基于理想格与中国剩余定理的无界全同态加密方案

郑志勇*，中国人民大学教育部金融计算与数字工程工程研究中心、河南省科学院，中国刘凤霞†，北京未来区块链与隐私计算高精尖创新中心、人工智能研究院，中国，电子邮件：shunliliu@buaa.edu.cn田坤‡，中国人民大学教育部金融计算与数字工程工程研究中心，中国，电子邮件：tkun19891208@ruc.edu.cn

arXiv:2301.12060v1 [cs.CR] 28 Jan 2023

摘要 我们提出一种无界全同态加密方案，即一种无需解密数据或知晓解密密钥，便可对加密数据执行任意所需函数计算的方案。这是对 Rivest、Adleman 和 Dertouzoss 于 1978年提出的一个长期问题，以及几年前 Peikert 提出的两个新问题（开放问题 10 和开放问题 11）的一种合理解决方案。

我们的方案与 Gentry 于 2009 年取得的突破性成果 [21, 22]完全不同。Gentry 的自举技术从一种功能足够强大、能够计算其自身解密函数的某种同态加密方案构造出全同态加密（FHE）方案。迄今为止，这仍是获得无界全同态加密的唯一已知方法。我们构造的无界全同态加密方案简单直接且无噪声，能够在无需自举变换技术的情况下，对任意经刷新的密文执行无界同态计算。

关键词 全同态加密、理想格、中国剩余定理、一般紧致背包问题。

1 引言

1978 年，Rivest、Adleman 和 Dertouzos [42] 提出了一个后来被称为全同态加密（FHE）的概念；当时他们将其称为隐私同态。简而言之，我们将密码系统表示为 $\mathcal{P} \xrightarrow{f} \mathcal{C} \xrightarrow{f^{-1}} \mathcal{P}$，其中 $\mathcal{P}$ 是明文空间， $\mathcal{C}$ 是密文空间， f 是依赖于公钥的加密函数，而 f^{-1} 是依赖于密钥的解密函数。假设 $\mathcal{P}$ 和 $\mathcal{C}$ 是两个交换环，并且

$$f^{-1}(c_1 + c_2) = f^{-1}(c_1) + f^{-1}(c_2), \quad f^{-1}(c_1 c_2) = f^{-1}(c_1) f^{-1}(c_2), \ \forall c_1, c_2 \in \mathcal{C},$$

那么， f 就称为全同态加密，或 FHE。在全同态加密 f下，对于任意多项式$p(x) \in \mathcal{C}[x]$，不难看出

$$f^{-1}(p(c)) = p^*\left(f^{-1}(c)\right), \quad \forall c \in \mathcal{C},$$

其中， $p^*(x) \in \mathcal{P}[x]$ 是 $\mathcal{P}$ 上对应的多项式。由于所有初等函数都可以用多项式近似，因此我们可以在不解密数据的情况下，对密文执行任何所需的计算。

1.1 无界全同态加密方案

众所周知，全同态加密在密码学中有着丰富的应用，但在三十多年的时间里，人们一直未能找到看似安全的方案。2009 年，Gentry [21, 22]提出了一种基于理想格的全同态加密候选方案，这一局面由此改变。该候选全同态加密方案是指一种部分同态方案，它只能对新鲜密文支持有限次数的同态计算；随后，通过自举变换将该方案转换为能够处理无限次同态计算的方案。Gentry 的开创性突破性工作引发了极大的关注，随后很快便涌现出许多相关研究 [7, 8, 9, 10, 12, 17, 18, 23, 24, 25, 26, 43]。尽管取得了重大进展，自举在计算上仍然代价高昂，因为它需要对整个解密函数进行同态求值。此外，无界全同态加密的自举还要求作出“循环安全性”假设，即在密钥自身加密的情况下，公开密钥的加密结果仍然是安全的。迄今为止，人们对这类假设知之甚少，也缺乏支持它们的理论依据，尤其是最坏情况困难性的依据。鉴于此，Peikert [38] 提出了两个与无界全同态加密相关的开放问题，如下所示。

- **开放问题 10：** 是否存在一种不依赖自举的无界全同态加密方案？是否存在一种自举方式，其计算开销低于完整解密？

- **开放问题 11：** 是否存在一种仅基于最坏情况复杂性假设即可证明安全的无界全同态加密方案？

1.2 基于 LWE 分布的全同态加密方案

迄今为止，所有已知的全同态加密方案都遵循 Gentry 的早期工作 [21] 中提出的相同基本框架。在一系列工作中，Brakerski 和 Vaikuntanathan [9, 10] 提出了基于 LWE 分布的“第二代”全同态加密构造 [40, 41]。2013年，Gentry、Sahai 和 Waters [27] 提出了另一种有趣的基于 LWE 的全同态加密方案，它具有一些独特且有利的性质。例如，GSW 方案在自举时，误差率仅发生小幅多项式因子增长。我们将在此详细介绍这些方案。

- **BV 全同态加密方案** 令 $1 < t < q$ 为两个正整数，使得 $(t,\ q) = 1$。在 BV 系统中，密钥 s 是一个 LWE 秘密，并使用模数 q下的 LWE 样本对明文 $u \in \mathbb{Z}_t$ 进行加密。我们使用最高有效位编码获得密文 c，其形式为

$$\langle c, s\rangle \equiv_\chi \lfloor \frac{qu}{t} \rceil (\mathrm{mod}\ q),$$

其中，χ 是定义在 $\mathbb{Z}_q$上的离散高斯分布，$\lfloor x \rceil$ 是将实数 x舍入到最近整数后的结果。我们使用密钥 s 对密文 c 进行解密，其形式为

$$f^{-1}(c) \equiv_\chi \lfloor \frac{t}{q} \cdot \langle c, s\rangle \rceil \,(\mathrm{mod}\ t)\,.$$

显然，有 $f^{-1}(c) = u$ （见 [52]）。为了说明该方案是某种全同态加密方案，我们可以使用消息的最低有效位编码（两种编码的等价性参见 [4] 的附录 A）。事实上，密文 c 满足

$$\langle s, c\rangle \equiv_\chi m\ (\mathrm{mod}\ q),\ \text{and}\ \ m \in \{nt + u \mid n \in \mathbb{Z}\} \cap [-\frac{q}{2}, \frac{q}{2}).$$

要解密 c，只需计算 $\langle s,c\rangle \in \mathbb{Z}_q$，将结果提升为 $\mathbb{Z}\cap[-\frac{q}{2},\frac{q}{2})$ 中的唯一代表元 m，并输出 $u \equiv m$（模 t）。显然，对密文 c 进行同态计算会产生噪声；如果噪声过大，就会破坏明文。因此，通过重新加密密文来降低噪声水平的自举技术，仍然是构建无界全同态加密方案的唯一已知方法。

• **GSW 全同态加密方案**GSW 全同态加密方案用 [1, 3, 5, 34, 39] 中描述的基于小工具矩阵的陷门来表述最为简洁。GSW 方案的核心是以下针对标签和陷门的加法与乘法同态映射。设 $\bar{A} \in \mathbb{Z}_q^{n\times\bar{m}}$ 是密钥为 $\bar{s} \in \mathbb{Z}_q^{n-1}$ 的 LWE 样本，对于 $i = 1,\ 2$，令

$$A_i = x_i G - \bar{A} R_i,$$

其中 $x_i \in \mathbb{Z}_q$，G 是维数为 $n \times nl$，$R_i \in \mathbb{Z}_q^{\bar{m}\times n}$ 是 $\mathbb{Z}_q$ 上的随机高斯矩阵，而 $\bar{m} = n + nl$（参见 [38] 第 50 页）。由于 $\begin{pmatrix} R_i \\ I_n \end{pmatrix}$ 是矩阵 $[\bar{A}, A_i]$，关于标签 $x_i I_n$ 的陷门，因此很容易验证

$$A_1 + A_2 = (x_1 + x_2)\, G - \bar{A}\,(R_1 + R_2)$$

and

$$A_1 G^{-1}(A_2) = x_1 x_2 G - \bar{A}\underbrace{\left(R_1 G^{-1}(A_2) + x_1 R_2\right)}_{R}$$

换言之，$\begin{pmatrix} R_1 + R_2 \\ I_n \end{pmatrix}$ 是矩阵 $[\bar{A}, A_1 + A_2]$ 的一个带有标签 $(x_1 + x_2)$ I_n 的陷门，而 $\begin{pmatrix} R \\ I_n \end{pmatrix}$ 是矩阵 $[\bar{A}, A_1 G^{-1}(A_2)]$ 的一个带有标签 $x_1 x_2 I_n$ 的陷门。即使采用了上述所有技术，同态运算也总会增加密文的误差率，每次运算增加的幅度最高可达一个多项式因子。因此，这里介绍的方案只能对先验有界深度的电路进行同态求值。

1.3 基于环上学习误差的全同态加密方案

如今，若干基于环上学习误差的构造已跻身最有前景的全同态加密候选方案之列。基于环上学习误差的方案中，最流行的有三种：（1）TFHE [15, 16] 尤其适用于对单个槽位执行组合运算，并且能够容忍较大的噪声，因此乘法深度也可以很大；（2）B/FV [7, 11, 20] 可执行大规模向量算术运算，只要被求值电路的乘法深度较小；（3）HEAAN[13, 14]——一种混合加密方案，已被证明在浮点计算中效率很高。下面将对这些方案作简要介绍。

• **TFHE方案** TFHE由三种主要的加密/解密方案组成，每种方案对应不同的明文空间。首先，TLWE方案对整个环面 $\mathbb{T}$ 上的消息进行加密，并生成 $\mathbb{T}^{N+1}$中的密文。其他两种方案是：

— TRGSW 加密环 $\mathcal{R}_\mathbb{Z}$（整数多项式）的元素，其 l^∞-范数（自然对应 $\mathcal{R} \simeq \mathbb{Z}^N$ 下相应向量在 $\mathbb{Z}^N$ 中的范数）有界。— TRLWE 加密 μ $\mathcal{R}_\mathbb{Z}$-模 $\mathbb{T}_\mathcal{R}$ 的元素，这些元素也可以通过自然双射 $\mathbb{T}_\mathcal{R} \simeq \mathbb{T}^N$ 视为 $\mathbb{T}^N$ 的元素。

存在一个外部乘积 $\boxdot_\alpha$，它取决于噪声参数 α（见推论 3.14[16]），并由此在 TRGSW 和 TRLWE 方案上赋予全同态加密模结构。

在 TFHE 中，消息 $\mu \in \mathbb{T}$ 的 TLWE 密文具有如下形式：$(a,\ b =< s,\ a > +\mu + e) \in \mathbb{T}^{N+1}$ 其中 $s \in \{0,1\}^N$ 是密钥，$a \in \mathbb{T}^N$ 是均匀随机的，$e \in \mathbb{T}$ 则是从以零为中心的噪声分布中采样得到的。类似地，对于 TRLWE，$\mu \in \mathbb{T}_{\mathcal{R}}$ 的密文形式为 $(a,\ b = s \cdot a + \mu + e) \in \mathbb{T}^2_{\mathcal{R}}$ 其中 $s \in \mathcal{B}$，$a \in \mathbb{T}_{\mathcal{R}}$ 是均匀随机的，且 $e \in \mathbb{T}_{\mathcal{R}}$。

