软件学报 ISSN 1000-9825, CODEN RUXUEW
Journal of Software,2016,27(6):1487−1497 [doi: 10.13328/j.cnki.jos.004991]

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

利用特征向量构造基于身份的全同态加密体制*

康元基[1], 顾纯祥[1,2], 郑永辉[1,2], 光 焱[1]

[1](信息工程大学,河南 郑州 450002)

[2](数学工程与先进计算国家重点实验室,江苏 无锡 214125)

通讯作者: 顾纯祥, E-mail: gcxiang5209@aliyun.com

摘 要: 全同态加密可以在不解密的条件下对密文进行有效运算,为云计算的数据隐私保护提供了一种理想的解决方案,但目前已有的全同态加密体制普遍存在公钥尺寸大、计算效率较低等问题.利用构造特征向量的思想,基于任意次数分圆环代数结构,提出全同态加密体制,并提出一种转换方法将该体制转换为基于身份的全同态加密体制.与已有体制相比,使用特征向量思想构造基于身份的体制有效地避免了计算密钥,实现了真正意义上基于身份的体制;相比次数为 2 的方幂特殊分圆环,使用任意次数分圆环最大会使加密体制的计算效率提升一倍,同时还可应用单指令多数据(single instruction multiple data,简称 SIMD)技术进一步提升计算和存储效率.

关键词: 全同态加密;特征向量;基于身份加密;任意分圆环

中图法分类号: TP309

中文引用格式: 康元基,顾纯祥,郑永辉,光焱.利用特征向量构造基于身份的全同态加密体制.软件学报,2016,27(6):1487−1497. http://www.jos.org.cn/1000-9825/4991.htm

英文引用格式: Kang YJ, Gu CX, Zheng YH, Guang Y. Identity-Based fully homomorphic encryption from eigenvector. Ruan Jian Xue Bao/Journal of Software, 2016,27(6):1487−1497 (in Chinese). http://www.jos.org.cn/1000-9825/4991.htm

Identity-Based Fully Homomorphic Encryption from Eigenvector

KANG Yuan-Ji[1], GU Chun-Xiang[1,2], ZHENG Yong-Hui[1,2], GUANG Yan[1]

[1](Information Engineering University, Zhengzhou 450002, China)

[2](State Key Laboratory of Mathematical Engineering and Advanced Computing, Wuxi 214125, China)

Abstract: Fully homomorphic encryption allows valid operation on encrypted data without decrypting, providing a new solution to data confidentiality and privacy protection. However, current fully homomorphic encryption schemes are faced with challenges like large size of public key or low efficiency in calculation. To achieve an efficient fully homomorphic encryption scheme, this work provides an identity-based fully homomorphic encryption scheme employing the idea of eigenvector and arbitrary cyclotomic rings. Compared with existing scheme, this identity-based fully homomorphic encryption with eigenvector is able to successfully avoid the evaluation key, resulting a true identity-based scheme. Compared with special cyclotomic rings whose degree is power of 2, utilizing arbitrary cyclotomic rings may double the efficiency of encryption schemes and further improve the efficiency of calculation and memory using SIMD technique.

Key words: fully homomorphic crypto system; eigenvector; identity-based encryption; arbitrary cyclotomic ring

* 基金项目: 河南省科技创新杰出青年基金(134100510002); 河南省基础与前沿技术研究(142300410002); 数学工程与先进计算国家重点实验室开放基金

Foundation item: The Province Foundation for Science Innovation Distinguished Young Scholars of He'nan (134100510002); He'nan Province foundation and Advanced Technology Study (142300410002); State Key Laboratory of Mathematical Engineering and Advanced Computing Open Foundation

收稿时间: 2015-08-08; 修改时间: 2015-10-09; 采用时间: 2015-12-05; jos 在线出版时间: 2016-01-21

CNKI 网络优先出版: 2016-01-22 10:14:36, http://www.cnki.net/kcms/detail/11.2560.TP.20160122.1014.001.html

云计算是当前非常流行的新型 IT 技术,代表着 IT 领域迅速向集约化、专业化发展的趋势.由于云计算的通用性及便利性,它得到大力推动和发展.但隐私保护问题与便利性的冲突已经成为制约云计算发展的重要因素,即:用户希望在享受云服务器便利性的同时,也可以保护自己的隐私不外泄.全同态加密体制允许服务器在不解密的条件下对数据进行有效运算,因此它成为解决上述冲突的一个重要方案.

但已有的全同态加密体制普遍存在密文运算效率低、公钥尺寸过大的问题,如何有效管理密钥,一直是体制应用面临的难题之一.基于身份加密利用用户的唯一身份标识(如电子邮箱地址等)作为公钥,用户私钥的生成由可信第三方来完成(可信第三方由云服务器提供或用户自行选取),具备不依赖公钥证书进行密钥管理的优点,因此,人们开始思考如何将基于身份加密的思想与全同态加密技术结合起来.但是以往基于身份的全同态加密体制(以下简称 IBFHE 体制)都必须借助运算密钥(evaluation key),无法实现真正意义上的 IBFHE 体制.直到 2013 年,Gentry 等人舍弃了运算密钥,利用特征向量方法构造了第一个真正意义上的 IBFHE 体制.这些体制大多以特殊分圆环作为基本代数结构,虽然特殊分圆环结构简单,使用方便,但在构造体制时,计算效率较低,无法使用 SIMD 等技术.因此,本文提出了任意分圆环上的陷门,借助该陷门和特征向量方法,提出了 IBFHE 体制.相比 Gentry 提出的环上 IBFHE 体制(以下简称 GSW 体制),本文的体制最多可将密文运算效率提升一倍.另外,以任意分圆环作为基本代数结构,还可应用 SIMD 技术,使得每个密文可对应多份明文,大大提升空间和计算效率.

本文第 1 节介绍目前有关全同态加密的相关工作.第 2 节介绍本文体制所需的基础知识.第 3 节首先给出构造本文体制所需要的基本公钥体制,再给出任意分圆环上特征向量体制并证明其正确性和安全性.第 4 节首先给出任意环上的陷门,然后构造任意分圆环上使用特征向量的基于身份加密体制,最后证明任意环上 FHE 体制到 IBFHE 体制的转换定理.第 5 节对以上内容作出总结.

1 相关工作

全同态加密(fully homomorphic encryption,简称 FHE)由 Rivest 等人[1]在 1978 年首次提出,若某种加密体制对各种运算都满足同态性质,意为密文进行某种运算后进行解密,得到的明文恰好是对应明文的运算结果.尽管概念简单,但全同态加密的设计实现难度很大.直到 2009 年,Gentry 在其博士论文[2]中基于理想格成功构造出第一个真正意义上的全同态加密体制(gentry 体制),使得该领域得到突破性进展.接下来的几年里,全同态领域的研究突飞猛进,各种全同态加密体制纷纷出现.

1.1 全同态加密体制研究现状

目前的全同态加密体制根据基于的数学难题及代数结构不同,大致分为以下几类:(1) 基于理想格的全同态加密体制;(2) 整数上的全同态加密体制;(3) 基于 LWE(learning with error)问题的全同态加密体制;(4) 基于 RLWE(环上 LWE)问题的全同态加密体制.

