基于抽象解密结构的全同态加密构造方法分析

宋新霞[①]　陈智罡*[②③]

[①](浙江万里学院基础学院　宁波　315100)

[②](浙江万里学院电子与计算机学院　宁波　315100)

[③](中国科学院信息工程研究所信息安全国家重点实验室　北京　100093)

摘　要：为什么能够在格上构造全同态加密?密文矩阵的本质及构造方法是什么?该文提出一个重要的概念：抽象解密结构。该文以抽象解密结构为工具，对目前全同态加密构造方法进行分析，得到抽象解密结构、同态性与噪音控制之间的关系，将全同态加密的构造归结为如何获得最终解密结构的问题，从而形式化地建立全同态加密构造方法。最后对 GSW 全同态加密方法分析，提出其密文矩阵是由密文向量堆叠而成。基于密文堆叠法，研究密文是矩阵的全同态加密的通用性原因，给出密文矩阵全同态加密与其它全同态加密之间的包含关系。

关键词：全同态加密；构造方法；抽象解密结构；密文堆叠；学习错误问题

中图分类号：TP309.7　　**文献标识码**：A　　**文章编号**：1009-5896(2018)07-1669-07

DOI: 10.11999/JEIT170997

Analysis of Constructing Fully Homomorphic Encryption Based on the Abstract Decryption Structure

SONG Xinxia[①]　CHEN Zhigang[②③]

[①](*College of Junior*, *Zhejiang Wanli University*, *Ningbo* 315100, *China*)

[②](*College of Electronics and Computer*, *Zhejiang Wanli University*, *Ningbo* 315100, *China*)

[③](*State Key Laboratory of Information Security*, *Institute of Information Engineering*, *Chinese Academy of Sciences*, *Beijing* 100093, *China*)

Abstract: Why can fully homomorphic encryption be constructed based on lattice? What is the essence and construction of the matrix? An important concept is proposed: Abstract decryption structure. Based on the abstract decryption structure, the main factors related to the homomorphic encryption are analyzed and relationship between abstract decryption structure, homomorphism and noise control is studied. The construction of the homomorphic encryption is attributed to the problem of how to obtain the final decryption structure. So the formal method of homomorphic encryption can be established. Thus the essential law of the construction method of the homomorphic encryption construction is expounded, which provides the clue and clue for the construction of the new full homomorphic encryption. The general reason of the full homomorphic encryption of the ciphertext matrix from the point of view of the ciphertexts stack method is studied. The relation between the full homomorphic encryption and the other homomorphic encryption is obtained. Finally, this paper gives a general method of constructing fully homomorphic encryption.

Key words: Fully homomorphic encryption; Construction method; Abstract decryption structure; Ciphertexts stack; Learning With Errors (LWE)

收稿日期：2017-10-24；改回日期：2018-04-03；网络出版：2018-05-11

通信作者：陈智罡　zhig.chen@foxmail.com

基金项目：浙江省科技厅公益性技术科研项目(2017C33079, LGG18F020001)，浙江省自然科学基金(LY17F020002)，密码科学技术国家重点实验室开放课题基金，宁波市自然科学基金(2017A610120)

Foundation Items: The Public Projects of Zhejiang Province (2017C33079, LGG18F020001), The Natural Science Foundation of Zhejiang Province (LY17F020002), The Foundation of the State Key Laboratory of Cryptology, The Ningbo Natural Science Foundation (2017A610120)

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。这种特殊的性质使得全同态加密有广泛的应用需求。2009 年 Gentry[1]提出第 1 个全同态加密，随后人们基于不同的困难问题，设计出一些全同态加密算法，例如：基于小主理想上的全同态加密[2]，基于整数上的全同态加密[3−6]，基于学习错误问题 LWE(环 LWE)上的全同态加密[7−10]。在这些全同态加密中，由于 LWE(环 LWE)上的全同态加密其形式简单、效率高，并且安全性归约到格上标准困难问题[11]，具有抗量子攻击的特性，成为目前主流的全同态加密。同时人们也不断对全同态加密进行优化[12−18]，目前已经实现了全同态加密算法库[19−21]。

为了研究解密结构与同态性之间的关系，我们抽象定义出一个重要概念：抽象解密结构。基于抽象解密结构我们定义了加法和乘法期盼解密结构的概念。将全同态加密的构造分解为两点：一是如何获得期盼解密结构，二是如何控制噪音大小。于是同态性问题归结为如何获得期盼解密结构的问题，噪音控制问题归结为分析噪音依赖主要项的问题。

本文通过抽象解密结构的观点，对现有全同态加密方法进行分析，通过期盼解密结构、噪音依赖主要项、最终解密结构等概念，统一了全同态加密构造方法。由于篇幅有限，我们忽略所有的证明过程。

注意，本文将 BitDecomp$(\bullet)$看作是行向量，而将 Powerof2$(\bullet)$看作是列向量。因此若 $\boldsymbol{c}$ 是一个 $l+1$ 维向量，则 BitDecomp$(\boldsymbol{c})$是一个 $(l+1)\times(l+1)$ 的方阵，Powerof2$(\boldsymbol{c})$是一个 $(l+1)^2$ 维的列向量。

