> 本文主要记录隐私计算中的同态加密（Homomorphic Encryption，HE）技术，包括部分同态加密（RSA、GM、ElGamal、Paillier）、近似同态加密（BGN）、有限级数全同态加密和全同态加密（DGHV、BGV、BFV、CKKS、GSW、FHEW、TFHE）等技术，**仅供参考**。

由于**篇幅限制**，将同态加密技术的介绍分为四个部分，**第一部分**讲述部分同态加密和近似同态加密技术；**第二部分**讲述 Bootstrapping 和 DGHV、BGV 全同态加密方案；**第三部分**讲述 SIMD 打包技术与 BFV、CKKS 全同态加密方案；**第四部分**讲述 GSW、FHEW、TFHE 全同态加密方案。

在本文中为**简化表示**，将加密记为 $Enc(\cdot)$，解密记为 $Dec(\cdot)$，不标明使用的公钥和私钥代表只有一对公私钥。本文中介绍的加密方案基本都依赖于各种**计算难题**，在之前的文章中有过介绍。

四、（有限级数）全同态加密（续）

4. BFV 加密方案

Fan 和 Vercauteren 在 Brakerski 的研究基础上提出了 BFV 方案[12]，该方案省去了 BGV 方案中多个模数的复杂构造，且降低了同态乘法计算产生的噪声。BFV 方案也利用 RLWE 假设。

在介绍 BFV 方案时，除了范数 $||\cdot||$ 默认为**无穷范数**（最大值）外，其余设置均采用和上述 BGV 方案一致的符号标记。此外，记 $r_q(x)$ 为 x 模 q 的**正常取模**结果（即结果取值满足 $r_q(x)\in[0,q-1]$）。

记 $\lfloor x\rfloor$ 为向下取整，$\lceil x\rceil$ 为向上取整，$\lfloor x\rceil$ 为四舍五入（取离得最近的整数）。

设置消息空间为多项式环 $m\in\mathbb{Z}_t[x]/(x^d+1)$ ，简记为 $m\in R_t$。

4.1 密钥生成算法

这里为简化理解省略了安全参数的要求，详细信息可以参考论文。

1. 随机选取模数 $q>t$，不要求 q,t 为素数，也**不要求它们互素**。计算 $\Delta=\lfloor\frac{q}{t}\rfloor$，即 $q=\Delta\cdot t+r_t(q)$。通常在 BFV 的优化中会设置 $t|q$ ，这里按照一般情况讨论。
2. 随机选取符合 RLWE 问题的 $a,s,e\in R_q$，并计算 $b=[-(as+e)]_q$。（可以随机选取，满足 $||s||=1$，同时设 $||e||\leq B$）。
3. 公钥为 a,b，私钥为 s。

4.2 加密算法

对于明文 $m\in R_t$，随机选取 $u,e_0,e_1\in R_{q_L}$，其中 $||u||=1$，且 e_0,e_1 满足 $||e_0||\leq B,||e_1||\leq B$ 从**小噪声分布**中采样（后续噪声不特殊说明都如此采样）。使用公钥加密过程如下：

$$\vec{c}=Enc(m)=(c_0,c_1)=([\Delta m+bu+e_0]_q,[au+e_1]_q)$$

得到的密文 $\vec{c}$ 可以看作是一个元素为多项式的二维向量。

4.3 解密算法

可以把私钥包装为一个二维向量 $\vec{s}=(1,s)$，使用该私钥解密过程如下：

$$m=Dec(\vec{c})=[\lfloor\frac{t\cdot[\vec{c}\cdot\vec{s}]_q}{q}\rceil]_t=[\lfloor\frac{t\cdot[c_0+c_1\cdot s]_q}{q}\rceil]_t$$