(1) 基于理想格的全同态加密体制

虽然首次实现了全同态加密体制,但 Gentry 体制的密文运算计算复杂度过高、公钥尺寸过大.为了得到性能更好的全同态加密体制,以达到高效实用的最终目的,全同态加密初期研究的大量成果可归结为 Gentry 体制的优化方案.针对 Gentry 体制公钥尺寸过大的问题,Smart 等人[3]提出优化方案,称为 SV 体制,SV 体制公钥尺寸很小,但密钥生成算法复杂度过高.借用 SV 体制的思想,Gentry 等人[24]给出 Gentry 加密体制的另一种优化方案,称为 GH 体制,GH 体制使用主理想格作基础,并使用 SV 体制中的公钥形式,但对密钥生成过程进行了简化.随后,Smart 等人[5]提出了 SIMD 技术:SIMD 技术本质上是一种并行思想,在 SV 体制和 GH 体制的基础上,使用中国剩余定理对明文空间进行分解,使得每份密文对应多份相互独立的明文,所以,利用 SIMD 技术可以减小单位明文对应的密文尺寸,更高效地利用空间和计算资源.

(2) 整数上的全同态加密体制

2009 年,Van Dijk 等人[4]提出一种新的全同态加密体制,该体制基于整数上近似最大公因子问题,称为 DGHV 体制.该体制结构简单,便于理解,但公钥尺寸极大,效率较低,无法满足实际应用的需求.到目前为止,Stehlé 等人在文献[7]中构造的体制计算复杂度约为$\Omega(\lambda^{35})$(λ为体制安全参数),该体制在此类体制中的优化已达

到较好效果.此类体制沿用 Gentry 博士论文中设计全同态加密体制的方法(以下称 Gentry 方法),但基于该方法设计的体制的安全性必须依赖一个额外的假设,即,稀疏子集合假设(sparse subset sum assumption,简称 SSSP),但该假设的强度缺乏严格证明.另外,Gentry 方法需要大量密文同态运算,因此,使用 Gentry 方法设计的全同态加密体制的计算复杂度很难降低.

(3) 基于 LWE 问题的全同态加密体制(以下简称 LWE 体制)

理想格上很多困难问题的难解性并未得到证明,因此,这类体制在安全性方法上也有一定的隐患.2011 年,Brakerski 和 Vaikuntanathan[8]构造了基于一般格上困难问题的全同态加密体制,称为 BV 体制,BV 体制基于 LWE 问题[9].与理想格上的体制相比,BV 体制使用的 LWE 问题难解性得到了严格证明[8,10],并且 BV 体制的解密运算计算复杂度低.Brakerski 等人[11]又在此基础上提出密钥转换(key switching)技术,实现对密文噪声的精确控制,使得 BV 体制的计算复杂度极大地降低.

(4) 基于 RLWE 问题的全同态加密体制(以下简称 RLWE 体制)

2010 年,Lyubashevsky 等人[12]首先定义了 RLWE 问题,RLWE 问题与 LWE 问题结构相似,因此许多优化方法可以通用于两类体制.而且,RLWE 体制相对于 LWE 体制在很多加密应用中具有优势:首先,LWE 体制在一些实际应用中效率不高(例如构造单向函数);其次,RLWE 体制中的带噪声乘法可以一次直接得到$\mathbb{Z}_q$上 n 个伪随机结果,相当于 LWE 体制中的 n 次乘法;再次,若使用快速傅立叶变换,那么 RLWE 体制中乘法效率会更高;最后,使用环中理想对应的格时,可以用标准嵌入(canonical embedding)来代替系数嵌入(coefficient embedding),进一步减少密文尺寸.目前的 RLWE 体制根据使用的环类别不同而分为两类:

i. 第 1 类使用的是特殊环,其分圆多项式的次数为 2 的方幂.

由于其结构简单,易于理解,并且具备上面提到的所有优点,故 Brakerski 和 Vaikuntanathan[13]按照构造基于 LWE 问题体制的思路,构造基于 RLWE 问题的全同态加密体制.随后,Brakerski 等人[11]又将 LWE 问题与 RLWE 问题统一起来,称为 GLWE 问题,并借此构造了一个基于 GLWE 问题的全同态加密体制.

ii. 第 2 类使用的是任意环,即,分圆多项式的次数可以取任意值.

特殊环代数结构简单,但同时也牺牲了很多性质:首先,特殊环分布稀疏,在同样满足安全性的前提下,使用任意环的体制会比使用特殊环的体制效率高最多一倍;第二,特殊环上的体制无法实现 SIMD 等技术,无法进一步提高效率.但任意环上的实用算法和分析工具很少,仅有 Lyubashevsky 等人[14]提出的一些算法和工具,故,虽然使用任意环效率很高,但后续的研究较少.

1.2 基于身份的全同态加密体制

1984 年,Shamir[15]首次提出了基于身份的加密(identity-based encryption,简称 IBE)体制,这是一种不需要证书的公钥加密体制.每个用户都拥有唯一的公开身份信息,用户公钥由此信息生成,所以不需要认证,而用户私钥由可信第三方生成.由于无须公钥证书,所以 IBE 体制避免了与证书有关的计算和存储,可以更有效地管理密钥,减小密钥尺寸.但直到 2001 年,可应用于实际的 IBE 体制设计方法才由 Boneh 等人[16]与 Cocks 等人[17]分别提出.文献[16,17]的方法分别基于双线性映射函数构造和二次剩余假设.近年来,格上的难题也被应用于构造基于身份加密体制,2008 年,Gentry 等人[18]在 Regev 加密体制[9]的基础上提出了 IBE 体制,并证明了其 CPA 安全性.

因此,人们自然地想到构造基于身份的全同态加密体制,将基于身份加密体制与全同态加密体制相结合,利用基于身份加密体制的优势来进一步提高全同态加密体制的效率.在研究的初期,IBFHE 体制都需要借助运算密钥来实现,并非真正意义上的基于身份加密体制,如文献[19].2013 年,Gentry 等人在文献[20]中提出了特征向量方法,成功地避免运算密钥,实现了真正意义上的 IBFHE 体制.另外,Gentry 也简要给出了在特殊分圆环上该体制的形式.

2 预备知识

对于正整数 k,定义$[k]$为集合$\{0,\ldots,k-1\}$;对于$\mathbb{R}^n$或$\mathbb{C}^n$上的向量 $\boldsymbol{x}$,定义其ℓ_2范数为$\|x\|_2=\left(\sum_i |x_i|^2\right)^{1/2}$,$\ell_\infty$范数

为$\|\boldsymbol{x}\|_\infty=\max_i|x_i|$.记$\mathbb{Z}_m^*$为比$m$小且与$m$互质的正整数集合,$\varphi(\cdot)$为欧拉函数.

空间$\mathbb{C}^{\mathbb{Z}_m^*}$定义为$\mathbb{C}^{\mathbb{Z}_m^*}=\{x=(x_{i_1},...,x_{i_{\varphi(m)}})\}$,$i_j$为$\mathbb{Z}_m^*$中第$j$个元素,$j\in[1,\ldots,\varphi(m)]$.空间$H\subseteq\mathbb{C}^{\mathbb{Z}_m^*}$定义为$H=\{\boldsymbol{x}\in\mathbb{C}^{\mathbb{Z}_m^*}\mid x_i=\overline{x_{m-i}},\forall i\in\mathbb{Z}_m^*\}$,在研究以分圆数域和理想格构造的加密体制时,使用该空间较为方便.