TLWE（分别为 TRLWE）的解密使用一个秘密的 κ-Lipschitz 函数（这里，$\kappa > 0$很小，我们所说的"相对于环面上的 l^∞-范数"）$\varphi_s :\ \mathbb{T}^N \times \mathbb{T} \to \mathbb{T}$（分别为 $\varphi_s :\ \mathbb{T}_{\mathcal{R}} \times \mathbb{T}_{\mathcal{R}} \to \mathbb{T}_{\mathcal{R}}$），称为相位。该相位由一个较小的（通常为二进制）密钥 $s \in \{0,1\}^N$（分别为 $s \in \mathcal{B}$）参数化，并定义为 $(a,\ b) \in \mathbb{T}^N \times \mathbb{T} \to b - < s,\ a >$（分别为 $(a,\ b) \to b - s \cdot a$）。相位是一个 κ-Lipschitz 函数，且 $\kappa \leqslant N + 1$很小，因此解密能够容忍误差，并支持对近似数进行运算。

密文分为新鲜密文（即直接加密明文生成的密文）和通过一系列同态运算生成的密文。无论哪种情况，都将密文视为一个随机变量，它取决于用于生成 a and e 的随机币，以及用于执行所有这些同态运算的随机币。

由于 $\varphi_s(a,b) = b - s \cdot a = \mu + e$，解密 μ 和噪声参数 α 分别是相位函数 $\varphi_s(a,b)$ 的均值和标准差（此处，均值和标准差是对加密算法中的随机币计算得出的）。

• **B/FV 方案** 在该方案中，消息空间是有限环 $\mathcal{R}_p = \mathbb{Z}_p[x]/ < x^N + 1 >$，其中 p 是某个整数（通常是 2 的幂或素数）。消息 $\mu \in \mathcal{R}_p$ 在商环 $\mathcal{R}_q$ 上加密（使用更大的模数 q），得到密文 $(a,b) \in \mathcal{R}_q^2$，其中 $a \in \mathcal{R}_q$ 是均匀随机选取的，b 从 $\mathcal{D}_{\mathcal{R}_q,\sigma,s\cdot a+\frac{p}{q}\mu}$中采样。这里，$\mathcal{D}_{\mathcal{R}_q,\sigma,\mu}$ 是定义在 $\mathcal{R}_q$ 上、以 μ 为中心、标准差为 σ 的离散高斯分布（离散表示取值均为整数）。此外，$s \in \mathcal{B}$ 是密钥。

两个密文 (a_1,b_1) 和 (a_2,b_2) 的同态加法通过逐分量相加实现。两个密文 (a_1,b_1) 和 $(a_2\ b_2 \quad a_i\ b_i\ \in \mathcal{R}_q^2 \quad \tilde{a_i}\ \tilde{b_i}\ \in,)$ 的 $\mathcal{R}^2$
同态乘法采用一种称为重线性化的技术：首先将 $(,)$ 提升为 $(\ ,)$，其中每个系数都被提升到 $[-q/2, q/2)$，然后将 μ_i 视为关于 s的线性多项式（即 $\mu_i \sim \frac{p}{q}(b_i + s \cdot a_i)$）。接着计算与乘积对应的二次多项式，即 $\frac{p}{q}(b_1 + s \cdot a_1) \cdot \frac{p}{q}(b_2 + s \cdot a_2)$，并使用 [20] 中描述的重线性化，将该乘积表示为 $\frac{p}{q}(b + s \cdot a)$，并确定系数 $(a,b) \in \mathcal{R}_q$。

每次乘法后，噪声幅度平均会增大一个较小的因子 $O(N)$，因此通常会执行模数重缩放步骤：将每个系数和模数 q 都除以同一个标量并取整，从而使噪声幅度恢复到 $O(1)$，以便后续操作能够在更小的密文上继续进行。

• **HEAAN方案** 在此方案中，消息空间是 $\mathcal{R}_q$ 的子集，其中包含范数为 $\leqslant B$ 的所有元素，范数上界为 B；元素 $x \in \mathcal{R}_q$ 的范数定义为 $||\tilde{x}||_\infty$。这里，$\tilde{x} \in \mathcal{R}_{\mathbb{R}}$ 是 x 的最小提升，即将系数提升到 $[-q/2, q/2)$。消息解密后会有常数个最低有效位无法恢复，这些位被视为噪声。

HEAAN 密文也是一个环学习带错误对 $(a,\ b) \in \mathcal{R}_q^2$，其中 $a \in \mathcal{R}_q$ 是均匀随机的，而 b 与 $s \cdot a + \mu$ 相等，误差服从标准差较小的高斯误差。这一次，明文和密文共享相同的空间，因此不使用重缩放因子 p/q。

两个消息相乘时，使用与 B/FV 相同的公式（包括重线性化）：如果两个输入消息都以 B 为界，且噪声为 $O(1)$，那么乘积消息以 B^2 为界，噪声为 $O（B）$。因此，通常会在此时执行模数重缩放步骤，将所有内容除以 B ，使噪声恢复到 $O(1)$（参见 [14]）。与 B/FV 不同，模数切换中的这次除法不仅会缩放密文，还会将明文缩放 B。可以通过给密文添加一个（公开的）标签来解决此问题，以跟踪执行了多少次除以 B 的操作。

最近，Boura、Gama、Georgieva 和 Jetchev [6] 提出了一种实用的混合方案，用于组合上述三种基于环上学习误差的全同态加密方案，并在它们之间进行切换。他们首先将不同的明文空间映射到一个公共代数结构中，然后应用高效的切换算法来实现这一点。这种方法有许多实际应用，例如，它已成为近期同态方案标准化倡议和通用应用程序接口的重要工具。

1.4 其他相关工作

在 Eurocrypt 2010 上，van Dijk、Gentry、Halevi 和 Vaikuntanathan [19]描述了一种基于整数环的全同态加密方案（另见 [12, 17, 18]）。与 Gentry 的方案一样，作者首先描述了一种部分同态方案，它支持对加密比特进行有限次数的加法和乘法。随后，他们应用 Gentry 的压缩解密技术，得到一个可自举方案；再通过 Gentry 的密文刷新过程，获得一个全同态方案。与 Gentry 最初的方案相比，该方案的主要优点在于概念简单，即所有操作都在整数环上进行，而不是在理想格上进行。然而，公钥过大，无法用于任何实用系统。在 [17] 和 [18], 中，作者通过在公钥元素中使用二次型而非线性型进行加密，将公钥大小从 $\tilde{\mathcal{O}}\left(\lambda^{10}\right)$ 缩减至 $\tilde{\mathcal{O}}\left(\lambda^{7}\right)$ 。

这是最新的无需使用噪声消除技术的方案（见 [28]）。2015年，Yagisawa 提出了一种基于有限域上的非结合八元数环的全同态加密方案[45]。该方案的密码学稳健性基于高次多元代数方程的复杂性。在他的下一篇论文中，他对该方案进行了一些改进[46]。Liu 提出了一种基于非交换环的对称全同态加密方案 [30]。Liu 的方案支持任意次数的加法和乘法，并且无论噪声消除机制的数量如何，都能正确解密；该方案基于近似最大公因数复杂性。Li 和 Wang 提出了一种无噪声对称全同态加密方案 [29] ，该方案使用非交换环上的矩阵。毋庸置疑，这些无噪声方案并不能解决全同态加密方案面临的问题，因为它们使用非结合环和非交换环来表示明文和密文。

1.5 我们的贡献

我们提出的无界全同态加密方案简单直接且无噪声，这与 Gentry 最初的构造截然不同。更具体地说，我们的全同态加密方案无需自举变换，即可对任意刷新后的密文进行无界同态计算。这是解决全同态加密开放问题的一种合理方案。

我们的解决方案分为三个步骤。首先，我们给出一种基于理想格和中国剩余定理的一般构造，其中包含三个高效算法，分别用于生成密钥、公钥和解密。明文空间是环的直和 $\mathbb{Z}_{t_i}$，其中t_i 是每个理想格 I_i $(1 \leqslant i \leqslant m)$ 的一维模数。密文空间 $\mathbb{Z}^n$是一个交换环，其运算包括向量的加法和卷积乘积 $\otimes$ ，因此，同态计算所需的代数结构可谓最简单。核心思想是为 $\mathbb{Z}^n$定义一种乘法运算，使得 $\mathbb{Z}^n$ 成为一个交换环，因此，可以将其视为

$I \subset \mathbb{Z}^n$ 既是 $\mathbb{Z}^n$中的理想，也是其中的格，特别是， $\mathbb{Z}^n/I$ 成为一个商环。利用这个环（$\mathbb{Z}^n$， $+$，$\otimes$），我们可以高效地运用中国剩余定理来生成公钥。接下来，我们给出一种基于主理想格和分圆域 [47]的一些基本结果、可高效计算且实用的系统。该实用系统的新颖之处在于，它建立了密码系统与数学中一个古老难题之间的联系：如何求解高次代数方程。根据著名的伽罗瓦理论，当代数方程的次数大于 5 时，不存在通用的求解方法。最后，我们基于任意环上的一般紧致背包问题，讨论了本方案的安全性，并证明其安全性完全建立在最坏情况复杂性假设之上。这也是对 Peikert 的开放问题 11 [38]的一种解答。

紧致背包问题在任意环上的推广可描述如下：给定 m 个环元素 a_1， a_2， $\cdots a_m \in R$ 以及目标值 $b \in R$，求系数 x_1， x_2， $\cdots$， $x_m \in X \subset R$ ，使得 $\sum_{i=1}^{m} a_i x_i = b$。此问题的计算复杂度取决于所选的环 R 以及 X的大小。已知当 R为整数环且 X为小整数集合 $\{0, 1, \cdots, 2^{m-1}\}$ 时，此问题可在准多项式时间内求解（参见 [2]和 [32]）。Micciancio [32] 研究了 R 为适当选取的模多项式环、 X 为小系数多项式子集时的背包问题，并证明：平均情况下求解该问题的难度，与在最坏情况下以多项式因子近似任意循环格覆盖半径的难度一样。

我们将这一结果推广到任意理想格，使得我们的全同态加密方案在平均情况下与求解任意理想格覆盖半径近似问题的最坏情况一样困难。

2 一般构造

令 $\mathbb{Z}[x]$ 为变量为 x、 $\phi(x) \in \mathbb{Z}[x]$ 的整数系数多项式环，并令 $\phi(x) = x^n - \phi_{n-1}x^{n-1} - \cdots - \phi_1 x - \phi_0$ 为给定多项式， $\langle \phi(x) \rangle$ 为 $\mathbb{Z}[x]$ 中由 $\phi(x)$ 生成的主理想，$R = \mathbb{Z}[x]/\langle \phi(x) \rangle$ 为商环。令 $\mathbb{R}^n$ 为 n 维欧几里得空间， $\mathbb{Z}^n \subset \mathbb{R}^n$ 为 $\mathbb{R}^n$ 中所有整数向量的集合。我们对 $\mathbb{R}^n$ 中的向量使用列记法。

商环 $\mathbb{Z}[x]/\langle \phi(x) \rangle$ 与所有整数向量 $\mathbb{Z}^n$ 之间存在一一对应关系：

$$a(x) = a_0 + a_1 x \cdots a_{n-1}x^{n-1} \in \mathbb{Z}[x]/\langle \phi(x) \rangle \xrightarrow{\tau} a = \begin{pmatrix} a_0 \\ a_1 \\ \vdots \\ a_{n-1} \end{pmatrix} \in \mathbb{Z}^n, \tag{2.1}$$

