# 各种全同态加密技术的分析与比较

摘要——可以对加密形式的数据进行计算——这是同态加密的本质。 同态加密解决了在第三方系统（例如云或不受信任的计算机、服务提供商等）上存储数据的安全问题。 最重要的同态加密类别是完全同态加密。 它允许对加密形式的数据进行无限数量的操作，并且系统输出在密文空间内。 本文提供了同态加密的基本原理及其各种分类，即部分同态加密、部分同态加密和完全同态加密。 主要强调全同态加密，研究利用理想格的硬度、整数、误差学习、椭圆曲线密码学等不同的全同态加密方案。

**关键词**：同态加密（HE）、部分同态加密（PHE）、有点同态加密（SWHE）、全同态加密（FHE）、第三方、椭圆曲线加密（ECC）。

# 一、引言

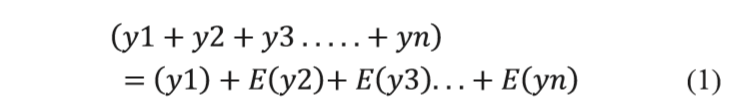
在 IT 领域，数据通常在第三方（云或不受信任的计算机、服务提供商等）上存储和处理。因此，出现了两个主要问题。首先，传统加密方案不提供第三方数据的安全性（即存储未加密的数据）。第三方可能会滥用数据。其次，要对加密数据执行任何类型的操作，首先要对其进行解密。这些担忧可能导致发现同态加密，该加密允许以加密形式对存储在第三方的数据执行计算，而无需对其进行解密。 1978 年出现了对加密数据进行计算的想法，称为隐私同态 [1]。同年 1978 年，他们还引入了 RSA。 RSA [1] 是非对称加密方案，即具有用于加密的公开密钥（即公共）和用于解密的机密密钥（即秘密），只有授权用户知道。 RSA 只允许对加密数据进行乘法运算。允许对加密数据进行加法和乘法无界操作的同态加密方案称为完全同态加密方案。全同态加密方案（FHE）是一个开放的问题。许多研究人员提出了他们的方案，即 El-Gamal 方案 [2] 但适用于乘法运算，Paillier 方案 [3] 但适用于加法运算等。

第一个完全同态加密方案来自Gentry [4] 给出了某种同态加密方案，这是一个值得注意的飞跃。 这是基于硬度理想晶格 [5]。

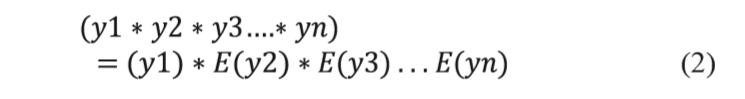
# 二、 文献调查

在本文中，我们将调查先前在与同态加密相关的密码学领域所做的研究。 研究和分析各种同态加密方案。 提供对称为完全同态加密的同态加密的最佳类别及其各种类别的见解。 同态加密概念取自抽象代数。 考虑明文 y1,y2...yn 和加密方案 E，如果它如下：

**A. 可加性：**



**B. 乘性性质：**



那么它是同态的。

为了创建任何类型的同态加密方案，我们使用加法和乘法布尔电路（AND 和 XOR 门）的组合。 考虑非对称加密的同态加密方案分为如下四种算法：

H=(生成密钥，加密，解密)

所有这些算法的运行时间取决于安全参数λ。

**a).创建密钥算法：**

它以安全参数 Ⅳ 为输入，即密钥中的位数，并输出密钥s和公钥p。

**b).加密算法：**

它以明文抣y1,y2...yn 作为输入。 它将明文分成位 (0,1)b1,b2...bi 并输出密文 c1,c2...ci



**c).评估算法：**

以p和函数 fun 作为输入，输出新的密文



**d). 解密算法：**

以密文c1,c2...cj和s为输入，输出明文 y1,y2...yn



同态加密分为三类，如图 1 所示：

**1. 部分同态加密（PHE）：**

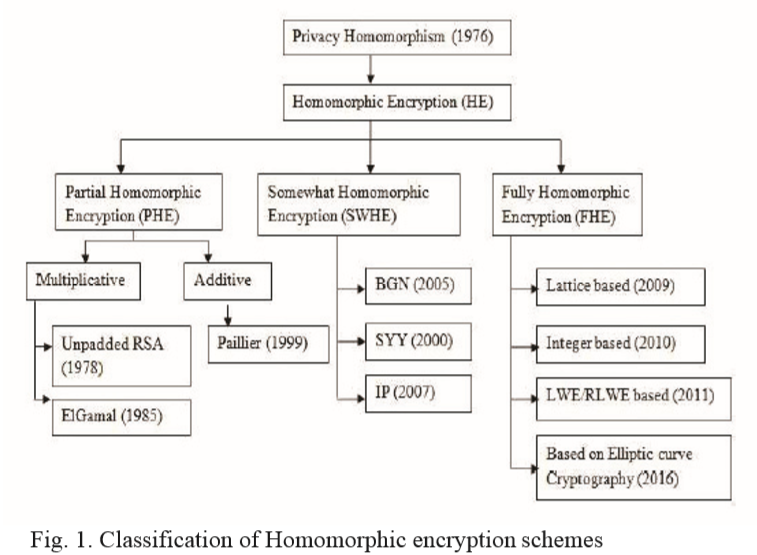
它允许加法或乘法运算，即只有一种任意数量的运算。 例如——未填充的 RSA、El-Gamal 等。