2 解密结构与同态性

本节定义了一个重要的基本概念：抽象解密结构。通过抽象解密结构的概念，研究其与同态性、噪音增长以及密钥长度增长之间的关系。最后引入最终解密结构的概念。如果密文在计算过程中保持最终解密结构，则具有全同态加密的特性。

2.1 抽象解密结构

在 LWE 加密方案中，解密形式是 $\lfloor (2/q)\cdot(\boldsymbol{c}\cdot\boldsymbol{s})\bmod q\rceil \bmod 2$，其中 $\boldsymbol{c}$ 是对明文 $m\in\{0,1\}$ 的加密，$\boldsymbol{s}$ 是密钥。在解密形式中，密文 $\boldsymbol{c}$ 与 $\boldsymbol{s}$ 的内积是一个重要的项，它可表示为

$$\boldsymbol{c}\cdot\boldsymbol{s}=\lfloor q/2\rceil\cdot m+e \pmod q \tag{1}$$

其中，$\lfloor\cdot\rceil$ 表示四舍五入，$\lfloor\cdot\rfloor$ 表示向下取整。只要噪音 e 是小的，就能够正确解密。从某种程度上，它反映了密文与明文及噪音之间的关系，因此可以用于分析密文计算的同态性与噪音增长。因此我们单独将其拿出来进行定义。

定义 1 抽象解密结构：在密文的解密形式中，我们将密文 $\boldsymbol{c}$ 与密钥 $\boldsymbol{s}$ 计算结果的结构形式抽象为

$$c\odot s=x\cdot m+e \pmod q \tag{2}$$

其中，$\odot$是抽象计算符号，m 是明文，e 是噪音，q 表示模，x 是常数。式(2)称为密文 c 与密钥 s 计算结果的抽象解密结构。

由 LWE 解密形式可知，抽象解密结构对应的解密形式为$\lfloor (1/x)(c\odot s)\bmod q\rceil \bmod 2$。只要噪音 e 是小的，就可以恢复出明文 m。

此外，由于每次加密时密文、明文和噪音都是变化的，而密钥是不变的，可将 c, m 和 e 视为变量，s 视为常量。从抽象解密结构 $c\odot s=x\cdot m+e$ 可以清楚的看到密文 c、明文 m 和噪音 e 三者之间是一次形式，即线性关系。这种线性关系直接蕴含了同态性，这也是为什么格上能够构造全同态加密的根本原因。后面将逐步论证。

抽象解密结构的定义适用于所有格上的加密方案。根据目前 LWE 以及环 LWE 上的已知加密方案，将其归类为 3 种类型的解密结构：第 1 种：$c\odot s=<c,s>=\lfloor q/2\rceil\cdot m+e \pmod q$；第 2 种：$c\odot s=<c,s>=m+2e \pmod q$；第 3 种：$c\odot s=c\cdot s=s\cdot m+e \pmod q$。前两种存在于 LWE 或环 LWE 上的加密[8,9]，最后一种存在于环 LWE 上的 NTRU 加密[22]。

密文计算结果的解密结构的形式反映了其同态性，下面的引理给出了这种关系。

引理 1 假设两个密文分别对明文 m_1 与 m_2 加密，且其抽象解密结构分别为 $x\cdot m_1+e_1 \pmod q$ 和 $x\cdot m_2+e_2 \pmod q$。如果两个密文相加具有解密结构的形式为

$$x\cdot(m_1+m_2)+e^{+} \pmod q \tag{3}$$

只要 e^{+}足够小，则其密文加法具有加法同态性。同理，如果两个密文相乘具有解密结构形式为

$$x\cdot(m_1\cdot m_2)+e^{\times} \pmod q \tag{4}$$

只要 $e^{\times}$ 足够小，则其密文乘法具有乘法同态性。

定义 2 期盼解密结构：称形如式(3)和式(4)的解密结构的形式，分别为密文加法和乘法的期盼解密结构。

当密文的加法或乘法具有期盼解密结构的形式，只要噪音是小的，则具有同态性。因此期盼解密结构为我们揭示了，密文计算结果具有什么样的密文解密结构才可能获得同态性。那么对于上述 3 种解密结构，通过什么样的密文计算形式才能够获得期盼解密结构呢？下面研究该问题。

2.2 密文乘法期盼解密结构的构造

同态性与两个因素有关，一是期盼解密结构，二是噪音大小。为了研究密文乘法期盼解密结构的构造，假设密文中的噪音是小的，使得研究的重点聚焦在密文乘法上。由于 LWE 及环 LWE 上的加密方案，其加法同态性是本身具有的，所以只关注乘法同态性。

根据期盼解密结构以及 3 种具体的解密结构，我们得出可以通过以下两种形式构造密文乘法的期盼解密结构：一是采用 $(c_1 \odot s)\cdot(c_2 \odot s)$ 形式，另一个是采用 $c_1 \cdot c_2 \cdot s$ 形式。下面研究上述两种形式与目前 3 种具体解密结构之间的关系。