记 $\tau(a(x)) = a$，或 $\tau^{-1}(a) = a(x)$。由于 $\tau(a(x) + b(x)) = \tau(a(x)) + \tau(b(x))$ τ 实际上是加法群同构。要将 τ 视为环同构，我们需要在 $\mathbb{Z}^n$ 中定义一个乘法算子。为此，设旋转矩阵 $H = H_\phi$ 为

$$H = \left(\begin{array}{ccc|c} 0 & \cdots & 0 & \phi_0 \\ \hline & & & \phi_1 \\ & I_{n-1} & & \vdots \\ & & & \phi_{n-1} \end{array}\right)$$

其中 I_{n-1} 是 $n-1$ 维单位矩阵。

D定义 2.1 对于任意 $\alpha \in \mathbb{R}^n$，由 α 生成的理想矩阵定义为

$$H^*(\alpha) = \left[\alpha, H\alpha, \cdots, H^{n-1}\alpha\right] \in \mathbb{R}^{n \times n}.$$

关于理想矩阵的一些基本性质可由以下引理描述，其证明参见 [49], 中的引理 2.5 或 [48]中的引理 5.2.4。

引理 2.1 设 $\alpha = \begin{pmatrix} \alpha_0 & & \\ \alpha_1 & & \\ & \ldots & \\ & & \alpha_{n-1} \end{pmatrix}$ 和 $\beta = \begin{pmatrix} \beta_0 & & \\ \beta_1 & & \\ & \ldots & \\ & & \beta_{n-1} \end{pmatrix}$ 是 $\mathbb{R}^n$中的任意两个向量，则有

(i) $H^*(\alpha) = \alpha_0 I_n + \alpha_1 H + \cdots + \alpha_{n-1} H^{n-1}$; (ii) $H^*(\alpha)H^*(\beta) = H^*(\beta)H^*(\alpha)$; (iii) $H^*(\alpha)H^*(\beta) = H^*(H^*(\alpha)\beta)$;$_n$(iv) $\det(H^*(\alpha)) = \prod \alpha(\omega_i)$;$_{i=1}$

其中 $\alpha(x) = \tau^{-1}(\alpha)$，且 ω_1， ω_2， $\cdots$， ω_n 是 $\phi(x)$ 的 n 个根。

根据引理 2.1 的 (iv)，当且仅当 $\alpha(x)$ 和 $\phi(x)$ 在复数域中没有公共根时， $H^*(\alpha)$ 才是可逆矩阵。现在，我们可以用理想矩阵来定义 $\mathbb{Z}^n$ 上的乘法算子。

定义 2.2 设 α， $\beta \in \mathbb{Z}^n$ 是两个整数向量，我们将卷积乘积 $\alpha \otimes \beta$ 定义为

$$\alpha \otimes \beta = H^*(\alpha)\beta.$$

显然，在卷积乘积下， $\alpha \otimes \beta$、 $\mathbb{Z}^n$ 成为一个交换环，其单位元为 $e = \begin{pmatrix} 1 & & \\ 0 & & \\ & \ldots\ldots & \\ & & 0 \end{pmatrix} \in \mathbb{Z}^n$，

因为 $\alpha \otimes \beta = \beta \otimes \alpha$ 和

$$\alpha \otimes e = e \otimes \alpha = \alpha, \quad \forall \alpha \in \mathbb{Z}^n.$$

有时，我们将这个环记作 $(\mathbb{Z}^n, +, \otimes) = \mathbb{Z}^n$。

引理 2.2 由 (2.1) 给出的对应关系 τ 是 $\mathbb{Z}^n/\langle\phi(x)\rangle$与 $\mathbb{Z}^n$之间的环同构，即有

$$\mathbb{Z}[x]/\langle\phi(x)\rangle \cong (\mathbb{Z}^n, +, \otimes).$$

证明。 由 [49] 的引理 2.4 或 [48],的引理 5.2.5，容易看出

$$\begin{aligned} &\tau(\alpha(x) + \beta(x)) = \alpha + \beta = \tau(\alpha(x)) + \tau(\beta(x)), \\ &\tau(\alpha(x)\beta(x)) = \alpha \otimes \beta = \tau(\alpha(x)) \otimes \tau(\beta(x)). \end{aligned}$$

结论立即成立。

□

根据理想格的定义， [31, 32, 37, 38, 50, 51], 理想格 $I \subset \mathbb{Z}^n$ 就是 $(\mathbb{Z}^n, +, \otimes)$ 的一个理想。我们将 $I \subset \mathbb{Z}^n$ 既视为 $\mathbb{Z}^n$ 的一个理想，也视为 $\mathbb{Z}^n$ 中的一个格；特别地， $\mathbb{Z}^n/I$ 是一个商环。

格 $I \subset \mathbb{R}^n$ 是 $\mathbb{R}^n$ [36, 37, 44]的离散加法群，通常记作 $I = \mathcal{L}(B)$，其中 $B = [\beta_1, \beta_2, \cdots, \beta_n] \in \mathbb{R}^{n\times n}$ 是 I的生成矩阵或一组基。本文讨论的所有格都是满秩格，这意味着 $\det(B) \neq 0$。如果 $I \subset \mathbb{Z}^n$，那么 I 称为整数

格。整数格的 Hermite标准形基 B [33, 47] 是一个上三角矩阵 $B=(b_{ij})_{n\times n}\in\mathbb{Z}^{n\times n}$，满足 $b_{ii}\geqslant 1(1\leqslant i\leqslant n)$，并且

$$b_{ij}=0,\ \text{if } 0\leqslant j<i\leqslant n,\ \text{and}\ \ 0\leqslant b_{ij}<b_{ii},\ \text{if } 0\leqslant i<j\leqslant n.$$

已知整数格存在唯一的 HNF基，其 Gram-Schmidt正交基是一个对角矩阵。更确切地说，若 $B=[\beta_1,\beta_2,\cdots,\beta_n]$ 是整数格的 HNF 基，$B^*=[\beta_1^*,\beta_2^*,\cdots,\beta_n^*]$ 是通过 Gram-Schmidt 正交化方法得到的对应正交基，则 $B^*=\text{diag}\{b_{11},b_{22},\cdots,b_{nn}\}$ 是一个对角矩阵（参见 [47] 的引理 7.26）。

定义 2.3 b_{11} 称为理想格 $I=\mathcal{L}(\beta_1,\ \beta_2,\ \cdots,\ \beta_n)$ 的一维模数，记为 $t(I)=b_{11}$。

设 $I\subset(\mathbb{Z}^n,\ +,\ \otimes)$ 是一个理想格。为获得商环 $\mathbb{Z}^n/I$ 的一组代表元，我们采用 Micciancio [33] 提出的正交平行多面体记法。以下引理参见 [47], 的引理7.45 和式 (7.131)，或 [33], 的 §4.1；其证明将在下文的引理2.6中给出。

引理 2.3 设 $I=\mathcal{L}(B)$ 是 $\mathbb{Z}^n$ 的一个满秩理想，B 是 I 的 HNF基，$B^*=\text{diag}\{b_{11},b_{22},\cdots,b_{nn}\}$ 是相应的正交基，则商环 $\mathbb{Z}^n/I$ 的一组代表元为

$$\mathcal{F}(I)=\left\{x=\begin{pmatrix}x_1\\x_2\\\vdots\\x_n\end{pmatrix}\in\mathbb{Z}^n\mid 0\leqslant x_i<b_{ii},\ 1\leqslant i\leqslant n\right\},$$

而 $\mathcal{F}(I)$ 称为 I 的正交平行多面体。

接下来，我们讨论理想格以及环 $(\mathbb{Z}^n,+,\otimes)$。设 $\alpha\in\mathbb{Z}^n$ 是一个给定向量，主理想格 $<\alpha>$ 是 $\mathbb{Z}^n$ 中由 α 生成的主理想。容易验证

$$<\alpha>=\left\{\alpha\otimes x\mid x\in\mathbb{Z}^n\right\}=\mathcal{L}(H^*(\alpha)).$$

因此，主理想格 $<\alpha>$ 的生成矩阵就是由 α 生成的理想矩阵。

$(\mathbb{Z}^n,+,\otimes)$ 中理想格之间的运算按通常方式定义，特别是两个理想 I 和 J 的加法与乘法定义为

$$I+J=\left\{\alpha+\beta\mid\alpha\in I,\ \beta\in J\right\},$$

$$IJ=\left\{\sum_{i<\infty}\alpha_i\otimes\beta_i\mid\alpha_i\in I,\ \beta_i\in J\right\},$$

and

$$I\cap J=\left\{\gamma\mid\gamma\in I,\ \text{and}\ \gamma\in J\right\}.$$

由于 $I+J$、IJ 和 $I\cap J$ 也是 $\mathbb{Z}^n$ 的理想，因此它们都是理想格。

定义 2.4 设 $I\subset\mathbb{Z}^n$、$J\subset\mathbb{Z}^n$ 是两个理想格。若 $I+J=\mathbb{Z}^n$，则称 I 与 J 互素，并记作 $(I,\ J)=1$。

很容易看出，两个理想格 I 和 J 互素，当且仅当存在$\alpha\in I$和 $\beta\in J$使得 $\alpha+\beta=e$，其中 e是 $(\mathbb{Z}^n,\ +,\ \otimes)$ 的单位元。

为了构造全同态加密方案，我们在环 $(\mathbb{Z}^n,\ +,\ \otimes)$ 中利用中国剩余定理；这是数论中的一个著名定理。

定理 1（中国剩余定理）设 $I_1, I_2, \cdots, I_m$ 是 $\mathbb{Z}^n$ 中两两互素的理想格，且 $\alpha_1, \alpha_2, \cdots, \alpha_m \in \mathbb{Z}^n$ 是 $\mathbb{Z}^n$ 中的 m 目标向量，则以下同余式存在一个公共解：

$$x \equiv \alpha_i \pmod{I_i},\ 1 \leqslant i \leqslant m,$$

并且 $x \in \mathbb{Z}^n$ 的解模理想格 $I_1 \cap I_2 \cdots \cap I_m$ 意义下唯一。

对于任意两两互素的格 $I_1, I_2, \cdots, I_m$，已知

$$I_1 \cap I_2 \cdots \cap I_m = I_1 I_2 \cdots I_m.$$

由上述中国剩余定理，立即可得以下推论。

推论 2.1 设 $I_1, I_2, \cdots, I_m$ 是 $\mathbb{Z}^n$ 中两两互素的理想格，则有以下环同构

$$\mathbb{Z}^n/I_1 I_2 \cdots I_m \cong \mathbb{Z}^n/I_1 \bigoplus \mathbb{Z}^n/I_2 \bigoplus \cdots \bigoplus \mathbb{Z}^n/I_m. \tag{2.2}$$

(2.2) 的右端是 m 商环 $\mathbb{Z}^n/I_i$ $(1 \leqslant i \leqslant m)$ 的直和，其中 $\bigoplus_{i=1}^{m} \mathbb{Z}^n/I_i$ 的加法和乘法由给出

$$(a_1, a_2, \cdots, a_m) + (b_1, b_2, \cdots, b_m) = (a_1 + b_1, a_2 + b_2, \cdots, a_m + b_m)$$

and

$$(a_1, a_2, \cdots, a_m) \otimes (b_1, b_2, \cdots, b_m) = (a_1 \otimes b_1, a_2 \otimes b_2, \cdots, a_m \otimes b_m).$$

证明。由于 I_1，I_2，……，I_m 两两互素，根据定理 1，存在 m 个向量 $A_i (1 \leqslant i \leqslant m)$ 属于 $\mathbb{Z}^n$，使得

$$A_i \equiv e \pmod{I_i}, \text{ and } A_i \equiv 0 \pmod{I_j}, \text{ if } j \neq i.$$

