构造了能够有效防御差分能量攻击及相关能量攻击的NTRU全同态掩码防御方案。可以发现，近十年来建立在格密码学基础之上的FHE方案大量涌现，格密码作为后量子密码中颇具潜力的密码体制，使全同态加密技术在量子计算时代仍具有重要的应用价值。

3.2　全同态加密

全同态加密支持密文域上无限次的加法和乘法

运算。Gentry提出了一种基于理想格的FHE方案，为FHE的研究奠定了基础，在Gentry的方案中Bootstrapping(自举)技术是实现全同态的关键，下面简要介绍Bootstrapping技术的原理。首先在使用Bootstrapping之前，我们已经可以进行有限次的密文同态运算，但是每进行一次同态运算后密文噪声都会相应增加，尤其是在进行同态乘运算时，密文噪声随运算次数呈指数形式增长，因此必须采取措施进行噪声控制。

如图1所示，对密文进行若干次同态运算后得到的密文c对应于明文m，且该密文噪声很大。D_c为解密电路且满足$D_c(\mathrm{sk})=\mathrm{Dec}_{\mathrm{sk}}(c)=m$, $\mathrm{Enc}_{\mathrm{pk}}(\mathrm{sk})$是用公钥直接对私钥进行加密得到的，将$\mathrm{Enc}_{\mathrm{pk}}(\mathrm{sk})$作为解密电路$D_c$的输入，其输出为密文$c^{'}$且$c^{'}$对应的明文仍为$m$。因为$\mathrm{Enc}_{\mathrm{pk}}(\mathrm{sk})$的噪声很小(low noise)，因此$c^{'}$的噪声也很小，从而达到了降噪的目的。

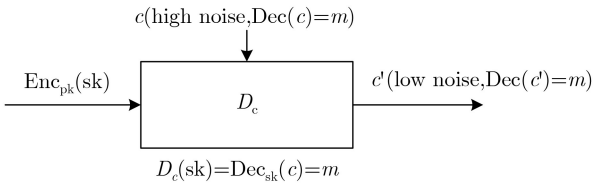

图 1 Bootstrapping原理

由于反复调用解密电路使FHE方案效率过低，因此很多人随后针对Bootstrapping进行了优化，Ducas等人[12]在EUROCRYPT2015上将Helib库中Bootstrapping操作的运行时间从6 min缩短至1 s以内，并相应提出了FHEW方案。Chillotti等人[13]随后在ASIACRYPT2016上对FHEW方案进一步优化，将Bootstrapping的运行时间从1 s以内缩短至0.1 s以内，并将其密钥大小从1 GB减小至24 MB。在EUROCRYPT2018上，Chen等人[14]通过应用“低位删除”多项式优化了开方运算，此举对下文要提到的FV和BGV方案中的Bootstrapping都有重要作用。若令密钥的1-范数为$h=\|s\|_1$，明文模数为$t=p^r$，则优化算法可以将FV方案的自举深度降至$\log_2 h+\log_2(\log_p(ht))$，将BGV方案的自举深度从$\log_2 h+2\log_2 t$降至$\log_2 h+\log_2 t$。除了优化Bootstrapping以外，另一种为全同态“提速”的有效手段是批处理(batch)技术，也可称为封装(Pack)技术，即允许将多个数据值加密为一个密文，并能够同态执行单指令多数据操作(Single Instruction Multiple Data, SIMD)。2014年，Smart等人[15]通过中国剩余定理分解明文空间，构造了支持SIMD操作的FHE方案。在EUROCRYPT2018上，Castryck等人[16]通过引入劳伦多项式编码技术对Smart的方案进行了改进，极大提高了明文封装容量以及在效率或安全性方面优化系统参数的灵活性。虽然通过不断优化Bootstrapping技术和引入Batching技术大幅提高了FHE方案的实现效率，但是离实际应用的要求还有一定距离，因此构造无噪声的FHE方案成为当前全同态加密研究的一个重要思路[17]。噪声的加入是为了保证FHE方案的安全性，但也带来了噪声控制的困扰，虽然无噪声的FHE方案被认为是不安全的，但该结论也并没有被严格证明，因此研究无噪声的FHE方案仍具有现实意义。2012年Kipnis等人[18]分别基于矩阵和多项式构造了无噪声FHE方案。2014年Nuida[19]在IACR Cryptology ePrint上提出了一个构造无噪声FHE方案的框架。同年，Gentry[20]基于完备群概念提出了一个无噪声FHE框架。除上述方案以外，近年来还出现了基于向量空间[21]，基于八元数环[22]，基于非交换环[23]等的无噪声FHE方案。但是目前现有无噪声FHE方案还并不能在可证明安全框架下严格做到安全可行。此外，GPU和FPGA等硬件架构的特点具有大幅度提高同态加密方案效率的潜力，大整数乘法是FHE算法中最为核心的计算环节，施佺等人[24]采用Verilog HDL语言完成了一个16×24 bit有限域FFT算法的FPGA设计，谢星等人[25]提出一种基于Schönhage-Strassen算法的768 kbit大整数乘法器FPGA设计，均较CPU平台的运算效率有大幅提速。表1总结了提高全同态加密效率的各类解决方案。

在Gentry体制之后，基于整数的FHE方案迅速成型。基于整数的FHE方案完全遵循Gentry的设计思路，其安全性基于AGCD困难问题。2010年Smart等人[26]基于整数与多项式设计了FHE方案，缩短了密钥和密文尺寸。同年，Dijk等人[27]提出了基于整数环上的FHE方案DGHV方案，这某种意义上是第1个基于整数的FHE方案，并且提出能够同时加密多个bit位数据的思路，但其缺点是计算过程比较复杂。此后很多人从DGHV方案入手，对整数上的FHE方案进行了优化。在EUROCRYPT 2013上，Cheon等人[28]引入批处理技术，允许并行处理多比特数据(以向量形式存储)，在EUROCRYPT 2015上Nuida等人[29]将方案的明文空间从Z_2扩展至Z_Q，其中Q为任意素数，同时当$Q=2$时，同态乘的算法复杂度从$O(\lambda(\log_2\lambda)^2)$降为$O(\lambda)$，该方案同样可以扩展为批处理FHE方案。目前FHE方案所基于的困难问题主要有两类，分别是Regev提出的RLWE问题和Howgrave-Graham[30]提出的AGCD问题。Cheon等人[31]在EUROCRYPT2015