引理 2　如果采用 $(c_1 \odot s)\cdot(c_2 \odot s)$ 形式构造密文乘法的期盼解密结构，则上述 3 种类型的解密结构都可通过该形式获得期盼解密结构，并且该形式构造密文乘法期盼解密结构的一个共同特征是密钥长度在计算过程中是改变并且增长的。

从引理 2 可知，采用 $(c_1 \odot s)\cdot(c_2 \odot s)$ 角度出发构造密文乘法的同态性适用于 3 种解密结构，具有通用性。但是其特征是会引起密钥长度的增长。所以为了获得更多的乘法次数，每次乘法后需要使用密钥交换约减密文长度。尽管密钥交换操作是构造全同态加密的基石，但是影响了计算的效率，而且使得密文乘法非常复杂。因此，一个自然的想法就是如何能够在密文计算过程中保持密钥长度不变，从而密文的长度也不变。

下面引理 3 告诉我们，基于第 3 种解密结构，从 $c_1 \cdot c_2 \cdot s$ 形式出发构造密文乘法的期盼解密结构，在计算过程中可以保持密钥长度不变。

引理 3　如果采用 $c_1 \cdot c_2 \cdot s$ 形式构造密文乘法的期盼解密结构，则上述 3 种类型的解密结构中，只有第 3 种类型的解密结构通过该形式可获得期盼解密结构，并且该形式构造密文乘法期盼解密结构的一个共同特征是在计算过程中密钥长度是保持不变的。

上述引理给出了从解密结构出发构造期盼解密结构的方法，即构造同态性的方法，但是有个前提是密文计算的噪音是小的才能够保证同态性的获得。下面研究解密结构与噪音增长之间的关系。

2.3 解密结构与噪音增长依赖主要项

不同的解密结构，其密文计算的噪音增长形式不同，可以通过噪音增长依赖主要项来刻画。

引理 4　如果从 $(c_1 \odot s)\cdot(c_2 \odot s)$ 形式构造密文乘法的同态性，则第 1 种解密结构噪音增长依赖的主要项是密钥的长度，第 2 种解密结构和第 3 种解密结构噪音增长依赖的主要项都是密文噪音的乘积。

引理 5　如果从 $c_1 \cdot c_2 \cdot s$ 形式构造密文乘法的同态性，则其噪音增长依赖的主要项是密文的长度。

当噪音增长依赖的主要项是 $\|c_1\|_\infty$ 时，导致噪音过大，一次乘法也计算不了。这种加密方案是 Somewhat 同态加密的一种极端情况，我们称之为零次同态加密。

定义 3　零次同态加密：如果加密方案由于噪音增长过大，导致一次乘法也计算不了，而无法获得同态性，则称之为零次同态加密。

例如第 1 种解密结构噪音增长依赖于密钥长度，其对应加密方案是零次同态加密方案。第 3 种解密结构噪音增长依赖于密文长度，其对应加密方案也是零次同态加密方案。

以上引理给出了密文乘积噪音增长的主要来源，因此对噪音依赖的主要项进行约减，可以降低密文乘积的噪音增长。例如，噪音增长依赖的主要项是密钥的长度，则可将密钥表示为 BitDecomp(s)，即将密钥按位展开，例如 Bra12 方案[8]。对于噪音增长依赖的主要项是密文噪音的乘积，则可使用模交换，例如 BGV 方案[9]。对于噪音增长依赖的主要项是密文的长度，则可将密文表示为 BitDecomp(c_1)，例如 GSW 方案[10]。注意，约减噪音的同时还需要满足期盼解密结构，否则同态性将丧失。

2.4 最终解密结构

上面是将同态性与噪音分开讨论的，下面将其合在一起讨论，因为只有这样才能获得真正的密文计算的同态性。那么这样的解密结构具有什么形式呢？下面引出最终解密结构的概念。

定义 4　最终解密结构：如果该解密结构在某种密文乘法计算形式下，能够获得密文乘法期盼解密结构，并且密文的噪音增长是小的，则称之为最终解密结构。

从定义可知，最终解密结构包含两个核心部分：一是解密结构，二是密文乘法计算形式。其意义为：该解密结构在该密文乘法计算形式下，具有潜在的同态性，并且能够正确解密，从而获得同态性。

注意噪音约减技术与同态性都隐含在最终密文乘法计算形式中。所以具有最终解密结构的密文具有密文计算同态性，而且密文计算的噪音是小的，所以能够进行下一次同态计算。

最终解密结构同时解决了密文计算的同态性和噪音增长问题。但是根据引理 2，有些全同态加密在密文计算的过程中密钥的长度是增长的(相应密文长度也增长)。因此在具体的全同态加密方案中，

还需要额外通过密钥交换技术解决密文计算过程中的密钥长度增长问题。由此得到下面的引理 6。

引理 6 如果密文在计算过程中始终保持最终解密结构，并且能够保持密钥长度(对应于密文长度)不变，则对应加密方案具有全同态加密的特性。

引理 6 刻画了要想获得全同态加密，需要解决密文计算的同态性、密文计算中噪音增长以及密钥长度增长的问题。而密文计算的同态性与密文计算中噪音增长的问题，可以通过构造最终解密结构来解决。密钥长度增长问题是由密文乘法的期盼解密结构的构造形式决定的，可以通过密钥交换技术解决。此外，如果密文计算的电路深度很浅(即密文乘法次数很小)，为了提高效率可以不进行密钥交换，此时的加密方案称为有限同态加密(Somewhat 同态加密)。

