密 码 学

同态加密技术及其应用

网络空间安全学院
朱 丹
zhudan@nwpu.edu.cn

章节安排

Outline

同态加密的概述

半同态加密技术

全同态加密技术

同态加密的应用

章节安排

Outline

同态加密的概述

半同态加密技术

全同态加密技术

同态加密的应用

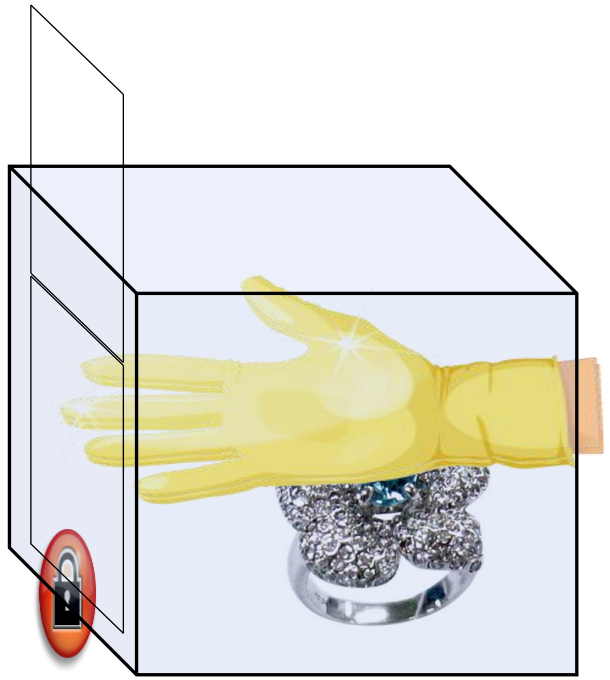
同态加密的概述

珠宝商Alice想让工人把钻石和金子打造成钻戒，但是工人在打造的过程中可能会偷原材料，能不能让工人**对原材料进行加工**，但是**得不到任何原材料**?

同态加密的概述

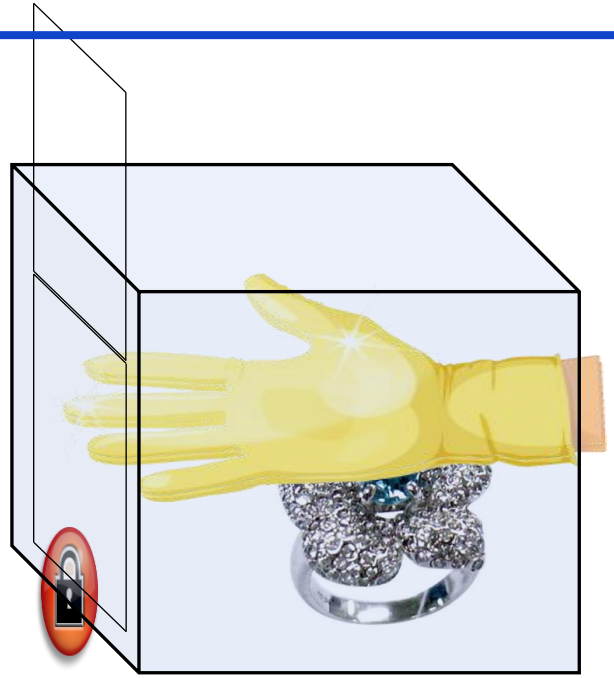
解决方案：

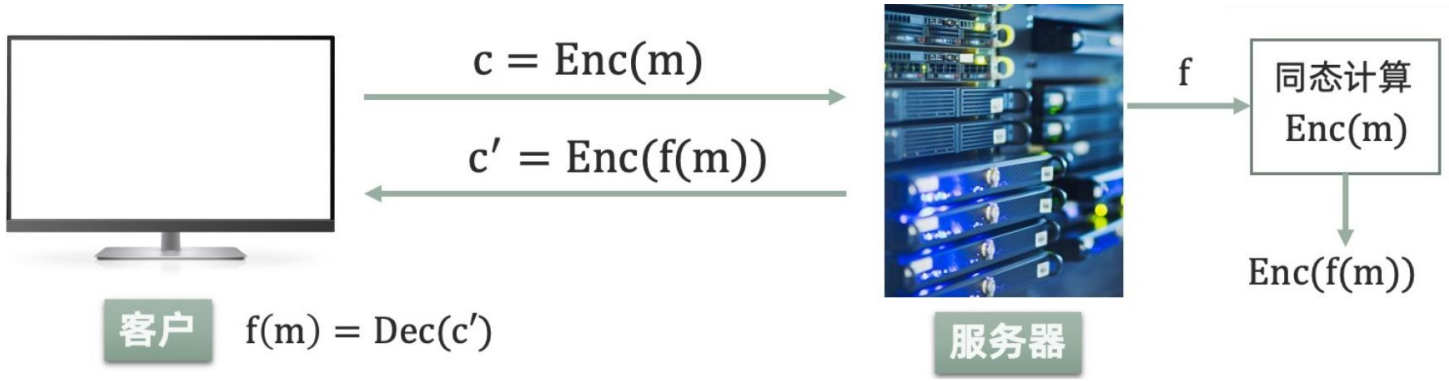
- Alice将金子锁在一个密闭的盒子里面，这个盒子安装了一个手套。工人可以戴着这个手套，对盒子内部的金子进行处理。
- 但是盒子是锁着的，所以工人不仅拿不到原材料，连处理过程中掉下的任何金子都拿不到。
- 加工完成后，Alice拿回这个盒子，把锁打开，就得到了金子