表 1　提高全同态加密效率的解决方案

方式	解决方案
优化Bootstrapping	Gentry09[2]：首次提出Bootstrapping
	Ducas15[12]：运行时间从6 min缩短至1 s以内
	Chillotti16[13]：运行时间从1 s以内缩短至0.1 s以内，密钥大小从1 GB减小至24 MB
	Chen18[14]：自举深度从$\log_2 h + 2\log_2 t$降至$\log_2 h + \log_2 t$
Batching	Smart14[15]：构造可支持SIMD操作的FHE方案
	Castryck18[16]：提高了明文封装容量和参数优化灵活性
无噪声FHE	Kipnis12[18]：基于矩阵和多项式的无噪声FHE方案MORE和PORE
	Gentry14[20]：基于完备群概念的无噪声FHE框架
FPGA设计	Shi18[24]：16×24 bit有限域FFT算法的FPGA设计
	Xie19[25]：768 kbit大整数乘法器FPGA设计

上将LWE问题归约为AGCD问题的一个变体，并在此基础上提出了一种新的基于AGCD的FHE方案，该方案的安全性不再依赖稀疏子集和的问题假设，且其性能优于此前所有的基于AGCD的FHE方案。现有的基于整数的FHE方案是针对两个参与者“一方加密，一方解密”(一对一)设计的，王彩芬等人[32]提出一种“多方加密，一方解密”(多对一)的FHE方案，与已有方案相比扩展了数据传输量，且提高了效率。除了基于整数的FHE方案以外，大量研究开始关注在实数域上的密文计算，Jaschke等人[33]提出一个有理数通过与2的幂迭代相乘可以近似表示为整数，不过相应也带来了额外的计算负担。另一方面，Dowlin等人[34]提出一种更高效的表示定点小数的方法，即将定点小数编码为整系数多项式，然而要想进行精确的小数运算，明文模需随电路深度的增加呈指数增大。在ASIACRYPT2017上，Cheon等人[35]构造了一种实数域上的FHE方案CKKS方案，可以对浮点数进行近似计算，方案加密时对明文进行舍入，解密时输出满足精度要求的近似值，通过使用Rescaling技术，在保证计算精度的同时将密文模数增长从指数增长变为线性增长，并通过使用批处理技术提高算法的计算效率。方案分别给出了在乘法逆、指数函数、逻辑运算和离散傅里叶变换这4种运算电路下的效率分析，效率都较为可观，但是该方案为层次型同态加密方案，不能通过Bootstrapping转化为全同态加密方案。随后在EUROCRYPT2018上，Cheon等人[36]基于Bootstrapping提出了一种更新低层级密文的新技术，将上述的层次型同态加密方案扩展为了全同态加密方案，该技术使用正弦函数近似代替模数约减操作，每次迭代操作仅包含1次同态乘运算，若对加密后的128个数字(精度为12 bit)进行密文更新，共耗时139.8 s。表2总结了利用全同态加密技术在处理整数和实数域上的研究进展。

基于对称密码体制的FHE算法，近年来多次出现在人们视野中。目前基于对称密码体制的同态加密算法主要有基于序列密码的和基于分组密码的两类，由于在循环迭代过程中噪声会迅速增大，基于分组密码的同态加密方案只能满足微弱的同态性，而基于序列密码的同态加密方案仅在第1次密文计算时满足较强的同态性，在EUROCRYPT2016上，Méaux等人[37]结合了这两类方案的优点，通过在序列密码中加入滤波置换(filter permutator)，使得每轮输出的噪声恒定不变，理论上讲，这种设

表 2　全同态加密在整数域和实数域上的研究进展

类型	解决方案
明文空间为整数的FHE	Gentry10[27]：第1个基于整数的FHE方案DGHV方案
	Cheon13[28]：将批处理技术引入DGHV方案
	Nuida15[29]：将DGHV方案的明文空间从Z_2扩展至Z_Q
	Cheon15[31]：将LWE问题归约为AGCD问题的一个变体
明文空间为实数的FHE	Jaschke16[33]：通过与2的幂迭代相乘近似将有理数表示为整数
	Dowlin17[34]：将定点小数编码为整系数多项式，但明文模随电路深度的增加呈指数增大
	Cheon17[35]：可进行浮点数近似计算的CKKS方案，但仅为层次型FHE方案
	Cheon18[36]：将文献[35]中的层次型同态加密方案扩展为全同态加密方案

计架构也适用于其他的FHE方案。随着量子计算理论的发展，未来必将迎来量子计算机应用的热潮，量子同态加密的概念也被随之提出。在CRYPTO2015中，Broadbent等人[38]正式给出了量子同态加密(Quantum homomorphic encryption)的定义，即实现量子信息的加密以及密文的量子同态运算，此外作者还相应给出了量子信息中IND-CPA的定义。随后在CRYPTO2016中，Dulek等人[39]基于文献[38]中所提出的架构，构造了第1个量子全同态加密(Quantum FHE, QFHE)方案，可以实现任意多项式级量子电路的密文运算。

3.3 可验证同态加密

可验证计算是在分布式计算和云计算环境下，保障数据外包时计算结果可靠性的重要手段[40]，构造可验证的同态加密方案成为保证数据完整性以及计算过程可靠可信的关键。在2002年Johnson等人首次在文献[41]中提出了同态签名(Homomorphic Signature, HS)的概念，此后相继出现了很多支持线性函数计算的同态签名方案。2011年Boneh等人[42]构造了首个能够执行确定阶数的多项式运算的同态签名方案。2013年Gneearo等人[43]形式化定义了同态消息认证(HomMAC)的概念，指出同态MAC可以看作同态签名方案的对称密钥版本。至此，同态签名和同态MAC都可以作为保护外包数据完整性和可靠性的有效手段，简言之，同态签名可实现公开验证(Public verification)，同态MAC可实现私人验证(Private verification)。目前，同态MAC方案的相关研究已取得了很多重要进展，在EUROCRYPT2013上，Catalano等人[44]提出了两个同态MAC的具体实现，均支持低次多项式运算且效率较高，但不能同时满足标签的简洁性(Succinctness)和方案的复合性(Composability)。随后他们在PKC-2014上对先前的工作进行了总结，抽象出了有限延展性编码的思想，允许同态MAC在满足简洁性的前提下，一定程度上同时满足复合性。2018年，白平等人[45]运用有限延展性编码的思想构造了基于默克尔哈希树的同态认证方案，虽然在复合度上有所不足，但可以在不同云服务器之间的数据传输过程中实现数据完整性和删除操作的可验证。