**2.部分同态加密（SWHE）：**

它允许加法和乘法运算，但运算次数是有限的。 例如 – BGN [7] 等。

**3.全同态加密（FHE）：**

它允许任意数量的加法和乘法运算。 例如 – 基于格的 [5]、基于整数的 [10]、基于错误的学习 [14] 等。



# 三、 完全同态加密方案

全同态加密是一种对密文进行任意加密的密码体制。 它允许程序在支持加密系统的任何类型的功能上运行。

A. 使用 Ideal Lattice (2009) 形成的 FHE 方案

Bootstrappable 加密方案是使用理想格 [5] 创建的，因为：在典型的基于格的算法中，算法的解密电路复杂度比未填充的 RSA 或 ElGamal 等方案要低得多。同态的加法和乘法性质是由理想格所提供的。

士绅建设包括三个步骤：

构造某种同态加密：构造一种求低阶多项式的方法数量有限的ADD和MULT操作。A.密文是一种形式

1641128482(1)

当u是理想格[5]中的向量，n是一个带有明文m的“误差”或“偏移”或“噪声”向量时，误差分量随着每个同态运算的应用而增加，达到一个不可避免的值，在某一点上不再允许密文解密。

压缩：压缩是用来减少深度解密电路，因为它增加到更高的值。SWHE方案解密电路工作良好，具有较小的深度。

引导：引导是为了减少噪音而对密文进行加密。如果一个同态加密方案能够评估自己(增广)解密电路，那么它就是可引导的。

1. 不使用引导的完全同态加密：

2010年，Gentry et. al. 提出了利用自举机制实现完全同态加密的思想。这允许对原始数据使用任意数量的加法，但只需一次乘法。

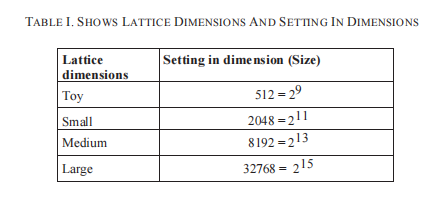
2013年，Wei et. al.提出了允许任意数目的加法和多重乘法的思想。

基于对称学习的全同态加密方案：然后，提出了基于对称学习机制的全同态加密方案，该方案主要基于机器学习技术来学习加密模式。该方法避免了自举和机器学习方法的使用，它使用了维数约简机制，从而缩短了原始文本，减少了解密机制的复杂性，不影响附加的假设。

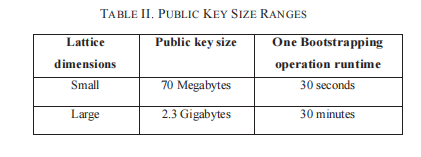
环全同态加密方案：在此基础上，提出了一种新的FHE加密方案--RFHE(环型全同态加密)，该方案不使用降噪机制，而是在降噪过程中加入一个非八元环。之后，刘氏提出了对称满同态加密方案，该方案依赖于非交换域，该方案排除了自举的可能性，并允许对原始数据进行更多的加法和乘法。它不使用噪音教育，而是依赖于类似的GCD机制。

1. 完全同态加密方案的实现

为了实现完全同态加密，Gentry和Halevi[8]使用了类似于Smart and vercateren[9]的变体。Smart和Vercauteren在将某些同态加密转换为完全同态加密时，无法实现引导功能。优化包括自举功能；加密等方面的批处理技术，以实现完全同态定义。在某种程度上同态加密中，密钥生成不需要完全多项式反转[8]。



上面的表1显示了在实现FHE时考虑了几个维度的格点。



上面的表2显示了用于小和大格维的公钥大小范围和一个引导操作运行时，并考虑了1-CPU 64位机器的一个启动操作运行时，具有较大的[8]。

D.利用整数形成的FHE格式（2010）

Van Dijk等人[10]提出了使用Gentry构造[5]的完全同态加密方案，但定义在整数上而不是理想格上，因为它们在概念上更简单，可以证明使用“基本”技术。Howgrave Graham分析了近似整数最大公约数（近似imate GCD）问题[11]的方案使用度。

