

NTRU 型无需密钥交换的全同态加密方案

宋新霞¹, 陈智罡², 周国民³

(1. 浙江万里学院基础学院, 浙江 宁波 315100;
2. 浙江万里学院电子与计算机学院, 浙江 宁波 315100;
3. 浙江警察学院计算机与信息技术系, 浙江 杭州 310053)

摘要: 详细分析了环LWE上NTRU基本加密方案的噪声特性与同态性, 引出了“零次同态加密”的概念, 并且说明了环LWE上NTRU基本加密方案是一个零次同态加密。提出了2个同态加密方案, 展示了如何基于NTRU零次同态加密, 设计NTRU型BGN同态加密方案与全同态加密方案。在该NTRU型全同态加密方案中, 其密钥在密文计算中始终保持不变, 因此, 无需密钥交换就获得了一个全同态加密方案。此外, 该NTRU型全同态加密的密文是一个向量, 相比密文是矩阵的GSW全同态加密方案, 具有存储与传输上的优势。

关键词: 全同态加密; NTRU加密; 环LWE问题; 密钥交换; BGN同态加密

中图分类号: TP309.7

文献标识码: A

doi: 10.11959/j.issn.2096-109x.2017.00117

NTRU-type fully homomorphic encryption scheme without key switching

SONG Xin-xia¹, CHEN Zhi-gang², ZHOU Guo-min³

(1. College of Junior, Zhejiang Wanli University, Ningbo 315100, China;
2. College of Electronic and Computer, Zhejiang Wanli University, Ningbo 315100, China;
3. Department of Computer and Information Technology, Zhejiang Police College, Hangzhou 310053, China)

Abstract: In order to construct a fully homomorphic encryption scheme based on NTRU cryptosystem from ring learning with errors, noise growth and homomorphic property in the NTRU cryptosystem were analyzed. The concept of zero homomorphic encryption was introduced and that the NTRU cryptosystem was zero homomorphic encryption was shown. A BGN homomorphic encryption scheme and a fully homomorphic encryption scheme were proposed based on the NTRU cryptosystem. In the proposed NTRU-type fully homomorphic encryption scheme, the secret key doesn't change in homomorphic multiplications. Thus a fully homomorphic encryption scheme can be obtained without key switching that was used in the previous fully homomorphic encryption schemes. Moreover, the ciphertext is a vector in the proposed NTRU-type fully homomorphic encryption scheme which has the advantage of storage and transmission compared to GSW fully homomorphic encryption scheme where the ciphertext is a matrix.

Key words: fully homomorphic encryption, NTRU cryptosystem, ring learning with errors, key switching, BGN homomorphic encryption

收稿日期: 2016-09-10; 修回日期: 2016-10-30. 通信作者: 陈智罡, zhig.chen@foxmail.com

基金项目: 浙江省自然科学基金资助项目 (No.LYNF020002); 浙江省公益性技术应用研究计划基金资助项目 (No.2017C33079); NSFC—浙江两化融合联合基金资助项目 (No.U1509219); 宁波市自然科学基金资助项目 (No.2016A610226)

Foundation Items: Zhejinag Provincial Natural Science Foundation of China (No.LYNF020002), The Public Projects of Zhejiang Province (No.2017C33079), NSFC-Zhejiang Joint Fund for the Integration of Industrialization Information (No.U1509219), Ningbo Natural Science Foundation (No.2016A610226)

1 引言

全同态加密能够在不知道密钥的情况下,对密文进行任意计算,这种特殊的性质使全同态加密有广泛的应用需求。同态加密的概念自1978年提出后^[1],一直是密码学界的开放难题,直到2009年Gentry提出第一个全同态加密方案^[2]。随后人们基于不同的困难问题,设计出一些全同态加密方案,如小数理想上的全同态加密方案^[3]、整数上的全同态加密方案^[4-6]、LWE(环LWE)上的全同态加密方案^[7-12]。在这些全同态加密方案中,由于环LWE上的全同态加密方案简单、效率高,安全性被归约到格上标准困难问题,并且被认为具有抗量子攻击的特性,所以成为目前主流的全同态加密方案。

目前,环LWE上的全同态加密方案所基于的基本公钥加密方案^[13,14]及其变形^[7],其本身具有加法同态属性,但不具有乘法同态属性。为了使密文能够进行乘法计算,定义密文乘积形式为张量密文 $c_1 \otimes c_2$,对应的密钥是 $s \otimes s$ 。尽管这样定义能够使密文进行乘法计算,但这导致了密文和密钥的维数膨胀,如果不对维数约减的话,将进行不了几次乘法。为此,文献[7]引入了密钥交换技术,通过密钥交换可以将维数膨胀的密文转换成一个正常维数的新密文,对应的密钥是一个正常维数的新密钥。可以说,密钥交换技术导致了环LWE上全同态加密方案的诞生,但密钥交换也是需要付出代价的。

