利用 RLWE 构造基于身份的全同态加密体制

辛 丹[1],顾纯祥[1],郑永辉[2],光 焱[1],康元基[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)

摘 要: 全同态加密为云计算中数据全生命周期隐私保护等难题的解决都提供了新的思路. 公钥尺寸较大是现有全同态加密体制普遍存在的问题. 本文将基于身份加密的思想和全同态加密体制相结合,利用环上容错学习问题(Ring Learning With Errors,RLWE),其中将环的参数 m 扩展到任意正整数,提出了一种基于身份的全同态加密体制. 体制以用户身份标识作为公钥,在计算效率和密钥管理方面都具有优势,安全性在随机喻示模型下可规约为判定性 RLWE 问题难解性假设.

关键词: 全同态加密; 基于身份加密; 环上容错学习问题
中图分类号: TN918.1 **文献标识码:** A **文章编号:** 0372-2112 (2016)12-2887-07
电子学报 URL: http://www.ejournal.org.cn **DOI:** 10.3969/j.issn.0372-2112.2016.12.011

Identity-Based Fully Homomorphic Encryption from Ring Learning with Errors Problem

XIN Dan[1], GU Chun-xiang[1], ZHENG Yong-hui[2], GUANG Yan[1], KANG Yuan-ji[1]
(1. *Information Engineering University, Zhengzhou, Henan* 450002, *China*;
2. *State Key Laboratory of Mathematical Engineering and Advanced Computing, Wuxi, Jiangsu* 214125, *China*)

Abstract: Fully homomorphic encryption provides a new idea on the solution of many problems, such as the whole life cycle of data privacy protection on cloud computing. Currently, the existing fully homomorphic encryption schemes share a common flaw of large size public keys. We construct an identity-based fully homomorphic encryption which compromises the merits of both kinds of encryption from ring learning with errors to work in arbitrary cyclotomic rings. To make user's identity as the unique public key, our scheme has advantage in computational efficiency and key management. The security of our scheme strictly reduces to hardness of decision ring learning with problem solving in the random oracle model.

Key words: fully homomorphic encryption; identity-based; ring learning with errors

1 引言

全同态加密(fully homomorphic encryption)允许用户在不解密的情况下,对密文进行任意次的运算,从而得到相对应明文进行运算后加密的结果. 这种新型加密技术,为很多难题的解决都提供了新的思路,例如云计算的隐私保护问题、密文检索等. 2009 年,Craig Gentry[1]基于"理想格"(ideal lattice)成功构造出第一个真正意义上的全同态加密体制,这一成果使该领域研究取得突破性进展.

参考 Gentry 的设计模式和理念,学术界基于不同的代数结构和数学难题提出了一系列的同态加密算法[2~4],但现有体制公钥尺寸通常比较大,密钥的有效管理一直是体制应用面临的一个难题. 基于身份加密[5](identity-based encryption)利用用户的唯一身份标识(如 E-mail 地址等)作为公钥,用户私钥由可信第三方生成,具有不依赖公钥证书进行密钥管理的优势. 2010 年美密会上,Naccache[6]将基于身份的全同态加密体制设计列为待解决的重要问题之一.

Gentry 等人[7]基于格上容错学习问题[8](Learning With Errors,LWE)设计了一种基于身份的同态加密体制,仅支持有限次加法和一次乘法的同态运算. 文献

收稿日期:2015-04-09;修回日期:2015-06-29;责任编辑:梅志强
基金项目:河南省科技创新杰出青年基金(No. 134100510002);河南省基础与前沿技术研究(No. 142300410002);数学工程与先进计算国家重点实验室开放基金资助

[9]提出基于对偶 Regev 体制构造全同态加密体制,并借助对偶 Regev 体制的加解密密钥的特点实现基于身份加密,在计算效率上有所提升,但运算公钥(evaluation key)尺寸过大. 2013 年,Gentry 等人[10]提出了一种利用近似特征向量构造基于身份的全同态加密方案,并使满足一定条件的基于身份加密体制(如文献[11])增加全同态运算能力,但该方案密文扩张严重. 光焱等人[12]利用前像可采样陷门单向函数[11]提取私钥的方式和重线性化方法[13],设计了一个基于身份的全同态加密体制,简称 GZG14 体制. 但该体制不能进行多比特加密.

Brakerski 和 Vaikuntanathan[14]提出了一个基于环上容错学习问题的全同态加密体制. 以该体制为首的一些体制[15,16]在环的参数 m 的选择上更偏爱选用 $m=2^k$($n=m/2$ 仍然是 2 的方幂),此时多项式 $\Phi_m(X)=X^n+1$ 分布稀疏,模多项式运算可以高效得通过快速傅里叶变换技术[17](Fast Fourier Transform,FFT)进行. 但这一特点也导致了在相同安全级别下,由于 m 只能取 2 的方幂,体制公钥尺寸以及计算时间大都比实际需要高得多,并且这种多项式也影响了单指令多数据(Single Instruction Multiple Data,SIMD)技术[18]的运用. 但是当环的参数 m 取任意正整数时,分圆多项式是不规则的,分布较密集,且多项式系数较大,并且多项式模运算存在很大的扩张系数[19](expansion factor),从而影响体制加解密效率. Lyubashevsky 等人[20]提出的标准嵌入(canonical embedding)将分圆域上的元素映射成复数域上的向量,则域上元素的加法和乘法运算便转换成向量的逐比特计算. 同时,通过张量分解技术[21](tensorial decomposition)将分圆域分解为素数子域的张量积,多项式模运算可以转换到较简单的素数子域中进行.

本文根据 Gentry 等人[11]提出的前像可采样陷门单向函数,设计了环上基于身份的私钥提取算法,对每一个身份标识,生成对应的用户私钥,通过"密钥转换"技术使基于身份的半全同态加密体制实现多级(leveled)同态运算. 和一般全同态加密体制相比,无须使用公钥证书进行身份认证,能够有效克服公钥尺寸对于体制应用效率的影响. 与现有基于身份的全同态加密体制相比,本文体制可以进行多比特加密,支持 SIMD 技术. 最后,证明体制在随机喻示模型,判定性 RLWE 问题假设的前提下选择明文安全的(Chosen Plaintext Attack,CPA).

2 基础知识

2.1 符号说明及相关基础定义

对于正整数 k,$[k]$表示集合$\{0,1,\cdots,k-1\}$. 向量用粗体小写字母表示,且默认为列向量形式,例如 $\boldsymbol{a}$,向量 $\boldsymbol{a}$ 的第 i 个分量表示为 $\boldsymbol{a}^{(i)}$. 矩阵用粗体大写字母表示,例如 $\boldsymbol{A}^{n\times m}$,矩阵的第 i 行向量表示为 $\boldsymbol{A}_i$. 矩阵的第 i 行第 j 列元素记为 $\boldsymbol{A}_{i,j}$. 向量和矩阵的上标 T 表示其转置,如 $\boldsymbol{A}^{\mathrm{T}}$. n 维向量 $\boldsymbol{a}$ 和 m 维向量 $\boldsymbol{b}$ 张量积 $\boldsymbol{a}\otimes\boldsymbol{b}=(\boldsymbol{a}^{(1)}\boldsymbol{b}^{(1)},\cdots,\boldsymbol{a}^{(1)}\boldsymbol{b}^{(m)},\cdots,\boldsymbol{a}^{(n)}\boldsymbol{b}^{(1)},\cdots,\boldsymbol{a}^{(n)}\boldsymbol{b}^{(m)})^{\mathrm{T}}$. 向量 $\boldsymbol{a}$ 的长度定义为向量的欧几里得范数$\|\boldsymbol{a}\|=\left(\sum_i(\boldsymbol{a}^{(i)})^2\right)^{1/2}$. 表 1 描述了本文所需要代数结构.