在ASIACRYPT2014上，Catalano等人[46]提出了适用于Paillier加密体制的可验证同态加密方案。Catalano等人针对同态加密方案的可验证问题引入了一个新的密码学原语LAEPuV(Linearly homomorphic Authenticated Encryption with Public Verifiability), 即支持公开验证的线性同态认证加密。线性同态签名是一种特殊的数字签名，它对消息和签名都具有同态性，其概念最早由Boneh等人[47]在2009年提出。LAEPuV方案即为在标准模型下的多项式同态签名方案，它在保护数据隐私安全和计算结果正确性的基础上，支持对计算结果的公开验证，即在仅有密文情况下，验证者依然可以进行验签。Catalano等人给出了LAEPuV在Paillier加密体制中的具体形式，证明了其适用性。在ASIACRYPT 2014上，Joo等人[48]对同态认证加密(Homomorphic Authenticated Encryption, HAE)进行了系统的研究，并首次给出了在HAE中IND-CPA和IND-CCA等安全概念的定义以及UF-CPA和UF-CCA等认证概念的定义。Joo等人指出当前现有的同态签名方案和同态MAC方案还存在很多局限性(比如仅支持次数较低的多项式函数，仅能进行有限次的验证查询[49])，并基于EF-GCD(Error-Free approximate GCD)假设构造了一种HAE方案，虽然该方案是类同态而不是全同态的，但是它同时满足作者所定义的IND-CPA和SUF-CCA安全性。

在上面提到的所有方案中，注意到方案中带标签的程序(Labeled-program)能够计算不同用户在不同时刻认证过的数据，前提条件是这些数据都是用同一个密钥进行认证加密的。Fiore等人[50]在ASIACRYPT2016上定义了多密钥同态签名(Multi-key Homomorphic Signature, M-HS)，适用于需要多方参与的场景，增强了同态签名的实用性，并在此基础上构造了确定阶数多项式深度的同态签名方案。然而现有M-HS方案签名的不可伪造性依赖于假设所有的签名者都是可信的，这一假设在M-HS的实际应用(如可验证多方计算)中并不符合实际，因此Lai等人[51]在ASIACRYPT2018中对存在任意数量不可信签名者的情形进行了研究，基于零知识证明中的ZK-SNARK技术提出了一种M-HS的通用结构，但是并没有分析该结构的认证安全性和实用性。在ASIACRYPT2017中Alagic等人[52]指出量子同态计算也可以通过无交互的方式进行验证，通过在密文计算算法的输出结果中增加密文计算日志可实现其可验证性，由此构造了一个可验证的量子全同态加密方案，并证明了该方案的正确性和安全性。如何能够既保证用户数据的私密性又保证计算结果的正确性，是云环境下执行运算的难题之一。表3总结了可验证同态加密的研究进展。

4 同态密码知识产权分析

随着同态加密技术的深入研究，一些基于同态加密的具体应用已被逐步推广，然而目前还不能满足对云中海量数据进行复杂运算的需求，因此针对

表 3　可验证同态加密研究进展

解决方案	研究进展	存在问题
Johnson02[41]	首次提出同态签名的概念	–
Boneh11[42]	首个可执行确定阶数多项式运算的同态签名方案	–
Gneearo13[43]	形式化定义了同态消息认证的概念	–
Catalano13[44]	支持低次多项式运算的同态MAC方案	不能同时满足简洁性和复合性
Catalano14[46]	引入了一个新的密码学原语LAEPuV	–
Joo14[48]	首次给出在HAE中IND-CPA和IND-CCA的定义	–
Bai18[45]	基于默克尔哈希树的同态认证方案	复合度上有所不足
Fiore16[50]	提出多密钥同态认证(M-HS)方案	可能存在不可信签名者
Lai18[51]	基于零知识证明提出了一种M-HS通用结构	没有分析其认证安全性和实用性
Alagic17[52]	可验证的量子全同态加密方案	–

同态加密算法的改进以及针对其实际应用的探索仍有一段很长的路要走。下面通过分析近几年与同态密码相关的知识产权，透视该技术目前的应用现状。

文献[53]基于CO-ACD(CO-Approximate Common Divisor)问题构造并实现了一个加法部分同态加密方案。文献[54]公开了一种基于同态加密的签名方案，具体可以应用于匿名证书、电子投票和群签名中。文献[55]公开了一种可验证计算正确性的全同态加密方案及其实现。文献[56]公开了一种有效提高同态乘效率全同态密码系统。文献[57]公开了一种支持有理数运算的同态加密方案。文献[58]公开了一个包含密钥交换、模交换和噪声动态管理的同态加密库。文献[59]公开了一种片上系统(System on Chip, SoC)的隐私保护验证方法，在验证时，参与验证的各方可以通过被加密的测试向量来验证IP核，以避免泄露不必要的信息。文献[60]发明了用于读取同态运算指令的计算机可读存储器，实现了两个终端之间的同态加密通信。

文献[61]公开了一种基于同态加密算法的个人图像安全检索方法，在不泄露用户检索信息和数据的前提下，实现图像的安全检索。文献[62]公开了一种云存储中基于同态加密的密文检索方法，保障了数据的隐私安全，同时使用树形结构来存储提高密文检索效率。文献[63,64]分别公开了一种基于同态加密的密文检索技术。文献[65]公开了一种基于同态加密的线性SVM(Support Vector Machine)模型训练算法，得以在云上训练密文SVM模型，从而避免泄露训练数据等隐私信息。文献[66]公开了一种基于全同态加密的生物特征认证技术，允许在密文状态下认证生物特征，从而避免用户信息泄露。当前，同态加密已被应用在机器学习隐私保护领域，较有代表性的是Gilad-bachrach等人[67]基于SEAL库提出的隐私保护神经网络模型Cryptonets，已较好地适用于小型神经网络。