采用 $(c_1 \odot s)\cdot(c_2 \odot s)$ 形式构造全同态加密时，第 1 种解密结构 $< c,s >= \lfloor q/2 \rfloor \cdot m + e \pmod q$ 的最终解密结构中的解密结构是

$$\begin{aligned} &< \text{Powerof2}(c), \text{BitDecomp}(s) > \\ &=< c,s >= \lfloor q/2 \rfloor \cdot m + e \pmod q \end{aligned} \tag{5}$$

该形式将同态性与噪音约减形成一个完整的形式描述。密文乘法同态的计算形式是

$$\lfloor (2/q)(\text{Powerof2}(c_1) \otimes \text{Powerof2}(c_2)) \rceil \pmod q \tag{6}$$

对应的密钥是 $\text{BitDecomp}(s) \otimes \text{BitDecomp}(s) \cdot \pmod q$。

第 2 种解密结构 $< c,s >= m + 2e \pmod q$，其最终解密结构中的解密结构还是 $< c,s >= m + 2e \pmod q$。采用的噪音约减技术是模交换，密文乘法同态的计算形式是

$$\left(q^* / q\right)\cdot\left(c_1 \otimes c_2\right) \tag{7}$$

对应的密钥是 $s \otimes s\left(\bmod q^*\right)$，其中 q^* 是用于模交换的模。

第 3 种解密结构与第 2 种解密结构一样。

采用 $(c_1 \odot s)\cdot(c_2 \odot s)$ 形式构造全同态加密，能够应用于全部 3 种解密结构，其构造方法通过上述引理已经刻画的非常清晰。注意，密文的加密形式在该形式构造全同态加密的过程中并没有改变，仍然使用基本加密形式。其原因是最终解密结构中的解密结构与最初的解密结构形式一样，所以加密形式也不变。由于基本加密形式具有期盼解密结构(即潜在的同态性)，主要面临的问题是控制密文计算过程中的噪音增长。因此为了获得同态性，在密文计算过程中加入了噪音约减技术。

但是根据引理 3，采用 $c_1 \cdot c_2 \cdot s$ 形式构造全同态加密只能应用于第 3 种解密结构。此外 $c_1 \cdot c_2 \cdot s$ 形式构造密文乘法的期盼解密结构，具有保证密钥长度不变的良好性质。下面我们研究 $c_1 \cdot c_2 \cdot s$ 形式构造全同态加密。

3 密文矩阵的解密结构

根据引理 3 知道，只有第 3 种解密结构能够采用 $c_1 \cdot c_2 \cdot s$ 形式构造密文乘法的同态性，那么能否利用第 1 种解密结构构造出第 3 种解密结构，从而 $c_1 \cdot c_2 \cdot s$ 形式能够应用于全部3种解密结构呢？下面研究该问题。

3.1 密文矩阵的解密结构

假设密文矩阵 $\boldsymbol{C}$ 表示在密钥 $\boldsymbol{s}$ 下对明文 m 的加密，根据抽象密文结构的定义，其解密结构应该具有形式 $\boldsymbol{C}\cdot\boldsymbol{s} = x\cdot m + e \pmod q$。注意这里每个符号都是一个变量，我们只考虑抽象层次的描述，具体的内容可以根据所依赖的困难问题给出。例如，如果是 LWE 上的加密，密钥变量 $\boldsymbol{s}$ 就代表一个 $\mathbb{Z}_q^{n+1}$ 上的向量，密文变量 $\boldsymbol{C}$ 代表的是一个宽度为 n+1 维的矩阵。

令密文 $\boldsymbol{C}_1$ 和 $\boldsymbol{C}_2$ 的抽象解密结构分别为 $\boldsymbol{C}_1\cdot\boldsymbol{s} = x\cdot m_1 + e \pmod q$ 和 $\boldsymbol{C}_2\cdot\boldsymbol{s} = x\cdot m_2 + e \pmod q$。加法的解密结构显然是满足期盼加密结构的，因此主要研究密文矩阵乘法的解密结构。

由上可知密文 $\boldsymbol{C}_1$ 和 $\boldsymbol{C}_2$ 的乘积所对应的抽象解密结构为 $\boldsymbol{C}_1\cdot\boldsymbol{C}_2\cdot\boldsymbol{s} = \boldsymbol{C}_1\cdot x\cdot m_2 + \boldsymbol{C}_1\cdot e \pmod q$。因此，当密文 $\boldsymbol{C}$ 的解密结构为式(8)形式

$$\boldsymbol{C}\cdot\boldsymbol{s} = \boldsymbol{s}\cdot m + e \pmod q \tag{8}$$