表 1 代数结构的描述

符号	描述及性质
$m,n,\hat{m},\mathbb{Z}_m^*$	分圆多项式次数 $n=\varphi(m)$,m 的素数幂分解式为 $m=\prod_l m_l$,当 m 是偶数时,$\hat{m}=m/2$,否则 $\hat{m}=m$,$\mathbb{Z}_m^*$ 是所有小于 m 且与 m 互素的正整数集合.
ζ_m,ω_m	$\zeta_m\in K,\omega_m\in\mathbb{C}$ 都为 m 次本原单位根.
$K=\mathbb{Q}(\zeta m)\cong\mathbb{Q}(X)/\Phi_m(X)\cong\otimes_l\mathbb{Q}(\zeta_{m_l})$	分圆数域 K,其中 $\Phi_m(X)=\prod_{i\in\mathbb{Z}_m^*}(X-\omega_m^i)\in\mathbb{Z}[X]$ 是分圆多项式,K 同构于素数子域$\mathbb{Q}(\zeta_{m_l})$的张量积.
$K_{\mathbb{R}}$	添加 ζ_m 到实数域$\mathbb{R}$,且满足 $K_{\mathbb{R}}=K\otimes\mathbb{R}$.
$\sigma_i:K\to\mathbb{C},i\in\mathbb{Z}_m^*$	K 到$\mathbb{C}$的环同态 σ_i,取 $i\in\mathbb{Z}_m^*$,$\sigma_i(\zeta_m)=\omega_m^i$.
$R=\mathbb{Z}(\zeta_m)\cong\mathbb{Z}[X]/\Phi_m(X)\cong\otimes_l\mathbb{Z}(\zeta_{m_l})$	R 是 K 的代数整数环,且同构于子环$\mathbb{Z}(\zeta_{m_l})$的张量积.
$\mathrm{Tr}(\cdot):K\to\mathbb{Q}$	K 到$\mathbb{Q}$的迹函数,取 $a\in K$,$\mathrm{Tr}(a)=\sum_i\sigma_i(a)$.
$R^\vee,R^\vee=\langle t^{-1}\rangle,g,t\in R$	R 的对偶 $R^\vee=\{a\in K:\mathrm{Tr}_{K/\mathbb{Q}}(aR)\subseteq\mathbb{Z}\}$,$t^{-1}$生成 R 的对偶分式理想,其中 $t^{-1}=g/\hat{m}$,$g=\prod_p(1-\zeta_p)\in R$,其中 p 所有能整除 m 的奇素数.
$\boldsymbol{p},\boldsymbol{p}',\boldsymbol{d}$	K 上幂基(power basis)为 $\boldsymbol{p}=(\zeta_m^j)_{j\in[n]}=(1,\zeta_m,\cdots,\zeta_m^{n-1})\in K^{[n]}$,$K$ 上张量幂基(powerful basis)为 $\boldsymbol{p}'=\otimes_l\boldsymbol{p}_l'$,$p_l'$ 是对应 $K_l=\mathbb{Q}(\zeta_{m_l})$的张量幂基;$\tau(\cdot):\zeta_m\to\zeta_m^{-1}$,$R^\vee$ 上分解基(decoding basis)为 $\boldsymbol{d}=\otimes_l\tau(\boldsymbol{p}'_l)^\vee$.

定理 1[21]　分解基有如下两条性质:(1)它的最大特征值 $s_1(\boldsymbol{d})=\sqrt{r'(m)/m}$,其中 $r'(m)$ 是所有能整除 m 的素数的乘积,$s_1(\boldsymbol{d})$ 的最大值为 1;(2)对于任意的元素 $a\in(R^\vee)^k$,都可以表示为 $a=\langle \hat{m}^{1-k}\boldsymbol{d},\boldsymbol{a}\rangle$,根据柯西-施瓦茨不等式,则对于 $\boldsymbol{a}^{(i)}$ 的绝对值存在关系式 $|\boldsymbol{a}^{(i)}|\leqslant\|a\|\hat{m}^{k-1}\sqrt{n}$.

2.2　RLWE 问题

Lyubashevsky 等人[21]给出了环 R 上理想格最坏情况下最短向量近似问题(worst-case approximate Shortest Vector Problem,SVP)到计算性环上容错学习问题的量子规约,接着给出了计算性环上容错学习问题到判定性环上容错学习问题(Decision Ring Learning With Errors,DRLWE)的一般性规约.

定义 2(RLWE 分布)

对于 $s\in R_q^\vee$(或者 $R^\vee$),$K_{\mathbb{R}}$上的分布 ψ,其中,$K_{\mathbb{R}}=K\otimes\mathbb{R}$,定义一个 $R_q\times(K_{\mathbb{R}}/qR^\vee)$ 上的 RLWE 分布 $A_{s,\psi}$,其变量是$(a,b=a\cdot s+e \bmod qR^\vee)$的形式,其中 a 取自 R_q 上的均匀分布,e 取自分布 ψ.

定义 3(RLWE 问题)

Ψ 是 $K_{\mathbb{R}}$上的一组分布,对于任意的一些 $s\in R_q^\vee$,分布 $\psi\in\Psi$,$\mathrm{RLWE}_{q,\Psi}$定义为:从 $A_{s,\psi}$分布上取一组相互独立的变量,求解其中包含的值 s.

定义 4(DRLWE 问题)

平均情况下判定性 RLWE 问题记为 $\mathrm{DRLWE}_{q,\psi}$,其定义为:均匀随机选取 $s\leftarrow R_q^\vee$,以不可忽略的优势区分相同数量的两组变量,两组变量分别取自分布 $A_{s,\psi}$和 $R_q\times(K_{\mathbb{R}}/qR^\vee)$上的均匀分布.

定理 5(DRLWE 问题难解性假设)

令 $\alpha=\alpha(n)>0$,$q=q(n)\geqslant 2$,素数 $q=1 \bmod m$ 且满足 $\alpha q\geqslant\omega(\sqrt{\log n})$. 若存在一个多项式时间算法解决每组 l 个变量的 $\mathrm{DRLWE}_{n,l,q,\psi}$问题,则存在一个有效算法解决 K 上理想格参数为 $\widetilde{O}(\sqrt{n}/\alpha)$的近似 SVP 问题,其中,$\psi$ 取自 $D_{\xi q}$,$\xi=\alpha\cdot(nl/\log(nl))^{1/4}$.