文献[68]公开了一种基于加法同态的隐藏分散贷款额获取贷款总和的方法，这是多方安全计算的一个应用场景。文献[69]公开了一种基于同态加密的多值打包方案。文献[70]公开了一种基于全同态加密的双方不经意传输方案。文献[71]公开了一种使用同态加密技术计算DNA编辑距离的方法，首先将DNA序列编码为字符串，然后在密文域实现两字符串间编辑距离的计算。文献[72]公开了一种基于同态加密的智能电网用户售电方法，使用同态加密技术加密用户的真实购电需求，结合身份认证保护用户的购电信息不被电力公司等获取。文献[73]基于同态加密技术公开了一种用于计算各分布式设备所贡献计算量的方法。文献[74]公开了一种基于同态加密技术生成条形码的技术，可以在密文域中根据从服务器接收到的生成请求来生成对应的标识码。文献[75]公开了一种基于同态加密算法保护程序代码的方案及其实现，以增加程序代码安全性。文献[76]公开了一种基于同态加密的通信技术，保障在通信过程中数据的计算安全和存储安全。表4总结了近年来同态加密相关的知识产权所聚焦的不同领域。

表 4　同态加密相关的知识产权聚焦的不同应用领域

文献	应用领域
文献[59,60]	硬件系统
文献[61–64]	密文检索
文献[65–67]	密文机器学习
文献[68]	安全多方计算
文献[69,70]	安全协议
文献[71–76]	其他应用

5 全同态加密库对比分析

目前已经有一些团队对FHE方案进行了软件实现，例如基于BGV方案的Helib、基于BFV方案的SEAL、基于GSW方案的TFHE等。下面分别分析Helib, SEAL和TFHE全同态加密库的运行效率。

2014年Brakerski等人[77]提出了BGV同态方案，使用模交换技术进行噪声管理，在不使用Bootstrapping的情况下构造出了层次性全同态加密方案；2013年Halevi等人[78]公开了实现BGV方案的函数库Helib，Helib是使用C++编写的同态加密函数库，着重聚焦使用SV密文封装技术和GHS优化算法[79]，2018年3月，IBM发布了新版本Helib同态加密库，通过重线性化，使效率提升了15～75倍。使用i5-1.6 GHz处理器，内存8 GB的Dell笔记本电脑进行效率测试，表5为level=2时Helib的运行效率，m表示模数。

表 5 Test_Timing效率测试结果(μs)

m	密钥生成	加密	解密	同态加	同态乘
4051	317037	6786	4039	97	26701
4369	571082	8041	5173	98	31477
4859	664138	10497	7554	193	41354

Fan等人[80]于2012年提出了BFV同态方案，该方案可视为对Brakerski所提方案[81]的优化，随后微软公开了基于BFV方案的同态加密库SEAL。2016年Bajard等人[82]提出了一个BFV方案的RNS变体(Residue number systems)。2017年微软发布SEAL2.3.0，使其可以支持Bajard等人的方案。2018年微软发布SEAL3.0，使其支持Cheon等人提出的CKKS方案，可以实现实数域上的密文近似计算。2019年发布SEAL3.2，增加了对.NET开发的完整支持，使.NET开发人员编写同态加密应用程序更为便捷。目前SEAL最新的版本为SEAL3.4。使用英特尔i5, 1.6 GHz处理器，8 GB内存的Dell笔记本电脑分别测试SEAL3.4中BFV方案和CKKS方案在默认参数下的运行效率。BFV方案在默认参数下的效率测试结果如表6所示，CKKS方案在默认参数下的效率测试结果如表7所示。其中Poly, Coeff和Plain为方案的3个主要参数，不同参数会影响方案的安全性、效率以及可进行同态运算的次数。

Gentry等人[7]于2013年提出了GSW同态方案，旨在基于LWE问题构造一个便于理解的、同态运算形式更为纯粹的FHE方案。基于GSW方案的同态加密库TFHE在2017年公布。TFHE使用C++语言编写，它可以运算由逻辑门电路组成的任意布尔电路，函数库支持对10种逻辑门电路的同态运算，包括与门、或门、非门、异或门、与非门、或非门和多路选择器等，每个门电路的单核运算时间约为13 ms，每个选择器花费大约26 ms，TFHE库与其他库的区别是其Bootstrapping不受门电路数量和结构的限制，这就意味着即使在运算电路未提前得知的情况下，它也能够实现对任意电路的密文同态运算。在ASIACRYPT2017中，Chillotti等人[83]针对TFHE提出了新的改进思路，通过使用垂直和水平两种密文封装技术大幅提升了其运行效率，并解决了门电路不可复合的问题。

表 6 SEAL中BFV方案效率测试(μs)

Poly	Coeff	Plain	加密	解密	同态加	同态乘	重线性化
4096	109	786433	93464	32306	314	390192	63711
8192	218	786433	267727	112898	1074	1510281	319876
16384	438	786433	884862	439232	4341	6146131	1846517

表 7 SEAL中CKKS方案效率测试(μs)

Poly	Coeff	加密	解密	同态加	同态乘	重线性化
4096	109	87557	3359	309	12476	63459
8192	218	274215	12748	1071	47599	314501
16384	438	964821	51465	4317	200248	1850888

6 结束语

综上可知，全同态加密技术历经十余年的发展，正逐步由理论层面步入应用阶段，阻碍全同态加密投入应用的效率问题也在一定程度上得到解决，电子投票、密文数据库、区块链隐私保护以及机器学习隐私保护等多元化的应用场景被相继开发，同态加密技术在未来仍具有重要的研究和应用价值。

同态加密技术未来的研究方向可以归纳为提高效率、提高安全性和应用研究3个方面。在效率方面，目前的同态加密方案大部分都是基于公钥密码体制而构建的，存在密钥尺寸大、密文尺寸大的问题，不能满足云上对海量数据进行密文操作的要求，要实现云环境中密文的快速稳定存储、计算等应用，一是可以进一步提高非对称FHE方案的效率，二是可以研究对称同态加密算法。相比非对称同态加密方案，对称同态加密方案的计算复杂度要低得多，然而现行对称同态加密方案仍存在实现效率低、密钥管理复杂、在实际应用中部署困难、存在安全漏洞等种种未解决的问题，仍需做进一步的深入研究。在安全性方面，可验证同态加密可以保障使用同态加密技术时的数据完整性和可认证性，