正确性

可以观察到在解密时：

$$[c_0+c_1\cdot s]_q=\Delta m+v+rq$$

其中 r 为整数，代表模 q 运算增加/减少的 q 的个数，$v=eu+e_0+e_1s$ 表示若干小噪声之和，考虑到 $||u||=||s||=1$，则 $||v||\le\gamma_R||e||||u||+||e_0||+\gamma_R||e_1||||s||=(2\gamma_R+1)B$。此时有：

$$\lfloor\frac{t\cdot[c_0+c_1\cdot s]_q}{q}\rceil=m+\frac{t}{q}(v-\epsilon m)+rt$$

其中，$\epsilon=\frac{q}{t}-\Delta=\frac{r_t(q)}{t}<1$，显然要解密成功，需满足 $\frac{t}{q}||v-\epsilon m||<\frac{1}{2}$ 使得**四舍五入消去该项**，从而有：

$$[\lfloor\frac{t\cdot[c_0+c_1\cdot s]_q}{q}\rceil]_t=[m+rt]_t=m$$

正确性成立。可以看出噪声大小主要取决于 $||v||$，应当综合安全和噪声影响合理设置参数。

安全性

由于解决 RLWE 问题是困难的，BFV 方案公开 a,b 作为公钥不会泄露 s 的取值，且在加密时 $u,e_0,e_1\in R_q$ 都是随机选取的，可以认为 BFV 方案是安全的。

加法同态性

BFV 加密方案具有**加法同态性**，可以验证：

$$\begin{aligned}Enc(m_0)+Enc(m_1)&=[\vec{c}_0+\vec{c}_1]_q\\&=(m_0+m_1+b(u_0+u_1)+e_{00}+e_{01},a(u_0+u_1)+e_{10}+e_{11})\\&=Enc(m_0+m_1)\end{aligned}$$

且噪声增长为线性：

$$\begin{aligned}[(\vec{c}_0+\vec{c}_1)\vec{s}]_q&=\Delta(m_0+m_1)+v_0+v_1+r_0q\\&=\Delta[m_0+m_1]_t+v_0+v_1+r_0q+r_1t\Delta\\&=\Delta[m_0+m_1]_t+v_0+v_1+r_1(t\Delta-q)+q(r_0+r_1)\end{aligned}$$

其中，噪声为 $v_0+v_1+r_1(t\Delta-q)+q(r_0+r_1)$，由于 $||r_1||\le1$（因为 $m_0,m_1\in R_t$，$||m_0+m_1||<2t$） 且 $||t\Delta-q||<t$，因此噪声最多额外增长 t。

乘法同态性

BFV 加密方案具有**乘法同态性**。记两个明文 m_0,m_1 对应的密文为 $\vec{c}_0=Enc(m_0)=(c_{00},c_{10})$ 和 $\vec{c}_1=Enc(m_1)=(c_{01},c_{11})$，不妨设：

$$\vec{c}_0\cdot\vec{s}=\Delta m_0+v_0+r_0q\vec{c}_1\cdot\vec{s}=\Delta m_1+v_1+r_1q\frac{t}{q}\cdot(\vec{c}_0\cdot\vec{s})\cdot(\vec{c}_1\cdot\vec{s})=c_0+c_1s+c_2s^2+r_a$$

其中易证 $||r_0||<\gamma_R\cdot||s||$，上述第三个等式的 r_a 为小数，且系数满足方程：

$$c_0=\lfloor\frac{t(c_{00}c_{01})}{q}\rceil c_1=\lfloor\frac{t(c_{00}c_{11}+c_{10}c_{01})}{q}\rceil c_2=\lfloor\frac{t(c_{10}c_{11})}{q}\rceil$$

证明可**参考 BGV 方案**中同态乘法计算中 c_0,c_1,c_2 的计算方式。由此可以看出 r_a 其实是 c_0,c_1,c_2 三项四舍五入舍掉的小数项，属于舍入误差，由于每项舍入最大为 $\frac{1}{2}$，因此满足：

$$||r_a||\le\frac{1}{2}(1+\gamma_R||s||+\gamma_R^2||s||^2)<\frac{1}{2}(1+\gamma_R||s||)^2$$