2.1 格基础

H中的格可定义为H的离散加法子群,由n个线性无关向量$B=\{\boldsymbol{b}_j\}\subset H$的所有整线性组合构成的集合,即$\Lambda=\Lambda(B)=\left\{\sum_j z_j\boldsymbol{b}_j:z_j\in\mathbb{Z}\right\}$;两组基$B,B'$生成同一个格当且仅当存在一个幺模矩阵$U$,使得$BU=B'$;$\Lambda(B)$的行列式与基的选取无关,定义为任意一组格基矩阵的行列式(如$|\det(B)|$);在欧式范数下,Λ的第1小量定义为格中最短非零向量长度:$\lambda_1(\Lambda)=\min_{\boldsymbol{0}\neq\boldsymbol{x}\in\Lambda}\|\boldsymbol{x}\|_2$.$\Lambda$的对偶格定义为$\Lambda^\vee=\left\{\boldsymbol{y}\in H:\forall\boldsymbol{x}\in\Lambda,\langle\boldsymbol{x},\overline{\boldsymbol{y}}\rangle=\sum_i x_iy_i\in\mathbb{Z}\right\}$.容易看出:

$$(\Lambda^\vee)^\vee=\Lambda.$$

对于$s>0$,定义高斯函数$\rho_s:H\leftarrow(0,1]$为$\rho_s(\boldsymbol{x})=\exp(-\pi\langle\boldsymbol{x},\boldsymbol{x}\rangle/s^2)=\exp(-\pi\|\boldsymbol{x}\|_2^2/s^2)$.归一化该函数就可得到连续高斯分布$D_s$,其概率密度为$s^{-n}\cdot\rho_s(\boldsymbol{x})$.

定义1. 对于H中任一向量$\boldsymbol{c}$,有格陪集$\Lambda+\boldsymbol{c}$和实数$s>0$,可定义$\Lambda+\boldsymbol{c}$上的离散高斯分布为

$$D_{\Lambda+\boldsymbol{c},s}(\boldsymbol{x})=\frac{\rho_s(\boldsymbol{x})}{\rho_s(\Lambda+\boldsymbol{c})}.$$

2.2 分圆域(环)性质

对于正数数m,在有理数域中添加m次本原单位根ζ_m,得到的域扩张$K=\mathbb{Q}(\zeta_m)$称为m次分圆数域,ζ_m的极小多项式定义为m次分圆数域:

$$\phi_m(x)=\prod_{i\in\mathbb{Z}_m^*}(x-\omega_m^i)\in\mathbb{Z}[x],$$

其中,$\omega_m\in\mathbb{C}$是$\mathbb{C}$中m次本原单位根(例如$\omega_m=\exp\left(2\pi\sqrt{-1}/m\right)$),故$K$与$\mathbb{Q}(x)/(\phi_m(x))$存在一个自然同构,由$\zeta_m\to x$给出.$\phi_m(x)$的次数为$n=|\mathbb{Z}_m^*|=\varphi(m)$,故可将$K$看作$\mathbb{Q}$上$n$维向量空间,并以$(\zeta_m^j)_{j\in[n]}=(1,\zeta_m,...,\zeta_m^{n-1})\in K^{[n]}$作为一组基,这组基称为幂基(power basis).所谓特殊分圆环,即m只取2的幂,即$m=2^k$,k为正整数.

域$K=\mathbb{Q}(\zeta_m)$中有n个自同构σ_i,对于所有$i\in\mathbb{Z}_m^*$,σ_i保持$\mathbb{Q}$中元素保持不变,将ζ_m映射为ζ_m^i,标准映射$\sigma:K\to K^{\mathbb{Z}_m^*}$定义为

$$\sigma(a)=(\sigma_i(a))_{i\in\mathbb{Z}_m^*}.$$

使用标准映射σ可以定义K中元素的欧式范数:

- 对于$a\in K$,a的欧式范数定义为$\|a\|_2=\|\sigma(a)\|_2=\left(\sum_i|\sigma_i(a)|^2\right)^{1/2}$;
- ℓ_∞范数定义为$\max_i|\sigma_i(a)|$;

迹函数$Tr=Tr_{K/\mathbb{Q}}:K\to\mathbb{Q}$定义为自同构之和:$Tr(a)=\sum_i\sigma_i(a)$.显然,对于任意$a,b\in K$和$c\in\mathbb{Q}$,迹函数满足$Tr(a+b)=Tr(a)+Tr(b)$和$Tr(c\cdot a)=c\cdot Tr(a)$;

对于K中任意的分式理想I,它的对偶定义为

$$I^\vee=\{a\in K:Tr(aI)\subseteq\mathbb{Z}\}.$$

很容易可以验证$(I^\vee)^\vee=I$,$I^\vee$也是一个分式理想,且$I^\vee$在σ映射下会变为I的对偶格.

下面介绍分圆环上的张量基,在构造本文体制时,它相比于幂基,生成陷门的效率更高,并且更适用于一些快速算法.定义如下:

定义2. $R=\mathbb{Z}(\zeta_m)$的张量基$\boldsymbol{p}$定义如下:

(1) 若m为某个素数的幂,那么$\boldsymbol{p}$定义为幂基$(\zeta_m^j)_{j\in[\varphi(m)]}$;

(2) 若m有素数幂分解$m=\prod_l m_l$,定义$\boldsymbol{p}=\otimes_l\boldsymbol{p}_l$,其中,$\boldsymbol{p}_l$为$R=\mathbb{Z}(\zeta_m)$的幂基.

2.3 RLWE问题

定义 3(RLWE 分布). 对于 $s \in R_q^\vee$ (秘密)和 $K_{\mathbb{R}}$ 上的一个误差分布 Ψ,那么 $R_q \times (K_{\mathbb{R}} / qR^\vee)$ 上的 RLWE 分布 $A_{s,\Psi}$中的一个抽样生成方式如下:均匀随机地选择 $a \leftarrow R_q$,选择 $e \leftarrow \Psi$,输出$(a, b=a \cdot s+e \bmod qR^\vee)$.

定义 4(DRLWE 假设). 无法以不可忽视的优势来区分以下两个分布:第 1 个是从 $A_{s,\Psi}$中独立抽样,其中随机选择 $s \leftarrow R_q^\vee$;第 2 个是从 $R_q \times (K_{\mathbb{R}} / qR^\vee)$ 中均匀随机地取出同样数量的相互独立的抽样,记作 $DRLWE_{q,\Psi}$假设.

在加密应用中,具有离散误差分布的 RLWE 问题通常更有用.我们可以自然地定义一个分布 $A_{s,\chi}$,其中,χ为 $R^\vee$上的离散误差分布,那么 b 就是 $R_q^\vee$ 上的元素.类似地,我们可以修改定义 4,令 $DRLWE_{q,\chi}$是区分 $A_{s,\chi}$和均匀地从 $R_q \times R_q^\vee$ 采样的问题.对于很多种类的离散误差分布,问题的离散形式的困难性是由问题的连续形式来产生的.下面的定理意味着:如果 $DRLWE_{q,\Psi}$在 l 个抽样的情况下是难的,那么 $DRLWE_{q,\chi}$在同样数目的抽样下也是难的.其中,误差分布χ是$[p \cdot \Psi]_{\omega+pR^\vee}$,$p$是一个与 q 互质的整数,$[\cdot]$是任意一个有效的离散化到$pR^\vee$的方法,ω是 $R_p^\vee$ 上一个任意元素,可以随着不同的采样而变化.特别地,对于 p=1,得到误差分布 $[\Psi]_{R^\vee}$.记 $DRLWE_{q,\Psi}$在 l 个抽样的情况下为 l–$DRLWE_{q,\Psi}$.