目前实现同态加密可验证的同态签名与同态MAC两种均还处在起步阶段。基于格上困难问题或其他困难问题设计的抗量子计算攻击的、高效的FHE方案目前是研究的主流，现有的大部分方案未考虑侧信道攻击(Side Channel Attacks, SCA)的影响，设计能够有效抵抗SCA的FHE方案是研究的重要方向之一。在应用方面，目前同态加密技术在安全多方计算、电子投票、机器学习和区块链隐私保护等领域都得到了重要应用，同态加密技术可以实现对数值型数据的同态运算，然而对于逻辑运算的处理有些无力，例如比较两个密文的大小，而这类运算在加密机器学习、密文检索等应用中都比较常见，尤其是随着大数据的快速发展，密文检索问题成为一个亟待解决的难题，设计基于同态加密的高效密文检索方案、利用同态加密技术实现加密机器学习都具有重要的现实意义。

参 考 文 献

[1] RIVEST R L, ADLEMAN L, and DERTOUZOS M L. On data banks and privacy homomorphisms[J]. *Foundations of Secure Computation*, 1978, 4(11): 169–180.

[2] GENTRY C. A fully homomorphic encryption scheme[D]. [Ph. D. dissertation]. Stanford University, 2009.

[3] BRAKERSKI Z and VAIKUNTANATHAN V. Fully homomorphic encryption from ring-LWE and security for key dependent messages[C]. The 31st Annual Cryptology Conference, Santa Barbara, USA, 2011: 505–524. doi: 10.1007/978-3-642-22792-9_29.

[4] BRAKERSKI Z and VAIKUNTANATHAN V. Efficient fully homomorphic encryption from (standard) LWE[C]. The 52nd IEEE Annual Symposium on Foundations of Computer Science, Palm Springs, USA, 2011: 97–106. doi: 10.1109/FOCS.2011.12.

[5] PAILLIER P. Public-key cryptosystems based on composite degree residuosity classes[C]. International Conference on the Theory and Application of Cryptographic Techniques, Prague, Czech Republic, 1999: 223–238. doi: 10.1007/3-540-48910-X_16.

[6] 李增鹏, 马春光, 周红生. 全同态加密研究[J]. 密码学报, 2017, 4(6): 561–578. doi: 10.13868/j.cnki.jcr.000208.
LI Zengpeng, MA Chunguang, and ZHOU Hongsheng. Overview on fully homomorphic encryption[J]. *Journal of Cryptologic Research*, 2017, 4(6): 561–578. doi: 10.13868/j.cnki.jcr.000208.

[7] GENTRY C, SAHAI A, and WATERS B. Homomorphic encryption from learning with errors: Conceptually-simpler, asymptotically-faster, attribute-based[C]. The 33rd Annual Cryptology Conference, Santa Barbara, USA, 2013: 75–92. doi: 10.1007/978-3-642-40041-4_5.

[8] 宋新霞, 陈智罡. 基于抽象解密结构的全同态加密构造方法分析[J]. 电子与信息学报, 2018, 40(7): 1669–1675. doi: 10.11999/JEIT170997.
SONG Xinxia and CHEN Zhigang. Analysis of constructing fully homomorphic encryption based on the abstract decryption structure[J]. *Journal of Electronics & Information Technology*, 2018, 40(7): 1669–1675. doi: 10.11999/JEIT170997.

[9] 李宗育, 桂小林, 顾迎捷, 等. 同态加密技术及其在云计算隐私保护中的应用[J]. 软件学报, 2018, 29(7): 1830–1851. doi: 10.13328/j.cnki.jos.005354.
LI Zongyu, GUI Xiaolin, GU Yingjie, *et al*. Survey on homomorphic encryption algorithm and its application in the privacy-preserving for cloud computing[J]. *Journal of Software*, 2018, 29(7): 1830–1851. doi: 10.13328/j.cnki.jos.005354.

[10] 李子臣, 张卷美, 杨亚涛, 等. 基于NTRU的全同态加密方案[J]. 电子学报, 2018, 46(4): 938–944. doi: 10.3969/j.issn.0372-2112.2018.04.023.
LI Zichen, ZHANG Juanmei, YANG Yatao, *et al*. A fully homomorphic encryption scheme based on NTRU[J]. *Acta Electronica Sinica*, 2018, 46(4): 938–944. doi: 10.3969/j.issn.0372-2112.2018.04.023.

[11] 杨亚涛, 刘博雅, 孙亚飞, 等. NTRU全同态掩码防御方案[J]. 计算机学报, 2019, 42(12): 2742–2753. doi: 10.11897/SP.J.1016.2019.02742.
YANG Yatao, LIU Boya, SUN Yafei, *et al*. Fully homomorphic masking defense scheme based on NTRU[J]. *Chinese Journal of Computers*, 2019, 42(12): 2742–2753. doi: 10.11897/SP.J.1016.2019.02742.

[12] DUCAS L and MICCIANCIO D. FHEW: Bootstrapping homomorphic encryption in less than a second[C]. The 34th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Sofia, Bulgaria, 2015: 617–640. doi: 10.1007/978-3-662-46800-5_24.

[13] CHILLOTTI I, GAMA N, GEORGIEVA M, *et al*. Faster fully homomorphic encryption: Bootstrapping in less than 0.1 seconds[C]. The 22nd International Conference on the Theory and Application of Cryptology and Information Security, Hanoi, Vietnam, 2016: 3–33. doi: 10.1007/978-3-662-53887-6_1.

[14] CHEN Hao and HAN K. Homomorphic lower digits removal and improved FHE bootstrapping[C]. The 37th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Tel Aviv, Israel, 2018: 315–337. doi: 10.1007/978-3-319-78381-9_12.