由于：

$$
\begin{aligned}
(\vec{c}_0 \cdot \vec{s}) \cdot (\vec{c}_1 \cdot \vec{s}) &= (\Delta m_0 + v_0 + r_0 q) \cdot (\Delta m_1 + v_1 + r_1 q) \\
&= \Delta^2 m_0 m_1 + \Delta(m_0 v_1 + m_1 v_0) + v_0 v_1 + q(v_0 r_1 + v_1 r_0) + q\Delta(m_0 r_1 + m_1 r_0) + q^2 r_0 r_1)
\end{aligned}
$$

设 $\epsilon = \frac{q}{t} - \Delta = \frac{r_t(q)}{t} < 1$，且 $m_0 m_1 = [m_0 m_1]_t + r_m t$ 以及 $v_0 v_1 = [v_0 v_1]_\Delta + r_v \Delta$，显然有 $||r_m|| < \frac{\gamma_R ||m_0|| ||m_1||}{t} = \frac{\gamma_R t}{4}$，同理 $||r_v|| < \frac{\gamma_R E^2}{\Delta}$（其中 $||v_i|| < E < \frac{\Delta}{2}$），因此有如下方程成立：

$$
\begin{aligned}
\frac{t}{q} \cdot (\vec{c}_0 \cdot \vec{s}) \cdot (\vec{c}_1 \cdot \vec{s}) &= \Delta m_0 m_1 + m_0 v_1 + m_1 v_0 + \frac{t}{q} v_0 v_1 + t(v_0 r_1 + v_1 r_0) + t\Delta(m_0 r_1 + m_1 r_0) + q t r_0 r_1 - \epsilon(\Delta m_0 m_1 + m_0 v_1 \\
&= \Delta [m_0 m_1]_t + m_0 v_1 + m_1 v_0 + \frac{t}{q}[v_0 v_1]_\Delta + t(v_0 r_1 + v_1 r_0) + (q - r_t(q))(r_m + m_0 r_1 + m_1 r_0) + r_v + q t r_0 r
\end{aligned}
$$

注意，只有算到当前这一步才可以对 q 取模，否则会影响正确性（因为要乘上 $\frac{t}{q}$ 这个小数，**不能提前取模**）。代入前式，有：

$$
\begin{aligned}
\frac{t}{q} \cdot (\vec{c}_0 \cdot \vec{s}) \cdot (\vec{c}_1 \cdot \vec{s}) &= c_0 + c_1 s + c_2 s^2 + r_a \\
&= \Delta [m_0 m_1]_t + m_0 v_1 + m_1 v_0 + t(v_0 r_1 + v_1 r_0) + (q - r_t(q))(r_m + m_0 r_1 + m_1 r_0) + r_v + q t r_0 r_1 + r_r
\end{aligned}
$$

其中 $r_r = \frac{t}{q}[v_0 v_1]_\Delta - \epsilon(\Delta m_0 m_1 + m_0 v_1 + m_1 v_0 + r_v)$ 为小数，且有：

$$
\begin{aligned}
||r_r|| &< \frac{t}{q} \cdot \frac{\Delta}{2} + \frac{t}{q} \cdot (\gamma_R \Delta (\frac{t}{2})^2 + \gamma_R \frac{t}{2} \cdot \frac{\Delta}{2} + \gamma_R \frac{t}{2} \cdot \frac{\Delta}{2} + \frac{\gamma_R \Delta}{4}) \\
&< \frac{1}{2} + \gamma_R (t + \frac{1}{2})^2
\end{aligned}
$$

将小数合并后取模，得到：

$$
\begin{aligned}
[c_0 + c_1 s + c_2 s^2]_q &= \Delta [m_0 m_1]_t + m_0 v_1 + m_1 v_0 + t(v_0 r_1 + v_1 r_0) - r_t(q)(r_m + m_0 r_1 + m_1 r_0) + r_v + r_r - r_a \\
&= \Delta [m_0 m_1]_t + v_2
\end{aligned}
$$

