**全同态加密算法BGV、BFV方案**

**背景： 在上文提到的Bootstrapping被提出后， 2011年两位大佬B和V提出了一个新的全同态加密体系，这一体系基于格加密的另一种假设Learning With Errors（LWE），他们发明的全同态系统简称为BGV系统，这是一个有限级数的同态加密系统，但是可以通过Bootstrapping的方式来变成全同态系统。**

**其基本特征包括：**

* 在算数电路上实现（种用于执行数值计算和算术运算的电子电路。它可以接收输入信号作为操作数，并通过各种逻辑和算术运算来生成输出结果）
* 在整数向量上进行高效的SIMD计算（一种并行计算的方式： SIMD指令集允许在单个指令周期内对多个数据元素执行相同的操作，如矩阵运算、多项式运算或向量运算，这种能力可以用于同时处理加密数据中的多个位或多个加密数据元素，从而加快加密计算的速度）
* 快速高精度整数算术
* 快速向量的标量乘法
* Leveled design（一种层次化管理的噪声控制手段，将同态操作划分为不同的级别，每个级别包含一组操作。这样的设计有助于更有效地控制同态操作中引入的噪声，使系统能够在不丢失准确性的情况下进行更多的计算，通常不使用bootstrapping）

**差别：**

* 模数变化问题上（即Modulus Switching）：BGV方案将消息放在最小字节位上，使用模数替换技术来保持噪声为一个常量。具体来说，每次乘法之后都会将模数Q缩小一个噪声B的大小Q / B，而每次乘法后变为平方的噪声B2，也被缩小了一个噪声的大小变为B，因此噪声可以保持为一个常量；而BFV方案将消息放在最大字节位上，所有的密文在做乘法后都会缩小Q/t。模数Q QQ保持不变，而噪声逐渐增加，噪声增加的量和BGV方案中Q缩小的量近似。
* 二者最大的计算区别在于乘法之后的scale down，BFV中因为采用了MSD编码，每次乘法完都需要scale down一个很大的Q/t，而对于BGV来说，只需要scale down一个和初始噪声差不多大小的模数，因此，当t取大一点的时候，BGV的效率是远远高于BFV的。