定理 1. 令 p 和 q 是互质整数,$[\cdot]$是任意一个将连续分布变为离散分布的方法,ω是 $R_p^\vee$ 上的任意元素.如果 $DRLWE_{q,\Psi}$问题对于给定某个数目 l 个抽样时是难的,那么 $DRLWE_{q,\Psi}$的变体:秘密是抽样自 $\chi = [p\Psi]_{\omega+pR^\vee}$ 在给定 l–1 个抽样时也是难的.

2.4 基于身份的全同态加密体制

全同态体制 FHE 分为 4 种算法:密钥生成 *KeyGen*、加密 *Enc*、解密 *Dec*、同态运算 *Eval*.前 3 种算法与一般的公钥加密体制类似,而同态运算则是对应代数结构上密文的运算,具体的定义见文献[2].

IBE 体制一般分为 4 种算法:参数选择 *Setup*、私钥提取 *Extract*、加密 *Enc*、解密 *Dec*.*Setup* 算法中生成主公私钥对;*Extract* 对于身份 ID 提取用户私;加解密与普通公钥体制类似,使用的密钥为用户公私钥对.若一个 IBE 体制同时也是 FHE 体制,即 IBFHE 体制,一般分为 5 种算法:参数选择 *Setup*、私钥提取 *Extract*、加密 *Enc*、解密 *Dec*、同态运算 *Eval*.前 4 种算法与 IBE 相同,同态运算算法与 FHE 体制中的 *Eval* 算法相同.

3 任意分圆环上使用特征向量的全同态加密体制

本节首先给出 LPR 公钥体制,并在此基础上提出任意分圆环上近似特向量全同态加密体制;最后,结合 SIMD 技术进一步提升该体制的效率.

3.1 LPR公钥体制

该体制是针对文献[14]公钥体制的变形,该体制可以转变为基于身份的加密体制.令 $R=\mathbb{Z}[\zeta_m]$为 m 次分圆数环,p,q 为互质的整数,其中,使用 p 定义明文空间 R_p,q 为 RLWE 中的模数,令 $l \geq 2$, Ψ是 $K_{\mathbb{R}}$ 上的连续高斯分布,$D_{R,r}$是 R 上离散高斯分布.体制共分为 3 个部分:*LPR.KeyGen*,*LPR.Enc*,*LPR.Dec*.

(1) 密钥生成算法 LPR.*KeyGen*:令 a_0=1,取 $e \in \Psi, s_0, \ldots, s_{l-1} \in D_{R,r}$,令 $\boldsymbol{si}=(s_1, \ldots, s_{l-1})$,令私钥 $sk=\boldsymbol{s}=(1, -\boldsymbol{si}) \in R^l$,在 R_q 上均匀随机取 $a_1, \ldots, a_{l-1}$,令 $pk = A = \left(a_l = \sum_{i \in [l]} a_i s_i, a_1, ..., a_{l-1}\right) \in R^l$ 为公钥,可以发现,$A \cdot \boldsymbol{s} = s_0$;

(2) 加密算法 LPR.*Enc*($\mu \in R_p$,*pk*):加密 μ 时,取 $e_0 \leftarrow [p\Psi]_{pR^\vee}$,$e_1 \leftarrow [p\Psi]_{t^{-1}\mu+pR^\vee}$,$e_2, ..., e_l \leftarrow [p\Psi]_{pR^\vee}$,令 $\boldsymbol{e}=(e_1, \ldots, e_l) \in (R^\vee)^l$,得到密文 $\boldsymbol{c} = e_0 \cdot A + \boldsymbol{e} \in (R_q^\vee)^l$;

(3) 解密算法 LPR.*Dec*($\boldsymbol{c}$,*sk*):计算 $d=\langle \boldsymbol{c}, \boldsymbol{s} \rangle \bmod qR^\vee$,输出明文$\mu=t \cdot d \bmod pR$.

正确性的讨论见文献[14],关于安全性有如下定理:

定理 3.1[14]. 若 $r > 2n \cdot q^{1/l+2/(nl)}$且$(l+1)$–$DRLWE_{q,\Psi}$的是难的,LPR 公钥体制具备 IND-CPA 安全性.

3.2 体制描述

选择模数 q,令 $l'=\lceil \log q \rceil$,$N=l\cdot l'$,取 $R_q^\vee$ 的一组好基 $\boldsymbol{p}=(p_1,\ldots,p_n)$(本文中的好基指这组基构成的矩阵的奇异值较小,如第 2.2 节中提到的张量基),首先定义本节中用到的几个函数:

- 对于 $\boldsymbol{a}\in(R_q^\vee)^l$,$BitDecomp(a)=(a_{1,1},...,a_{1,l'},...,a_{l,1},...,a_{l,l'})\in(R_q^\vee)^N$,其中,$a_{i,j}$ 是 a_i 二进制表示的第 j 个比特;
- 对于 $\boldsymbol{b}=(b_{1,1},...,b_{1,l'},...,b_{l,1},...,b_{l,l'})\in(R_q^\vee)^N$,定义以下函数:

$$BitDecomp^{-1}(\boldsymbol{b})=\left(\sum_{i=1}^{l'}2^{i-1}\cdot b_{1,i},...,\sum_{i=1}^{l'}2^{i-1}\cdot b_{l,i}\right)\in(R_q^\vee)^l;$$

$$Flatten(\boldsymbol{b})=BitDecomp(BitDecomp^{-1}(\boldsymbol{b}));$$

$$Powersof\,2(\boldsymbol{a})=(a_0,2a_0,...,2^{l-1}a_0,a_1)\in(R_q^\vee)^N.$$

若这些函数的自变量为矩阵,意为将矩阵的每一行看作向量进行函数调用.体制分为密钥生成算法 *AE.KeyGen*、加密算法 *AE.Enc*、解密算法 *AE.Dec*、密文运算算法 *AE.Evaluate* 这 4 个部分.

(1) *AE.KeyGen*:首先令 $a_0=1$,取 $e\in\Psi,s_0,\ldots,s_{l-1}\in D_{R,r}$,令 $\boldsymbol{si}=(s_1,\ldots,s_{l-1}),\boldsymbol{s}=(1,-\boldsymbol{si})\in R^l$,在 R_q 上均匀随机 $a_1,\ldots,a_l$,令 $pk=A=\left(a_l=\sum_{i\in[l]}a_is_i,a_1,...,a_{l-1}\right)\in R^l$ 为公钥,私钥 $sk=\boldsymbol{v}\leftarrow Powersof2(\boldsymbol{s})\in R^N$;

(2) *AE.Enc*($\mu'\in R_p,pk$):先生成 N 个 LPR 公钥体制中 0 的密文,令矩阵 C'的每一行分别是这些 0 的加密结果,则 $C'\in(R_q^\vee)^{N\times l}$,令密文矩阵为 $C\leftarrow Flatten(\mu'\cdot I_N+BitDecomp(C'))\in(R_q^\vee)^{N\times N}$ (I_N 为 N 维单位矩阵);

(3) *AE.Dec*(C,sk):计算 $C\cdot\boldsymbol{v}=\mu'\cdot\boldsymbol{v}+BitDecomp(C')\cdot\boldsymbol{v}=\mu'\cdot\boldsymbol{v}+C'\cdot\boldsymbol{s}$,解密时只需一行即可,令 C_i 为 C 的第 i 行,计算 $y_i=\langle C_i,\boldsymbol{v}\rangle$,输出 $\mu'=y_i/\boldsymbol{v}_i$;

(4) *AE.Evaluate*(C_1,C_2):令密文矩阵 C_1 加密明文 μ_1,C_2 加密明文 μ_2.令 $C_1\cdot\boldsymbol{v}=\mu_1\cdot\boldsymbol{v}+\boldsymbol{e}_1',C_2\cdot\boldsymbol{v}=\mu_2\cdot\boldsymbol{v}+\boldsymbol{e}_2'$,其中,$\boldsymbol{e}'$和 $\boldsymbol{e}_2'$ 为 N 个 *LPR* 公钥体制中加密 0 的密文与 $\boldsymbol{v}$ 相乘的结果(即 N 个 $e_0\cdot s_0+\langle\boldsymbol{e},\boldsymbol{s}\rangle$,该结果模 pR 得到明文 0).