利用 RLWE 问题构造实际体制时,ψ 通常取错误分布 $\chi=\lfloor p\cdot\psi\rceil_{\omega+pR^\vee}$,其中,$p$ 与 q 互素,$\omega\in R_p^\vee$. 则 $\mathrm{DRLWE}_{n,l,q,\chi}$问题两组变量分别取自分布 $A_{s,\chi}$和 $R_q\times R_q^\vee$ 上的均匀分布,问题的困难性不变[21].

$\lfloor\cdot\rceil$表示连续高斯分布的离散化. 设空间 $H=\{\boldsymbol{x}\in\mathbb{C}^{\mathbb{Z}_m^*}:\boldsymbol{x}^{(i)}=\overline{\boldsymbol{x}^{(m-i)}},\forall i\in\mathbb{Z}_m^*\}$,格基 $\boldsymbol{B}=\{\boldsymbol{b}_j\}$ 生成格 $\Lambda=L(\boldsymbol{B})$. 取点 $\boldsymbol{x},\boldsymbol{c}\in H$,计算 $\boldsymbol{y}\leftarrow\lfloor\boldsymbol{x}\rceil_{\Lambda+\boldsymbol{c}}$,分为以下 4 步:(1)生成格 Λ 的陪集 $\Lambda+\boldsymbol{c}'$,$\boldsymbol{c}'=\boldsymbol{c}-\boldsymbol{x}$;(2)将 $\boldsymbol{c}'$表示成 $\boldsymbol{c}'=\sum_i a_i\boldsymbol{b}_i \bmod \Lambda$,$a_i\in[0,1)$,随机选取一组相互独立的值 $f_i\in\{a_i-1,a_i\}$;(3)计算 $f=\sum_i f_i\boldsymbol{b}_i\in\Lambda+\boldsymbol{c}'$;(4)输出向量 $\boldsymbol{y}=\boldsymbol{x}+\boldsymbol{f}$.

$\chi=\lfloor p\cdot\psi\rceil_{\omega+pR^\vee}$分布是通过连续高斯分布 $p\cdot\psi$ 上的点离散到 $pR^\vee$的陪基上生成的. 由于分解基的最大特征值至多为 1,在离散化过程中对高斯分布参数影响较小,所以当噪声取自 $R^\vee$时,一般选择分解基进行高斯采样.

2.3　前像可采样陷门单向函数

文献[12]给出了一般格上的前像可采样陷门单向函数,将离散正态分布映射到近似均匀分布上,且满足在拥有陷门的情况下,能够从近似均匀分布上将原始离散正态分布恢复出来. 首先给出陷门的生成方式.

命题 6　对于 $n\in\mathbb{N}^*$,素数 $q=q(n)$,$l\geqslant 5n\log q$,存在算法 $\mathrm{TrapGen}(1^n)$,输入参数为 1^n,可以在多项式时间内输出$(\boldsymbol{A},S)$. 其中,矩阵 $\boldsymbol{A}$ 在 $\mathbb{Z}_q^{n\times l}$ 上均匀分布,向量集合

$$S\subset\Lambda^\perp(\boldsymbol{A},q)=\{\boldsymbol{e}\in\mathbb{Z}_q^l:\boldsymbol{A}\cdot\boldsymbol{e}=\boldsymbol{0} \bmod q\} \quad (1)$$

是满秩的,且$\|S\|\leqslant l^{2.5}$.

在命题 6 的基础上定义函数 f_A:

定义 7(前像可采样陷门单向函数)

对于算法 $\mathrm{TrapGen}(1^n)$生成的矩阵 $\boldsymbol{A}$,定义函数 f_A:$\mathbb{Z}_q^l\rightarrow\mathbb{Z}_q^n$ 为 $f_A(\boldsymbol{e})=\boldsymbol{A}\cdot\boldsymbol{e} \bmod q$,向量 $\boldsymbol{e}\leftarrow D_{\mathbb{Z}_q^l,r}$,参数 $r\geqslant\omega(\sqrt{\log l})$. 在拥有陷门的情况下,函数 f_A 是可逆的,逆函数是 $f_A^{-1}:\mathbb{Z}_q^n\rightarrow\mathbb{Z}_q^l$. 任意选取 $\boldsymbol{u}\in\mathbb{Z}_q^n$,向量 $\boldsymbol{e}$ 计算步骤如下:(1)计算满足等式 $\boldsymbol{A}\cdot\boldsymbol{t}=\boldsymbol{u} \bmod q$ 的特解 $\boldsymbol{t}$;(2)利用陷门 S 进行前像采样,求得分布 $D_{\Lambda^\perp,r,-\boldsymbol{t}}$上的向量 $\boldsymbol{v}$;(3)输出 $\boldsymbol{e}=\boldsymbol{t}+\boldsymbol{v}$.

命题 8(f_A 陷门单向性)　若函数 f_A 规约到非齐次小整数解问题难解性,则是一个前像可采样陷门单向函数,即式(1)对于输入 $\boldsymbol{e}\leftarrow D_{\mathbb{Z}_q^l,r}$,函数输出向量的概率分布与 $\mathbb{Z}_q^n$ 上的均匀分布不可区分;(2)在陷门 S 的作用下,逆函数 $f_A^{-1}(\boldsymbol{u})$输出向量 $\boldsymbol{e}'$服从分布 $D_{\mathbb{Z}_q^l,r}$,且满足 $\boldsymbol{A}\cdot\boldsymbol{e}'=\boldsymbol{u} \bmod q$.

3　基于身份的全同态加密体制模型

本小节根据光焱等人提出的基于身份的全同态加密体制模型[13],该模型结合了基于身份加密和全同态加密两种特点. 在格上构造一般全同态加密体制时,密钥生成的顺序是首先随机选择私钥,然后根据格上困难(例如 LWE 问题)计算生成用户公钥. 而在基于身份加密体制中,公私钥对的产生顺序恰好相反,首先根据身份标识 id 得到公钥 $\mathrm{pk}_{\mathrm{id}}$,随后以 id 或 $\mathrm{pk}_{\mathrm{id}}$作为私钥提取算法的输入,计算出相应的身份私钥. 例如,文献[12]提出了一种格上基于身份的公钥加密体制,通过引入哈希函数和前像可采样陷门单向函数,分别实现从身份信息到公钥的转换以及提取私钥的功能.

定义 9(基于身份的全同态加密体制模型)

基于身份的全同态加密体制 IBFHE 由 5 个算法组

成,分别是初始化、私钥提取、加密、解密和密文运算,即 IBFHE = {Setup, Extract, Enc, Dec, Eval}.

初始化算法 Setup:输入安全参数 1^λ,算法输出加密体制的一对公开参数 param、主私钥 msk.

私钥提取算法 Extract:输入公开参数 param、主私钥 msk 和身份标识 id,为每一个身份标识 id 输出一个身份私钥 $\mathrm{sk}_{\mathrm{id}}$.