[15] SMART N P and VERCAUTEREN F. Fully homomorphic SIMD operations[J]. *Designs, Codes and Cryptography*,

2014, 71(1): 57–81. doi: 10.1007/s10623-012-9720-4.

[16] CASTRYCK W, ILIASHENKO I, and VERCAUTEREN F. Homomorphic SIM^{2}D operations: Single instruction much more data[C]. The 37th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Tel Aviv, Israel, 2018: 338–359. doi: 10.1007/978-3-319-78381-9_13.

[17] 王励成, 李婧. 无噪声全同态加密浅析[J]. 密码学报, 2017, 4(6): 579–595. doi: 10.13868/j.cnki.jcr.000209.
WANG Licheng and LI Jing. Simple analysis on noiseless fully homomorphic encryptions[J]. *Journal of Cryptologic Research*, 2017, 4(6): 579–595. doi: 10.13868/j.cnki.jcr.000209.

[18] KIPNIS A and HIBSHOOSH E. Efficient methods for practical fully-homomorphic symmetric-key encryption, randomization, and verification[J]. *Urban Research & Practice*, 2012, 7(3): 255–257.

[19] NUIDA K. A simple framework for noise-free construction of fully homomorphic encryption from a special class of non-commutative groups[J]. *IACR Cryptology ePrint Archive*, 2014, 2017: 97.

[20] GENTRY C. Computing on the edge of chaos: Structure and randomness in encrypted computation[J]. *Electronic Colloquium on Computational Complexity*, 2014, 21: 106.

[21] LIU Dongxi. Practical fully homomorphic encryption without noise reduction[J]. *IACR Cryptology ePrint Archive*, 2015, 2015: 468.

[22] YAGISAWA M. Improved fully homomorphic encryption without bootstrapping[J]. *IACR Cryptology ePrint Archive*, 2017, 2017: 763.

[23] LI Jing and WANG Licheng. Noise-free symmetric fully homomorphic encryption based on noncommutative rings[J]. *IACR Cryptology ePrint Archive*, 2015, 2015: 641.

[24] 施佺, 韩赛飞, 黄新明, 等. 面向全同态加密的有限域FFT算法FPGA设计[J]. 电子与信息学报, 2018, 40(1): 57–62. doi: 10.11999/JEIT170312.
SHI Quan, HAN Saifei, HUANG Xinming, *et al*. Design of finite field FFT for fully homomorphic encryption based on FPGA[J]. *Journal of Electronics & Information Technology*, 2018, 40(1): 57–62. doi: 10.11999/JEIT170312.

[25] 谢星, 黄新明, 孙玲, 等. 大整数乘法器的FPGA设计与实现[J]. 电子与信息学报, 2019, 41(8): 1855–1860. doi: 10.11999/JEIT180836.
XIE Xing, HUANG Xinming, SUN Ling, *et al*. FPGA design and implementation of large integer multiplier[J]. *Journal of Electronics & Information Technology*, 2019, 41(8): 1855–1860. doi: 10.11999/JEIT180836.

[26] SMART P N and VERCAUTEREN F. Fully homomorphic encryption with relatively small key and ciphertext sizes[C]. The 13th International Conference on Practice and Theory in Public Key Cryptography, Paris, France, 2010: 420–443. doi: 10.1007/978-3-642-13013-7_25.

[27] VAN DIJK M, GENTRY C, HALEVI S, *et al*. Fully homomorphic encryption over the integers[C]. The 29th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Riviera, France, 2010: 24–43. doi: 10.1007/978-3-642-13190-5_2.

[28] CHEON J H, CORON J, KIM J, *et al*. Batch fully homomorphic encryption over the integers[C]. The 32nd Annual International Conference on the Theory and Applications of Cryptographic Techniques, Athens, Greece, 2013: 315–335. doi: 10.1007/978-3-642-38348-9_20.

[29] NUIDA K and KUROSAWA K. (Batch) Fully homomorphic encryption over integers for non-binary message spaces[C]. The 34th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Sofia, Bulgaria, 2015: 537–555. doi: 10.1007/978-3-662-46800-5_21.

[30] HOWGRAVE-GRAHAM N. Approximate integer common divisors[C]. International Cryptography and Lattices Conference, Providence, USA, 2001: 51–56. doi: 10.1007/3-540-44670-2_6.

[31] CHEON J H and STEHLÉ D. Fully homomophic encryption over the integers revisited[C]. The 34th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Sofia, Bulgaria, 2015: 513–536. doi: 10.1007/978-3-662-46800-5_20.

[32] 王彩芬, 成玉丹, 刘超, 等. 基于整数的多对一全同态加密方案[J]. 电子与信息学报, 2018, 40(9): 2119–2126. doi: 10.11999/JEIT171194.
WANG Caifen, CHENG Yudan, LIU Chao, *et al*. Multiple to one fully homomorphic encryption scheme over the integers[J]. *Journal of Electronics & Information Technology*, 2018, 40(9): 2119–2126. doi: 10.11999/JEIT171194.

[33] JASCHKE A and ARMKNECHT F. Accelerating homomorphic computations on rational numbers[C]. The 14th International Conference on Applied Cryptography and Network Security, Guildford, UK, 2016: 405–423. doi: 10.1007/978-3-319-39555-5_22.

[34] DOWLIN N, GILAD-BACHRACH R, LAINE K, *et al*. Manual for using homomorphic encryption for bioinformatics[J]. *Proceedings of the IEEE*, 2017, 105(3): 552–567. doi: 10.1109/JPROC.2016.2622218.

[35] CHEON J H, KIM A, KIM M, *et al*. Homomorphic encryption for arithmetic of approximate numbers[C]. The 23rd International Conference on the Theory and Applications of Cryptology and Information Security, Hong

Kong, China, 2017: 409–437. doi: 10.1007/978-3-319-70694-8_15.

[36] CHEON J H, HAN K, KIM A, *et al*. Bootstrapping for approximate homomorphic encryption[C]. The 37th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Tel Aviv, Israel, 2018: 360–384. doi: 10.1007/978-3-319-78381-9_14.

[37] MÉAUX P, JOURNAULT A, STANDAERT F X, *et al*. Towards stream ciphers for efficient FHE with low-noise ciphertexts[C]. The 35th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Vienna, Austria, 2016: 311–343. doi: 10.1007/978-3-662-49890-3_13.