一方面,每次密文乘法计算后,都要将乘积密文与密钥交换矩阵相乘,从而进行密钥交换得到一个正常维数的密文,极大地影响了计算效率;另一方面,密钥交换矩阵是公钥,对一个深度为 L 的全同态加密方案,在公钥中需要包含 L 个密钥交换矩阵。在环LWE的全同态加密方案下,每个密钥交换矩阵是 $3\lceil \log q \rceil \times 2$ 的矩阵,密钥交换矩阵的尺寸是 $6\lceil \log q \rceil n \log q \approx 6n \log^2 q$,而在LWE的全同态加密方案下,每个密钥交换矩阵是 $(n+1)^2 \lceil \log q \rceil \times (n+1)$ 的高维矩阵,密钥交换矩阵的尺寸是 $(n+1)^3 \log^2 q$ 。可见,密钥交换矩阵占用了大量空间。因此,如何去除密钥交换过程是全同态加密研究中一个非常重要的问题。

一个自然的想法就是如果密文是多项式,则多项式的乘积不会引起密文维数的增长。环LWE上的NTRU加密方案的密文是一个多项式,本文首先分析了该方案的噪声特性与同态性,引出了“零次同态加密”的概念,说明NTRU加密方案是一个“零次同态加密”,即密文乘积 $c_1 \cdot c_2$ 本身具有潜在的乘法同态性,但由于噪声增长依赖于密文 c_1 的长度,导致密文乘积噪声过大而丧失了乘法同态性。此外,密钥在密文乘积中是保持不变的。这与先前的张量积形式构造的全同态加密方案是不同的。

为了约减噪声,本文将密文 c_1 的系数展开成位的形式,同时为了获得同态性,将密文 c_2 从多项式“提升”到向量 c_2' ,其中,向量中的每个元素是分别对明文 $2^i m$ ($i=0, \dots, l$) 的加密。即向量中的第一个密文是NTRU加密的原始密文,其他密文都是为了同态性而存在的。密文乘积是行向量与列向量的乘积,即 $\text{BitDecomp}(c_1) \cdot c_2'$,其中, $\text{BitDecomp}(c_1)$ 输出的是行向量。从而构建出一个BGN加密方案,该方案具有加法同态性,但是只能进行一次乘法计算。是因为密文乘积的结果没有提供为了同态性而存在的元素。在此基础上,将密文 c_1 也从多项式“提升”到向量。密文进行乘积时,将向量中的每个元素展开成位的形式,形成一个矩阵,密文乘积是矩阵与向量的乘积,从而获得了乘法同态性,构造出一个全同态加密方案。

本文详细展示了如何基于NTRU零次同态加密,设计一个NTRU型BGN同态加密方案与全同态加密方案。在该NTRU型全同态加密方案中,其密钥在密文计算中始终保持不变,因此无需密钥交换就获得了一个全同态加密方案。此外,该NTRU型全同态加密的密文是一个向量,而GSW全同态加密中的密文是矩阵^[10],因此具有存储与传输上的优势。

2 预备知识

1) 基本符号

令 $q > 1$ 是整数, $\mathbb{Z}_q$ 表示集合 $\left\{-\frac{q}{2}, \frac{q}{2}\right\}$ 。

$R = \frac{\mathbb{Z}[x]}{f(x)}$ 是一个多项式环,其中, $f(x)$ 是一个次数为 n 的多项式, R 上的元素都是次数小于 n 的多

项式。本文选取 $f(x)$ 为一个 n 次分圆多项式 $\varphi(x) = x^n + 1$, n 是 2 的幂次方。 R_q 表示 R 上的多项式的系数属于 $\mathbb{Z}_q$ 的多项式集合。

本文的向量默认为列向量。向量用小写粗体表示, 矩阵用大写粗体表示。 R 上的元素用小写表示。 $()^T$ 表示转置。令 $a \in R$, 则 $a = \sum_{i=0}^{n-1} a_i x^i$, 其中, $a_i \in \mathbb{Z}$ 是多项式 a 的系数, 定义 $\|a\|_\infty = \max\{a_i, a_i \in \mathbb{Z}\}$ 表示无穷范数, 即多项式 a 的系数的最大值。对于 $a, b \in R$, 有 $\|ab\|_\infty \leq n\|a\|_\infty \|b\|_\infty$ 。