则密文加法和乘法满足所对应的期盼解密结构，当噪音是小时，则可获得同态性。显然密文矩阵的解密结构属于第 3 种解密结构。

3.2 密文矩阵的最终解密结构

根据引理 5，形如式(8)的解密结构其噪音增长依赖的主要项是密文 $\boldsymbol{C}_1$，因此为了约减噪音可以将密文 $\boldsymbol{C}_1$ 表示为二进制位的形式，即 $\text{BitDecomp}(\boldsymbol{C}_1)$，则其噪音主要项由 $\boldsymbol{C}_1\cdot e$ 变为 $\text{BitDecomp}(\boldsymbol{C}_1)\cdot e$。注意这里 $\text{BitDecomp}(\boldsymbol{C}_1)$ 是对密文矩阵 $\boldsymbol{C}_1$ 中的行进行操作，即将行表示成二进制位的形式。密文乘积的解密结构变为

$$\begin{aligned} &\text{BitDecomp}(\boldsymbol{C}_1)\cdot\boldsymbol{C}_2\cdot\boldsymbol{s} \\ &= \text{BitDecomp}(\boldsymbol{C}_1)\cdot\boldsymbol{s}\cdot m_2 \\ &\quad + \text{BitDecomp}(\boldsymbol{C}_1)\cdot e_2 \pmod q \end{aligned} \tag{9}$$

但是式(9)不满足乘法期盼解密结构，即其同态性丧失，原因是 $\text{BitDecomp}(\boldsymbol{C}_1)$ 对应的密钥是 $\text{Powerof2}(\boldsymbol{s})$ 而不是 $\boldsymbol{s}$。为了再次获得同态性，需要调整密文 $\boldsymbol{C}$ 的解密结构为

$$\boldsymbol{C}\cdot\boldsymbol{s}=\text{Powerof2}(\boldsymbol{s})\cdot m+e\ (\text{mod}\,q) \tag{10}$$

对应的密文乘积解密结构变为

$$\begin{aligned}&\text{BitDecomp}(\boldsymbol{C}_1)\cdot\boldsymbol{C}_2\cdot\boldsymbol{s}\\&=\text{BitDecomp}(\boldsymbol{C}_1)\cdot\text{Powerof2}(\boldsymbol{s})\cdot m_2\\&\quad+\text{BitDecomp}(\boldsymbol{C}_1)\cdot e_2(\text{mod}\,q)\\&=\text{Powerof2}(\boldsymbol{s})\cdot m_1\cdot m_2+m_2\cdot e_1+e^{\times}(\text{mod}\,q)\end{aligned} \tag{11}$$

此时密文乘积 $\text{BitDecomp}(\boldsymbol{C}_1)\cdot\boldsymbol{C}_2$ 所对应的解密结构不但满足期盼解密结构，而且满足噪音是小的要求。

因此，式(10)的解密结构是密文矩阵的最终解密结构，该形式是将同态性、噪音约减、密钥不变三者融合在一起的完整表达。密文乘法同态的计算形式是 $\text{BitDecomp}(\boldsymbol{C}_1)\cdot\boldsymbol{C}_2$，对应密钥是 $\boldsymbol{s}$。从解密结构式(8)到最终解密结构式(10)，形式上添加了若干项，其目的是配合约减噪音与保持同态性。

4　密文堆叠的加密形式

LWE 的密文可以抽象成式(12)的形式：

$$\begin{aligned}\boldsymbol{c}&\leftarrow(m,0,\cdots,0)+\boldsymbol{A}^{\mathrm{T}}\boldsymbol{r}(\text{mod}\,q)\\&=(m,0,\cdots,0)+\boldsymbol{c}_0(\text{mod}\,q)\end{aligned} \tag{12}$$

其中，m 是明文，$\boldsymbol{A}=[\boldsymbol{b}\mid\boldsymbol{A}']$ 是 LWE 矩阵也是公钥(即有性质 $\boldsymbol{A}\boldsymbol{s}=\boldsymbol{b}-\boldsymbol{A}'\boldsymbol{s}'=\boldsymbol{e}'$，其中 $\boldsymbol{e}'$ 是错误向量，$\boldsymbol{s}=(1,-\boldsymbol{s}')$ 是私钥)，$\boldsymbol{r}$ 是随机向量。注意 $\boldsymbol{c}_0$ 是对 0 的加密。

由于 LWE 上的密文是向量，所以设计 LWE 上密文是矩阵的全同态加密，一个直观的想法就是将若干个 LWE 密文向量堆叠成一个矩阵 $\boldsymbol{C}$。但是，这种堆叠不是简单的堆叠，而是需要满足同态性以及噪音增长需求。

假设密文 $\boldsymbol{C}$ 是由一些 LWE 密文堆叠而成，根据 LWE 加密形式可以抽象为

$$\boldsymbol{C}\leftarrow\boldsymbol{M}+\boldsymbol{C}_0(\text{mod}\,q) \tag{13}$$