[38] BROADBENT A and JEFFERY S. Quantum homomorphic encryption for circuits of low T-gate complexity[C]. The 35th Annual Cryptology Conference, Santa Barbara, USA, 2015: 609–629. doi: 10.1007/978-3-662-48000-7_30.

[39] DULEK Y, SCHAFFNER C, and SPEELMAN F. Quantum homomorphic encryption for polynomial-sized circuits[C]. The 36th Annual International Cryptology Conference, Santa Barbara, USA, 2016: 3–32. doi: 10.1007/978-3-662-53015-3_1.

[40] 薛锐, 吴迎, 刘牧华, 等. 可验证计算研究进展[J]. 中国科学: 信息科学, 2015, 45(11): 1370–1388. doi: 10.1360/N112014-00336.
XUE Rui, WU Ying, LIU Muhua, *et al*. Progress in verifiable computation[J]. *Scientia Sinica Informationis*, 2015, 45(11): 1370–1388. doi: 10.1360/N112014-00336.

[41] JOHNSON R, MOLNAR D, SONG D, *et al*. Homomorphic signature schemes[C]. Cryptographers' Track at the RSA Conference, San Jose, USA, 2002: 244–262. doi: 10.1007/3-540-45760-7_17.

[42] BONEH D and FREEMAN D M. Homomorphic signatures for polynomial functions[C]. The 30th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Tallinn, Estonia, 2011: 149–168. doi: 10.1007/978-3-642-20465-4_10.

[43] GENNARO R and WICHS D. Fully homomorphic message authenticators[C]. The 19th International Conference on the Theory and Application of Cryptology and Information Security, Bengaluru, India, 2013: 301–320. doi: 10.1007/978-3-642-42045-0_16.

[44] CATALANO D and FIORE D. Practical homomorphic MACs for arithmetic circuits[C]. The 32nd Annual International Conference on the Theory and Applications of Cryptographic Techniques, Athens, Greece, 2013: 336–352. doi: 10.1007/978-3-642-38348-9_21.

[45] 白平, 张薇, 李聪. 云环境下运用基于编号Merkle Hash Tree的同态认证方案[J]. 中国科技论文, 2018, 13(2): 181–185. doi: 10.3969/j.issn.2095-2783.2018.02.013.
BAI Ping, ZHANG Wei, and LI Cong. Using rank-based Merkle Hash Tree into homomorphic authentication during cloud[J]. *China Sciencepaper*, 2018, 13(2): 181–185. doi: 10.3969/j.issn.2095-2783.2018.02.013.

[46] CATALANO D, MARCEDONE A, and PUGLISI O. Authenticating computation on groups: New homomorphic primitives and applications[C]. The 20th International Conference on the Theory and Application of Cryptology and Information Security, Kaoshiung, Taipei, China, 2014: 193–212. doi: 10.1007/978-3-662-45608-8_11.

[47] BONEH D, FREEMAN D, KATZ J, *et al*. Signing a linear subspace: Signature schemes for network coding[C]. The 12th International Conference on Practice and Theory in Public Key Cryptography, Irvine, USA, 2009: 68–87. doi: 10.1007/978-3-642-00468-1_5.

[48] JOO C and YUN A. Homomorphic authenticated encryption secure against chosen-ciphertext attack[C]. The 20th International Conference on the Theory and Application of Cryptology and Information Security, Kaoshiung, Taipei, China, 2014: 173–192. doi: 10.1007/978-3-662-45608-8_10.

[49] YANG Yatao, ZHANG Shuang, YANG Junming, *et al*. Targeted fully homomorphic encryption based on a double decryption algorithm for polynomials[J]. Tinghua Science and Technology, 2014, 19(05):478–485. doi: 10.1109/TST.2014.6919824.

[50] FIORE D, MITROKOTSA A, NIZZARDO L, *et al*. Multi-key homomorphic authenticators[C]. The 22nd International Conference on the Theory and Application of Cryptology and Information Security, Hanoi, Vietnam, 2016: 499–530. doi: 10.1007/978-3-662-53890-6_17.

[51] LAI R W F, TAI R K H, WONG H W H, *et al*. Multi-key homomorphic signatures unforgeable under insider corruption[C]. The 24th International Conference on the Theory and Application of Cryptology and Information Security, Brisbane, Australia, 2018: 465–492. doi: 10.1007/978-3-030-03329-3_16.

[52] ALAGIC G, DULEK Y, SCHAFFNER C, *et al*. Quantum fully homomorphic encryption with verification[C]. The 23rd International Conference on the Theory and Applications of Cryptology and Information Security, Hong Kong, China, 2017: 438–467. doi: 10.1007/978-3-319-70694-8_16.

[53] UNIV SEOUL NAT R and DB FOUND. Additive homomorphic encryption and decryption method based on the CO-ACD problem and apparatus using the same[P]. South Korea, KR20160017226A, 2016.

[54] CAMENISCH J L and LEHMANN A. Signature scheme for homomorphic message encoding functions[P]. US,

20180234254, 2018.

[55] CHEN Wenbin, LEI Hao, and YANG Qinqin. Method, apparatus, and system for authenticating fully homomorphic message[P]. US, 20160119346, 2016.

[56] UNIV MOHAMMED V RABAT. Quaternion-based, efficient fully-homomorphic cryptosystem[P]. Morocco, WO2018124869A1, 2018.

[57] LAINE K, PLAYER R L, and CHEN Hao. Rational number arithmetic in homomorphic encryption[P]. US, 20180131506, 2018.

[58] GENTRY C B, HALEVI S, and SMART N P. Homomorphic evaluation including key switching, modulus switching, and dynamic noise management[P]. US, 10057057, 2018.

[59] MANIATAKOS M, KONSTANTINOU C, and KELIRIS A. Systems and methods for privacy-preserving functional IP verification utilizing fully homomorphic encryption[P]. US, 20160254912A1, 2016.

[60] HOFFSTEIN J and SILVERMAN J H. Homomorphic encryption[P]. US, 20180212750, 2018.