如果 q 不是 2 的幂, 则用 $\lceil \log q \rceil$ 表示 $1 + \lfloor \log q \rfloor$ 。令 $l = \lfloor \log q \rfloor$, $a \in R$, a 可以表示成位的形式 $a = \sum_{i=0}^l 2^i u_i$, 其中, $u_i \in R_2$ 。定义 $\text{BitDecomp}(a) = (u_0, u_1, \dots, u_l) \in R_2^{\lceil \log q \rceil}$, $\text{Powerof2}(a) = (a, 2a, \dots, 2^l a) \in R_q^{\lceil \log q \rceil}$ 。有性质 $\langle \text{BitDecomp}(a), \text{Powerof2}(a) \rangle = \langle a, b \rangle \bmod q$ 。注意, $\text{BitDecomp}()$ 的输出看作是行向量, $\text{Powerof2}()$ 的输出看作是列向量。因此, 若 $c \in R_q^l$ 是一个 l 维向量, 则 $\text{BitDecomp}(c)$ 是一个 $l \times l$ 的方阵。

使用 $x \leftarrow \mathcal{D}$ 表示 x 从分布 $\mathcal{D}$ 中取样。为了简单起见, 定义 B 边界分布为从该分布取样的值不超过 B 。如果 $\mathcal{D}$ 是 R 上的 B 边界分布, $x \leftarrow \mathcal{D}$ 表示 x 是一个 B 边界的多项式, 即 $\|x\|_\infty \leq B$ 。

2) 环 LWE 问题与判定小多项式比问题

本文方案的安全性基于判定环 LWE 问题和判定小多项式比问题。环 LWE 问题是 LWE 问题在环上的推广^[13,14]。判定小多项式比问题参考文献[15]。

3) 全同态加密

一个同态加密方案包含 4 个概率多项式算法: 公钥和密钥生成算法、加密算法、解密算法、密文计算算法。具体定义参考文献[2, 7]。另外, BGN 同态加密指的是具有加法同态性, 但是只能进行一次乘法的方案^[16,17]。

3 NTRU 型 BGN 同态加密方案

本节基于文献[11]提出的 NTRU 基本加密方案, 设计一个 BGN 同态加密方案, 该方案具有加法同态性, 但是只能进行一次乘法同态计算。

首先对 NTRU 基本加密方案的加密噪声和解密噪声进行分析, 为后面同态加密方案的噪声分析奠定基础。

3.1 NTRU 基本加密方案的噪声分析

消息空间是 $\{0,1\}$, 环 $R = \mathbb{Z} \frac{[x]}{\varphi(x)}$, 其中, $\varphi(x)$

是一个 n 次分圆多项式, 即 $\varphi(x) = x^n + 1$, n 是 2 的幂次方。所有的密文计算都是在环 R_q 上进行。错误分布 χ 是一个离散高斯分布 $D_{\mathbb{Z}^n, r}$, 其中, r 是标准偏离。从环 R 上的错误分布 χ 中取样, 如 $e \leftarrow \chi$, 则 $e \in R$ 且是一个界为 $r\sqrt{n}$ 的多项式。 λ 是安全参数, 模 q 是素数。设置上述参数使在环 LWE 上能够获得 2^λ 安全。

$\text{E.SecretKeygen}(1^\lambda)$: 选取 $f \leftarrow \chi$, 计算 $f \leftarrow 2f+1$ 使 $f \equiv 1 \pmod{2}$ 。若 f 在 R_q 上是不可逆的, 则重新选取 f 。令私钥 $sk = f \in R$ 。

$\text{E.PublicKeygen}(sk)$: 选取 $g \leftarrow \chi$, 计算 $h = 2g f^{-1} \in R_q$, 令公钥 $pk = h$ 。

$\text{E.Enc}(pk, m)$: 消息 $m \in \{0,1\}$, 选取 $s, e \leftarrow \chi$, 输出密文 $c \leftarrow m + hs + 2e \in R_q$ 。 $\text{E.Dec}(sk, c)$: 输出 $m \leftarrow cf \bmod 2$ 。

下面从加密噪声和解密噪声的角度说明方案的正确性, 也便于下文对同态操作的噪声进行分析。

引理 1 加密噪声

q, n, R_q, χ 是上述加密方案的参数, 令 χ 的上界是 B 。任意 $f \leftarrow \chi$, 计算 $f \leftarrow 2f+1$ 使 $f \equiv 1 \pmod{2}$ 。若 f 在 R_q 上是不可逆的, 则重新选取 f 。任意 $m \in \{0,1\}$ 。令 $h \leftarrow \text{E.PublicKeygen}(f)$, $c \leftarrow \text{E.Enc}(h, m)$, 则存在 v 且 $\|v\|_\infty \leq 3nB^2 + nB$, 使如下等式成立

$$cf = mf + 2v \in R_q$$

其中, v 为密文的噪声。

证明 根据基本加密方案有

$$cf = mf + hsf + 2ef = mf + 2gs + 2ef = mf + 2v \in R_q$$

由于 χ 的上界是 B , 所以 g, s, e 的系数上界是 B , f 的系数上界是 $2B+1$ 。又可知, gs 的系数上界是 nB^2 , ef 的系数上界是 $nB(2B+1)$, 所以, v 的系数上界是 $3nB^2 + nB$, 即 $\|v\|_\infty \leq 3nB^2 + nB$ 。