其中，$\boldsymbol{M}$ 是关于明文 m 的未知量，$\boldsymbol{C}_0$ 的每一行是对 0 的加密。则密文 $\boldsymbol{C}$ 的解密结构为

$$\boldsymbol{C}\cdot\boldsymbol{s}\leftarrow\boldsymbol{M}\cdot\boldsymbol{s}+\boldsymbol{C}_0\cdot\boldsymbol{s}=\boldsymbol{M}\cdot\boldsymbol{s}+\boldsymbol{e}(\text{mod}\,q) \tag{14}$$

称该解密结构为“实际解密结构”，其中 $\boldsymbol{e}$ 是噪音变量。

根据引理 6 的结论，如果上述实际解密结构满足最终解密结构的形式，则式(13)的加密形式将满足同态性与噪音增长要求，即是一个全同态加密。因此，我们在最终解密结构与实际解密结构之间建立等式关系，求出关于明文 m 的未知量 $\boldsymbol{M}$，即可得到具体的加密形式。

4.1 密文矩阵的零次同态加密形式

以 LWE 加密为例，我们用 LWE 密钥 $\boldsymbol{s}$ 代替式(8)解密结构中的密钥变量 s，在解密结构与实际解密结构之间建立等式关系有：

$$\boldsymbol{M}\cdot\boldsymbol{s}+\boldsymbol{e}=\boldsymbol{s}\cdot m+\boldsymbol{e}(\text{mod}\,q) \tag{15}$$

因此有 $\boldsymbol{M}\cdot\boldsymbol{s}=\boldsymbol{s}\cdot m\ (\text{mod}\,q)$，解出 $\boldsymbol{M}$ 得到 $\boldsymbol{M}=m\cdot\boldsymbol{I}(\text{mod}\,q)$，其中 $\boldsymbol{I}$ 为单位矩阵。根据式(13)，矩阵 $\boldsymbol{C}$ 的加密形式为

$$\boldsymbol{C}\leftarrow m\cdot\boldsymbol{I}+\boldsymbol{C}_0(\text{mod}\,q) \tag{16}$$

由于密钥 $\boldsymbol{s}$ 是长度为 $n+1$ 的向量，则根据式(8)可知密文 $\boldsymbol{C}$ 是 $(n+1)\times(n+1)$ 的矩阵，而 $\boldsymbol{I}$ 为 $(n+1)\times(n+1)$ 的单位矩阵。

上述加密就是将 LWE 加密转化为密文是矩阵的一个零次同态加密方案。上述形式充分说明了密文矩阵 $\boldsymbol{C}$ 是由若干 LWE 密文向量堆叠而成，其中密文矩阵 $\boldsymbol{C}$ 中的第 1 个密文向量 $\boldsymbol{c}_1$ 是对明文 m 真正的加密，而其它密文向量都是对明文 0 的加密，可以看成是为了形成密文矩阵 $\boldsymbol{C}$ 而添加的辅助项。下面通过噪音约减将其构造为一个全同态加密。

4.2 密文矩阵的全同态加密形式

同理，如果在最终解密结构与实际解密结构之间建立等式关系有

$$\begin{aligned}\boldsymbol{M}\cdot\boldsymbol{s}+\boldsymbol{e}&=\text{Powerof2}(\boldsymbol{s})\cdot m+\boldsymbol{e}(\text{mod}\,q)\\&=\boldsymbol{G}\cdot\boldsymbol{s}\cdot m+\boldsymbol{e}(\text{mod}\,q)\end{aligned} \tag{17}$$

其中，$\boldsymbol{G}=\text{Powerof2}(\boldsymbol{I})$，$\boldsymbol{I}$ 为单位矩阵。注意 $\text{Powerof2}(\boldsymbol{I})$是对 $\boldsymbol{I}$ 中的每一列进行操作。式(17)是一个关于未知量 $\boldsymbol{M}$ 的方程，从中解出 $\boldsymbol{M}$ 得到 $\boldsymbol{M}=\boldsymbol{G}\cdot m$。根据式(13)，矩阵 $\boldsymbol{C}$ 的加密形式为：$\boldsymbol{C}\leftarrow\boldsymbol{G}\cdot m+\boldsymbol{C}_0(\text{mod}\ \ q)$。注意该加密形式对应的最终解密结构为式(10)，密文乘法同态的计算形式是 $\text{BitDecomp}(\boldsymbol{C}_1)\cdot\boldsymbol{C}_2$，密钥 $\boldsymbol{s}$ 在计算过程中保持不变。

上述推导过程给出了一种通用的保持密钥不变的全同态加密的设计方法。该设计方法具有“机械化”的特征，就像求解数学公式一样，在最终解密结构与实际解密结构之间建立关于明文的等式关系，从而求解出一个全同态加密方案。该方法具有通用性。