对于任意 $\alpha = (\alpha_1,\ \alpha_2,\ \ldots\ldots,\ \alpha_m) \in \mathbb{Z}^n/I_1 \bigoplus \mathbb{Z}^n/I_2 \bigoplus \cdots \bigoplus \mathbb{Z}^n/I_m$，再次根据定理 1，存在唯一解 $x \in \mathbb{Z}^n/I_1 I_2 \cdots I_m$，使得

$$\begin{cases} x \equiv \alpha_1 \pmod{I_1} \\ \quad\vdots \\ x \equiv \alpha_m \pmod{I_m} \end{cases}$$

我们定义 $f(\alpha) = x$，它正是所需的从 $\mathbb{Z}^n/I_1 \bigoplus \mathbb{Z}^n/I_2 \bigoplus \cdots \bigoplus \mathbb{Z}^n/I_m$ 到 $\mathbb{Z}^n/I_1 I_2 \cdots I_m$ 的环同构。利用 A_1，A_2，……，A_m，显然可以通过以下方式写出 f

$$f(\alpha) = f((\alpha_1, \alpha_2, \ldots, \alpha_m)) = \alpha_1 \otimes A_1 + \cdots + \alpha_m \otimes A_m.$$

设 $\beta = (\beta_1,\ \beta_2,\ \ldots\ldots,\ \beta_m)$ 是 $\bigoplus_{i=1}^{m} \mathbb{Z}^n/I_i$ 的另一个元素，很容易看出

$$\begin{aligned} f(\alpha + \beta) &= f((\alpha_1 + \beta_1, \alpha_2 + \beta_2, \ldots, \alpha_m + \beta_m)) \\ &= \alpha_1 \otimes A_1 + \cdots + \alpha_m \otimes A_m + \beta_1 \otimes A_1 + \cdots + \beta_m \otimes A_m \\ &= f(\alpha) + f(\beta). \end{aligned}$$

为验证 $f(\alpha \otimes \beta) = f(\alpha) \otimes f(\beta)$，由于

$$f(\alpha) \equiv \alpha_i \pmod{I_i}, \text{ and } f(\beta) \equiv \beta_i \pmod{I_i}, \ 1 \leqslant i \leqslant m.$$

由此可得

$$f(\alpha) \otimes f(\beta) \equiv \alpha_i \otimes \beta_i \pmod{I_i}, \ 1 \leqslant i \leqslant m.$$

根据 f 的定义，我们有

$$\begin{aligned} f(\alpha \otimes \beta) &= f((\alpha_1 \otimes \beta_1, \alpha_2 \otimes \beta_2, \ldots, \alpha_m \otimes \beta_m)) \\ &= f(\alpha) \otimes f(\beta). \end{aligned}$$

这证明 f 是一个环同构。 □

我们将逆同构 f^{-1} 扩展到整个空间 $\mathbb{Z}^n$，定义为 $f^* = f \circ \pi$：

$$f^* : \mathbb{Z}^n \xrightarrow{\pi} \mathbb{Z}^n / I_1 I_2 \ldots I_m \xrightarrow{f^{-1}} \bigoplus_{i=1}^{m} \mathbb{Z}^n / I_i,$$

其中，π 是从 $\mathbb{Z}^n$ 到其商环 $\mathbb{Z}^n / I_1 I_2 \ldots I_m$ 的自然同态。容易$_m$看出，f^* 是从 $\mathbb{Z}^n$ 到 $\bigoplus \mathbb{Z}^n / I_i$ 的同态，并且 $_{i=1}$

$$f^*(f(u)) = f^{-1}(f(u)) = u, \ \forall u \in \bigoplus_{i=1}^{m} \mathbb{Z}^n / I_i, \tag{2.3}$$

在我们的方案中，f^* 将充当解密的角色，并且在接下来的讨论中，我们总是将 f^* 写作 f^{-1}。

由于 $\mathbb{Z}$ 是一个环，我们希望将这个环嵌入到 $(\mathbb{Z}^n, +, \otimes)$ 中。为此，我们定义一个从 $\mathbb{Z}$ 到 $\mathbb{Z}^n$ 的嵌入映射

$$\forall a \in \mathbb{Z}, \ a \to \overline{a} = \begin{pmatrix} a \\ 0 \\ \vdots \\ 0 \end{pmatrix} \in \mathbb{Z}^n. \tag{2.4}$$

引理 2.4 在嵌入映射下，$a \to a$, $\mathbb{Z}$ 成为 $(\mathbb{Z}^n, \overline{+}, \overline{\otimes})$ 的一个子环；也就是说，对于任意 $a \in \mathbb{Z}$, $b \in \mathbb{Z}$, 都有 $a + b = a \overline{+} b$ 和 $ab = a \overline{\otimes} b$。

证明。 由 (2.4)，我们有

$$\overline{a+b} = \begin{pmatrix} a+b \\ 0 \\ \vdots \\ 0 \end{pmatrix} = \begin{pmatrix} a \\ 0 \\ \vdots \\ 0 \end{pmatrix} + \begin{pmatrix} b \\ 0 \\ \vdots \\ 0 \end{pmatrix} = \overline{a} + \overline{b}$$

and

$$\overline{a} \otimes \overline{b} = \begin{pmatrix} ab \\ 0 \\ \vdots \\ 0 \end{pmatrix} = \overline{a \cdot b},$$

该引理立刻可得。 □

引理 2.5 设 $I \subset \mathbb{Z}^n$ 是一个理想格， $t = t(I)$ 是根据定义 2.3 给出的其一维模数。那么，对于任意 a， $b \in \mathbb{Z}$，我们有

$$a \equiv b \pmod{t} \Longleftrightarrow \overline{a} \equiv \overline{b} \pmod{I}.$$

证明。 根据假设， I 是一个满秩格，其HNF基可写为

$$B = \begin{pmatrix} b_{11} & * & * & * \\ & b_{22} & * & * \\ & 0 & \ddots & * \\ & & & b_{nn} \end{pmatrix}.$$

如果$a \equiv b$ （模 I），则存在一个向量 $x = \begin{pmatrix} x_1 \\ \cdots\cdots \\ x_n \end{pmatrix} \in \mathbb{Z}^n$ 使得

$$\overline{a} - \overline{b} = Bx = \begin{pmatrix} a-b \\ 0 \\ \vdots \\ 0 \end{pmatrix}.$$

由于 $b_{nn}x_n = 0$，且 $b_{nn} \geqslant 1$，我们有 $x_n = 0$；同样，由于$b_{n-1,\ n-1}x_{n-1} + b_{n-1,\ n}x_n = 0$，可推出 $x_{n-1} = 0$。因此，我们有 $x_n = x_{n-1} = \cdots = x_2 = 0$，并且 $a - b = x_1 b_{11} = x_1 t \Rightarrow a \equiv b$ （模 t）。反之，如果 $a \equiv b$ （模 t），则 $a - b = qt$，并且

$$\overline{a} - \overline{b} = B \begin{pmatrix} q \\ 0 \\ \vdots \\ 0 \end{pmatrix} \in I \Longrightarrow \overline{a} \equiv \overline{b} \pmod{I}.$$

该断言成立。 □

对于任意给定的两两互素的理想格 I_1， I_2， $\cdots$， I_m，使用中国剩余定理生成公钥 A_1， A_2，$\cdots$， A_m，其中$A_i \in \mathbb{Z}^n (1 \leqslant i \leqslant m)$使得

$$\text{其中 } e = \begin{pmatrix} 1 \\ 0 \\ \cdots \\ 0 \end{pmatrix} \in \mathbb{Z}^n \text{ 是（} \mathbb{Z}^n, +, \otimes \text{）的单位元。} \quad A_i \equiv e \pmod{I_i}, \text{ and } A_i \equiv 0 \pmod{I_j}, \text{ if } j \neq i, \tag{2.5}$$

现在，我们描述如下无界全同态加密方案 s.

为了验证上述方案的同态加法和乘法，根据引理 2.4，$m\mathbb{Z}$ 是（$\mathbb{Z}^n$， $+$， $\otimes$）的子环。根据引理 2.5，我们可以将直和 $\bigoplus_{i=1}^{m} \mathbb{Z}_{t_i}$ 嵌入 $\bigoplus_{i=1}^{m} \mathbb{Z}^n/I_i$，因此 $\bigoplus_{i=1}^{m} \mathbb{Z}_{t_i}$ 也是 $\bigoplus_{i=1}^{m} \mathbb{Z}^n/I_i$ 的子环。因此，完全同态这一性质可直接由一个环同态 f^*（或 f^{-1}）得出:

$$\bigoplus_{i=1}^{m} \mathbb{Z}_{t_i} \hookrightarrow \bigoplus_{i=1}^{m} \mathbb{Z}^n/I_i \xrightarrow{f} \mathbb{Z}^n/I_1 I_2 \ldots I_m \xleftarrow{f^*} \mathbb{Z}^n.$$

算法 1：一般无界全同态加密方案

- **密钥：** 选取 m 两两互素的理想格 $I_1, I_2, \cdots, I_m$ 作为$\mathbb{Z}^n$ 中的解密密钥。

- 公钥：令 $t_i = t(I_i)$ 为 $I_i\,(1 \leqslant i \leqslant m)$ 的一维模数。m明文空间是环 $\mathcal{P} = \bigoplus \mathbb{Z}_{t_i}$ 的直和，其中 $\mathcal{P}$ 中的加法和$i=1$乘法由 $(a_1, a_2, \cdots, a_m) + (b_1, b_2, \cdots, b_m) = (a_1 + b_1, a_2 + b_2, \cdots, a_m + b_m)$、$(a_1, a_2, \cdots, a_m) \cdot (b_1, b_2, \cdots, b_m) = (a_1 b_1, a_2 b_2, \cdots, a_m b_m)$ 给出。用于加密的公钥为 $\{A_1, A_2, \cdots, A_m\} \subset \mathbb{Z}^n$，且每个 A_i 均由式 (2.5) 给出。m

- **加密：** 对于任意明文 $u = (u_1, u_2, \cdots, u_m) \in \mathcal{P} = \bigoplus \mathbb{Z}_{t_i}$，加密$i=1$函数 f 定义为 $c = f(u) = u_1 \otimes A_1 + u_2 \otimes A_2 + \cdots + u_m \otimes A_m$，其中 u_i 是 u_i的嵌入。

$$(2.6)$$

- **解密：** 对于任意密文 $c \in \mathbb{Z}^n$，我们使用密钥 $I_1, I_2, \cdots, I_m$ 进行解密 t
  c。由于对于每个 $i, 1 \leqslant i \leqslant m$，都有 $c \equiv u_i \pmod{I_i}$，且 $c \bmod I_i$ 是 I_i 的正交平行多面体 $\mathcal{F}(I_i)$ 中唯一的向量，因此有 s
  $c \bmod I_i = \overline{u}_i$，由 (2.3) 可得
  $$f^{-1}(c) = (u_1, u_2, \cdots, u_m) = u.$$

更确切地说，设 $c_1 = f(u)$ 和 $c_2 = f(v)$ 是任意两个密文，其中 $u = (u_1, u_2, \cdots, u_m) \in$ m $\bigoplus_{i=1} \mathbb{Z}_{t_i}$，且 $v = (v_1, v_2, \cdots, v_m) \in \bigoplus_{i=1}^{m} \mathbb{Z}_{t_i}$。注意，对于所有 $i, 1 \leqslant i \leqslant m$，

$$c_1 + c_2 \equiv \overline{u_i} + \overline{v_i} \pmod{I_i}, \text{ and } c_1 \otimes c_2 \equiv \overline{u_i} \otimes \overline{v_i} \pmod{I_i}.$$