引理 1 给出了初始密文 (新鲜密文) 的噪声上界。由于密文计算过程中噪声会增长, 而解密的正确性与密文中噪声大小是相关的, 引理 2 给出了密文能够正确解密的噪声界。

引理2 解密噪声

任意 $f, c \in R_q$, 且有 $f \equiv 1 \pmod{2}$ 。若满足

$$cf = mf + 2v \in R_q$$

其中, $m \in \{0,1\}$, $\|v\|_\infty < \frac{q}{4}$ 。则有

$$\text{E.Dec}(f, c) = m$$

证明 如果 $\|v\|_\infty < \frac{q}{4}$, 则有

$$\text{E.Dec}(f, c) = cf \pmod{2} = mf + 2v \pmod{2} = mf \pmod{2} = m$$

引理2说明在解密过程中, 只要保持形如“ $mf + 2v$ ”的解密结构, 且 $\|v\|_\infty < \frac{q}{4}$, 就能够正确解密。

这种保持解密结构的思想在下文设计同态加密属性的过程中非常有用。

3.2 NTRU 型 BGN 同态加密方案

上述 NTRU 基本加密方案具有加法同态性, 但不具有乘法同态性。为了获得乘法同态性, 本文将上述 NTRU 基本加密方案的密文提升成向量的形式, 向量中每个元素是对如下明文的加密: $m, m2, \dots, m2^l$, 向量的长度是 $l = \lceil \log q \rceil - 1$ 。BGN 同态加密方案的参数选择和 NTRU 基本加密方案相同, 方案如下。

1) $\text{BGN.SecretKeygen}(1^\lambda)$: 调用 $sk \leftarrow \text{E.SecretKeygen}(1^\lambda)$ 。

2) $\text{BGN.PublicKeygen}(sk)$: 调用 $pk \leftarrow \text{E.PublicKeygen}(sk)$ 。

3) $\text{BGN.Enc}(pk, m)$: 消息 $m \in \{0,1\}$, 选取 s_i , $e_i \leftarrow \mathcal{X}$ ($i=0, \dots, l$), 输出密文向量 $c = (c_i)$ ($i=0, \dots, l$), 其中, $c_i \leftarrow m2^i + hs_i + 2e_i \in R_q$ 。

4) $\text{BGN.Dec}(sk, c)$: 输出 $m \leftarrow c_0 f \pmod{2}$ 。

5) $\text{BGN.Add}(pk, c_1, c_2)$: 输出 $c_1 + c_2 \in R_q^{l+1}$ 。

6) $\text{BGN.Mult}(pk, c_1, c_2)$: 令 c_{10} 是密文向量 c_1 中的第一个元素, 输出 $\text{BitDecomp}(c_{10}) \cdot c_2 \in R_q^{l+1}$ 。

注意 $\text{BitDecomp}(c_{10})$ 是一个行向量, 其中每个元素是一个系数为 0 或 1 的多项式, 而 c_2 是一个列向量。

上述 BGN 方案的正确性、安全性和 NTRU 基本加密方案是一样的。该 BGN 加密方案的乘法密文的长度非常短, 只是一个多项式, 与基本加密方案的密文长度相同。下面分析这 2 个方案的同态性。

3.3 同态性

由于上述 NTRU 基本加密方案和 BGN 同态加密方案的加法同态性是显然的, 下面只关注其乘法同态性。

3.3.1 NTRU 基本加密方案的同态性

令 $c_i \in R_q$ ($i=1,2$) 是用基本加密方案对明文 $m_i \in \{0,1\}$ 的加密, 其对应密钥是 f , 有 $c_i f = m_i f + 2v_i \in R_q$, 且满足 $\|v_i\|_\infty < \frac{q}{4}$ 。令 $c^\times = c_1 \cdot c_2$, 则 $c^\times f = c_1 \cdot$

$$(m_2 f + 2v_2) = m_2(m_1 f + 2v_1) + 2c_1 v_2 = m_1 m_2 f + 2m_2 v_1 + 2c_1 v_2$$

其中, v_2 和 v_1 的系数都是小的, 但是由于 c_1 是 R_q 上的密文, 所以其系数的界为 $\frac{q}{2}$, 因此密文乘积的噪声主要依赖于密文 c_1 的长度, 由于 $\|c_1 v_2\|_\infty \leq n \frac{q}{2} \|v_2\|_\infty$, 显然噪声值远大于 $\frac{q}{4}$, 因此