加密算法 Enc:输入公开参数 param、身份标识 id 和明文消息 μ,输出与身份标识 id 相关的密文 c.

解密算法 Dec:输入与身份标识 id 相关的密文 c 和 id 对应的身份私钥 $\mathrm{sk}_{\mathrm{id}}$,输出明文消息 μ.

密文运算算法 Eval:输入运算 $f:\{0,1\}^t\to\{0,1\}$ 和属于同一身份标识 id 加密的一组密文 $c_1,c_2,\cdots,c_t$,输出新的密文 c,且满足 $\mathrm{Dec}_{\mathrm{sk}_{\mathrm{id}}}(c)=f(\mathrm{Dec}_{\mathrm{sk}_{\mathrm{id}}}(c_1),\cdots,\mathrm{Dec}_{\mathrm{sk}_{\mathrm{id}}}(c_t))$.

定义 10(基于身份的全同态加密体制的 IND-CPA 安全性)

由于密文同态运算属性,因此任何全同态加密体制都不可能抵抗适应性选择密文攻击(CCA2),IBFHE 体制采用传统的选择明文攻击下的不可区分性(IND-CPA). IND-CPA 攻击游戏如下:

初始化:挑战者 C 调用 IBFHE. Setup 算法,输出体制的公开参数 param 和主私钥,将 param 交给攻击者 A.

阶段 1:A 任意选择身份标识 $\mathrm{id}_i\in\{0,1\}^*$ 访问私钥提取喻示,得到对应的私钥 $\mathrm{sk}_{\mathrm{id}_i}$,并将 id_i 加入到身份列表 P.

挑战过程:阶段 1 完成后,A 选择一个挑战身份 $\mathrm{id}^*\notin P$,以及两个长度相等的挑战明文 $\{\mu_0^*,\mu_1^*\}$,交给挑战者 C. C 随机选择 $b\in\{0,1\}$,调用加密算法 IBFHE. Enc,输入身份标识 id^*、挑战明文 μ_b^*,输出密文 $c^*=\mathrm{IBFHE.Enc}(\mathrm{id}^*,\mu_b^*)$,交给攻击者 A.

阶段 2:攻击者 A 自由选择身份 $\mathrm{id}'\in\{0,1\}^*$,要求 $\mathrm{id}'\neq\mathrm{id}^*$,获得相应的私钥 $\mathrm{sk}_{\mathrm{id}'}$.

猜测过程:A 猜测目标密文 c^* 所对应的明文,输出猜测结果 b',若 $b'=b$,则攻击者在游戏中获胜.

攻击者在游戏中获胜的概率为 $\Pr|\mathrm{Adv}_{\mathrm{Game}}[\mathrm{A}]|$,其优势为 $\mathrm{Adv}_{\mathrm{CPA}}[\mathrm{A}]=|\Pr|\mathrm{Adv}_{\mathrm{Game}}[\mathrm{A}]|-1/2|$,若对于任意一个多项式时间的 A,$\mathrm{Adv}_{\mathrm{CPA}}[\mathrm{A}]$ 可忽略,则该体制是 IND-CPA 安全的.

4 体制构造

4.1 基础同态加密体制

设 λ 为安全参数,$q=q(n)\geqslant 2$,m 次分圆数域 $K=\mathbb{Q}(\zeta_m)$,$R=\mathbb{Z}(\zeta_m)$,令 $n=\varphi(m)$,$R_q=R/qR$,张量幂基 $\boldsymbol{p}$. 哈希函数 $\mathrm{H}:\{0,1\}^*\to\mathbb{Z}_q^{n\times n}$,当 m 是偶数,$\hat{m}=m/2$,否则 $\hat{m}=m$. 构造体制如下:

初始化算法 IBSHE. Setup(1^λ):输入安全参数 1^λ,根据命题 6 生成矩阵 $\boldsymbol{A}\in\mathbb{Z}_q^{n\times l}$ 及其陷门 $S\subset\Lambda^\perp(\boldsymbol{A},q)$,分别作为体制的公开参数 param 和主私钥 msk.

私钥生成算法 IBSHE. Extract($\boldsymbol{A},S,\mathrm{id}$):输入公开参数 param、身份标识 id,$\boldsymbol{U}=\mathrm{H}(\mathrm{id})\in\mathbb{Z}_q^{n\times n}$,$\boldsymbol{U}=\{\boldsymbol{u}_1,\cdots,\boldsymbol{u}_n\}$,该矩阵的概率分布与 $\mathbb{Z}_q^{n\times n}$ 上的均匀随机分布统计不可区分,利用陷门 S 对 $\boldsymbol{u}_i$ 进行前像采样,得到 $\boldsymbol{e}_i=f_A^{-1}(\boldsymbol{u}_i)$,$\boldsymbol{E}=(\boldsymbol{e}_1,\cdots,\boldsymbol{e}_n)\in\mathbb{Z}_q^{l\times n}$,输出私钥 $\boldsymbol{e}=\boldsymbol{E}\boldsymbol{p}\in R_q^l$.

加密算法 IBSHE. Enc($\boldsymbol{A},\mathrm{id},\mu$):输入公钥 mpk、身份标识 id、明文消息 $\mu\in R_p$,哈希身份标识 id,计算 $\boldsymbol{U}=\mathrm{H}(\mathrm{id})\in\mathbb{Z}_q^{n\times n}$,$u=\boldsymbol{p}^{\mathrm{T}}\boldsymbol{U}\boldsymbol{p}\in R_q$,选择噪声 $\boldsymbol{X}^{(0)},\cdots,\boldsymbol{X}^{(l)}\leftarrow\lfloor p\cdot\psi\rceil_{pR^\vee}$,$\boldsymbol{x}=(\boldsymbol{x}^{(i)})_{i\in[l]}$,并且随机选择“小”多项式 $r\leftarrow R_q$(即多项式系数 $\{0,\pm 1\}$). 选择噪声 $\boldsymbol{x}\leftarrow\lfloor p\cdot\psi\rceil_{t^{-1}\mu+pR^\vee}$,计算 $\rho=ru+x\in R^\vee$,$\boldsymbol{v}=-r\boldsymbol{p}^{\mathrm{T}}\boldsymbol{A}+p\boldsymbol{x}\in R_q^l$,输出 $c=(\rho,\boldsymbol{v})$.

解密算法 IBSHE. Dec($c,\boldsymbol{e}$):输入密文 c、私钥 $\boldsymbol{e}$,计算 $x=(\rho+\boldsymbol{v}\boldsymbol{e})\bmod p$,输出明文消息 $\mu=t\cdot x \bmod pR$.

有两个明文消息 $\mu,\mu'\in R_p$,噪声 $x\leftarrow\lfloor p\cdot\psi\rceil_{t^{-1}\mu+pR^\vee}$,$x'\leftarrow\lfloor p\cdot\psi\rceil_{t^{-1}\mu'+pR^\vee}$,加密结果分别为 $c=(\rho,\boldsymbol{v})$,$c'=(\rho',\boldsymbol{v}')$. 对应变量 Y 的多项式分别为 $c(Y)=\rho+\boldsymbol{v}Y$,$c'(Y)=\rho'+\boldsymbol{v}'Y$.