根据引理 2.4，可得

$$c_1 + c_2 \equiv \overline{u_i + v_i} \pmod{I_i}, \text{ and } c_1 \otimes c_2 \equiv \overline{u_i v_i} \pmod{I_i}.$$

因此，根据引理 2.5，我们有

$$\begin{aligned} f^{-1}(c_1 + c_2) &= (u_1 + v_1, u_2 + v_2, \cdots, u_m + v_m) \\ &= (u_1, u_2, \cdots, u_m) + (v_1, v_2, \cdots, v_m) \\ &= f^{-1}(c_1) + f^{-1}(c_2), \end{aligned}$$

and

$$\begin{aligned} f^{-1}(c_1 \otimes c_2) &= (u_1 v_1, u_2 v_2, \cdots, u_m v_m) \\ &= (u_1, u_2, \cdots, u_m)(v_1, v_2, \cdots, v_m) \\ &= f^{-1}(c_1) \cdot f^{-1}(c_2). \end{aligned}$$

这就是我们所期望的无界全同态加密。

在我们的一般无界全同态加密方案算法中，如何使用密钥 $I_1, I_2, \ldots, I_m$ 解密密文 $c \in \mathbb{Z}^n$？这里我们给出一个引理，证明在 I_i 的正交平行多面体 $\mathcal{F}(I_i)$ 中，只有一个向量 $u_i \in \mathbb{Z}^n$ 满足 $c \equiv u_i$ （模 I_i），并详细给出计算 u_i 的算法。

引理2.6 给定一个理想格 I，对于任意向量 $c \in \mathbb{Z}^n$，存在唯一的向量 $w \in \mathcal{F}(I)$，使得 $c \equiv w$ (模 I)。

证明。 假设 $B=[\beta_1,\beta_2,\ldots,\beta_n]$ 是 I 的HNF基，且 $B^*=[\beta_1^*,\beta_2^*,\ldots,\beta_n^*]$ 是 B 的对应正交基。将 c 写成 $[\beta_1^*,\beta_2^*,\ldots,\beta_n^*]$ 的线性组合，即

$$c=\sum_{i=1}^{n}c_i\beta_i^*,\ c_i=\frac{<c,\beta_i^*>}{<\beta_i^*,\beta_i^*>}.$$

n n n设 $w=\sum c_i\beta_i^*-\sum k_i\beta_i$, $k_1,k_2,\ldots,k_n\in\mathbb{Z}$, 则 $c-w=\sum k_i\beta_i\in I$。接下来，我们证明只有一组整数 $k_1,k_2,\ldots,k_n$ 满足 $w\in\mathcal{F}(I)$，即

$$w_i=\frac{<w,\beta_i^*>}{<\beta_i^*,\beta_i^*>}\in[0,1),\ \forall 1\leqslant i\leqslant n.$$

首先，我们确定 k_n 的值。由于

$$w_n=\frac{<w,\beta_n^*>}{<\beta_n^*,\beta_n^*>}=c_n-k_n\frac{<\beta_n,\beta_n^*>}{<\beta_n^*,\beta_n^*>}=c_n-k_n,$$

因此，当 $k_n=[c_n]$ 时，这里 $[x]$ 表示不大于实数 x 的最大整数，我们有$w_n\in[0,1)$。其次，我们确定 k_{n-1}。注意

$$w_{n-1}=\frac{<w,\beta_{n-1}^*>}{<\beta_{n-1}^*,\beta_{n-1}^*>}=c_{n-1}-k_{n-1}-k_n\frac{<\beta_n,\beta_{n-1}^*>}{<\beta_{n-1}^*,\beta_{n-1}^*>},$$

因此，只有一个整数

$$k_{n-1}=\left[c_{n-1}-[c_n]\frac{<\beta_n,\beta_{n-1}^*>}{<\beta_{n-1}^*,\beta_{n-1}^*>}\right]$$

满足 $w_{n-1}\in[0,1)$。同理，我们可以确定任意的 k_i, $\forall 1\leqslant i\leqslant n-1$,

$$w_i=\frac{<w,\beta_i^*>}{<\beta_i^*,\beta_i^*>}=c_i-k_i-\frac{<\sum\limits_{j=i+1}^{n}k_j\beta_j,\beta_i^*>}{<\beta_i^*,\beta_i^*>},$$

因此，只有一个整数

$$k_i=\left[c_i-\frac{<\sum\limits_{j=i+1}^{n}k_j\beta_j,\beta_i^*>}{<\beta_i^*,\beta_i^*>}\right]$$

n n使得 $w_i\in[0,1)$, $\forall 1\leqslant i\leqslant n-1$。最重要的是，只有一个向量 $w=\sum c_i\beta_i^*-\sum k_i\beta_i\in$ $i=1$ $i=1$$\mathcal{F}(I)$ 使得 $c\equiv w\ (\mathrm{mod}\ I)$。

□

基于 引理2.6，我们给出了一个用于解密我们的一般全同态加密方案的算法。

算法2：全同态加密方案的解密算法

- 对于任意密文 $c\in\mathbb{Z}^n$，给定一个具有 HNF 基 $B=[\beta_1,\beta_2,\ldots,\beta_n]$ 和相应正交基 $B^*=[\beta_1^*,\beta_2^*,\ldots,\beta_n^*]$ 的满秩理想格 I_i，我们n只能找到一个向量 $u_i=c-\sum k_i\beta_i\in\mathcal{F}(I)$，使得$c\equiv u_i$ (模 I_i)，其中$i=1$ —

$$k_n=\left[\frac{<c,\beta_n^*>}{<\beta_n^*,\beta_n^*>}\right],\ k_i=\left[\frac{<c,\beta_i^*>}{<\beta_i^*,\beta_i^*>}-\frac{<\sum\limits_{j=i+1}^{n}k_j\beta_j,\beta_i^*>}{<\beta_i^*,\beta_i^*>}\right],\ i=n-1,n-2,\ldots,1.$$

为了创建一种高效算法来生成上述无界全同态加密方案的密钥，我们假设 $\phi(x)$ 是一个不可约多项式，因此主理想 $<\phi(x)>$ 是 $\mathbb{Z}[x]$ 中的素理想，且商环 $\mathbb{Z}[x]/<\phi(x)>$ 是一个整环；等价地，$(\mathbb{Z}^n, +, \otimes)$ 成为一个整环。在此假设下，我们看到，在$\mathbb{Z}^n$ 中，任意多个两两互素理想几乎会自动出现，下面描述这一过程。

算法3：秘密密钥生成算法

- **第一步**。 随机选取一个非零向量 $\alpha \in \mathbb{Z}^n$ 作为输入，输出如下两个互素理想 I_1 和 I_2，其中

$$I_1 =<\alpha>, \text{ and } I_2 =<e-\alpha>.$$

- **第二步**。 随机选取两个非零向量 $\alpha_1 \in I_1$ 和 $\alpha_2 \in I_2$ 作为输入，输出如下理想 I_3，其中

$$I_3 =<e-\alpha_1 \otimes \alpha_2>.$$

容易看出， I_1， I_2， I_3 是两两互素理想。

- **最后一步**。 假设选取了 $m-1$ 个两两互素理想 I_1， I_2，……， I_{m-1}，然后随机选取 $\alpha_1 \in I_1$、 $\alpha_2 \in I_2$、 ……、 $\alpha_{m-1} \in I_{m-1}$、 $\alpha_i \neq 0$，输出理想 I_m 由下式给出

$$I_m =<e-\alpha_1 \otimes \alpha_2 \otimes \cdots \otimes \alpha_{m-1}>.$$

显然， I_1， I_2，……， I_m 是 $\mathbb{Z}^n$中的两两互素理想。

为了构造一个寻找公钥的高效算法，我们首先证明

引理 2.7 设 I_1、 I_2、……、 I_m 是 $\mathbb{Z}^n$ 中两两互素的理想，并且每个 I_i 都是由 α_i 生成的主理想，即 $I_i =<\alpha_i>$。令

$$d_i = \bigotimes_{j=1, j\neq i}^{m} \alpha_j,\ 1 \leqslant i \leqslant m.$$

那么对于任意 d_i，都存在一个向量 $\mathcal{D}_i \in \mathbb{Z}^n$ 使得

$$d_i \otimes \mathcal{D}_i \equiv e \pmod{I_i},\ 1 \leqslant i \leqslant m.$$

证明。 根据假设， I_1、 I_2、……、 I_m 两两互素，因此有

$$(I_i, I_1 I_2 \cdots I_{i-1} I_{i+1} \cdots I_m) = 1,\ 1 \leqslant i \leqslant m.$$

换言之，我们有 $(I_i, <d_i>) = 1$，或者

$$<\alpha_i> + <d_i> = \mathbb{Z}^n.$$

因此，存在一个向量 $\mathcal{D}_i \in \mathbb{Z}^n$ 使得 $d_i \otimes \mathcal{D}_i \equiv e$ （模 I_i），从而立即得到引理 2.7。

□

如何求出引理 2.7 定义的向量 $\mathcal{D}_i$？ 我们引入一种多项式时间算法来获得 $\mathcal{D}_i (1 \leqslant i \leqslant m)$，并通过取 $A_i = d_i \otimes \mathcal{D}_i (1 \leqslant i \leqslant m)$生成公钥 $\{A_1, A_2, \ldots, A_m\}$。

算法 4：公钥生成算法

- 设 $I_i =< \alpha_i >$ $(1 \leqslant i \leqslant m)$ 两两互素，并且

$$d_i(x) = \prod_{j=1, j\neq i}^{m} \tau^{-1}(\alpha_i),\ 1 \leqslant i \leqslant m,$$

其中，密钥为 $I_i =< \alpha_i >$ $(1 \leqslant i \leqslant m)$，$\tau^{-1}$ 是由（2.1）给出的 τ 的逆映射。

由于 $d_i(x)$ 和 $\tau^{-1}(\alpha_i)$ 是商环 $\mathbb{Z}[x]/ < \phi(x) >$ 中的互素多项式，因此可得

$$< d_i(x) > + < \tau^{-1}(\alpha_i) >= \mathbb{Z}[x]/ < \phi(x) > .$$

因此，存在多项式 $\mathcal{D}_i(x)$ 使得

$$d_i(x)\mathcal{D}_i(x) \equiv 1 \pmod{\tau^{-1}(\alpha_i)}.$$

令 $\mathcal{D}_i = \tau(\mathcal{D}_i(x))$，以及 $A_i = d_i \otimes \mathcal{D}_i$、$1 \leqslant i \leqslant m$。

为了讨论该方案的安全性，我们注意到所有风险都来自加密算法（2.6）。我们将这种风险描述为环（$\mathbb{Z}^n$，$+$，$\otimes$）上的广义紧致背包问题，如下所示：

$$\sum_{i=1}^{m} a_i \otimes x_i = u, \quad |x_i| \leqslant \beta, \tag{2.7}$$

其中 $a_1, a_2, \cdots, a_m$ 是给定的 m 个向量，$\mathbb{Z}^n$中的 $u \in \mathbb{Z}^n$ 是目标向量，且 $\beta = \max\limits_{1\leqslant i\leqslant m} t_i$。我们将在下一节说明安全性。

另一方面，对于任意 $a \in \mathbb{Z}$，我们看到 $H^*(a) = aI_n$。因此，这个问题可以转化为标准的环 SIS 问题：假设 $A = [A_1, A_2, \cdots, A_m] \in \mathbb{Z}^{n\times m}$，其中 A_i 是由式（2.5）给出的公钥，$u \in \mathbb{Z}^n$ 是目标向量，求 $x = \begin{pmatrix} x_1 \\ \cdots \\ x_n \end{pmatrix} \in \mathbb{Z}^n$，使得

