# 现代密码学

## 第五十六讲 全同态加密

信息与软件工程学院

# 第五十六讲 全同态加密

- 同态的定义
- 早期的同态加密算法
- 全同态加密

# 同态的定义

- 同态来源于近世代数
- 定义：设<G,*>和<H, ›>是两个群，f是群G到群H的映射，如果对于任意a,b∈G，**都有**f(a*b)=f(a)  f(b)，则称f是群G到群H的一个同态映射。

# 同态加密的定义

- 定义：设E(k,x)表示用加密算法E和密钥k对x进行加密，F表示一种运算，如果对于加密算法E和运算F，存在有效算法G使得：

$$E(k,F(x_1, x_2, \cdots, x_n)=F(E(k,x_1),E(k,x_2),\cdots,E(k,x_n)))$$

- 就称加密算法E对于运算F是同态的。
- 如果$F(x_1, x_2, \cdots, x_n)= \sum_{i=1}^{n} x_i$，则称该加密算法为加法同态加密算法。
- 如果$F(x_1, x_2, \cdots, x_n)= \prod_{i=1}^{n} x_i$，则称该加密算法为乘法同态加密算法。
- 如果定义中的等式对包含加法与乘法混合运算的$F(x_1, x_2, \cdots, x_n)$都成立，那么该加密方案就是一个全同态加密方案

# 同态加密的起源

- **1978年，Rivset, Adleman 和Dertouzos ，隐私同态**
- 应用场景：“保密数据库(private data banks)”
  - 用户将个人敏感数据加密后存储在一个不可信的服务器中, 并给出正确的查询应答
  - “保密数据库”的思想已经基本完整涵盖了数据存储与数据处理过程, 完全可以将其视作当今流行的安全云存储与安全云计算融合的一种概念性雏形
- 全同态加密思想有着与公钥加密思想比肩齐名的重要地位，实用的全同态加密方案则将催生新型分布式计算模式
- 全同态加密概念自提出后近30 年来, 一直被密码学界誉为“密码学圣杯”

# 第五十六讲 全同态加密

- 同态的定义
- 早期的同态加密算法
- 全同态加密

# RSA的同态性

- 设n=pq，（n,e）为公钥，d为私钥
- RSA的加密函数为

$$E(m)=c=m^e\ (\mathrm{mod}n)$$

因此，若有

$$c_1=E(m_1)=m_1^e\ (\mathrm{mod}n)\ 和 c_2=E(m_2)=m_2^e\ (\mathrm{mod}n)$$

则有

$$c_1c_2=E(m_1)E(m_2)=(m_1)^e(m_2)^e\ (\mathrm{mod}n)=(m_1m_2)^e\ (\mathrm{mod}n)=E(m_1m_2)$$

即RSA满足乘法同态

# ElGamal的同态性

- 设p为一个素数，g是$Z_p$中的生成元。ElGamal的加密密钥$y=g^x(\mathrm{mod}p)$，其中x是随机选取的私钥。
- ElGamal的加密函数为：$C_1=g^k(\mathrm{mod}p)$，$C_2=y^kM(\mathrm{mod}p)$
- 因此，若有

$$E(M_1)=(C_{11},C_{12})=(g^{k_1}(\mathrm{mod}p),y^{k_1}M_1(\mathrm{mod}p))$$
$$E(M_2)=(C_{21},C_{22})=(g^{k_2}(\mathrm{mod}p),y^{k_2}M_2(\mathrm{mod}p))$$

- 则有

$$E(M_1)E(M_2)=(g^{k_1}(\mathrm{mod}p),y^{k_1}M_1(\mathrm{mod}p))\ (g^{k_2}(\mathrm{mod}p),y^{k_2}M_2(\mathrm{mod}p))$$
$$=(g^{k_1+k_2}(\mathrm{mod}p),y^{k_1+k_2}M_1M_2(\mathrm{mod}p))$$
$$=E(M_1M_2)$$

即ElGamal满足乘法同态性。

# 第五十六讲 全同态加密

- 同态的定义
- 早期的同态加密算法
- 全同态加密

# 全同态加密

- 全同态加密是指能够在不知道密钥的情况下，对密文进行任意计算，即对于任意有效的f及明文m，有性质f(E (m))=E (f(m))。这种特殊的性质使得全同态加密有广泛的理论与实际应用，如云计算安全、密文检索、安全多方计算等

- 从理论上讲，所有的函数都可以由加法和乘法多次复合来实现，因此全同态加密算法在设计的时候可以首先考虑其对加法和乘法都同态，再将其扩展到任意函数之上。

# 基于格的全同态加密发展的三个阶段

- 基于理想格以Gentry方案为蓝图的FHE构造
- 基于LWE假设,利用密钥交换等技术来实现FHE的构造
- 基于LWE假设,利用近似特征向量构造的FHE方案

# 第一阶段

- 2009年，Gentry 的FHE体制：
  - 基于理想格(ideal lattice) 上的有界编码问题(BDDP) 和稀疏子集和问题(SSSP)
- 构造过程：
  - 设计一个具备有限次密文运算的同态加法和同态乘法的近似同态(SWHE)加密体制
  - 引入“Bootstrapping” 程序，利用重加密的方法对密文进行更新，以此控制噪声膨胀，保证解密正确性，从而实现任意次的密文同态运算
- 缺点：
  - 无法抵抗选择密文攻击(CCA)，只能达到选择明文攻击(CPA) 安全

# 第二阶段

- 2011 年，Brakerski 和Vaikuntanathan
  - 基于Ring-LWE 假设
- 构造步骤：
  - 生成一个便于描述和分析的SWHE 方案，其安全性量子规约到理想格上的最坏情形困难问题
  - 利用Gentry的压缩范式(squashing) 和Bootstraping 程序将SWHE 转化为真正的FHE 方案
- 改进方案
  - 使用 Relinearization 技术，将基于 LWE 假设的 Regev 方案 转换为SWHE 方案
  - 提出一种新的 Dimension-Modulus Reduction 技术来实现 Bootstraping 程序，而不再使用Gentry 的压缩范式

# 第三阶段

- **2013 年， Gentry-Sahai-Waters(GSW)方案**
  - 近似特征向量方法来构建**FHE** 方案
- 构造方法：
  - 该方案的同态加法和同态乘法都只是通过做简单的矩阵加法和乘法来实现
  - **GSW-FHE** 方案相对简单、快速, 容易理解
  - 实施同态运算时不需要使用计算公钥, 而只需借助用户的公钥即可实现

# 全同态的应用

- 基于全同态加密的安全多方计算
- 基于全同态加密的密文处理
- 函数加密
- 不可区分性混淆器

# 感 谢 聆 听!

liaoyj@uestc.edu.cn