一般建筑：

创建密钥算法：奇数整数键k∈ [ 2n - 1,2n)。

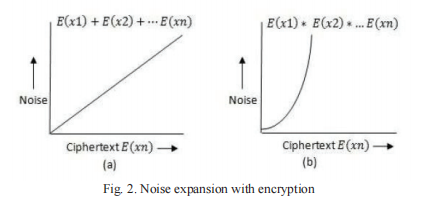
加密算法(k，x)：用于加密X∈{0，1}，集合密文是一个整数值，其残数mod p与明文具有相似的齐次性，类似于c=k\*q+2r+x，其中整数q，r在绝对值小于k/2的情况下随机选取。

解密算法(k，c)：x=输出(Cmod K)mod 2。

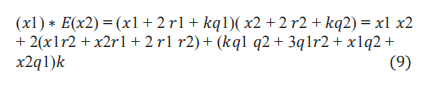
约束：x+2r<k/2并选择r：r o2√n和q ≈ 2n^3

加法上的同态：(x1)+E(x2)=x1+2r1+kq1+x2+2r2+kq2=(x1+x2)+2(r1+r2)+(q1+q2)

Nois=(x1+x2)+2(r1+r2)，其生长线性如图2(a)所示。



乘法上的同态：



如图2(b)所示，Nois=x1x2+2(x1r2+x2r1+2r2r2)，呈指数增长。

这是一个对称格式，但很容易转化为非对称格式。公钥是使用“零加密”(特别是整数)形成的。

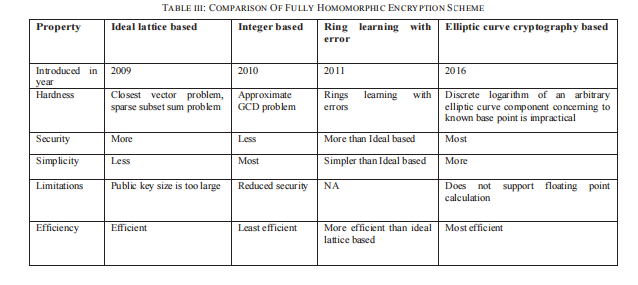
1641137628(1)

在上面描述的qi，ri是私钥，加密解密用于解密密文。由于这里存在不有效的算法，为了在多项式时间内从给定的pis中恢复k，因此该方案被认为是安全的。

E.FHE计划使我们在错误中学习(2011)

带误差学习(LWE)是文[12]所提到的偶数后量子算法在实际时间内最难解决的问题之一。Regev首次提出了“从错误中学习”问题[13]，它将格问题的最坏情况下的硬度降低为带误差的学习问题(LWE)[14]。Brakerski和Vaik Untanathan提出了用环学习与误差(RLWE)相结合的化学方法[14].RLWE采用多项LWE(PLWE)。为了理解RLWE的假设，例如，在一个具有形式(ri，rik+yi)的环上取无同源样本，其中k是随机的“秘密环元素”，ri’s在环中是均匀随机的，而I是“小P环元素，窃听者不能区分随机对的。”这一系列样品中的环元素[14]。这进一步归结为SVP的最坏情况。该方案也是利用Gentry的自举和压缩技术[5]从Swhe构造的。为了避免在该方案中压缩，以依赖LWE[14]的“稀疏”版本为代价，将最坏的硬问题降到最坏的情况。压扁的交替是线性化的。再线性化减小了密文的大小。生成密钥所需的格基的非生成。RLWEScheme是圆形的，这意味着它允许安全地加密它的自秘密密钥。环元素与LWE相比，RLWE具有更高的效率，对于秘密密钥的线性函数而言，RLWE是循环安全的(与密钥相关的安全)。

1. 使用椭圆曲线密码形成的FHE（2016)



上图3显示了使用椭圆曲线密码学进行同态加密所涉及的步骤。用户想要处理数据，首先要进入私有云。私有云具有加密和解密机(EDM)，它负责加密和解密数据。公共云以加密的形式对数据执行计算操作，并将获得的结果返回到EDM。EDM将向用户提供所需的结果数据。