推论 1　如果基本加密方案的密文抽象解密结构具有 $c\odot s=x\cdot m+e(\text{mod}q)$形式，则可以构造一个密文是矩阵的全同态加密。密文矩阵 $\boldsymbol{C}$ 具有形式 $\boldsymbol{C}\leftarrow\boldsymbol{G}\cdot m+\boldsymbol{C}_0(\text{mod}\,q)$，其中 $\boldsymbol{G}=\text{Powerof2}(\boldsymbol{I})$ 且 $\boldsymbol{I}$ 为单位矩阵，$\boldsymbol{C}_0$ 的每一行是对 0 的加密。最终解密结构为 $\boldsymbol{C}\cdot\boldsymbol{s}=\text{Powerof2}(\boldsymbol{s})\cdot m+\boldsymbol{e}(\text{mod}\,q)$。密文 $\boldsymbol{C}_1$ 和 $\boldsymbol{C}_2$ 乘积的计算形式为 $\text{BitDecomp}(\boldsymbol{C}_1)\cdot\boldsymbol{C}_2(\text{mod}\,q)$。

5　通用构造方法

基于前面的理论，本节给出一个通用的全同态加密设计方法。

5.1 构造思想

根据前面的分析，我们认为设计格上全同态加密的基石是解密结构，技术关键是构造一种满足密文乘法同态性的密文计算形式(即期盼解密结构)，技术路径是采用两种形式构造，即 $(c_1 \odot s)\cdot(c_2 \odot s)$ 形式或 $c_1 \cdot c_2 \cdot s$ 形式，目标是构造出最终解密结构。

5.2 通用构造方法

通用构造方法如下：

(1)建立解密结构： 目前格上加密方案的解密结构都可以抽象为：$c \odot s = x \cdot m + e(\mathrm{mod}\, q)$，可以具体细分为 3 种形式，见 3.1 节。

(2)构造密文乘法的期盼解密结构：分析同态性： 假设噪音是小的情况下，分析同态性的获得。目前可以采用两种形式构造，一是采用 $(c_1 \odot s)\cdot(c_2 \odot s)$ 形式，另一个是采用 $c_1 \cdot c_2 \cdot s$ 形式。

(3)分析噪音依赖主要项：噪音控制： 不同的解密结构，其密文计算的噪音增长形式不同，可以通过分析噪音增长依赖主要项，并且选择相应方法对其约减，从而达到在密文计算过程中控制噪音增长目的。

(4)建立最终解密结构：获得同态性： 如果控制噪音后依然保持同态性，则(1)中的解密结构就是最终解密结构。否则需要回到第 1 步，建立新的解密结构，直到获得最终解密结构。

(5)加密形式： 如果最终解密结构中的解密结构与原解密结构相同，则使用相同的加密算法。如果不同，则根据新的解密结构推导出新的加密算法。

(6)解密形式： 解密形式不变。

(7)密钥交换： 如果密文计算过程中，密钥及密文的维数增长了，则可以使用密钥交换方法对维数进行约减。否则不需要使用密钥交换。所以密钥交换可以看成是一个独立的组件。

定理 1 如果一个加密方案的解密结构具有抽象解密结构的形式，就能够构造一个全同态加密方案。

定理 1 可以通过上述通用设计方法得到。定理 1 说明了抽象解密结构在构造全同态加密中的重要性。如果具有了抽象解密结构，在不考虑噪音的情况下，可以获得乘法期盼解密结构。这也说明了为什么 LWE 上的加密能够构造全同态加密的原因。

6 结论

综上所述，本文提出的抽象解密结构概念，为研究全同态加密构造方法提供了有利的工具。本文从研究同态性入手，利用期盼解密结构研究密文计算形式与同态性之间的关系，并且研究解密结构与噪音依赖主要项之间的关系。最后通过最终解密结构的概念将同态性与噪音控制两个问题统一进行研究，并且探讨密文计算形式与最终解密结构之间的关系，从而研究全同态加密构造方法的本质。回答了为什么格上能够构造全同态加密的原因，格上这些全同态加密方案之间的关系是什么，是否存在一个统一的方法描述所有方案，以及 GSW 全同态加密具有通用性的原因。最后给出通用的全同态加密构造方法。相信本文回答的这些问题对于构造新的全同态加密方案，以及基于其它数学问题构造全同态加密方案，提供新的思路和理论依据，具有重要的意义。

参 考 文 献

[1] GENTRY C. Fully homomorphic encryption using ideal lattices[C]. Proceedings of the 41st Annual ACM Symposium on Theory of Computing, Bethesda, USA, 2009: 169–178. doi: 10.1145/1536414.1536440.

[2] SMART N P and VERCAUTEREN F. Fully homomorphic encryption with relatively small key and ciphertext sizes[C]. International Conference on Practice and Theory in Public-Key Cryptography, Berlin, Heidelberg, 2010: 420–443. doi: 10.1007/978-3-642-13013-7_25.

[3] DIJK M, GENTRY C, HALEVI S, *et al*. Fully homomorphic encryption over the integers[C]. Advances in Cryptology-EUROCRYPT 2010, Berlin, Heidelberg, 2010: 24–43.

[4] CORON J S, NACCACHE D, and TIBOUCHI M. Public key compression and modulus switching for fully homomorphic encryption over the integers[C]. Advances in Cryptology-EUROCRYPT 2012, Berlin, Heidelberg, 2012: 446–464. doi: 10.1007/978-3-642-29011-4_27.