其中：

$$
v_2 = (m_0 v_1 + m_1 v_0) + t(v_0 r_1 + v_1 r_0) - r_t(q)(r_m + m_0 r_1 + m_1 r_0) + r_v + r_r - r_a
$$

经过大量放缩，可以得出噪声上界为：

$$
\begin{aligned}
||v_2|| &< \gamma_R t E + \gamma_R^2 t E ||s|| + t\gamma_R (\frac{t}{4} + \gamma_R ||s||) + \frac{\gamma_R E}{2} + \gamma_R (t + \frac{1}{2})^2 + \frac{1}{2} + \frac{(\gamma_R ||s|| + 1)^2}{2} \\
&< \gamma_R t E (\gamma_R ||s|| + 1) + t^2 \gamma_R^2 (||s|| + 1)^2 + \gamma_R t E (\gamma_R ||s|| + 1) + \frac{1}{2} t^2 \gamma_R^2 (||s|| + 1)^2 + t^2 \gamma_R^2 (||s|| + 1)^2 \\
&= 2\gamma_R t E (\gamma_R ||s|| + 1) + 2t^2 \gamma_R^2 (||s|| + 1)^2
\end{aligned}
$$

由于设置 $||s|| = 1$，可以从上式看出，经过同态乘法计算，噪声从 E 增长到大约 $2\gamma_R^2 t E$，并不像 BGV 方案中平方增长，这也是 BFV 方案的主要创新点。BGV 方案中每做一次乘法都需要进行一次模数转换，而 BFV 中噪声增长**并非平方级别**，不进行模数转换。

BFV 方案之所以噪声不是平方增长，是因为 BFV 在得到 v_2 时进行了一次**放缩**（乘 $\frac{t}{q}$），通过该放缩可以粗略理解为直接**减少了一个次方的噪声**，因此相较于 BGV 方案噪声减少很多。

但类似于 BGV 方案，BFV 方案同态乘法运算后密文也会变成三维向量 (c_0, c_1, c_2)，需要通过 Relinearisation 转换回二维向量。一个可行的办法在 BGV 方案已经讲述过了（BGV同态乘法中的**密钥转换**），BFV 还额外提供了另一个解决方法，通过**类似模数转换**的操作来实现，具体地说，该操作实现如下转换：

$$
[c_0 + c_1 s + c_2 s^2]_q = [c_0' + c_1' s + r]_q
$$

其中 r 为转换引入的噪声，值很小。该方法通过选择一个随机数 $p > q$，然后在 R_{pq} 密文空间中对 ps^2 进行加密，得到：

$$
rlk = ([-(as + e) + ps^2]_{pq}, a)
$$

其中，$a \in R_{pq}$，$||e|| < B_k$（B_k 的选取需要满足一些条件，在论文中给出了公式）。随后可以得到 $c_2 s^2$ 的密文（不直接加密 $c_2 s^2$ 的原因是在预处理阶段不知道 c_2 的取值）：

$$
(c_{20}, c_{21}) = ([\lfloor \frac{c_2 rlk[0]}{p} \rceil]_q, [\lfloor \frac{c_2 rlk[1]}{p} \rceil]_q)
$$

该操作的正确性可以按照 BGV 中的模数转换理解（但不完全一样），为了方便理解，可以堪称上述密文计算相当于从模数 pq 转换为模数 q，因此乘上一个**模数转换缩放因子** $\frac{q}{pq}=\frac{1}{p}$。

正确性容易证明：

$$\begin{aligned}c_{20}+c_{21}s&=c_2s^2+\lfloor\frac{-c_2(as+e)}{p}\rceil+\lfloor\frac{c_2a}{p}\rceil s\\&=c_2s^2+r\end{aligned}$$

其中 r 的大小主要成分为 $\frac{c_2e}{p}$，外加一点小舍入误差，可以得到：

$$\begin{aligned}||r||&<||\frac{c_2e}{p}||+\frac{1}{2}+\gamma_R\cdot\frac{1}{2}\cdot||s||+||\frac{c_2as}{p}||-||\frac{c_2as}{p}||\\&=\frac{\gamma_RqB_k}{p}+\frac{\gamma_R||s||+1}{2}\end{aligned}$$