密文乘积无法正确解密。所以在乘法同态计算中, 由于噪声依赖于密文导致噪声值过大, 从而一次乘法也无法进行。所以基本加密方案不具有乘法同态性。

这种由于噪声阻碍了同态性的获得的方案, 称为零次同态加密。零次同态加密可以看成是部分同态加密 (somewhat homomorphic encryption) 的极端情况。

3.3.2 BGN 加密方案的同态性

令 c 为用 BGN 加密方案对明文 $m \in \{0,1\}$ 的加密, 对应密钥是 f 。根据解密定义可知 $c f = (c_0 f, c_1 f, \dots, c_l f)^T = (m f + f h s_0 + 2f e_0, m_2 f + f h s_1 + 2f e_1, \dots, m \cdot 2^l f + f h s_l + 2f e_l)^T = (m, m_2, \dots, m_2^l)^T f + 2v = m \text{Powerof2}(f) + 2v$, 其中, $v = g s_i + e_i f$ ($i=0, \dots, l$)。注意 $\text{Powerof2}(f)$ 表示的是一个列向量。

令 $c_i \in R_q^{l+1}$ ($i=1, 2$) 是用 BGN 同态加密方案对明文 $m_i \in \{0,1\}$ 的加密, 其对应密钥是 f , 其中, c_{10} 是密文向量 c_1 中的第一个元素。令 $c^\times = \text{BitDecomp}(c_{10}) \cdot c_2$, 则有

$$\begin{aligned} c^\times f &= \text{BitDecomp}(c_{10}) \cdot (m_2 \text{Powerof2}(f) + 2v_2) \\ &= m_1 m_2 f + 2m_2 v_{10} + 2 \text{BitDecomp}(c_1) \cdot v_2 \in R_q \end{aligned}$$

由于 v_{10} 、 $\text{BitDecomp}(c_1)$ 和 v_2 都是小的, 所以密文乘法可以正确解密, 从而密文进行一次乘法计算。

但是如果 $c^\times$ 再和另外一个乘法密文 $c^{\times'}$ 进行乘法计算, 由于没有 $c^\times$ 和 $c^{\times'}$ 的向量形式密文, 所以按照上述乘法定义将无法计算, 从而只能进

行一次乘法计算。

下面构造一个 NTRU 层次型全同态加密方案。

4 层次型全同态加密方案

在该层次型全同态加密方案中, 密钥在密文计算过程中是保持不变的, 不需要密钥交换。方案如下。

1) FHE.Setup(λ, L): 输入安全参数 λ 和电路深度 L , 输出多项式次数 n 、分圆多项式 $\varphi(x) = x^n + 1$, 其中, n 是 2 的幂次方; 环 $R = \frac{\mathbb{Z}[x]}{\varphi(x)}$ 上的噪声分布 χ , 其界为 B ; 素数模 q 。令 $l = \lceil \log q \rceil - 1$ 。

2) FHE.KeyGen(λ): 选取 $f' \leftarrow \chi$, 计算 $f \leftarrow 2f' + 1$ 使 $f \equiv 1 \pmod{2}$ 。若 f 在 R_q 上是不可逆的, 则重新选取 f' 。令私钥 $sk = f \in R$ 。选取 $g \leftarrow \chi$, 计算 $h = 2gf^{-1} \in R_q$, 令公钥 $pk = h$ 。

3) FHE.Enc(pk, m): 消息 $m \in \{0, 1\}$, 选取 $s_i, e_i \leftarrow \chi$ ($i=0, \dots, l$), 输出密文向量 $c = c_i$ ($i=0, \dots, l$), 其中, $c_i \leftarrow m2^i + hs_i + 2e_i \in R_q$ 。

4) FHE.Dec(sk, c): 输出 $m \leftarrow c_0 f \pmod{2}$ 。

5) FHE.Add(pk, c_1, c_2): 输出 $c_1 + c_2 \in R_q^{l+1}$ 。

6) FHE.Mult(pk, c_1, c_2): 输出 $\text{BitDecomp}(c_1) \cdot c_2 \in R_q^{l+1}$ 。

下面分析该方案的安全性。

定理 1 选择参数 (n, χ, q) 使小多项式比问题和环 LWE 问题的困难性假设成立。 h 和 $hs_i + 2e_i$ ($i=1, \dots, l$) 如全同态加密方案所述, 则分布 $(h, hs_i + 2e_i)$ 与 $R_q \times R_q$ 上均匀选取的元素是不可区分的。

证明 对于任意的 i , 根据加密算法的定义, $hs_i + 2e_i$ 相当于对 0 的加密。根据文献[11]中的小多项式比问题假设, gf^{-1} 与 R_q 上均匀选取的元素不可区分, 所以, 公钥 $h = 2gf^{-1}$ 也是与 R_q 上均匀选取的元素不可区分。又根据文献[14]中 RLWE 困难性的假设, $hs_i + 2e_i$ 与 R_q 上均匀选取的元素不可区分, 所以, 密文 c_i 与 R_q 上均匀选取的元素不可区分。由此证明了上述全同态加密方案的安全性。