[61] 西安电子科技大学. 基于同态加密算法的个人图像安全检索方法[P]. 中国, 108418995A, 2018.
Xidian University. Homomorphic encryption algorithm-based individual image safe retrieving method[P]. China, 108418995A, 2018.

[62] 南京邮电大学, 江苏省新通智能交通科技发展有限公司. 一种云存储中基于同态加密的密文检索方法[P]. 中国, 108011713A, 2018.
Nanjing University of Posts and Telecommunications, Jiangsu Xintong Intelligent Transportation Technology Development Co., Ltd. Ciphertext retrieval method based on homomorphic encryption in cloud storage[P]. China, 108011713A, 2018.

[63] 深圳市全同态科技有限公司, 胡和平. 一种全同态加密的密文查询方法和系统[P]. 中国, 106953722A, 2017.
Shenzhen Quantong Technology Co., Ltd and HU Heping. Fully homomorphic encryption cryptograph query method and system[P]. China, 106953722A, 2017.

[64] HUAWEI TECH CO LTD. System and method for searching over encrypted data using homomorphic encryption[P]. China, EP3264669A1, 2018.

[65] 电子科技大学. 一种基于向量同态加密的隐私保护的线性SVM模型训练算法[P]. 中国, 108521326A, 2018.
University of Electronic Science and Technology of China. Linear SVM model training algorithm for privacy protection based on vector homomorphic encryption[P]. China, 108521326A, 2018.

[66] 陈智罡. 基于全同态加密的认证方法和用户设备以及认证服务器[P]. 中国, 107819587A, 2018.
CHEN Zhigang. Authentication method based on homomorphic encryption, user equipment and authentication server[P]. China, 107819587A, 2018.

[67] GILAD-BACHRACH R, DOWLIN N, LAINE K, *et al*. CryptoNets: Applying neural networks to encrypted data with high throughput and accuracy[C]. The 33rd International Conference on Machine Learning, New York City, USA, 2016: 201–210.

[68] 上海凭安征信服务有限公司. 一种基于加法同态加密的隐藏分散贷款额获取贷款总和的方法[P]. 中国, 107330678A, 2017.
Shanghai Ping An Credit Service Co., Ltd. Method of hiding scattered loan sum and acquiring loan sum based on based on addition homomorphic encryption[P]. China, 107330678A, 2017.

[69] PATEL S and YUNG M M M. Systems and methods for a multiple value packing scheme for homomorphic encryption[P]. US, 20160359617, 2016.

[70] BACON D F, BENT G A, BERGAMASCHI F A, *et al*. Efficient two party oblivious transfer using a leveled fully homomorphic encryption[P]. US, 20170147835, 2017.

[71] UNIV SEOUL NAT R and DB FOUND. Method for calculating edit distance between DNA genomic sequence through homomorphic encryption[P]. South Korea, KR20170096387A, 2017.

[72] 西安邮电大学. 一种基于同态加密的智能电网用户售电方法[P]. 中国, 107172043A, 2017.
Xi'an University of Posts & Telecommunications. Intelligent power grid user power-selling method based on homomorphic encryption[P]. China, 107172043A, 2017.

[73] DOW A, DOW E M, GILCHRIST J P, *et al*. Distributed computing utilizing homomorphic encryption[P]. US, 20160380761A1, 2016.

[74] SAMSUNG SDS CO LTD. Apparatus for generating barcode using homomorphic encryption and method thereof[P]. South Korea, KR20170048767A, 2017.

[75] 北京洋浦伟业科技发展有限公司. 基于同态加密算法保护程序代码安全的方法和装置[P]. 中国, 107124261A, 2017.
Beijing Yangpu Weiye Technology Development Co., Ltd. Method and apparatus for protecting security of program code based on homomorphic encryption algorithm[P]. China, 107124261A, 2017.

[76] 南京汽车集团有限公司. 基于同态加密的信息安全传输装置、传输方法及存储方法[P]. 中国, 107682379A, 2018.
Nanjing Automobile Group. Information safety transmission device and method based on homomorphic encryption and storage method[P]. China, 107682379A, 2018.

[77] BRAKERSKI Z, GENTRY C, and VAIKUNTANATHAN V. (Leveled) fully homomorphic encryption without bootstrapping[J]. *ACM Transactions on Computation*

Theory, 2014, 6(3): 13. doi: 10.1145/2633600.

[78] HALEVI S and SHOUP V. HElib—An implementation of homomorphic encryption[EB/OL]. https://github.com/shaih/HElib/.

[79] GENTRY C, HALEVI S, and SMART N P. Homomorphic evaluation of the AES circuit[C]. The 32nd Annual Cryptology Conference, Santa Barbara, USA, 2012: 850–867. doi: 10.1007/978-3-642-32009-5_49.

[80] FAN J and VERCAUTEREN F. Somewhat practical fully homomorphic encryption[J]. *IACR Cryptology ePrint Archive*, 2012, 2012: 144.

[81] BRAKERSKI Z. Fully homomorphic encryption without modulus switching from classical GapSVP[C]. The 32nd Annual Cryptology Conference, Santa Barbara, USA, 2012: 868–886. doi: 10.1007/978-3-642-32009-5_50.

[82] BAJARD J C, EYNARD J, HASAN M A, *et al*. A full RNS variant of FV like somewhat homomorphic encryption schemes[C]. The 3rd International Conference on Selected Areas in Cryptography, St. John's, Canada, 2016: 423–442. doi: 10.1007/978-3-319-69453-5_23.

[83] CHILLOTTI I, GAMA N, GEORGIEVA M, *et al*. Faster packed homomorphic operations and efficient circuit bootstrapping for TFHE[C]. The 23rd International Conference on the Theory and Applications of Cryptology and Information Security, Hong Kong, China, 2017: 377–408. doi: 10.1007/978-3-319-70694-8_14.

杨亚涛：男，1978年生，副教授，研究方向为信息安全、同态密码系统、密码协议和算法设计.

赵　阳：男，1995年生，硕士生，研究方向为同态加密与信息安全.

张卷美：女，1963年生，副教授，研究方向为密码计算方法、同态密码.

黄洁润：女，1995年生，硕士生，研究方向为格密码与信息安全.

高　原：女，1979年生，讲师，主要研究方向为信息安全与算法.

责任编辑：马秀强