可以通过合理选取 p 的值来控制该噪声，这样一来，BFV 方案就**以非平方增长的噪声代价实现了同态乘法计算**，能够去除 BGV 方案中复杂的模数构造及大量的模数转换，提高效率。

5. SIMD 技术

SIMD（Simple Instruction Multiple Data）技术在全同态加密中特指一种**数据打包技术**，在 BGV、BFV、CKKS 这些第二代全同态加密方案中具有重要的作用。在介绍 CKKS 加密方案前，先介绍一下 SIMD 打包技术。

BGV 和 BFV 中的 SIMD 技术

由上述 BGV 和 BFV 方案的介绍可知，它们都利用 **RLWE 问题**进行数据加密和运算，加密的明文是一个多项式 $m\in\mathbb{Z}_t[x]/(x^d+1)$，而在实际应用中要处理的数据通常**整数或浮点数**，且往往需要将若干数据以向量表示进行**并行运算**，因此需要一种编码方式，**将向量编码至多项式**，同时还要满足加法和乘法等操作的**正确性**。

BGV 和 BFV 处理整数向量，设要编码的明文向量为 $m=(1,3)$，希望将其编码至多项式环 $m'\in\mathbb{Z}_{16}[x]/(x^2+1)$ 中，一种符合**直觉**的做法是直接将向量作为多项式系数，得到：

$$m'=1+3x$$

该编码满足加法的并行计算：

$$m'+m'=2+6x=Encode(m+m)$$

但**不满足乘法**的并行计算（向量按位乘法 $\odot$）：

$$m'\times m'=1+6x+9x^2=-8+6x\neq Encode(m\odot m)$$

因此该编码方式并不能正确的实现若干数的并行计算，只能对单个数进行编码计算。而 SIMD 技术就是一种能够正确实现并行计算的向量至多项式的编码方式。

单位根和本原单位根

首先了解一些前置知识，即**单位根**和**本原单位根**相关性质。

在**复数域**中，若 $x^n=1$，则称 x 为 n 次单位根。

若 n 次单位根 x 满足对任意 $1\leq i<n$ 有 $x^i\neq 1$，则称 x 为 n 次本原单位根。

显然 $\omega_n=e^{\frac{2\pi i}{n}}$ 为一个 n 次本原单位根，且能生成所有的 n 次单位根 $\{\omega_n^0,\omega_n^1,\cdots,\omega_n^{n-1}\}$。

对于一个 $2n$ 次本原单位根 $\omega_{2n}=e^{\frac{2\pi i}{2n}}$，显然有 $\omega_{2n}^n=-1$，则 $\{\omega_{2n},\omega_{2n}^3,\omega_{2n}^5,\cdots,\omega_{2n}^{2n-1}\}$ 为方程 $x^n+1=0$ 的 n 个解，因此有如下因式分解：

$$x^n+1=(x-\omega_{2n})(x-\omega_{2n}^3)\cdots(x-\omega_{2n}^{2n-1})$$

且由于上述分解每一项**互素**，根据**中国剩余定理**，模 x^n+1 意义下的多项式可以分解为 n 个模 $x-\omega_{2n}^i$ 的多项式，SIMD 编码就是根据上述分解实现的。

具体地，对于待编码向量 $m=(m_0,m_1,\cdots,m_{n-1})$，设其对应的 SIMD 编码多项式为 $p(x)=p_0+p_1x+\cdots+p_{n-1}x^{n-1}$，则有 $p(x)\ mod\ (x-\omega_{2n}^{2i+1})=m_i$ （即可以转换为 $p(x)=m_i+p_1'(x-\omega_{2n}^{2i+1})+p_2'(x-\omega_{2n}^{2i+1})^2+\cdots+p_{n-1}(x-\omega_{2n}^{2i+1})^{n-1}$），因此有：