下面从同态性和噪声约减 2 个角度进行分析, 从而说明上述方案的正确性。

4.1 同态性分析

由于方案的加法同态性是显然的, 所以只关

注其乘法同态性。

令 $c_i \in R_q^{l+1}$ ($i=1, 2$) 是用扩展加密方案对明文 $m_i \in \{0, 1\}$ 的加密, 其对应密钥是 f , 且有 $c_i f = m_i \text{Powerof2}(f) + 2v_i$, 其中, v_i 中的每个元素都是小的。令 $c^\times$ 是 c_1 与 c_2 的乘积, 由乘法定义可知 $c^\times = \text{BitDecomp}(c_1) \cdot c_2 \in R_q^{l+1}$ 。注意 $\text{BitDecomp}(c_1)$ 是一个 $(l+1) \times (l+1)$ 的方阵, 方阵中的每个元素都是一个多项式, 其系数为 0 或 1, 而 c_2 是一个列向量, 所以乘积的结果 $c^\times$ 依旧是一个长度为 $l+1$ 的向量。下面验证其乘法同态性。

$$\begin{aligned} c^\times f &= \text{BitDecomp}(c_1) \cdot (m_2 \cdot \text{Powerof2}(f) + 2v_2) \\ &= m_2 \cdot (c_1 f) + 2 \text{BitDecomp}(c_1) \cdot v_2 \\ &= m_1 m_2 \cdot \text{Powerof2}(f) + 2m_2 v_1 + 2 \text{BitDecomp}(c_1) \cdot v_2 \end{aligned}$$

$v_2 \in R_q^{l+1}$

由于 v_1 、 $\text{BitDecomp}(c_1)$ 和 v_2 中的元素都是小的, 根据解密算法可以正确解密。因此方案具有乘法同态性。

4.2 密文计算的噪声分析

本节对上述方案的加法和乘法的噪声进行分析, 从而说明方案可以进行多项式深度的同态密文电路计算。

令 $c_i \in R_q^{l+1}$ ($i=1, 2$) 是方案对明文 $m_i \in \{0, 1\}$ 加密的初始密文, 其对应密钥是 f , 且有 $c_i f = m_i \text{Powerof2}(f) + 2v_i$, 其中, $v_i = v_{ij} = gs_j + ef$ ($i=0, 2; j=0, \dots, l$)。令 $E = 3nB^2 + nB$, 则初始密文 c_i 的噪声上界是 E , 即 $\|v_i\|_\infty \leq E$ 。下面分析密文加法与乘法的噪声。

1) 加法噪声分析

根据方案的加法定义, 令 $c^+ = c_1 + c_2$, 则有

$$\begin{aligned} c^+ f &= c_1 f + c_2 f \\ &= (m_1 \text{Powerof2}(f) + 2v_1) + (m_2 \text{Powerof2}(f) + 2v_2) \end{aligned}$$

$$= (m_1 + m_2) \text{Powerof2}(f) + 2(v_1 + v_2)$$

由于 $\|v_i\|_\infty \leq E$ ($i=1, 2$), 所以 $\|v_1 + v_2\|_\infty \leq 2E = 6nB^2 + 2nB$ 。

2) 乘法噪声分析

根据乘法定义, 令 $c^\times = \text{BitDecomp}(c_1) \cdot c_2 \in R_q^{l+1}$, 则有 $c^\times f = m_1 m_2 \text{Powerof2}(f) + 2m_2 v_1 + 2 \text{BitDecomp}(c_1) \cdot v_2 \in R_q^{l+1}$ 。令 c_{1j} 是矩阵 $\text{BitDecomp}(c_1)$ 中的第 j 行向量, 则 c_{1j} 中有 $l+1$ 个系数为 0 或 1 的多项式。另外根据 $\|v_2\|_\infty \leq 3nB^2 + nB$, 得到

$\|c_{1j} \cdot v_2\|_\infty \leq nl(3nB^2 + nB) = nlE$ 。令 $N = nl \approx n \log q$ ，有 $\|BitDecomp(c_1) \cdot v_2\|_\infty \leq NE$ 。由于 $\|v_1\|_\infty \leq E$ ，由此可知 c^x 的噪声为 $(N+1)E$ 。