$Ax = u$，且 $0 < |x| \leqslant \beta$。令 q 为一个足够大的正整数，这个问题可以转化为 SIS 问题的非齐次版本，即求一个短整数解，使其满足 $Ax \equiv u \pmod{q}$。不难证明，对于典型参数，齐次问题与非齐次问题本质上是等价的。

根据 Ajtai 的开创性工作 [2, 3], , SIS 问题的困难性可归约到最坏情况格问题。更准确地说，对于任意 $m = \text{poly}(n)$、任意 $\beta > 0$，以及任意充分大的 $q \geqslant \beta \cdot \text{poly}(n)$，以不可忽略的概率求解 $\text{SIS}_{n,q,\beta,m}$ 至少与求解判定近似最短向量问题 GapSVP_γ 一样困难，其中参数为某个 $\gamma = \beta \cdot \text{poly}(n)$（另见 [35]及 [38] 的定理 4.1.2）。因此，我们的全同态加密方案的安全性完全基于最坏情况复杂性假设，这是对 [38] 的**开放问题 11**的一种合理解答。

3 整数环 $\mathbb{Z}^n$ 上的广义紧凑背包问题

本节讨论基于环 $(\mathbb{Z}^n, +, \otimes)$ 上一般紧凑背包问题的方案安全性。在 [32], Micciancio 已证明，如果我们能够求解 $\mathbb{Z}_q^n$ 上的背包问题，其中 q是足够大的正整数，那么就存在一个概率多项式时间算法，可以求解任意 n 维满秩循环格的覆盖半径问题。首先

我们基于先前的工作 [51], , 将 Micciancio 的结果推广到任意理想格，然后将背包问题从 $\mathbb{Z}_q^n$推广到 $(\mathbb{Z}^n, +, \otimes)$。为完整起见，我们给出一份完整的证明，尽管此处提出的方法与 Micciancio 的原始证明相当相似。

定义 3.1 设 L 是一个满秩格， $\gamma(n)$ 是 n 的一个参数， $\gamma(n) \geqslant 1$，CDPγ问题是求一个 r ，使得

$$\rho(L) \leqslant r \leqslant \gamma(n)\rho(L),$$

其中 $\rho(L) = \max_{x\in\mathbb{R}^n} \mathrm{dist}(x, L)$，且 $\mathrm{dist}(x, L) = \min_{\alpha\in L} |x-\alpha|$。

定义 3.2 设 L 是一个满秩格， $S = \{s_1, s_2, \cdots, s_n\} \subset L$ 是 n 个线性无关的格向量。 $S^* = \{s_1^*, s_2^*, \cdots, s_n^*\}$ 是通过格拉姆-施密特方法从 S 得到的正交基。我们定义

$$\sigma(S) = \Big(\sum_{i=1}^{n} |s_i^*|^2\Big)^{\frac{1}{2}}.$$

下面给出我们的主要结果，以表明对于任意 n 维满秩理想格，整数环上的广义背包问题至少与覆盖半径问题一样困难。

定理 2 设 $m = O(\log n)$， $k = O(\log n)$， $\phi_{\max} = \max\{|\phi_0|, |\phi_1|, \ldots, |\phi_{n-1}|\}$， $M = \sqrt{2 + 2\phi_{\max}^2}$， $W = \frac{M^n-1}{M-1}$， $\gamma \geqslant 16mkn^3W$。如果我们能够求解背包问题 (2.7)，那么就存在一个正的概率多项式时间算法，能够求解任意n 维满秩理想格 L 的覆盖半径问题 CDPγ 。

注：在 Micciancio 的原始工作中， [32], 参数 γ 大于 $16mkn^3$，我们要求 $\gamma \geqslant 16mkn^3W$，其中 W 由 $\frac{M^n-1}{M-1}$ 给出。主要区别在于估计任意两个向量 α 和 β的卷积乘积 $\alpha \otimes \beta$ 的长度。对于循环格，显然有 $|\alpha \otimes \beta| \leqslant \sqrt{n}|\alpha||\beta|$；但对于理想格，这并非易事。

引理 3.1 对于任意 α， $\beta \in \mathbb{Z}^n$，有

$$|\alpha \otimes \beta| \leqslant W|\alpha| \cdot |\beta|,$$

其中 W 在定理 2 中定义。

证明。 我们先证明 $|H\alpha| \leqslant M|\alpha|$。令 $\alpha = (\alpha_0, \alpha_1, \ldots\ldots, \alpha_{n-1})^T$，则

$$\begin{aligned}
|H\alpha|^2 &= \phi_0^2\alpha_0^2 + (\alpha_0 + \phi_1\alpha_1)^2 + \cdots + (\alpha_{n-2} + \phi_{n-1}\alpha_{n-1})^2 \\
&\leqslant \phi_0^2\alpha_0^2 + 2(\alpha_0^2 + \phi_1^2\alpha_1^2) + \cdots + 2(\alpha_{n-2}^2 + \phi_{n-1}^2\alpha_{n-1}^2) \\
&\leqslant 2(\alpha_0^2 + \cdots + \alpha_{n-2}^2) + 2\phi_{\max}^2(\alpha_0^2 + \alpha_1^2 + \cdots + \alpha_{n-1}^2) \\
&\leqslant (2 + 2\phi_{\max}^2)|\alpha|^2.
\end{aligned}$$

因此 $|H\alpha| \leqslant M|\alpha|$。类似地,

$$|H^2\alpha| \leqslant M|H\alpha| \leqslant M^2|\alpha|.$$

同理，我们可以得到 $|H^k\alpha| \leqslant M^k|\alpha|, \forall 1 \leqslant k \leqslant n-1$。令 $\beta = (\beta_0, \beta_1, \ldots\ldots, \beta_{n-1})^T$，可得

$$\begin{aligned}
|\alpha \otimes \beta| &= |H^*(\alpha)\beta| = |\beta_0\alpha + \beta_1 H\alpha + \cdots + \beta_{n-1}H^{n-1}\alpha| \\
&\leqslant \sum_{i=0}^{n-1} |\beta_i H^i\alpha| \leqslant \sum_{i=0}^{n-1} M^i|\alpha||\beta| = \frac{M^n-1}{M-1}|\alpha| \cdot |\beta|.
\end{aligned}$$

我们完成了这一证明。 □

设 $L = \mathcal{L}(B) \subset \mathbb{R}^n$ 是一个满秩理想格， $q \geqslant 4mkn^2W^2$， $\{e_0, e_1, \cdots, e_{n-1}\} \subset \mathbb{Z}_q^n$ 是一个标准正交基， $S = \{s_1, s_2, \cdots, s_n\} \subset L$ 是一组 n 线性无关向量。我们定义参数

$$\mu = \left(\frac{4nq}{\gamma} + \frac{W}{2}\right)\sigma(S). \tag{3.1}$$

根据 [48], 中的第 3 章引理 1.6，存在一个格向量 $c \in L$ ，使得 $|c - \mu e_0| \leqslant \frac{1}{2}\sigma(S)$，令 $B' = q(H^*(c))^{-1}B$。由此可知，由 B' 生成的格 $\mathcal{L}(B')$ 满足 $q\mathbb{Z}^n \subset \mathcal{L}(B')$，根据 [48]中的第 3 章引理 2.1。因此， $q\mathbb{Z}^n$ 是 $\mathcal{L}(B')$ 中的一个加法子群。随机选取商群 $G = \mathcal{L}(B')/q\mathbb{Z}^n$ 中的 mk 个元素 $x_{ij}^{'}$ $(1 \leqslant i \leqslant m, 1 \leqslant j \leqslant k)$， $x_{ij}^{'}$ 的整数向量 $w_{ij}^{'}$ 定义为

$$w_{ij}^{'} = \lfloor x_{ij}^{'} \rceil \in \mathbb{Z}^n,\ 1 \leqslant i \leqslant m,\ 1 \leqslant j \leqslant k.$$

Let

$$a_{ij} \equiv w_{ij}^{'} \pmod q,\quad a_i \equiv \sum_{j=1}^{k} w_{ij}^{'} \pmod q,$$

假设 $A = (a_1, a_2, \cdots, a_m) \in \mathbb{Z}_q^{n\times m}$。由于背包问题 (2.7) 在 $\mathbb{Z}^n$ 上可解，因此它也可以在 $\mathbb{Z}_q^n$ 上求解。令 $y = (y_1, y_2, \cdots, y_m) \in \mathbb{Z}_q^{n\times m}$ 和 $\hat{y} = (\hat{y}_1, \hat{y}_2, \cdots, \hat{y}_m) \in \mathbb{Z}_q^{n\times m}$ 为两个 m 不同的整数矩阵，使得 $\sum a_i \otimes (y_i - \hat{y}_i) = 0$， $|y_i| \leqslant \sqrt{n}$， $|\hat{y}_i| \leqslant \sqrt{n}, \forall 1 \leqslant i \leqslant m$。我们 $_{i=1}$ 定义 $^{-}$

$$x_{ij} = \frac{1}{q}H^*(c)x_{ij}^{'}, w_{ij} = \frac{1}{q}H^*(c)w_{ij}^{'}, 1 \leqslant i \leqslant m, 1 \leqslant j \leqslant k,$$

and

$$s' = \sum_{i=1}^{m}\sum_{j=1}^{k}(x_{ij} - w_{ij}) \otimes (y_i - \hat{y}_i). \tag{3.2}$$

那么， x_{ij} 是给定理想格 $L = \mathcal{L}(B)$ $(1 \leqslant i \leqslant m,\ 1 \leqslant j \leqslant k)$中的一个格向量，并且根据 [48]第 3 章中的引理 2.2， s' 也是 $L = \mathcal{L}(B)$中的一个格向量。

下一个引理给出了 s'长度的估计，其证明与 Micciancio 的证明略有不同。

引理 3.2 设 L是满秩理想格， $S = \{s_1, s_2, \cdots, s_n\} \subset L$ 是一组线性无关向量。记 $|S| = \max\limits_{1\leqslant i\leqslant n} |s_i|$， s' 是式 (3.2) 中定义的格向量，则

$$|s'| \leqslant \frac{1}{2}|S|.$$

证明。 除了关于参数的一些计算外，此证明与 [48]中第 3 章引理 2.3 的证明类似。我们先证明 $|s'| \leqslant \frac{1}{2\sqrt{n}}\sigma(S)$。根据式 (3.2) 中 s' 的定义,

$$|s'| \leqslant \sum_{i=1}^{m}\sum_{j=1}^{k}\left|(x_{ij} - w_{ij}) \otimes (y_i - \hat{y}_i)\right|. \tag{3.3}$$

$$x_{ij} - w_{ij} = \frac{1}{q}H^*(c)(x_{ij}^{'} - w_{ij}^{'}) = \frac{1}{q}c \otimes (x_{ij}^{'} - w_{ij}^{'}).$$

令 $\alpha = c - \mu e_0$，其中 μ 在（3.1）中定义。则 $|\alpha| \leqslant \frac{1}{2}\sigma(S)$，并且

$$x_{ij} - w_{ij} = \frac{1}{q}(\alpha + \mu e_0) \otimes (x_{ij}^{'} - w_{ij}^{'}) = \frac{1}{q}H^*(\alpha + \mu e_0)(x_{ij}^{'} - w_{ij}^{'})$$

$$= \frac{1}{q}\mu H^*(e_0)(x_{ij}^{'} - w_{ij}^{'}) + \frac{1}{q}H^*(\alpha)(x_{ij}^{'} - w_{ij}^{'})$$
$$= \frac{\mu}{q}(x_{ij}^{'} - w_{ij}^{'}) + \frac{1}{q}H^*(\alpha)(x_{ij}^{'} - w_{ij}^{'}).$$