$$\begin{bmatrix}m_0\\m_1\\\vdots\\m_{n-1}\end{bmatrix}=\begin{bmatrix}(\omega_{2n})^0&(\omega_{2n})^1&\cdots&(\omega_{2n})^{n-1}\\(\omega_{2n}^3)^0&(\omega_{2n}^3)^1&\cdots&(\omega_{2n}^3)^{n-1}\\\vdots&\vdots&\ddots&\vdots\\(\omega_{2n}^{2n-1})^0&(\omega_{2n}^{2n-1})^1&\cdots&(\omega_{2n}^{2n-1})^{n-1}\end{bmatrix}\times\begin{bmatrix}p_0\\p_1\\\vdots\\p_{n-1}\end{bmatrix}=\begin{bmatrix}p(\omega_{2n})\\p(\omega_{2n}^3)\\\vdots\\p(\omega_{2n}^{2n-1})\end{bmatrix}$$

为了得到消息向量 $m=(m_0,m_1,\cdots,m_{n-1})$ 的 SIMD 编码 $p(x)=p_0+p_1x+\cdots+p_{n-1}x^{n-1}$，可以通过如下线性变换得到：

$$\begin{bmatrix}p_0\\p_1\\\vdots\\p_{n-1}\end{bmatrix}=\begin{bmatrix}(\omega_{2n})^0&(\omega_{2n})^1&\cdots&(\omega_{2n})^{n-1}\\(\omega_{2n}^3)^0&(\omega_{2n}^3)^1&\cdots&(\omega_{2n}^3)^{n-1}\\\vdots&\vdots&\ddots&\vdots\\(\omega_{2n}^{2n-1})^0&(\omega_{2n}^{2n-1})^1&\cdots&(\omega_{2n}^{2n-1})^{n-1}\end{bmatrix}^{-1}\times\begin{bmatrix}m_0\\m_1\\\vdots\\m_{n-1}\end{bmatrix}$$

类似地，在模 p 意义上，若 $n|\varphi(p)$，则一定存在 n 次本原单位根（当 n 整除群的阶时，阶为 n 的子群一定存在）。

设 ω_{2n} 为模 p 意义下的一个 $2n$ 次本原单位根，则有如下因式分解：

$$x^n+1=(x-\omega_{2n})(x-\omega_{2n}^3)\cdots(x-\omega_{2n}^{2n-1})$$

与复数域不同的点在与这里的 ω_{2n}^i 均为 $\mathbb{Z}_q$ 中的**整数**，例如：

$$x^2+1=(x-4)(x-13)\ mod\ 17$$

其余如中国剩余定理分解、SIMD编码均与复数域一致。

模意义下的 SIMD 编码

记 BGV 或 BFV 加密的多项式环为 $\mathbb{Z}_q[x]/(x^n+1)$，对于消息向量 $m=(m_0,m_1,\cdots,m_{n-1})\in\mathbb{Z}_q^n$，编码后的多项式为：$p(x)=p_0+p_1x+\cdots+p_{n-1}x^{n-1}$，满足：

$$\begin{bmatrix}p_0\\p_1\\\vdots\\p_{n-1}\end{bmatrix}=\begin{bmatrix}(\omega_{2n})^0&(\omega_{2n})^1&\cdots&(\omega_{2n})^{n-1}\\(\omega_{2n}^3)^0&(\omega_{2n}^3)^1&\cdots&(\omega_{2n}^3)^{n-1}\\\vdots&\vdots&\ddots&\vdots\\(\omega_{2n}^{2n-1})^0&(\omega_{2n}^{2n-1})^1&\cdots&(\omega_{2n}^{2n-1})^{n-1}\end{bmatrix}^{-1}\times\begin{bmatrix}m_0\\m_1\\\vdots\\m_{n-1}\end{bmatrix}$$