同态加法 IBSHE. Add:

$$c(Y)+c'(Y)=\rho+\boldsymbol{v}Y+\rho'+\boldsymbol{v}'Y=\rho+\rho'+(\boldsymbol{v}+\boldsymbol{v}')Y \tag{2}$$

将私钥 $\boldsymbol{e}$ 代入:

$$\begin{aligned}\mathrm{Dec}_e[c(Y)+c'(Y)]&=\rho+\boldsymbol{v}\boldsymbol{e}+\rho'+\boldsymbol{v}'\boldsymbol{e}\\&=x+x'+p\boldsymbol{x}\boldsymbol{e}+p\boldsymbol{x}'\boldsymbol{e}\end{aligned} \tag{3}$$

令噪声 $\tilde{x}=x+x'+p\boldsymbol{x}\boldsymbol{e}+p\boldsymbol{x}'\boldsymbol{e}\in R^\vee$,则根据定义 2 中分解基的性质 $|\boldsymbol{a}^{(i)}|\leqslant\|a\|\hat{m}^{k-1}\sqrt{n}$,此时 $\hat{m}^{k-1}=1$,只要 $\|x+x'+p\boldsymbol{x}\boldsymbol{e}+p\boldsymbol{x}'\boldsymbol{e}\|<q/(2\sqrt{n})$,则解密正确,再对结果模 p,得到 $x+x'$,明文消息 $\mu+\mu'=t\cdot(x+x')\bmod pR$.

同态乘法 IBSHE. Mult:

$$\begin{aligned}c(Y)\cdot c'(Y)&=(\rho+\boldsymbol{v}Y)\times(\rho'+\boldsymbol{v}'Y)\\&=\rho\rho'+(\rho\boldsymbol{v}'+\rho'\boldsymbol{v})Y+\boldsymbol{v}Y\boldsymbol{v}'Y\end{aligned} \tag{4}$$

将私钥 $\boldsymbol{e}$ 代入:

$$\begin{aligned}\mathrm{Dec}_e[c(Y)\cdot c'(Y)]&=(ru+x-r\boldsymbol{p}^{\mathrm{T}}\boldsymbol{A}\boldsymbol{e}+p\boldsymbol{x}\boldsymbol{e})\\&\quad\times(r'u+x'-r'\boldsymbol{p}^{\mathrm{T}}\boldsymbol{A}\boldsymbol{e}+p\boldsymbol{x}'\boldsymbol{e})\\&=x\cdot x'+2p^2\boldsymbol{x}\boldsymbol{e}\boldsymbol{x}'\boldsymbol{e}+xp\boldsymbol{x}'\boldsymbol{e}+x'p\boldsymbol{x}\boldsymbol{e}\end{aligned} \tag{5}$$

令 $e'=x\cdot x'+2p^2\boldsymbol{x}\boldsymbol{e}\boldsymbol{x}'\boldsymbol{e}+xp\boldsymbol{x}'\boldsymbol{e}+x'p\boldsymbol{x}\boldsymbol{e}\in(R^\vee)^2$,与上述分析方法类似,根据性质 $|\boldsymbol{a}^{(i)}|\leqslant\|a\|\hat{m}^{k-1}\sqrt{n}$,只要

$\|e'\| < q/(2\hat{m}\sqrt{n})$,则解密正确. 再对结果模 p,得到 $x \cdot x'$,恢复明文 $\mu\mu' = t^2 \cdot (x \cdot x') \bmod pR$. 经过一次同态乘法,密文 $c_{\text{mult}} = (\rho\rho', \rho\boldsymbol{v}' + \rho'\boldsymbol{v}, \boldsymbol{v} \otimes \boldsymbol{v}')$.

4.2　密钥转换技术

通过一次同态乘法,密文向量维数从 $l+1$ 增加到 l^2+l+1,可以预见,随着同态乘法的继续进行,密文元素乘指数增长,下面介绍密钥转换技术可以使密文的元素个数保持不变.

令 $I = (R^\vee)^2$,同态乘法的密文向量为 $\boldsymbol{c} = I_q^j$,$\boldsymbol{s} = (1, \boldsymbol{e}, \boldsymbol{e} \otimes \boldsymbol{e}) \in R_q^j$,在模 p 意义下,存在关系式 $\langle \boldsymbol{c}, \boldsymbol{s} \rangle = e \bmod qI$, $e \leftarrow t^{-2}\mu + pI$. 令 $b = \lceil \log q \rceil$, $j = l^2 + l + 1$,取向量 $\boldsymbol{g} = (1, 2, 4, \cdots, 2^{b-1}) \in \mathbb{Z}_q^b$, $\boldsymbol{G} = \boldsymbol{I} \otimes \boldsymbol{g}^{\mathrm{T}} \in \mathbb{Z}_q^{j \times bj}$,其中 $\boldsymbol{I}$ 为单位矩阵. 选取转换私钥 $\boldsymbol{s}' \leftarrow R_q^l$. 密钥转换技术分为以下 4 步进行:

(1)给关系式 $\langle \boldsymbol{c}, \boldsymbol{s} \rangle = e \bmod qI$ 乘因式 $\hat{m}$,则 $\langle t \cdot \hat{m} \cdot \boldsymbol{c}, t^{-1}\boldsymbol{s} \rangle = \hat{m} \cdot e \bmod qR^\vee$;

(2)令 $\boldsymbol{y} = t \cdot \hat{m} \cdot \boldsymbol{c} \in R_q^j$,使用逐项舍入算法计算 $\boldsymbol{x}$,满足 $\boldsymbol{G}\boldsymbol{x} = \boldsymbol{y} \in R_q^j$;

(3)对于 $i \in [bj]$, $\boldsymbol{\rho} = (\boldsymbol{\rho}^{(i)})_{i \in [bj]}$, $\boldsymbol{V} = (\boldsymbol{v}_1, \cdots, \boldsymbol{v}_{bj})$,计算 IBSHE. $\mathrm{Enc}(\boldsymbol{A}, \mathrm{id}, 0) = (\boldsymbol{\rho}^{(i)}, \boldsymbol{v}_i)$,并满足 $c(\boldsymbol{s}') \bmod p = \boldsymbol{f}^{(i)} \leftarrow \lfloor p \cdot \psi \rceil_{pR^\vee}$, $\boldsymbol{f} = (\boldsymbol{f}^{(i)})_{i \in [bj]}$,且 $\langle \boldsymbol{x}, \boldsymbol{f} \rangle$ 足够小;