由于 $w_{ij}^{'} = \lfloor x_{ij}^{'} \rceil \in \mathbb{Z}^n$，我们有

$$|x_{ij}^{'} - w_{ij}^{'}| \leqslant \frac{1}{2}\sqrt{n},$$

结合引理 3.1，我们得到

$$\begin{aligned}
|x_{ij} - w_{ij}| &\leqslant \frac{\mu}{q}|x_{ij}^{'} - w_{ij}^{'}| + \frac{1}{q}|\alpha \otimes (x_{ij}^{'} - w_{ij}^{'})| \\
&\leqslant \frac{\mu}{q} \cdot \frac{1}{2}\sqrt{n} + \frac{1}{q} \cdot W \cdot \frac{1}{2}\sigma(S) \cdot \frac{\sqrt{n}}{2} \\
&= \frac{\sqrt{n}}{2q}\left(\frac{4nq}{\gamma} + \frac{W}{2}\right)\sigma(S) + \frac{\sqrt{n}W}{4q}\sigma(S) \\
&= \sigma(S)\left(\frac{2n^{\frac{3}{2}}}{\gamma} + \frac{\sqrt{n}W}{2q}\right) \\
&\leqslant \sigma(S)\left(\frac{1}{8} \cdot \frac{1}{mkn^{\frac{3}{2}}W} + \frac{1}{8} \cdot \frac{1}{mkn^{\frac{3}{2}}W}\right) \\
&= \sigma(S)\frac{1}{4mkn^{\frac{3}{2}}W}.
\end{aligned}$$

根据（3.3），我们知道

$$|s'| \leqslant mkW \max_{i,j}|x_{ij} - w_{ij}| \cdot \max_{i}|y_i - \hat{y}_i|$$
$$\leqslant mkW \cdot \frac{\sigma(S)}{4mkn^{\frac{3}{2}}W} \cdot 2\sqrt{n} = \frac{\sigma(S)}{2\sqrt{n}}.$$

由于

$$\sigma(S) \leqslant \left(\sum_{i=1}^{n}|s_i|^2\right)^{\frac{1}{2}} \leqslant \sqrt{n}|S|,$$

我们可以得到

$$|s'| \leqslant \frac{\sigma(S)}{2\sqrt{n}} \leqslant \frac{\sqrt{n}|S|}{2\sqrt{n}} = \frac{1}{2}|S|.$$

因此，引理 3.2 的证明完成。

□

根据上述引理，定理 2 可直接由 Micciancio 的方法 [32] 得出。从定理 2 可知，$\mathbb{Z}^n$ 上的一般紧凑背包问题至少与任意理想格的覆盖半径问题 CDP$_\gamma$ 一样难。因此，我们的无界全同态加密方案的安全性完全基于最坏情况复杂性假设，因此它是对 [38] 的**开放问题 11**的一种合理解答。

4 一个实用系统

作为示例，我们利用分圆域 [44] 的一些基本结果，介绍一个用于全同态加密的实用系统。假设 p 是一个奇素数，且 $Q(\xi_p)$ 是分圆域，$\xi_p = e^{\frac{2\pi i}{p}}$ 是一个本原 p 次单位根。令

$$\mathbb{Z}[\xi_p] = \left\{ \sum_{i=0}^{p-1} a_i \xi_p^i \mid a_i \in \mathbb{Z} \right\}.$$

已知 $\mathbb{Z}[\xi_p]$ 是域 $Q(\xi_p)$ 的代数整数环。因此，$\mathbb{Z}[\xi_p]$ 是一个戴德金整环（因此我们有唯一的素理想分解等；参见 [44] 的命题 1.2）。

为了为 $\mathbb{Z}^n$构造一个交换环，我们选取 $\phi(x) = x^{p-1} + x^{p-2} + \cdots + x + 1 \in \mathbb{Z}[x]$。显然，$\phi(x)$ 是 ξ_p. 的最小多项式。令 $n = p - 1$，于是根据 $\phi(x)$ 和旋转矩阵 H_ϕ，我们得到一个环 $(\mathbb{Z}^n, +, \otimes)$；容易看出（参见 [49] 的式 (3.2)）

$$(\mathbb{Z}^n, +, \otimes) \cong \mathbb{Z}[x]/\langle \phi(x) \rangle \cong \mathbb{Z}[\xi_p].$$

因此，$\mathbb{Z}^n$ 成为一个戴德金整环。

对于任意整数 $q \in \mathbb{Z}$，我们定义整数向量 $\alpha_q \in \mathbb{Z}^n$ 如下：

$$\alpha_q = \begin{pmatrix} q \\ 0 \\ \vdots \\ 0 \\ 1 \end{pmatrix} \in \mathbb{Z}^n.$$

由 α_q 生成的主理想 $\langle \alpha_q \rangle$ 记作

$$I_q = \langle \alpha_q \rangle = \mathcal{L}(H^*(\alpha_q)).$$

引理 4.1 如果 q_1 和 q_2 是两个不同的素数，那么I_{q_1} 和 I_{q_2} 是 $\mathbb{Z}^n$中的互素理想格。

证明。假设 q 是一个素数。由于 $(\mathbb{Z}^n, +, \otimes) \cong \mathbb{Z}[x]/\langle \phi(x) \rangle$，我们看到多项式$\tau^{-1}(\alpha_q) = \alpha_q(x) = x^{n-1} + q \in \mathbb{Z}[x]$是艾森斯坦型多项式，因此它是 $\mathbb{Z}[x]$上的不可约多项式。将 $\alpha_q(x)$视为 $\mathbb{Z}[x]/\langle \phi(x) \rangle$的多项式，显然，它也是 $\mathbb{Z}[x]/\langle \phi(x) \rangle$中的不可约多项式。根据假设，$q_1$ 和 q_2 是不同的素数，我们证明主理想 $\langle \alpha_{q_1}(x) \rangle$和 $\langle \alpha_{q_2}(x) \rangle$ 在$\mathbb{Z}[x]/\langle \phi(x) \rangle$中是互素理想。由于 $\mathbb{Z}[x]/\langle \phi(x) \rangle$ 是一个戴德金整环，如果$\langle \alpha_{q_1}(x) \rangle$ 和 $\langle \alpha_{q_2}(x) \rangle$ 不互素，那么，在 $\mathbb{Z}[x]/\langle \phi(x) \rangle$ 中存在一个素理想 P，使得

$$\langle \alpha_{q_1}(x) \rangle \subset P, \quad \text{and} \quad \langle \alpha_{q_2}(x) \rangle \subset P.$$

因此，对于任意正整数 $k \geq 1$，

$$\left\langle \alpha_{q_1}^k(x) \right\rangle \subset P^k, \quad \text{and} \quad \left\langle \alpha_{q_2}^k(x) \right\rangle \subset P^k.$$

已知存在一个正整数 $k \geqslant 1$，使得 $P^k = \langle d(x) \rangle$ 是一个主理想，因此我们有

$$\left\langle \alpha_{q_1}^k(x) \right\rangle \subset \langle d(x) \rangle, \quad \text{and} \quad \left\langle \alpha_{q_2}^k(x) \right\rangle \subset \langle d(x) \rangle.$$

换言之，我们有 $d(x) \mid \alpha_{q_1}^k(x)$，且 $d(x) \mid \alpha_{q_2}^k(x)$。然而，这是不可能的，因为 $\alpha_{q_1}(x)$ 和 $\alpha_{q_2}(x)$ 是 $\mathbb{Z}[x]/\langle \phi(x) \rangle$ 中的两个不可约多项式，并且 $\alpha_{q_1}(x) \neq \alpha_{q_2}(x)$。

这证明了 $\langle \alpha_{q_1}(x) \rangle$ 和 $\langle \alpha_{q_2}(x) \rangle$ 是 $\mathbb{Z}[x]/\langle \phi(x) \rangle$中的互素理想。等价地，$I_{q_1}$ 和 I_{q_2} 是 $\mathbb{Z}^n$.中的两个互素理想格 □

引理 4.2 主理想 I_q 的一维模数为

$$t_q = t(I_q) = q^n - q^{n-1} + \cdots - q + 1.$$

证明。 不难计算得出 $\det(H^*(\alpha_q)) = q^n - q^{n-1} + \cdots - q + 1$. 由于多项式$x^n - x^{n-1} + \cdots - x + 1$是 $\mathbb{Z}$上的不可约多项式，我们立即得到引理的结论。

□

根据引理 4.1 和引理 4.2，我们得到如下密钥生成算法:

算法 5：秘密密钥生成算法

- 随机选取 m 个不同的素数 $q_1, q_2, \cdots, q_m$，使得 $q_i \neq p$。主理想格

$$I_{q_i} = \langle \alpha_{q_i} \rangle, \quad 1 \leq i \leq m$$

是密钥，相应的一维模数 t_{q_i} 由下式给出

$$t_{q_i} = t(I_{q_i}) = q_i^n - q_i^{n-1} + \cdots - q_i + 1. \tag{4.1}$$

为获得公钥的可达算法，我们定义向量 $d_i(1 \le i \le m)$ 如下

$$d_i = \alpha_{q_1} \otimes \alpha_{q_2} \otimes \cdots \otimes \alpha_{q_{i-1}} \otimes \alpha_{q_{i+1}} \otimes \cdots \otimes \alpha_{q_m} = \otimes_{\substack{j=1 \\ j \neq i}}^{m} \alpha_{q_j}, \quad 1 \le i \le m.$$

引理 4.3 对于每个向量 $d_i(1 \le i \le m)$，都存在一个向量 $\mathcal{D}_i \in \mathbb{Z}^n$，使得

$$d_i \otimes \mathcal{D}_i \equiv e \,(\mathrm{mod}\ I_{q_i}),$$

其中 $e = \begin{pmatrix} 1 \\ 0 \\ \cdots \\ 0 \end{pmatrix}$ 是 rimg $(\mathbb{Z}^n, +, \otimes)$ 的单位元。

证明。 根据引理 4.1， $I_{q_1}, I_{q_2}, \cdots, I_{q_m}$ 是两两互素理想，因此我们有 $\left(I_{q_i}, I_{q_1} I_{q_2} \cdot I_{q_{i-1}} I_{q_{i+1}} \cdot I_{q_m}\right) = 1$。换言之，我们有 $(\langle \alpha_{q_i} \rangle, \langle d_i \rangle) = 1$，或者

$$\langle \alpha_{q_i} \rangle + \langle d_i \rangle = \mathbb{Z}^n.$$

因此，存在一个向量 $\mathcal{D}_i \in \mathbb{Z}^n$，使得 $\mathcal{D}_i \otimes d_i \equiv e$(模 I_{q_i})。我们有引理 4.3。

□

我们提出一种多项式时间算法，用于求出引理 4.3 中出现的向量 $\mathcal{D}_i$，然后代入 $A_i = d_i \otimes \mathcal{D}_i$，得到公钥 A_1， A_2， $\cdots$， A_m。求向量 $\mathcal{D}_i$ 的多项式时间算法如下。

算法 6：公钥生成算法

- 令

  $$d_i(x) = \prod_{\substack{j=1 \\ j \neq i}}^{m} \left(x^{n-1} + q_j\right), 1 \le i \le m.$$