同态加法为 $(C_1+C_2)\cdot\boldsymbol{v}=(\mu_1+\mu_2)\cdot\boldsymbol{v}+(\boldsymbol{e}_1'+\boldsymbol{e}_2')$;

同态乘法为 $(C_1\cdot C_2)\cdot\boldsymbol{v}=C_1\cdot(\mu_2\cdot\boldsymbol{v}+\boldsymbol{e}_2')=\mu_2\cdot(\mu_1\cdot\boldsymbol{v}+\boldsymbol{e}_1')+C_1\cdot\boldsymbol{e}_2'=\mu_1\cdot\mu_2\cdot\boldsymbol{v}+\mu_2\cdot\boldsymbol{e}'+C_1\cdot\boldsymbol{e}_2'=\mu_1\cdot\mu_2\cdot\boldsymbol{v}\bmod pR$.

3.3 *AE*体制正确性与安全性分析

- 正确性

解密算法输出为

$$\begin{aligned}y_i/\boldsymbol{v}_i&=\langle C_i,\boldsymbol{v}\rangle/\boldsymbol{v}_i\\&=\langle(\mu'\cdot(I_N)_i+BitDecomp(C_i')),\boldsymbol{v}\rangle/\boldsymbol{v}_i\\&=\mu'\cdot\boldsymbol{v}_i/\boldsymbol{v}_i\\&=\mu',\end{aligned}$$

其中,$(I_N)_i$ 表示矩阵 I_N 的第 i 行,C_i' 表示 C'的第 i 行.

由于 C'的每一行都是加密 0 得到的加密结果,所以 $\langle BitDecomp(C_i'),\boldsymbol{v}\rangle$ 的结果就是 0.

- 关于体制的安全性有如下定理

定理 2. 设系统参数 $n=n(\lambda),q=q(\lambda),L=L(\lambda)$为安全参数$\lambda$的多项式,取错误分布$\chi=\chi(\lambda)$为环上高斯分布 $D_{R,r}$,$r>2n\cdot q^{1/l+2/(nl)}$,$n\geq 2\lg q$,在 $DRLWE_{q,\chi}$假设的前提下,AE 体制是 IND-CPA 安全的.

证明:定理证明采用基于游戏序列的证明方法,用 $Adv_{\mathrm{Game}}[A]$来定义攻击者 A 在 Game 中的优势.

- **Game 0**

Game 0 即标准的 IND-CPA 游戏:挑战者 C 调用密钥生成算法 AE.*KeyGen* 生成公钥 pk,并将其交给攻击者 A,A没有访问解密谕示的能力,因此选择挑战明文 $\mu_0^*,\mu_1^*\in R_q$,C 从中随机选择 μ_b^*,加密生成挑战密文 c^*并将其交给攻击者 A,A 猜测 c^*对应明文为μ_b.攻击者 A 的优势记为

$$Adv_{CPA}[A]=|\Pr[A(pk,AE.Enc(pk,\mu_0^*))]-\Pr[A(pk,AE.Enc(pk,\mu_1^*))]| \quad (1)$$

- **Game 1**

Game 1 与 Game 0 的区别在于公钥的生成方式.Game 1 的公钥 pk 直接从 R^l 中均匀随机取得.由文献[14]推论 7.5 可知,公钥 pk 与 R^l 上的均匀分布的统计距离在 $2^{-\Omega(n)}$ 以内.即,A 区分 Game 0 与 Game 1 的概率小于 $2^{-\Omega(n)}$,因此:

$$|Adv_{\text{Game1}}[A]-Adv_{CPA}[A]|<2^{-\Omega(n)} \tag{2}$$

- **Game 2**

在 Game 1 的基础上,加密算法被修改,密文中的 C'不再是 0 的密文,而是从 $(R_q^{\vee})^{N\times l}$ 均匀随机抽取.由文献[14]引理 8.1 与 $DRLWE_{q,\chi}$假设可知,修改前与修改后的 C'是计算不可区分的.因此,A 区分 Game 1 与 Game 2 的概率小于 n 的可忽略函数,记作 $negl(n)$,因此有:

$$|Adv_{\text{Game2}}[A]-Adv_{\text{Game1}}[A]|\leq negl(n) \tag{3}$$

- **Game 3**

在 Game3 中,C 给出的挑战密文不再由加密算法生成,而是直接从 $(R_q^{\vee})^{N\times N}$ 生成.

由 $C=Flatten(\mu'\cdot I_N+BitDecomp(C'))$知,$BitDecomp^{-1}(C)=\mu'\cdot BitDecomp^{-1}(I_N)+C'$.由于此前 Game 2 中 C'已替换为 $(R_q^{\vee})^{N\times l}$ 上的随机值,因此,$BitDecomp^{-1}(C)$与 $(R_q^{\vee})^{N\times l}$ 上的随机分布计算不可区分,即,C 与 $(R_q^{\vee})^{N\times N}$ 上的随机分布计算不可区分,故有:

$$|Adv_{\text{Game3}}[A]-Adv_{\text{Game2}}[A]|\leq negl(n) \tag{4}$$

至此,在 Game 3 中,挑战者所给出的公钥、密文都服从均匀分布,且与目标密文之间完全独立,因此,A 在 Game 3 中能取得的优势为 0,即:

$$Adv_{\text{Game3}}[A]=0 \tag{5}$$

结合公式(3.1)~公式(3.5),可得:

$$Adv_{\text{CPA}}[A]\leq 2^{-\Omega(n)}+2negl(n).$$

因此,在 $DRLWE_{q,\chi}$假设成立的情况下,$Adv_{\text{CPA}}[A]$可忽略,即,AE 体制是 IND-CPA 的,安全性得证. □

3.4 SIMD技术

从文献[5]的分析可以看出,SIMD 技术实际是一种并行思想.目前,SIMD 技术相继被应用到 LWE 体制和 RLWE 体制中,实现了两种 SIMD 全同态加密体制[21,22].文献[21]中,Gentry 等人使用了包括 SIMD 技术在内的多种优化效率方法,极大地降低了计算复杂度.而基于该体制实现的 AES 加密算法实验[23],证明该体制在一定程度上已可以应用于实际.

具体方法是:将整个明文空间 $R_p=R/pR$(其中,$R=\mathbb{Z}(x)/(\phi_m(x))$)分解为相同大小的子环,待加密的明文分别属于这些子环,然后将它们合成为 R_p,对合成明文进行加密,即,相当于并行加密了子环上的所有明文.故,使用 SIMD 技术将大幅提升加解密的效率.但特殊分圆环不能进行分解,故,使用特殊分圆环无法使用 SIMD 技术.