(4)引入辅助信息 $\delta = (\boldsymbol{h}^{(i)}, \boldsymbol{v}_i)_{i=0}^{[bj]}$, $\boldsymbol{h}^{(i)} = \boldsymbol{\rho}^{(i)} + (t^{-1}\boldsymbol{G}\boldsymbol{s})^{(i)} \bmod qR^\vee$. 设转换后密文 $(\rho', \boldsymbol{v}')$, $\boldsymbol{v}' = \boldsymbol{x}\boldsymbol{V}$, $\rho' = \sum_{i \in [bj]} \boldsymbol{h}^{(i)}\boldsymbol{x}^{(i)} = \langle \boldsymbol{x}, \boldsymbol{\rho} \rangle + \langle \boldsymbol{x}, t^{-1}\boldsymbol{G}^{\mathrm{T}}\boldsymbol{s} \rangle$,将转换私钥 $\boldsymbol{s}'$ 代入 $c(Y)$:

$$\begin{aligned} c(\boldsymbol{s}') &= \rho' + \boldsymbol{v}'\boldsymbol{s}' \\ &= \langle \boldsymbol{x}, \boldsymbol{\rho} \rangle + \langle \boldsymbol{x}, t^{-1}\boldsymbol{G}^{\mathrm{T}}\boldsymbol{s} \rangle + \boldsymbol{x}\boldsymbol{V}\boldsymbol{s}' \bmod p \\ &= \langle \boldsymbol{x}, \boldsymbol{f} \rangle + \langle \boldsymbol{x}, t^{-1}\boldsymbol{G}^{\mathrm{T}}\boldsymbol{s} \rangle \\ &= \langle \boldsymbol{x}, \boldsymbol{f} \rangle + \hat{m} \cdot e \bmod qR^\vee \end{aligned} \tag{6}$$

噪声 $e^* = \langle \boldsymbol{x}, \boldsymbol{f} \rangle + \hat{m} \cdot e \in R^\vee$, $\langle \boldsymbol{x}, \boldsymbol{f} \rangle$ 足够小,恢复明文消息 $g \cdot \mu = t \cdot \hat{m} \cdot e \bmod pR$.

4.3　基于身份的全同态加密体制

初始化算法 IBFHE. $\mathrm{Setup}(1^\lambda, 1^L)$:输入安全参数 λ,以及电路层数 L. 调用 IBFHE. $\mathrm{Setup}(1^\lambda)$ 算法输出公开参数 param,主私钥 msk.

私钥生成算法 IBFHE. $\mathrm{Extract}(\boldsymbol{A}, S, \mathrm{id})$:调用算法 IBSHE. $\mathrm{Extract}(\boldsymbol{A}, S, \mathrm{id})$ 输出私钥 $\boldsymbol{e}$. 设 $\boldsymbol{e}_0 = \boldsymbol{e}$,在 R_q^l 中均匀随机选择其余 L 个向量 $\boldsymbol{e}_1, \boldsymbol{e}_2, \cdots, \boldsymbol{e}_L$. 令 $\boldsymbol{s}_i = (1, \boldsymbol{e}_i, \boldsymbol{e}_i \otimes \boldsymbol{e}_i)$,按照 4.2 节计算身份标识 id 对应的运算密钥 $\mathrm{evk}_{\mathrm{id}} = \{\delta_{i \to i+1}\}_{i=0}^{L}$,存储 $(\mathrm{id}, \{\boldsymbol{e}_0, \boldsymbol{e}_1, \boldsymbol{e}_2, \cdots, \boldsymbol{e}_L\})$,将 $\mathrm{evk}_{\mathrm{id}}$ 公开.

加密算法 IBFHE. $\mathrm{Enc}(\boldsymbol{A}, \mathrm{id}, \mu)$:利用 R-IBSHE. $\mathrm{Enc}(\boldsymbol{A}, \mathrm{id}, \mu)$,输出得到初始密文 $c = (\rho, \boldsymbol{v})$,使用额外的信息来标识密文所处的电路层,例如 $c_i = (\rho_i, \boldsymbol{v}_i, i)$,其中 i 表示密文所处的层级.

解密算法 IBFHE. $\mathrm{Dec}(c_i, \boldsymbol{e}_i)$:对于密文 $c_i = (\rho_i, \boldsymbol{v}_i, i)$,私钥为 $\boldsymbol{e}_i$ 由密文所在的层级决定,计算 $x_i = (\rho_i + \boldsymbol{v}_i\boldsymbol{e}_i) \bmod p$,恢复明文消息 $\mu = t^i \cdot x_i \bmod pR$.

密文运算算法 IBFHE. $\mathrm{Eval}(f, c_1, \cdots, c_t, \mathrm{evk}_{\mathrm{id}})$:任意 f 运算都可以表示为同态乘法与任意次的加法运算的组合形式. 同态加法直接调用 IBSHE. Add 算法. 在进行同态乘法时,必须先获得此层级的运算密钥 $\delta_{i \to i+1}$,再调用 IBSHE. Mult 算法进行运算.

5　体制分析

5.1　正确性与安全性分析

体制正确性分析如下:对于密文 $c_i = (\rho_i, \boldsymbol{v}_i, i)$ 而言,对应的私钥为 $\boldsymbol{e}_i$,记变量 Y 的多项式 $c(Y) = \rho_i + \boldsymbol{v}_i Y$,则解密过程可看作 $c(\boldsymbol{e}_i) = \rho_i + \boldsymbol{v}_i\boldsymbol{e}_i = x_i + p\hat{x}_i$, $\hat{x}_i$ 根据层级 k 而有所不同,当 $i = 0$ 时, $\hat{x}_i = \boldsymbol{x}\boldsymbol{e}_0$. 只要满足条件

$$q > 2\|x_i + p\hat{x}_i\|\hat{m}^{k-1}\sqrt{n} \tag{7}$$

则解密正确,$c(\boldsymbol{e}_i)$ 模 p 得到噪声 x_i,利用 $\mu = t^i \cdot x_i \bmod pR$ 恢复出明文.

定理 11　设 $m = \lambda$, $n = \varphi(m)$, $q = \mathrm{poly}(n) \geqslant 2$, $l \geqslant 5n\log q$,在随机喻示模型,$\mathrm{DRLWE}_{n,l,q,\chi}$ 问题假设的前提下 IBFHE 体制是 IND-CPA 安全的.

证明　使用基于游戏的证明方法,用 $\mathrm{Adv}_{\mathrm{Game}}[\mathrm{A}]$ 来定义攻击者 A 在下列游戏中的优势.