下面分析深度为 L 的密文电路计算的噪声。这里只考虑乘法，因为乘法的噪声增长远大于加法的噪声增长。首先，分析深度为 2 的乘法电路，令 c_1^x 和 c_2^x 是经过深度为 1 的乘法电路计算的结果，其噪声分别为 v_1' 和 v_2' ，由上可知 $\|v_1'\|_\infty$ 、 $\|v_2'\|_\infty \leq (N+1)E$ 。经过第 2 层乘法电路计算后，其结果记为 c_3^x ，则有 $c_3^x f = m_1 m_2 Powerof2(f) + 2m_2 v_1' + 2BitDecomp(c_1) \cdot v_2'$ 。由于 $\|v_2'\|_\infty \leq (N+1)E$ ，所以 $\|BitDecomp(c_1) \cdot v_2'\|_\infty \leq N(N+1)E$ 。另外 $\|v_1'\|_\infty \leq (N+1)E$ ，所以 c_3^x 的噪声为 $(N+1)^2 E$ 。以此类推，经过深度为 L 的电路计算，其噪声至多为 $(N+1)^L E$ 。只要 $(N+1)^L E$ 不超过 $\frac{q}{4}$ ，密文就能够正确解密。

另外，已知最好的求解 LWE 问题的时间是 $2^{n \log(\frac{q}{B})^{-1}}$ ，环 LWE 问题也类似，所以对于 $\varepsilon < 1$ ，选取 $q = 2^{n^\varepsilon}$ 以及选取 B 为关于 n 的多项式，根据 $(N+1)^L E < \frac{q}{4}$ ，则有 $L \approx \log q \approx n^\varepsilon$ 。这意味着基于上述加法与乘法的定义，方案能够执行一个多项式深度的电路计算，因此是一个层次型全同态加密方案。

4.3 乘法计算优化

在上述 2 个密文乘法计算中，噪声主要依赖于第一个密文（被乘数）的噪声，所以，改变乘法顺序可以优化密文计算。该事实也在文献[18]中观察到。如 $c_i \in R_q^{t+1}$ ($i=1, \dots, 4$) 是 4 个初始密文，每个密文中的噪声都为 E 。上述电路乘法是两两相乘，即将乘积 $c_1 c_2 c_3 c_4$ 分成 $c_5 \leftarrow c_1 c_2$ 和 $c_6 \leftarrow c_3 c_4$ ，然后再计算 $c_5 c_6$ 。如果按照顺序方式乘积，首先计算 $c_5 \leftarrow c_1 c_2$ ，再计算 $c_6 \leftarrow c_5 c_3$ ，最后计算 $c_7 \leftarrow c_6 c_4$ 。根据上面的噪声分析， c_5 的噪声是 $(N+1)E$ ， c_6 的噪声是 $(N+1)E + NE = (2N+1)E$ ， c_7 的噪声是 $(2N+1)E + NE = (3N+1)E$ 。以此类推，那么经过深度为 L 的电路计算，其噪声至多为 $(LN+1)E$ 。这意味着对同样的 L ，经过乘法优化， q 可以取为关于 n 的多项式，即 q 可以变得更小，使计算效率提高。或者说对于同样的 q ，电路深度 L 可以更深。关于全同态加密电路深度与具体参数问题

可以参考文献[19~21]。

5 结束语

环 LWE 上的 NTRU 基本加密方案的密文形式非常简单，就是 R_q 上的一个多项式，因此其乘积形式也非常自然简单，就是 2 个密文多项式的乘积，但其密文乘积的噪声主要依赖于乘积中的第一个密文，所以密文乘积的噪声过大，导致一次乘法也进行不了。为了约减噪声，本文将第一个密文表示成位的形式，将第 2 个密文由多项式提升到向量，设计了一个环 LWE 上的 NTRU 型 BGN 同态加密方案。该 BGN 加密方案的乘法密文的长度非常短，只是一个多项式，与基本加密方案的密文长度相同。然后，将第一个密文也从多项式提升到向量形式，通过上述约减噪声的方法获得了乘法同态性。由于密文乘积是一个方阵与向量的乘积，所以密文乘积的结果还是向量，并没有导致密文乘积的膨胀，从而获得了一个无需密钥交换的全同态加密方案。本文方案与密文是矩阵的 GSW 全同态加密相比，具有存储与传输上的优势。

参考文献:

- [1] RIVEST R L, ADLEMAN L, DERTOUZOS M L. On data banks and privacy homomorphisms[J]. Foundations of Secure Computation, 1978, 4(11): 169-180.
- [2] GENTRY C. Fully homomorphic encryption using ideal lattices[C]//The 41st Annual ACM Symposium on Theory of Computing. 2009: 169-178.
- [3] SMART N P, VERCAUTEREN F. Fully homomorphic encryption with relatively small key and ciphertext sizes[M]//Public Key Cryptography-PKC 2010. Berlin: Springer, 2010: 420-443.
- [4] DIJK M V, GENTRY C, HALEVI S, et al. Fully homomorphic encryption over the integers[M]//Advances in Cryptology-Eurocrypt 2010. Berlin: Springer, 2010: 24-43.
- [5] JEAN-SÉBASTIEN C, AVRADIP M, NACCACHE D, et al. Fully homomorphic encryption over the integers with shorter public keys[M]//Advances in Cryptology-CRYPTO 2011. Berlin Heidelberg: Springer, 2011: 487-504.
- [6] JEAN-SÉBASTIEN C, NACCACHE D, TIBOUCHI M. Public key compression and modulus switching for fully homomorphic encryption over the integers[M]//Advances in Cryptology-Eurocrypt 2012. Berlin Heidelberg: Springer, 2012: 446-464.
- [7] BRAKERSKI Z, VAIKUNTANATHAN V. Efficient fully homomorphic encryption from (standard) LWE[C]//IEEE 52nd Annual Symposium on Foundations of Computer Science, IEEE Computer Society. 2011: 97-106.