[5] CORON J S, MANDAL A, NACCACHE D, *et al*. Fully homomorphic encryption over the integers with shorter public keys[C]. Advances in Cryptology-CRYPTO 2011, Berlin, Heidelberg, 2011: 487–504. doi: 10.1007/978-3-642-22792-9_28.

[6] CHEON J H and STEHL D. Fully homomophic encryption over the integers revisited[C]. Advances in Cryptology-EUROCRYPT 2015, Sofia, Bulgaria, 2015: 513–536. doi: 10.1007/978-3-662-46800-5_20.

[7] BRAKERSKI Z and VAIKUNTANATHAN V. Efficient fully homomorphic encryption from (standard) LWE[C]. IEEE 52nd Annual Symposium on Foundations of Computer Science, Los Alamitos, 2011: 97–106. doi: 10.1109/FOCS.2011.12.

[8] BRAKERSKI Z. Fully homomorphic encryption without modulus switching from classical gapsvp[C]. Advances in Cryptology-CRYPTO 2012, Berlin, Heidelberg, 2012: 868–886. doi: 10.1007/978-3-642-32009-5_50.

[9] BRAKERSKI Z, GENTRY C, and VAIKUNTANATHAN V. (Leveled) Fully homomorphic encryption without bootstrapping[C]. The 3rd Innovations in Theoretical Computer Science Conference, Cambridge, Massachusetts, 2012: 1–36. doi: 10.1145/2090236.2090262.

[10] GENTRY C, SAHAI A, and WATERS B. Homomorphic encryption from learning with errors: conceptually-simpler, asymptotically-faster, attribute-Based[C]. Advances in Cryptology – CRYPTO 2013, Berlin, Heidelberg, 2013: 75–92. doi: 10.1007/978-3-642-40041-4_5.

[11] REGEV O. On lattices, learning with errors, random linear codes, and cryptography[C]. The 37th Annual ACM Symposium on Theory of Computing, Baltimore, 2005: 84–93. doi: 10.1145/1060590.1060603.

[12] COSTACHE A and SMART N P. Which ring based somewhat homomorphic encryption scheme is best?[C]. CT-RSA 2016, San Francisco, CA, 2016: 325–340. doi: 10.1007/978-3-319-29485-8_19.

[13] GENTRY C, HALEVI S, and SMART N. Fully homomorphic encryption with polylog overhead[C]. Advances in Cryptology-EUROCRYPT 2012, Berlin, Heidelberg, 2012: 465–482. doi: 10.1007/978-3-642-29011-4_28.

[14] OZTURK E, DOROZ Y, SAVAS E, *et al*. A custom accelerator for homomorphic encryption applications[J]. *IEEE Transactions on Computers*, 2017, 66(1): 3–16. doi: 10.1109/TC.2016.2574340.

[15] CANETTI R, RAGHURAMAN S, RICHELSON S, *et al*. Chosen-ciphertext secure fully homomorphic encryption[C]. International Conference on Practice and Theory in Public-Key Cryptography, Amsterdam, 2017: 213–240. doi: 10.1007/978-3-662-54388-7_8.

[16] GAVIN G. An efficient somewhat homomorphic encryption scheme based on factorization[C]. The 15th International Conference Cryptology and Network Security, Milan, 2016: 451–464. doi: 10.1007/978-3-319-48965-0_27.

[17] BENARROCH D, BRAKERSKI Z, and LEPOINT T. FHE over the integers: decomposed and batched in the post-quantum regime[C]. International Conference on Practice and Theory in Public-Key Cryptography, Amsterdam, Netherlands, 2017: 271–301. doi: 10.1007/978-3-662-54388-7_10.

[18] CHILLOTTI I, GAMA N, GEORGIEVA M, *et al*. Faster fully homomorphic encryption: Bootstrapping in less than 0.1 seconds[C]. International Conference on the Theory and Application of Cryptology and Information Security, Hanoi, Vietnam, 2016: 3–33. doi: 10.1007/978-3-662-53887-6_1.

[19] HALEVI S and SHOUP V. Algorithms in HElib[C]. Advances in Cryptology-CRYPTO 2014, Santa Barbara, CA, 2014: 554–571. doi: 10.1007/978-3-662-44371-2_31.

[20] CHEN H, LAINE K, PLAYER R, *et al*. Simple encrypted arithmetic library-SEAL v2.1[C]. Proceedings of the Financial Cryptography and Data Security, Sliema, Malta, 2017: 3–18. doi: 10.1007/978-3-319-70278-0_1.

[21] CROCKETT E and PEIKERT C. $\Lambda o\lambda$: Functional lattice cryptography[C]. Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, Vienna, Austria, 2016: 993–1005. doi: 10.1145/2976749.2978402.

[22] L PEZ-ALT A, TROMER E, and VAIKUNTANATHAN V. On-the-fly multiparty computation on the cloud via multikey fully homomorphic encryption[C]. Proceedings of the 44th Symposium on Theory of Computing, New York, USA, 2012: 1219–1234. doi: 10.1145/2213977.2214086.

宋新霞：　女，1973 年生，副教授，研究方向为代数与编码.

陈智罡：　男，1972 年生，教授，研究方向为全同态加密与格密码.