Game 0:Game 0 即标准的 IND-CPA 游戏,攻击者 A 选择一个挑战身份 id^*,以及从明文空间中随机选择两个挑战明文 $\{\mu_0^*, \mu_1^*\}$,交给挑战者 C. C 计算对应的运算密钥 $\mathrm{evk}_{\mathrm{id}^*}$,并加密生成挑战密文 c^*,将其交给攻击者 A. A 猜测 c^* 所对应的明文,A 的优势记为:

$$\begin{aligned} &\mathrm{Adv}_{\mathrm{CPA}}[\mathrm{A}] = \\ &|\Pr[\mathrm{A}(\mathrm{id}^*, \mathrm{IBFHE.Enc}(\boldsymbol{A}, \mathrm{id}^*, \mu_0^*) = 1] - \\ &\Pr[\mathrm{A}(\mathrm{id}^*, \mathrm{IBFHE.Enc}(\boldsymbol{A}, \mathrm{id}^*, \mu_1^*) = 1]| \end{aligned} \tag{8}$$

Game 1:Game 1 改变 Game 0 加密过程中 $\mathrm{H}(\mathrm{id}^*)$ 的生成方式. Game 1 中 $\mathrm{H}(\mathrm{id}^*)$ 不再从随机喻示模型下 $\mathrm{H}(\cdot)$ 的访问列表中获得,而从 $\mathbb{Z}_q^{n \times n}$ 中均匀随机选取. 攻击者 A 无法区分 Game 0 与修改后的 Game1,因此:

$$|\mathrm{Adv}_{\mathrm{Game1}}[\mathrm{A}] - \mathrm{Adv}_{\mathrm{CPA}}[\mathrm{A}]| = 0 \tag{9}$$

Game 2:Game 2 与 Game 1 基本相同,区别是运算密钥 $\mathrm{evk}_{\mathrm{id}^*}$ 的生成方式,在 Game 2 中不再计算 $\mathrm{evk}_{\mathrm{id}} = \{\delta_{i \to i+1}\}_{i=0}^{L}$ 作为运算密钥,挑战者 C 从 R_q^{bj} 中均匀随机抽取一组 $\mathrm{evk}_{\mathrm{id}^*}$ 交给攻击者 A. 故 A 在 Game2 与 Game1 中优势的差值等于攻击者 A 成功解决 L 个 $\mathrm{DRLWE}_{n,bj,q,\chi}$ 实例中至少一个的概率:

$$|\mathrm{Adv}_{\mathrm{Game2}}[\mathrm{A}]-\mathrm{Adv}_{\mathrm{Game1}}[\mathrm{A}]| =1-\prod_{i=0}^{L}(1-\mathrm{Adv}_{\mathrm{DRLWE}_{n,lj,q,\chi}}[\mathrm{A}_i]) \tag{10}$$

Game 3:Game 3 与 Game 2 的区别在于加密算法,密文中 $\boldsymbol{v}$ 不通过 $\boldsymbol{v}=-r\boldsymbol{p}^{\mathrm{T}}\boldsymbol{A}+p\boldsymbol{x}$ 进行计算,而是从 R_q^l 中随机均匀选取. Game 3 和 Game 2 中 A 优势的差值等于其解决 $\mathrm{DRLWE}_{n,l,q,\chi}$ 问题的优势:

$$|\mathrm{Adv}_{\mathrm{Game3}}[\mathrm{A}]-\mathrm{Adv}_{\mathrm{Game2}}[\mathrm{A}]|=\mathrm{DRLWE}_{n,l,q,\chi}\mathrm{Adv}[\mathrm{A}] \tag{11}$$

Game 4:改变 Game 3 中的密文生成方式,不再计算 $c^*=(\rho,\boldsymbol{v})$,挑战密文在 $R_q\times R_q^l$ 随机均匀选择. 此 Game 中公钥 u 是从 R_q 中均匀选取的,因此 $\rho=ru+x\in R^{\vee}$ 是 $\mathrm{DRLWE}_{n,1,q,\chi}$ 问题实例,即

$$|\mathrm{Adv}_{\mathrm{Game4}}[\mathrm{A}]-\mathrm{Adv}_{\mathrm{Game3}}[\mathrm{A}]|=\mathrm{DRLWE}_{n,l,q,\chi}\mathrm{Adv}[\mathrm{A}] \tag{12}$$

在 Game 4 中,挑战者 C 公钥和密文都是均匀随机选取的,与明文空间无关,所以在 Game 4 中 A 的优势为零,即 $\mathrm{Adv}_{\mathrm{Game4}}[\mathrm{A}]=0$.

在上述游戏中,C 在挑战阶段之外的其他阶段中的行为均与 Game 0 相同. 因此,在 $\mathrm{DRLWE}_{n,l,q,\chi}$ 假设成立的情况下,$\mathrm{Adv}_{\mathrm{CPA}}[\mathrm{A}]$可忽略,IBFHE 体制是 IND-CPA 安全的.

5.2 效率分析

本文提出的 IBFHE 体制将基于身份的思想引入全同态加密体制中,相比之下,Brakerski[14] 提出的方案在实际应用过程中,必须借助公钥证书进行合法性认证,还包括公钥证书分发、管理等开销,且参数 m 的选择必须是 2 的方幂. 与现有的基于身份的全同态加密体制 GZG14 相比,IBFHE 体制支持 R_p 上的多比特加密.

选取 GZG14 体制作为参照对象,体制在实现 L 级同态运算的情况下,通过以下三个方面综合比较 IBFHE 体制的优势.

密钥尺寸方面:GZG14 体制私钥序列由一个 m 维向量和 L 个 n 维向量组成,长度为 $Ln\log q+5n\log^2 q$,公钥分为加密公钥和运算密钥尺寸为 $Ln^2\log^2 q+n\log q$;IBFHE 体制私钥序列为 $L+1$ 个 R_q^l 上元素,长度为 $(L+1)5n^2\log^2 q$,公钥分为加密公钥和运算密钥尺寸约为 $n^2\log q+50Ln^3\log^4 q$.

密文尺寸方面:GZG14 体制明文空间为 $\{0,1\}$,密文 $c\in\mathbb{Z}_q^n\times\mathbb{Z}_q$,尺寸为 $(n+1)\log q$;IBFHE 体制明文空间为 R_p,密文是 $c\in R_q^l\times R_q$,尺寸为 $(5n\log q+1)n\log q$.

计算复杂度方面:GZG14 体制加密时主要进行 $5n^2\log q+n$ 乘法和 $5n^2\log q+n$ 次加法,解密时进行 $5n\log q$ 乘法和 $5n\log q$ 次加法;IBFHE 体制主要进行 $5n^2\log q+5n^3\log q\log n$ 乘法和 $5n^2\log q+5n\log q$ 次加法,解密时进行 $5n^2\log q\log n$ 乘法和 $n\log q$ 次加法. 如表 2 所示.

表 2 效率分析对比

	明文空间	加密复杂度(模 q 意义下)	解密复杂度(原始密文)	密文尺寸	公钥证书
GZG14	$\{0,1\}$	$5n^2\log q+n$ 次乘 $5n^2\log q+n$ 次加	$5n\log q$ 次乘 $5n\log q$ 次加	$(n+1)\log q$	无
IBFHE	R_p	$5n^2\log q+5n^3\log q\log n$ 次乘 $5n^2\log q+5n\log q$ 次加	$5n^2\log q\log n$ 次乘 $n\log q$ 次加	$(5n\log q+1)n\log q$	无

综合以上从三个方面对 IBFHE 体制进行分析,同 GZG14 体制相比,虽然体制的计算复杂度稍高,但是体制的优势主要集中体现加密的明文空间上,实现了多比特加密.