在加密体制中,一般 p 都为质数,但$\langle p\rangle$一般不是质理想,接下来讨论对 pR 进行理想分解.令 $d\geq 0$ 为满足 p^d 能整除 m 的最大整数,令 $h=\varphi(p^d)$,令 $a\geq 1$ 为模 m/p^d 意义下 p 的乘法逆元,由文献[6]知,$\phi_m(x)$可分解为 $\prod_i(f_i(x))^h$,那么 pR 可分解为 $\boldsymbol{p}_1^h\boldsymbol{p}_2^h...\boldsymbol{p}_e^h$,其中,$e=\varphi(m)/(ha)$,$\boldsymbol{p}_i=\langle p,f_i(\zeta)\rangle$是范数为 p^a 且两两不同的质理想.

第 3.2 节的 IBFHE 中,明文空间为 R_p,故可将其如上分解,实现并行加密.若 $\phi_m(x)$可分解为 k 个首一不可约多项式,就可以同时加密 k 个明文.

3.5 效率分析

AE 体制相比 GSW 体制,最大的区别就在于使用任意分圆环来代替特殊分圆环.由于特殊分圆环分布稀疏,所以在相同安全性条件下,使用任意分圆环的计算效率最高可达使用特殊分圆环的两倍,这是由于特殊分圆环的分圆多项式为$\phi_m(x)=2^{m/2}+1$,举例来说,若 m 取 256 时并不能满足安全性条件,故只能取 512.然而在 256 与 512 之间有许多可达到与 512 相同安全性的值,例如 257,这样,任意分圆环与特殊分圆环的维数相差近乎两倍,那么

环上运算的效率会相差至少两倍.任意分圆环的另一个优势在于,它可以利用中国剩余定理进行划分.因此,明文空间也可以分割为多份,就能支持 SIMD 技术.

表 1 给出了两种体制在相同安全性条件下的效率分析对比.q 为两种体制的模数,安全参数κ取 257,m 为分圆多项式次数,$n=\varphi(m)$,那么 GSW 体制中 n=512,AE 体制中 n=257.可以看出,两种体制的环维数相差接近两倍.令两种体制中公钥维数 l=10.表中乘法与加法均指环上运算,但对于 AE 体制来说,环上运算所占用的空间较少.另外,AE 体制相比基于 LWE 问题的体制,公钥尺寸也极大地缩小,以文献[8]的 BV 体制为例,在格维数 n=192 的情况下,公钥尺寸将达到 50.6MB.从表 3.1 可看出,AE 体制的公钥尺寸仅仅只有 75.3KB.

Table 1 Analysis and comparison of efficiency

表 1 效率分析对比

体制	κ	n	$\lceil \log q \rceil$	加密复杂度	解密复杂度	公钥尺寸 (KB)	私钥尺寸 (KB)
GSW	257	512	30	3 000 次乘 93 000 次加	301 次乘 299 次加	150	1 500
AE	257	257	30	3 000 次乘 93 000 次加	301 次乘 299 次加	75.3	752.9

4 任意分圆环上使用特征向量的基于身份公钥加密体制

4.1 任意环上的陷门生成

本节构造了任意环上的陷门,采用文献[18]的思想,从整数环上的陷门转化为任意环上的陷门.此陷门在接下来构造基于身份的体制时使用.

对于矩阵 $A \in R_q^{k\times l}$,定义:

- $\Lambda^{\perp}(A)=\{\boldsymbol{y}\in R^l: A\boldsymbol{y}=\boldsymbol{0} \bmod qR\}$;
- $\mathcal{L}^{\perp}(A)=\{z\in\mathbb{Z}^{\ell}: A\boldsymbol{z}=\boldsymbol{0} \bmod q\}$.

显然,$\Lambda^{\perp}(A)$和$\mathcal{L}^{\perp}(A)$都是格.关于这两个格的基,有以下引理:

引理 1. 令 $A,\Lambda^{\perp}(A),\mathcal{L}^{\perp}(A)$定义如下:若 B 是$\mathcal{L}^{\perp}(A)$的任意一组$\mathbb{Z}$-基,$\boldsymbol{b}$ 是 R 的任意一组$\mathbb{Z}$-基,那么 $B\otimes\boldsymbol{b}^T$ 是$\Lambda^{\perp}(A)$的一组$\mathbb{Z}$-基.

给定格$\Lambda=\mathcal{L}(B)$的一组好基 $B=\{\boldsymbol{b}_i\}$,设Λ为 n 维,若使用空间 H 中一个点 $\boldsymbol{c}$ 来表示格陪集$\Lambda+\boldsymbol{c}$,那么通过前像采样,可以得到$\Lambda+\boldsymbol{c}$ 上的符合离散高斯分布的一系列点.采样的方法记作 SampleR,具体流程如下:

1. 遍历 $i\leftarrow 1,\ldots,n$:
   (a) 使用基 B 将 $\boldsymbol{c}$ 表示为 $\boldsymbol{c}=\sum_i c_i b_i$,其中,$c_i\in[0,1]$;
   (b) 随机从$\{c_i-1,c_i\}$中选取一个元素,并令其为 f_i;
2. 输出 $f=\sum_i f_i\boldsymbol{b}_i$.

接下来即可使用上述引理及采样方法进行陷门的构造,陷门构造过程共分为 3 步:

(1) 选择矩阵 A 为 $R_q^{k\times l}$ 上均匀随机的矩阵,由引理 4.1,选取$\mathcal{L}^{\perp}(A)$的一组好基及 R 的一组好基(例如张量基),生成$\Lambda^{\perp}(A)$的好基 $\boldsymbol{T}$ 作为陷门;

(2) 陷门函数 f_A 定义为 $f_A(\boldsymbol{x})=A\boldsymbol{x} \bmod qR$;

(3) 若给出 $\boldsymbol{u}\in R_q^l$,要计算向量 $\boldsymbol{x}$,首先计算满足等式 $A\cdot\boldsymbol{t}=\boldsymbol{0} \bmod qR$ 的特解 $\boldsymbol{t}$;然后,利用陷门 $\boldsymbol{T}$ 进行前像采样,求得分布$\Lambda-\boldsymbol{t}$ 上符合离散高斯分布的向量 $\boldsymbol{v}$,输出 $\boldsymbol{x}=\boldsymbol{t}+\boldsymbol{v}$.

4.2 基于身份的公钥加密体制

在基于身份的体制中,定义随机喻示 $H:\{0,1\}^*\rightarrow R_q^l$ 可将身份映射为 LPR 公钥,使用第 4.1 节中提出的陷门,则任意环上近似特征向量的基于身份加密体制 IBAE 如下:

(1) 参数生成 *IBAE.Setup*:由陷门 $\boldsymbol{T}$ 生成陷门函数 f_A,令主公钥为 A,也即 LPR 体制中的公钥,主私钥为 $\boldsymbol{T}$;

(2) 私钥提取 *IBAE.Extract*(A,$\boldsymbol{T}$,id):令 $\boldsymbol{u}=H(id)$,使用 $\boldsymbol{T}$ 进行前像采样,得到用户私钥 $\boldsymbol{s}\leftarrow f_A^{-1}(\boldsymbol{u})$;

(3) 加密算法 *IBAE.Enc*(A,id,m):使用身份 id 加密明文 $m\in R_2$,首先令 $\boldsymbol{u}=H(id)\in R_q^l$,输出密文:

$$\boldsymbol{c}=LPR.Enc(m,\boldsymbol{u});$$

(4) 解密算法 *IBAE.Dec*($\boldsymbol{s}$,$\boldsymbol{c}$):执行 *LPR.Dec*($\boldsymbol{c}$,$\boldsymbol{s}$).