# 四、增值结果

我们的目标是实现一个实际可行的无限制的FHE方案。FHE方案的一个例子如下：

1.基于晶格的方案在IBM系统×3500服务器[8]和6Intel xeon2.4GHz处理器[16]上使用语言C++和NTL库实现。

2.基于整数的方案是在SAGE软件上实现的英特尔核心i5,3.30 GHz x4,8 Gb RAM[17]。

3.RLWE是在HELib中使用C-++语言和一个数学库NTL[18]实现的。

4.利用基于HE的椭圆曲线密码学对GPS数据[15]进行了实证评估和测试。

通过对上述全同态加密方案进行深入研究和分析，进行了比较具有硬度、引入年份、方案安全性、效率等性能。比较的结果列于表1中。

# 结论

和未来工作同态加密存在于30年后仍是有待研究的问题。各种同态加密方案都有一定的改进范围。该改进可以在任何方面完成，如改进密钥的生成或加密、解密等。实现成本很高，同态加密方案的复杂性也很高。它在将来可以减少。本文对同态加密方案进行了分类，重点关注各种类型的FHE。在实际应用中实现了基于格、整数、误差环学习和椭圆曲线密码学的FHE方案。上面提供了每个方法的示例。FHE并不是在每个平台上都是实际实现的。上述FHE方案只支持单个用户设置尽管应用程序从不同用户获取多个数据的[19]。

# 参考文献

[1] Rivest, R. L., Adleman, L., & Dertouzos, M. L. (1978). On data banks and privacy homomorphisms. Foundations of secure computation, 4(11), 169-180.

[2] ElGamal, T. (1985). A public key cryptosystem and a signature scheme based on discrete logarithms. IEEE transactions on information theory, 31(4), 469-472.

[3] Paillier, P. (1999, May). Public-key cryptosystems based on composite degree residuosity classes. In Eurocrypt (Vol. 99, pp. 223-238).

[4] Gentry, C. (2009). A fully homomorphic encryption scheme. Stanford University.

[5] Gentry, C. (2009, May). Fully homomorphic encryption using ideal lattices. In STOC (Vol. 9, No. 2009, pp. 169-178).

[6] Parmar, P. V., Padhar, S. B., Patel, S. N., Bhatt, N. I., & Jhaveri, R. H. (2014). Survey of various homomorphic encryption algorithms and schemes. International Journal of Computer Applications, 91(8).

[7] Boneh, D., Goh, E. J., & Nissim, K. (2005, February). Evaluating 2- DNF Formulas on Ciphertexts. In TCC (Vol. 3378, pp. 325-341).

[8] Gentry, C., & Halevi, S. (2011, May). Implementing Gentry's FullyHomomorphic Encryption Scheme. In EUROCRYPT (Vol. 6632, pp. 129-148).

[9] Smart, N. P., & Vercauteren, F. (2010, May). Fully Homomorphic Encryption with Relatively Small Key and Ciphertext Sizes. In Public Key Cryptography (Vol. 6056, pp. 420-443).

[10] Van Dijk, M., Gentry, C., Halevi, S., & Vaikuntanathan, V. (2010, May). Fully homomorphic encryption over the integers. In Annual International Conference on the Theory and Applications of Cryptographic Techniques (pp. 24-43). Springer Berlin Heidelberg.

[11] Howgrave-Graham, N. (2001, March). Approximate integer common divisors. In CaLC (Vol. 1, pp. 51-66).

[12] Acar, A., Aksu, H., Uluagac, A. S., & Conti, M. (2017). A Survey on Homomorphic Encryption Schemes: Theory and Implementation. arXiv preprint arXiv:1704.03578.

[13] Regev, O. (2009). On lattices, learning with errors, random linear codes, and cryptography. Journal of the ACM (JACM), 56(6), 34.

[14] Brakerski, Z., & Vaikuntanathan, V. (2011, August). Fully homomorphic encryption from ring-LWE and security for key dependent messages. In Annual cryptology conference (pp. 505-524). Springer, Berlin, Heidelberg.

[15] Hong, M. Q., Wang, P. Y., & Zhao, W. B. (2016, April). Homomorphic Encryption Scheme Based on Elliptic Curve Cryptography for Privacy Protection of Cloud Computing. In Big Data Security on Cloud (BigDataSecurity), IEEE International Conference on High Performance and Smart Computing (HPSC), and IEEE International Conference on Intelligent Data and Security (IDS), 2016 IEEE 2nd International Conference on (pp. 152-157). IEEE.

[8] Smart, N. P., & Vercauteren, F. (2014). Fully homomorphic SIMD operations. Designs, codes and cryptography, 1-25.

[9] Gerasimov, A. N., Epishkina, A. V., & Kogos, K. G. (2017, February). Research of homomorphic encryption algorithms over integers. In Young Researchers in Electrical and Electronic Engineering (EIConRus), 2017 IEEE Conference of Russian (pp. 398-403). IEEE.

[10] Halevi, S., & Shoup, V. (2013). Design and implementation of a homomorphic-encryption library. IBM Research (Manuscript), 6, 12- 15.

[11] Tourky, D., ElKawkagy, M., & Keshk, A. (2016, October). Homomorphic encryption the “Holy Grail” of cryptography. In Computer and Communications (ICCC), 2016 2nd IEEE International Conference on (pp. 196-201). IEEE.