- [8] BRAKERSKI Z, GENTRY C, VAIKUNTANATHAN V. (Leveled) fully homomorphic encryption without bootstrapping[C]//The 3rd Innovations in Theoretical Computer Science Conference. 2012: 309-325.
- [9] BRAKERSKI Z. Fully homomorphic encryption without modulus switching from classical gapSVP[M]//Advances in Cryptology-CRYPTO 2012. Berlin Heidelberg: Springer, 2012: 868-886.
- [10] GENTRY C, SAHAI A, WATERS B. Homomorphic encryption from learning with errors: conceptually-simpler, asymptotically-faster, attribute-based[M]//Advances in Cryptology-CRYPTO 2013. Berlin Heidelberg: Springer, 2013: 75-92.
- [11] LÓPEZ-ALT A, TROMER E, VAIKUNTANATHAN V. On-the-fly multiparty computation on the cloud via multikey fully homomorphic encryption[C]//The 44th Symposium on Theory of Computing. 2012: 1219-1234.
- [12] CHEN Z G, WANG J, ZHANG Z N, et al. A fully homomorphic encryption scheme with better key size[J]. China Communications, 2014, 11(9): 89-99.
- [13] REGEV O. On lattices, learning with errors, random linear codes, and cryptography[C]//The 37th Annual ACM Symposium on Theory of Computing. 2005: 84-93.
- [14] LYUBASHEVSKY V, PEIKERT C, REGEV O. On ideal lattices and learning with errors over rings[M]//Advances in Cryptology-EUROCRYPT 2010. Berlin Heidelberg: Springer, 2010: 1-23.
- [15] STEHLÉ D, STEINFELD R. Making NTRU as secure as worst-case problems over ideal lattices[M]//Advances in Cryptology-EUROCRYPT 2011. Berlin Heidelberg: Springer, 2011: 27-47.
- [16] GENTRY C, HALEVI S, VAIKUNTANATHAN V. A simple BGN-type cryptosystem from LWE[M]//Advances in Cryptology-EUROCRYPT 2010. Berlin Heidelberg: Springer, 2010: 506-522.
- [17] BONEH D, GOH E J, NISSIM K. Evaluating 2-DNF formulas on ciphertexts[C]//Theory of Cryptography: Second Theory of Cryptography Conference(TCC 2005). 2005: 325-41.
- [18] BRAKERSKI Z, VAIKUNTANATHAN V. Lattice-based FHE as secure as PKE[C]//The 5th Conference on Innovations in Theoretical Computer Science. 2014: 1-12.
- [19] 陈智罡, 宋新霞, 赵秀凤. 一个 LWE 上的短公钥多位全同态加密方案[J]. 计算机研究与发展, 2016, 53(10): 2216-2223.
CHEN Z G, SONG X X, ZHAO X F. A multi-bit fully homomorphic encryption with better key size from LWE[J]. Journal of Computer Research and Development, 2016, 53(10): 2216-2223.
- [20] 陈智罡, 石亚峰, 宋新霞. 全同态加密具体安全参数分析[J]. 密码学报, 2016, 3(5): 480-491.
CHEN Z G, SHI Y F, SONG X X. Estimating concert security parameters of fully homomorphic encryption[J]. Journal of Cryptologic Research, 2016, 3(5): 480-491.
- [21] 陈智罡, 王箭, 宋新霞. 全同态加密研究[J]. 计算机应用与研究, 2014, 31(6): 1624-1631.
CHEN Z G, WANG J, SONG X X. Survey on fully homomorphic encryption[J]. Application Research of Computer, 2014, 31(6): 1624-1631.

作者简介:



宋新霞 (1973-), 女, 陕西户县人, 浙江万里学院副教授, 主要研究方向为代数密码。



陈智罡 (1972-), 男, 四川资中人, 博士, 浙江万里学院副教授, 主要研究方向为全同态加密、格公钥密码学。



周国民 (1971-), 男, 浙江义乌人, 浙江警察学院副教授, 主要研究方向为网络安全与执法。