4.3 IBAE体制正确性与安全性分析

由第 3.1 节中关于 LPR 体制的正确性分析可知,IBAE 体制的正确性同理.关于安全性有如下定理:

定理 3. 若 LPR 体制具备 IND-CPA 安全性,并且其公钥在 R^l 上均匀地随机分布,那么 IBAE 体制在随机喻示模型下是 IND-adaptive ID-CPA 安全的.

证明:若存在一个针对 IBAE 体制的多项式时间攻击者 A,在 IND-ID-CPA 攻击游戏中优势为ε(不可忽略),并且有 Q_{oragle} 次喻示访问权限条件,那么我们可以构造一个针对 LPR 体制的攻击者 B,其在 IND-CPA 攻击游戏中优势为$\varepsilon/Q_{\text{oragle}}$.

攻击者 B 的输入 LPR 体制中公钥 $\boldsymbol{u}^*\in R_q^l$,$B$ 首先随机选取 $i\in\{1,\ldots,Q_{\text{oragle}}\}$,并模拟 *IBAE* 攻击游戏:

(1) 模拟随机喻示:对于 A 的第 j 次访问 id_j,若 $j=i$,那么保存三元组(id_j,$\boldsymbol{u}^*$,⊥),并将 $\boldsymbol{u}^*$交给 A;若 $j\neq i$,则调用 *LPR.KeyGen*,生成公私钥对($\boldsymbol{u}_j$,$\boldsymbol{s}_j$),保存三元组(id_j,$\boldsymbol{u}_j$,$\boldsymbol{s}_j$),并将 $\boldsymbol{u}_j$ 交给 A;

(2) 模拟私钥提取喻示:若 A 以身份 id 访问私钥提取喻示,不失一般性地假设 A 已经用 id 访问过随机喻示,因此,B 只需查询已保存的三元组(id,$\boldsymbol{u}$,$\boldsymbol{s}$),将 $\boldsymbol{s}$ 交给 A,若 $\boldsymbol{s}=\perp$,那么输出一个随机值并终止;

(3) 模拟挑战密文:当 A 生成挑战明文 μ_0^*,μ_1^* 和挑战身份 id^*时,不失一般性地假设 A 已经用 id^*访问过随机喻示,若 $id^*\neq id$,即(id^*,$\boldsymbol{u}^*$,⊥)并未保存过,那么输出一个随机值并终止;否则,B 向 *LPR* 体制攻击游戏的挑战者发起挑战,得到挑战密文 c^*,并将 c^*交给 A.

当 A 终止并输出结果时,B 也输出同样的结果并终止.

在模拟过程中,B 没有终止并输出结果的概率为 $1/Q_{\text{oragle}}$(即 $id^*=id_i$ 的概率),这时,B 成功模拟出 IBAE 攻击游戏.根据假设可知,A 在这种情况下攻击成功的优势为ε.故,B 攻击 IBAE 体制的优势为$\varepsilon/Q_{\text{oragle}}$. □

4.4 基于身份的体制向基于身份的全同态体制的转化

本节介绍一种将基于 RLWE 的 IBE 体制(并且满足某些性质)转化为 IBFHE 的方法,该方法是文献[20]中转化方法的关于环的变体.若一个 IBE 体制满足以下性质,那么都可以使用该方法进行转换:

(1) 对于身份 id,令私钥为 $\boldsymbol{s}_{id}\in R^l$,对应密文为 $\boldsymbol{c}_{id}\in(R_q^\vee)^l$,那么 $\boldsymbol{s}_{id}$ 第 1 项为 1;

(2) 若 $\boldsymbol{c}_{id}$ 加密了 0,那么$\langle\boldsymbol{c}_{id},\boldsymbol{s}_{id}\rangle=0 \bmod pR^\vee$;

(3) 0 的加密结果与 $(R_q^\vee)^l$ 上的均匀分布不可区分.

定理 4. 若一个 IBE 体制 E 满足上述 3 条性质,那么该体制可以转化为一个 IBFHE 体制.

证明:IBFHE 使用 E 的参数设置和密钥生成算法,并将 E 的主公钥加入 AE 中,令 $l'=\lceil\log q\rceil$,$N=l\cdot l'$.为加密明文$\mu\in\{0,1\}$,加密者使用 E 的加密算法生成 N 个 0 的加密结果,令 C'_{id} 为 $N\times l$ 的矩阵,且它的每一行分别是这些密文,输出 $C_{id}=Flatten(\mu\cdot I_N+BitDecomp(C'_{id}))$, 若 $\boldsymbol{s}_{id}$ 为身份 id 对应的私钥,那么解密者运行 AE 的解密算法来恢复μ,同态运算的讨论与第 3.2 节中相同.

令 $\boldsymbol{v}_{id}=Powersof2(\boldsymbol{s}_{id})$,那么由于性质(2), $C_{id}\cdot\boldsymbol{v}_{id}=\mu\cdot\boldsymbol{v}_{id}+C'_{id}\cdot\boldsymbol{s}_{id}=\mu\cdot\boldsymbol{v}_{id} \bmod pR^\vee$,故解密是正确的.若存在一个攻击者可以从上述 IBFHE 体制中区分 C'_{id} 和 $(R_q^\vee)^{N\times l}$ 上的均匀矩阵,则由性质(3),该攻击者也可以以不可忽略的优势解决 $DRLWE_{q,\chi}$,即,证明了该体制安全性.故定理得证. □

显然,第 4.2 节提出的 IBAE 体制满足上面 3 条性质,故由上面定理,可将 IBAE 体制与第 3.2 节的 AE 体制结合得到一个 IBFHE 体制(IBAFHE 体制).本体制以任意分圆环作为基本代数结构,因此与 AE 体制一样,IBAE

体制也可实现 SIMD 技术.本节利用特征向量构造一个真正意义上的 IBFHE 体制,相比之下,Brakerski 等人[13]提出的体制在实际应用中必须借助公钥证书进行认证,而且还需要证书分发、管理.

4.5 效率分析与对比

与文献[19]提出的 IBFHE(GZF 体制)相比,IBAFHE 体制以 RLWE 问题作为基础,因此密文运算效率较高,加解密计算复杂度有很大降低,并且密文尺寸更短.表 2 给出了 IBAFHE 与 GZF 体制在相同安全条件下的效率分析与对比.n 为体制所使用格的维数(即 $R_q^\vee$ 或 R_q 对应的理想格维数),格维数都取 192,GZF 体制的公钥尺寸分为加密公钥和运算密钥两部分,而 IBAFHE 的公钥尺寸只包含加密公钥,故公钥尺寸大大缩小;另外,由于 IBAFHE 体制可使用 SIMD 技术,加解密效率可进一步提高,由第 3.4 节的分析,理想 qR 可分解为 $h=\varphi(q^d)$个质理想,IBAFHE 的加密时最多可以同时加密 h 份明文,故 IBAFHE 的加解密效率还可提高为 h 倍;GZF 体制的私钥是整数上向量,IBAFHE 的私钥是环上向量,故私钥尺寸有所增加.IBAFHE 与 GSW 中基于身份的全同态体制相比,由于 GSW 中体制所使用的基础结构是特殊分圆环,因此要达到同等安全条件,GSW 体制的维数至少要取 256,公钥尺寸就会变大,相比本文体制大了 33.3%.另外,GSW 同样无法使用 SIMD 技术.