容易验证该编码符合**多项式加法与乘法**和整数向量**加法和按位乘法**的对应关系，以乘法为例，有：

$$p(x)\times p'(x)\ mod\ (x-\omega_{2n}^{2i+1})=m_i\times m_i'$$

因此该编码可以用于 BGV 和 BFV 的并行同态计算，从而大大提高实际应用中的效率。

CKKS 的 SIMD 技术

在介绍 CKKS 之前首先介绍一下应用在 CKKS 中的 SIMD 编码技术。

CKKS 方案明文空间为**复数向量** $m\in\mathbb{C}^{\frac{n}{2}}$。对于一个 $2n$ 次本原单位根 $\omega_{2n}=e^{\frac{2\pi i}{2n}}$，由其生成的 $\{\omega_{2n},\omega_{2n}^3,\omega_{2n}^5,\cdots,\omega_{2n}^{2n-1}\}$ 为方程 $x^n+1=0$ 的 n 个解，且满足 $\omega_{2n}^i=\overline{\omega_{2n}^{2n-i}}$ （$\overline{\omega}$ 为 ω 的**共轭复数**），因此对多项式 $p(x)\in\mathbb{C}[x]/(x^n+1)$，设 $p(x)=p_0+p_1x+\cdots+p_{n-1}x^{n-1}$，有 $p(\omega_{2n}^i)=\overline{p(\omega_{2n}^{2n-i})}$，因此有 $p^i=\overline{p^i}$，所以由 $\{\omega_{2n},\omega_{2n}^3,\omega_{2n}^5,\cdots,\omega_{2n}^{2n-1}\}$ 插值而得的多项式 $p(x)$ 的系数**均为实数**（虚部为0）。

CKKS 方案正是利用这一点**将复数向量编码至实数多项式**，考虑到 $p(\omega_{2n}^i) = \overline{p(\omega_{2n}^{2n-i})}$，这意味着待编码向量必须满足 $m_i = \overline{m_{n-1-i}}$，这正是 $m \in \mathbb{C}^{\frac{n}{2}}$ 长度为 $\frac{n}{2}$ 的原因，要将其**扩展**至 m'：

$$m' = (m'_0, m'_1, \cdots, m'_{n-1}) = (m_0, m_1, \cdots, m_{\frac{n}{2}-1}, \overline{m_{\frac{n}{2}-1}}, \cdots, \overline{m_0})$$

将该过程记为 $m' = \pi^{-1}(m)$，显然有 $m = \pi(m')$。设 m' 通过**中国剩余定理**编码为多项式 $p(x)$，该过程记作 $p(x) = \sigma^{-1}(m')$，同时有 $m' = \sigma(p(x))$。

由于编码后的多项式系数为实数，而 CKKS 要使用 RLWE 问题进行加密，因此要将其**转换为整数**。直接转换会引入大量的精度损失，CKKS 方案引入一个**缩放因子** Δ，将多项式系数乘以该缩放因子后取整得到整数多项式（和**安全多方计算**将实数转为定点数存储的方式类似）。

具体地，CKKS 中的编码过程为 $Ecd(m, \Delta)$：

$$Ecd(m, \Delta) = p(x) = \lfloor \Delta \cdot \sigma^{-1}(\pi^{-1}(m)) \rceil$$

同样的，有解码过程记为 $Dcd(p(x), \Delta)$：

$$Dcd(p(x), \Delta) = m = \pi(\sigma(\lfloor \Delta^{-1} \cdot p(x) \rceil))$$

6. CKKS 加密方案

CKKS 方案由 Cheon、Andrey Kim、Miran Kim 和 Song 发表[13]，主要特点是它的明文空间为复数向量，这代表着它支持浮点数（实际上是**编码成定点数**）的加密和运算。浮点数的支持主要体现在加密前的消息编码上，编码之后的加密和运算与 BGV 和 BFV 类似。在介绍本方案时，取模等符号表示与前文 BFV 方案相同，设 CKKS 方案中密文空间多项式为 $R_q = \mathbb{Z}_q[x]/(x^n + 1)$。