  由于多项式 $x^{n-1} + q_i$ 和 $x^{n-1} + q_j (j \neq i)$ 在 $\mathbb{Z}[x]/\langle \phi(x) \rangle$ 中互素，因此可得 $\left(x^{n-1} + q_i,\ d_i(x)\right) = 1$。所以，存在一个多项式 $\mathcal{D}_i(x)$，使得 $d_i(x)\mathcal{D}_i(x) \equiv 1$ (模 $\left(x^{n-1} + q_i\right)$) .根据第 2 节给出的映射 τ，我们得到 $\mathcal{D}_i = \tau(\mathcal{D}_i(x))$。

现在，我们描述如下基于分圆域的全同态加密方案的可达算法。

全同态加密的性质可直接由一般构造得出。我们主要讨论这一实用全同态加密系统的安全性。显然，一维模数 $t_i(1 \le i \le m)$ 的消息会带来额外风险。这等价于求解高次代数方程

$$x^n - x^{n-1} + \cdots - x + 1 = t$$

对于给定的目标值 $t \in \mathbb{Z}$。这是数学中的一个古老难题，根据著名的伽罗瓦理论，没有通用的方法可以找到其解。因此，我们得出结论， I_{q_i}的一维模数 t_i 不会带来特殊风险。

算法 7：无界全同态加密方案的可达算法

- **密钥：** 令 $q_1, q_2, \cdots, q_m$ 为 m 个不同的素数，满足 $q_i \neq p$。这些 m两两互素的主理想格 $I_{q_1}, I_{q_2}, \cdots, I_{q_m}$ 是用于解密的密钥。
- **公钥：** 令 $A_i = d_i \otimes \mathcal{D}_i (1 \leqslant i \leqslant m)$，则 A_1，A_2，$\cdots$，A_m 是用于加密的公钥。明文空间为$\mathcal{P} = \mathbb{Z}_{t_1} \bigoplus \mathbb{Z}_{t_2} \bigoplus \cdots \bigoplus \mathbb{Z}_{t_m}$，其中 t_i 是由式 (4.1) 给出的 I_{q_i} 的一维模数。m
- **加密：** 对于任意明文 $u = (u_1, u_2, \cdots, u_m) \in \bigoplus \mathbb{Z}_{t_i}$，则$_{i=1}c = f(u)$ $= \bar{u}_1 \otimes A_1 + \bar{u}_2 \otimes A_2 + \cdots + \bar{u}_m \otimes A_m$，其中 $\bar{u}_i$ 是将 u_i 嵌入到 $\mathbb{Z}^n$ 中的嵌入。
- **解密：** 对于给定的密文 $c \in \mathbb{Z}^n$，在正交平行多面体 $\mathcal{F}(I_{q_i})$ 中存在唯一的向量 $\bar{u}_i$，使得 $c \equiv \bar{u}_i (\text{mod } I_{q_i})$，$1 \leq i \leq m$。因此，有$f^{-1}(c) = (u_1, u_2, \cdots, u_m) = u.$

5 结论

在本文中，我们构造了首个无需使用自举变换技术的无界全同态加密方案。如何构造一种用于生成密钥和公钥的概率算法，使得本方案的安全性仅依赖于短整数解问题（SIS）或环短整数解问题（R-SIS），仍然是一个有待解决的问题。据我们所知，目前还没有直接与 SIS 或 R-SIS 相关联的密码系统。另一方面，全同态签名是全同态加密的对偶问题，我们将在后续工作中构造全同态签名方案。

致谢 本研究是在我们访问河南省科学院期间完成的，作者感谢王天泽教授和黄景洛教授的邀请与接待。

参考文献

[1] S. Agrawal、D. Boneh 和 X. Boyen。标准模型下高效的格（H）IBE。载于 EUROCRYPT，553-572，2010年。[2] M. Ajtai。生成格问题的困难实例。Quaderni di Matematica，13:1-32，2004年。初步版本发表于 STOC 1996。[3] M. Ajtai。生成短基问题的困难实例。载于 ICALP，1-9，1999 年。[4] J. Alperin-Sheriff 和 C. Peikert。准线性时间内的实用自举。载于 CRYPTO，1-20，2013年。[5] J. Alwen 和 C. Peikert。为困难随机格生成更短的基。Theory of Computing Systems，48(3):535-553，2011年4月。初步版本发表于 STACS 2009。[6] C. Boura、N. Gama、M. Georgieva 和 D. Jetchev。CHIMERA：结合基于环-LWE 的全同态加密方案。J. Math. Cryptol.，316-338，2020年。

[7]Z. Brakerski。无需模数切换、基于经典 GapSVP 的全同态加密。载于 CRYPTO，868-886，2012年。[8] Z. Brakerski、C. Gentry 和 V. Vaikuntanathan。（分级）无需自举的全同态加密。TOCT，6(3):13，2014年。初步版本发表于 ITCS 2012。[9] Z. Brakerski 和 V. Vaikuntanathan。基于环-LWE、并针对密钥相关消息保证安全性的全同态加密。载于 CRYPTO，505-524，2011年。[10] Z. Brakerski 和 V. Vaikuntanathan。基于（标准）LWE 的高效全同态加密。SIAM J. Comput.，43(2):831-871，2014年。初步版本发表于 FOCS 2011。[11] H. Chen、K. Laine 和 R. Player。简易加密算术库 SEAL v2.1。载于金融密码学与数据安全—FC 2017，3-18，2017年。[12] J. H. Cheon、J.-S. Coron、J. Kim、M. S. Lee、T. Lepoint、M. Tibouchi 和 A. Yun。整数上的批量全同态加密。载于 EUROCRYPT，315-335，2013年。[13] J. H. Cheon、K. Han、A. Kim、M. Kim 和 Y. Song。近似同态加密的自举。载于 EUROCRYPT，360-384，2018年。[14] J. H. Cheon、A. Kim、M. Kim 和 Y. S. Song。用于近似数的算术的同态加密。载于 ASIACRYPT，409-437，2017年。[15] I. Chillotti、N. Gama、M. Georgieva 和 M. Izabachene。更快速的全同态加密：在不到 0.1 秒内完成自举。载于 ASIACRYPT，3-33，2016年。[16] I. Chillotti、N. Gama、M. Georgieva 和 M. Izabachene。TFHE：环面上的快速全同态加密。IACR 密码学电子印刷档案，2018年。[17] J.-S. Coron、A. Mandal、D. Naccache 和 M. Tibouchi。整数上的全同态加密及更短的公钥。载于 CRYPTO，487-504，2011年。[18] J.-S. Coron、D. Naccache 和 M. Tibouchi。整数上全同态加密的公钥压缩与模数切换。载于 EUROCRYPT，446-464，2012年。[19] M. van Dijk、C. Gentry、S. Halevi 和 V. Vaikuntanathan。整数上的全同态加密。载于 EUROCRYPT，24-43，2010年。[20] J. Fan 和 F. Vercauteren。略具实用性的全同态加密。IACR 密码学电子印刷档案，2012年。[21] C. Gentry。一种全同态加密方案。博士论文，斯坦福大学，2009年。[22] C. Gentry。使用理想格的全同态加密。载于 STOC，169-178，2009年。[23] C. Gentry。计算加密数据的任意函数。ACM 通讯，53(3):97-105，2010年。[24] C. Gentry。关于基于最坏情形困难性的全同态加密。载于 CRYPTO，116-137，2010年。[25] C. Gentry、S. Halevi、C. Peikert 和 N. P. S mart。BGV 风格同态加密中的域切换。计算机安全杂志，21(5):663-684，2013年。初步版本发表于 SCN 2012。[26] C. Gentry、S. Halevi 和 N. P. Smart。具有多对数开销的全同态加密。载于 EUROCRYPT，465-482，2012年。

[27] C. Gentry、A. Sahai 和 B. Waters。基于带误差学习的同态加密：概念更简单、渐近速度更快、基于属性的方案。载于 CRYPTO，75–92，2013年。[28] K.G. Kogos、K.S. Filippova 和 A.V. Epishkina。全同态加密方案：研究现状。载于 EIConRus，463–466，2017年。[29]J. Li 和 L. Wang。基于非交换环的无噪声对称全同态加密。载于 IACR 密码学电子印刷档案，2015年。[30] D. Liu。无需噪声消除的实用全同态加密。载于 IACR 密码学电子印刷档案，2015年。[31] V. Lyubashevsky、C. Peikert 和 O. Regev。论环上的理想格与带误差学习。载于 EUROCRYPT，1–23，2010年。[32] D. Micciancio。广义紧致背包、循环格，以及基于最坏情况复杂性假设的高效单向函数。载于 SFCS，356–365，2002年。[33] D. Micciancio。使用 Hermite标准形改进基于格的密码系统。载于 CaLC，126–145，2001年。[34] D. Micciancio 和 C. Peikert。格的陷门：更简单、更紧致、更快速、更小。载于 EUROCRYPT，700–718，2012年。[35] D. Micciancio 和 C. Peikert。小参数下 SIS 和 LWE 的困难性。载于 CRYPTO，21–39，2013年。[36] D. Micciancio 和 O. Regev。基于高斯测度的从最坏情况到平均情况的归约。载于 SIAM 计算杂志，37(1)：267–302，2007年。初步版本见 FOCS 2004。[37] D. Micciancio 和 O. Regev。基于格的密码学。载于《后量子密码学》，147–191。Springer，2009年。[38] C. Peikert。格密码学十年。载于《理论计算机科学基础与趋势》，1–90，2016年。[39] C. Peikert 和 B. Waters。有损陷门函数及其应用。载于 SIAM 计算杂志，40(6)：1803–1844，2011年。初步版本见 STOC 2008。[40] O. Regev。论格、带误差学习、随机线性码与密码学。载于《J. ACM》，56(6)：1–40，2009年。初步版本见 STOC 2005。[41] O. Regev。带误差学习问题。载于 IEEE 计算复杂性会议，191–204，2010年。[42] R. L. Rivest、L. Adleman 和 M. L. Dertouzos。论数据库与隐私同态。载于《安全计算基础》，4(11)：169–180，1978年。[43] N. P. Smart 和 F. Vercauteren。全同态SIMD运算。《设计、编码与密码学》，71(1)：57–81，2014年。初步版本见电子印前报告 2011/133。[44]L. C. Washington。《数学研究生教材——分圆域导论》。施普林格出版社，纽约、海德堡、柏林，1980年。[45] M. Yagisawa。无需自举的全同态加密。载于 IACR 密码学电子印刷档案，2015年。

[46] M. Yagisawa。八元数环上的全同态加密。载于 IACR 密码学电子印刷档案，2015年。[47] Z. Zheng。《现代密码学》第一卷——信息与数学原理经典导论。Springer，2022年。[48] Z. Zheng、K. Tian 和 F. Liu。《现代密码学》第二卷——信息与数学原理经典导论。Springer，2022年。[49] Z. Zheng、F. Liu 和 M. Chen。论高维 RSA 算法——一种基于格与代数数论的公钥密码系统。IJLRET，8(9)：1–16，2022年。[50]Z. Zheng、F. Liu、W. Huang、J. Xu 和 K. Tian。NTRUEncrypt 的一种推广——基于理想格的密码系统。《信息安全杂志》，165–180，2022年。[51] Z. Zheng、F. Liu、Y. Lu 和 K. Tian。循环格、理想格与平滑参数的界。《信息安全杂志》，272–293，2022年。[52] Z. Zheng 和 K. Tian。关于具有更一般扰动的 LWE 密码系统。《信息安全杂志》，127–139，2022年。