Table 2 Analysis and comparison of efficiency

表 2 效率分析对比

体制	n	$\lceil \log q \rceil$	加密复杂度	解密复杂度	公钥尺寸	私钥尺寸	是否可使用 SIMD 技术
GZF	192	12	965 000 次乘 965 000 次加	5 000 次乘 5 000 次加	≥50.6MB	76.5KB	否
GSW	256	30	3 000 次乘 93 000 次加	301 次乘 299 次加	75KB	750KB	否
IBAFHE	92	30	3 000 次乘 93 000 次加	301 次乘 299 次加	56.25KB	562.5KB	是

5 总 结

在云计算的背景下,全同态加密有着广阔的应用前景,但效率低下的问题一直制约着全同态加密在实际中的应用.因此,本文先给出基本的公钥体制和一种陷门生成算法,然后针对全同态加密体制效率低下的问题,结合近似特征向量方法和 SIMD 技术,使用任意分圆环提出了一个 IBFHE 体制,相比已有的 IBFHE 体制,效率大大提升.

References:

[1] Rivest RL, Adleman L, Dertouzos ML. On data banks and privacy homomorphisms. Foundations of Secure Computation, 1978, 4(11):169−180.

[2] Gentry C. Fully homomorphic encryption using ideal lattices. 2009,9:169−178. http://www.cs.cmu.edu/~odonnell/hits09/gentry-homomorphic-encryption.pdf [doi: 10.1145/1536414.1536440]

[3] Smart NP, Vercauteren F. Fully homomorphic encryption with relatively small key and ciphertext sizes. In: Proc. of the Public Key Cryptography (PKC 2010). Berlin, Heidelberg: Springer-Verlag, 2010. 420−443. [doi: 10.1007/978-3-642-13013-7_25]

[4] Van Dijk M, Gentry C, Halevi S, Vaikuntanathan V. Fully homomorphic encryption over the integers. In: Proc. of the Advances in Cryptology (EUROCRYPT 2010). Berlin, Heidelberg: Springer-Verlag, 2010. 24−43. [doi: 10.1007/978-3-642-13190-5_2]

[5] Smart NP, Vercauteren F. Fully homomorphic SIMD operations. Designs, Codes and Cryptography, 2014,71(1):57−81. [doi: 10.1007/s10623-012-9720-4]

[6] Shoup V. A Computational Introduction to Number Theory and Algebra. Cambridge University Press, 2009. [doi: 10.1017/ CBO 9781139165464]

[7] Stehlé D, Steinfeld R. Faster fully homomorphic encryption. In: Proc. of the Advances in Cryptology (ASIACRYPT 2010). Berlin, Heidelberg: Springer-Verlag, 2010. 377−394. [doi: 10.1007/978-3-642-17373-8_22]

[8] Brakerski Z, Vaikuntanathan V. Efficient fully homomorphic encryption from (standard) LWE. SIAM Journal on Computing, 2014, 43(2):831−871. [doi: 10.1109/focs.2011.12]

[9] Regev O. On lattices, learning with errors, random linear codes, and cryptography. Journal of the ACM, 2009,56(6):34. [doi: 10.1145/1060590.1060603]

[10] Peikert C. Public-Key cryptosystems from the worst-case shortest vector problem. In: Proc. of the 41st Annual ACM Symp. on Theory of Computing. ACM Press, 2009. 333−342. [doi: 10.1145/1536414.1536461]

[11] Brakerski Z, Gentry C, Vaikuntanathan V. (Leveled) fully homomorphic encryption without bootstrapping. In: Proc. of the 3rd Innovations in Theoretical Computer Science Conf. ACM Press, 2012. 309−325. [doi: 10.1145/2090236.2090262]

[12] Lyubashevsky V, Peikert C, Regev O. On ideal lattices and learning with errors over rings. Journal of the ACM, 2013, 60(6):43. [doi: 10.1145/2535925]

[13] Brakerski Z, Vaikuntanathan V. Fully homomorphic encryption from ring-LWE and security for key dependent messages. In: Proc. of the Advances in Cryptology (CRYPTO 2011). Berlin, Heidelberg: Springer-Verlag, 2011. 505−524. [doi: 10.1007/978-3-642-22792-9_29]

[14] Lyubashevsky V, Peikert C, Regev O. A toolkit for ring-LWE cryptography. In: Proc. of the Advances in Cryptology (EUROCRYPT 2013). Berlin, Heidelberg: Springer-Verlag, 2013. 35−54. [doi: 10.1007/978-3-642-38348-9_3]

[15] Shamir A. Identity-Based cryptosystems and signature schemes. In: Proc. of the Advances in Cryptology. Berlin, Heidelberg: Springer-Verlag,1985. 47−53. [doi: 10.1007/3-540-39568-7_5]

[16] Boneh D, Lynn B, Shacham H. Short signatures from the Weil pairing. In: Proc. of the Advances in Cryptology (ASIACRYPT 2001). Berlin, Heidelberg: Springer-Verlag, 2001. 514−532. [doi: 10.1007/3-540-45682-1_30]

[17] Cocks C. An identity based encryption scheme based on quadratic residues. In: Proc. of the Cryptography and Coding. Berlin, Heidelberg: Springer-Verlag, 2001. 360−363. [doi: 10.1007/3-540-45325-3_32]

[18] Gentry C, Peikert C, Vaikuntanathan V. Trapdoors for hard lattices and new cryptographic constructions. In: Proc. of the 40th Annual ACM Symp. on Theory of Computing. ACM Press, 2008. 197−206. [doi: 10.1145/1374376.1374407]

[19] Guang Y, Gu CX, Zhu YF, Zheng YH, Fei JL. Identity-Based fully homomorphic encryption from learning with error problem. Journal on Communications, 2014,35(2):111−117 (in Chinese with English abstract).

[20] Gentry C, Sahai A, Waters B. Homomorphic encryption from learning with errors: Conceptually-Simpler, asymptotically-faster, attribute-based. In: Proc. of the Advances in Cryptology (CRYPTO 2013). Berlin, Heidelberg: Springer-Verlag, 2013. 75−92. [doi: 10.1007/978-3-642-40041-4_5]

[21] Gentry C, Halevi S, Smart NP. Fully homomorphic encryption with polylog overhead. In: Proc. of the Advances in Cryptology (EUROCRYPT 2012). Berlin, Heidelberg: Springer-Verlag, 2012. 465−482. [doi: 10.1007/978-3-642-29011-4_28]

[22] Brakerski Z, Gentry C, Halevi S. Packed ciphertexts in LWE-based homomorphic encryption. In: Proc. of the Public-Key Cryptography (PKC 2013). Berlin, Heidelberg: Springer-Verlag, 2013. 1−13. [doi: 10.1007/978-3-642-36362-7_1]

[23] Gentry C, Halevi S, Smart NP. Homomorphic evaluation of the AES circuit. In: Proc. of the Advances in Cryptology (CRYPTO 2012). Berlin, Heidelberg: Springer-Verlag, 2012. 850−867. [doi: 10.1007/978-3-642-32009-5_49]

[24] Gentry C, Halevi S. Implementing Gentry's fully-homomorphic encryption scheme. In: Proc. of the EUROCRYPT 2011. 2011. 129−148. [doi:10.1007/978-3-642-20465-4_9]

附中文参考文献:

[19] 光焱,顾纯祥,祝跃飞,郑永辉,费金龙.利用容错学习问题构造基于身份的全同态加密体制.通信学报,2014,35(2):111−117.

康元基(1992－),男,辽宁凤城人,主要研究领域为全同态加密技术.

郑永辉(1976－),男,博士,讲师,主要研究领域为密码学.

顾纯祥(1976－),男,博士,副教授,主要研究领域为密码学.

光焱(1983－),男,博士,讲师,主要研究领域为密码学,网络信息安全.