6.1 密钥生成算法

1. 随机选取模数 q_0 以及大小在**缩放因子** Δ 附近的随机数 p，再生成 L 个模数 $q_i = q_0 \cdot p^i (1 \leq i \leq L)$。
2. 随机选取符合 RLWE 问题的 $a, s, e \in R_{q_L}$，并计算 $b = [-as + e]_{q_L}$。
3. 公钥为 a, b，私钥为 s

6.2 加密算法

对于明文 $z \in \mathbb{C}^{\frac{n}{2}}$，首先应用 SIMD 技术将其**编码**为多项式 $m = Ecd(z, \Delta) \in R_{q_L}$，随后随机选取 $v, e_0, e_1 \in R_{q_L}$，其中 v 很小，且 e_0, e_1 满足从**小噪声分布**中采样。使用公钥加密过程如下：

$$\vec{c} = Enc(m) = (c_0, c_1) = ([m + bv + e_0]_{q_L}, [av + e_1]_{q_L})$$

6.3 解密算法

可以把私钥包装为一个二维向量 $\vec{s} = (1, s)$，对于模数为 q_l 的密文 $\vec{c}$，使用该私钥解密过程如下：

$$m = Dec(\vec{c}) = [\vec{c} \cdot \vec{s}]_{q_l} = [m + e']_{q_l}$$

随后利用 SIMD **解码**技术计算得到明文 $z = Dcd(m, \Delta)$。

正确性

CKKS 方案的正确性与 BFV 方案类似，只需解密时噪声满足 $||\frac{e'}{\Delta}|| < \frac{1}{2}$ 即可。

安全性

CKKS 的安全性也与 BFV 方案类似，依赖于 RLWE 问题的求解难度。

加法同态性

CKKS 加密方案具有加法同态性，可以验证：

$$
\begin{aligned}
Enc(m_0) + Enc(m_1) &= [\vec{c}_0 + \vec{c}_1]_{q_l} \\
&= \left(m_0 + m_1 + b(v_0 + v_1) + e'\right) \\
&= Enc(m_0 + m_1)
\end{aligned}
$$

与 BFV 方案类似，噪声增长较小。

乘法同态性

CKKS 加密方案具有乘法同态性，验证流程与 BFV 方案类似，不再赘述。注意 CKKS 方案执行完乘法后密文也会**变成三维**，因此也需要执行 Relinearisation （或者称之为密钥转换）将其转换为二维。

与此同时，考虑到 CKKS 在编码时数据放大了 Δ 倍，则执行完同态乘法后数据放大 Δ^2 倍，同时噪声增长较大。CKKS 方案采用类似 BGV 方案的**模数转换**的技术来控制噪声并将放缩倍数调回 Δ 倍，这也是为什么密钥生成时选取 $L+1$ 个模数需要满足 $q_l = q_{l-1} \cdot p$ 且 $p \approx \Delta$ 的原因。

具体缩放操作可以参考 BGV 模数转换，简单来说相当于将密文放缩至 $\frac{q_{l-1}}{q_l} = \frac{1}{p}$ 倍。p 不需要严格等于 Δ，乘法后的放缩相当于把由乘法导致的**有效位数的增加**大致去除掉，即时少去除或多去除一位也仅会产生较小的精度影响。

CKKS 方案每执行一次同态乘法计算都需要进行一次模数转换，因此在不执行 Bootstrapping 技术的情况下也属于**有限级数全同态加密**，由于 Bootstrapping 技术的实现较为复杂，且效率低，通常这类第二代全同态加密方案在实际应用中都被当作有限级数全同态加密使用。

下一部分将介绍 GSW、FHEW、TFHE 全同态加密方案。

参考文献（续）

- [12] J. Fan and F. Vercauteren, “Somewhat Practical Fully Homomorphic Encryption,” 2012, 2012/144. Accessed: Jul. 15, 2025. [Online]. Available: https://eprint.iacr.org/2012/144
- [13] J. H. Cheon, A. Kim, M. Kim, and Y. Song, “Homomorphic Encryption for Arithmetic of Approximate Numbers,” in Advances in Cryptology – ASIACRYPT 2017, Cham: Springer International Publishing, 2017, pp. 409–437.