6 结束语

全同态加密为解决云计算数据隐私保护问题、密文检索等难题提供了一个新的思路. 本文在任意分圆环的代数特性上,利用 RLWE 构造了一种基于身份的全同态加密体制,将身份标识作为用户公钥,从而使身份认证和管理不依靠公钥证书,并且具备全同态运算的能力. 与利用 LWE 构造的同类体制相比,支持多比特加密以及 SIMD 技术. 最后,给出了体制在随机喻示模型下的安全性证明,将安全性规约到判定性 RLWE 问题的难解性上.

参考文献

[1] Gentry C. Fully homomorphic encryption using ideal lattices[A]. Proceedings of 41rd ACM Symposium on Theory of Computing(STOC2009)[C]. Bethesda, Maryland, USA:Springer Berlin Heidelberg,2009. 169 - 178.

[2] Coron J S, Naccache D, Tibouchi M. Public key compression and modulus switching for fully homomorphic encryption over the integers[A]. Proceedings of the 31st Annual Eurocrypt Conference[C]. Cambridge, United Kingdom: Springer Berlin Heidelberg,2012. 446 - 464.

[3] Brakerski Z, Vaikuntanathan V. Efficient fully homomorphic encryption from (standard) LWE[J]. SIAM Journal on Computing,2014,43(2):831 - 871.

[4] López-Alt A, Tromer E, Vaikuntanathan V. On-the-fly multiparty computation on the cloud via multikey fully homomorphic encryption[A]. Proceedings of the 44th Annual

ACM Symposium on Theory of Computing[C]. New York,USA:ACM,2012. 1219 – 1234.

[5] Shamir A. Identity-based cryptosystems and signature schemes[A]. Advances in Cryptology[C]. Santa Barbara,USA:Springer Berlin Heidelberg,1985. 47 – 53.

[6] Naccache D. Is theoretical cryptography any good in practice? Invited talk at Crypto/CHES 2010[EB/OL]. http://www. iacr. org/workshops/ches/ches2010,2010-08-17.

[7] Gentry C,Halevi S,Vaikuntanathan V. A simple BGN-type cryptosystem from LWE[A]. Advances in Cryptology-EUROCRYPT 2010[C]. French Riviera:Springer Berlin Heidelberg,2010. 506 – 522.

[8] Regev O. On lattices, learning with errors, random linear codes, and cryptography[A]. Proceeding of 37th Annual ACM Symposium on the Theory of Computing[C]. Baltimore,MD,USA:ACM,2005. 84 – 93.

[9] Brakerski Z. Fully homomorphic encryption without modulus switch-ing from classical GapSVP[A]. Advances in Cryptology-CRYPTO 2012[C]. Santa Barbara,CA,USA:Springer Berlin Heidelberg,2012. 868 – 886.

[10] Gentry C, Sahai A, Waters B. Homomorphic encryption from learning with errors: Conceptually-simpler, asymptotically-faster, attribute-based[A]. Proceedings of the 33th Annual International Cryptology Conference[C]. Santa Barbara,USA:Springer Berlin Heidelberg,2013. 75 – 92.

[11] Gentry C, Peikert C, Vaikuntanathan V. Trapdoors for hard lattices and new cryptographic constructions[A]. Proceedings of the Fortieth Annual ACM Symposium on Theory of Computing[C]. Victoria, British Columbia, Canada:ACM,2008. 197 – 206.

[12] 光焱,祝跃飞,顾纯祥,等. 利用容错学习问题构造基于身份的全同态加密体制[J]. 通信学报,2014,35(2):111 – 117.
Guang Yan, Zhu Yue-fei, Gu Chun-xiang, et al. Identity-based fully homomorphic encryption from LWE problem[J]. Journal on Communications,2014,35(2):111 – 117.

[13] Zvika Brakerski,Vinod Vaikuntanathan. Efficient fully homomorphic encryption from (standard) LWE[A]. Proceedings of the IEEE 52nd Annual Symposium on Foundations of Computer Science[C]. Palm Springs, California,USA:IEEE,2011. 97 – 106.

[14] Brakerski Z, Vaikuntanathan V. Fully homomorphic encryption from ring-LWE and Security for key dependent messages[A]. Advances in Cryptology-CRYPTO 2011[C]. Santa Barbara, CA, USA: Springer Berlin Heidelberg,2011. 505 – 524.

[15] Lyubashevsky V, Peikert C, Regev O. On Ideal Lattices and Learning with Errors over Rings[A]. Advances in Cryptology-EUROCRYPT 2010[C]. French Riviera: Springer Berlin Heidelberg,2010. 1 – 23.

[16] Peikert C,Rosen A. Lattices that admit logarithmic worst-case to average-case connection factors[A]. Proceedings of the 39th Annual ACM Symposium on Theory of Computing[C]. San Diego,CA:ACM,2007. 478 – 487.

[17] Lyubashevsky V,Micciancio D,Peikert C,et al. SWIFFT: A modest proposal for FFT hashing[A]. Fast Software Encryption,15th International Workshop,FSE 2008[C]. Lausanne,Switzerland:Springer Berlin Heidelberg,2008. 54 – 72.

[18] Smart N P,Vercauteren F. Fully homomorphic SIMD operations[J]. Designs, Codes and Cryptography ,2014,71(1):57 – 81.

[19] Lyubashevsky V, Micciancio D. Generalized compact knapsacks are collision resistant[A]. 33rd International Colloquium, ICALP 2006, Automata, Languages and Programming[C]. Venice, Italy: Springer, 2006. 144 – 155.

[20] Lyubashevsky V, Peikert C, Regev O. On ideal lattices and learning with errors over rings[J]. Journal of the ACM (JACM),2013,60(6):43.

[21] Lyubashevsky V, Peikert C, Regev O. A toolkit for ring-LWE cryptography[A]. EUROCRYPT, 2013[C]. Athens, Greece: Springer, 2013. 35 – 54.

作者简介

辛　丹　女,1991 年 8 月出生于陕西西安. 现为信息工程大学硕士研究生. 主要研究方向为全同态加密,在国内外期刊发表学术论文 2 篇.
E-mail:xindan625@126. com

顾纯祥(通信作者)　男,1976 年出生于安徽霍山. 现为信息工程大学副教授,研究生导师,主要研究方向为网络与信息安全,在国内外重要期刊和会议上发表相关学术论文 30 余篇,其中被 SCI 收录 20 余篇.
E-mail:gcxiang5209@ alinyun. com

郑永辉　男,1976 年出生于江西乐平. 现为信息工程大学讲师,主要研究方向为密码学、网络与信息安全,在国内外重要期刊和会议上发表相关学术论文 10 余篇.
E-mail:yonghui. zh@ 163. com

光　焱　男,1983 年出生于河南新乡. 现为信息工程大学讲师,主要研究方向为密码学、网络与信息安全,在国内外重要期刊和会议上发表相关学术论文 10 余篇.
E-mail:gyinarmy@126. com

康元基　男,1992 年出生于内蒙古牙克石. 现为信息工程大学研究生,主要研究方向为密码学、网络与信息安全.