同态加密的概述

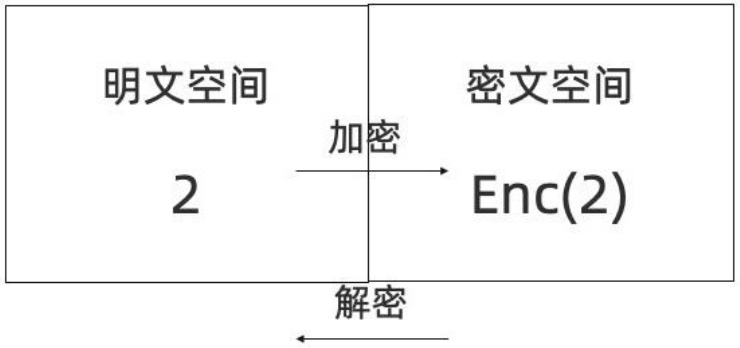
- 盒子：加密算法
- 盒子上的锁：用户密钥
- 将原材料放进盒子并用锁锁上：将数据用**同态加密方案**进行加密
- **加工**：应用同态特性，在无法取得数据的条件下直接对加密结果进行处理
- 开锁：对结果进行解密，直接得到处理后的结果

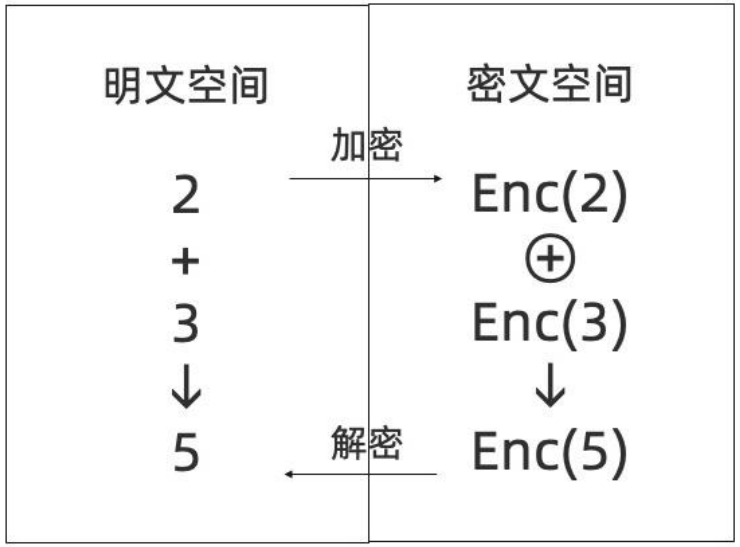




同态加密的概述

- 普通加密算法
  - 只能加密
- 同态加密算法
  - 密文空间具有特定的算符
  - 明文上的加法对应密文空间的⊕
  - 明文上的乘法对应密文空间的⊗





同态加密的概述

	类别		支持密文加密文的次数	支持密文乘密文的次数	举例
半同态	加法同态		∞	0	Paillier
半同态	乘法同态		0	∞	El Gamal
半同态	Somewhat同态*	基于ECC	∞	1	BGN
半同态	Somewhat同态*	基于(R)LWE	∞	L≥1	BFV、BGV
全同态	全同态 with bootstrapping		∞	∞	BFV、BGV

章节安排

Outline

同态加密的概念

半同态加密技术

全同态加密技术

同态加密的应用

半同态加密技术

法国密码学家Paillier发表于1999年欧密——Paillier密码算法

- 密钥生成
  - 生成两个大质数p, q，$n = p \times q$，$\lambda = lcm(p-1, q-1)$，$g = n + 1$
  - g, n作为公钥公开，λ作为私钥保存
- 对消息m加密
  - 选择随机数r，计算$c = g^m \times r^n \ mod \ n^2$
- 对密文c解密
  - 计算$m = \dfrac{\frac{\left(c^\lambda \ mod \ n^2\right)-1}{n}}{\frac{\left(g^\lambda \ mod \ n^2\right)-1}{n}}$

法国密码学家Paillier发表于1999年欧密——Paillier密码算法

- 正确性验证

$$c^{\lambda}\ mod\ n^2 = (g^m \times r^n)^{\lambda}\ mod\ n^2$$
$$= g^{m\lambda} \times r^{n\lambda}\ mod\ n^2$$
$$= g^{m\lambda}\ mod\ n^2$$
$$= (1+n)^{m\lambda}\ mod\ n^2$$
$$= 1 + nm\lambda\ mod\ n^2$$

$r^{n\lambda} \bmod n^2 = 1$

- 同理， $g^{\lambda}\ mod\ n^2 = 1 + n\lambda\ mod\ n^2$
- $\frac{(1+nm\lambda-1)/n}{(1+n\lambda-1)/n} = m$

法国密码学家Paillier发表于1999年欧密——Paillier密码算法

- 为什么$r^{n\lambda} \bmod n^2 = 1$?

$$r^{n\lambda} = r^{pq \cdot lcm(p-1,q-1)}$$

$$= r^{p(p-1)\cdot k}$$

$$= r^{\varphi(p^2)} \cdot r^k$$

所以，$r^{n\lambda} - 1$一定能被p^2整除

同理，$r^{n\lambda} - 1$一定能被q^2整除

综上，$r^{n\lambda} - 1$一定能被n^2整除

半同态加密技术

法国密码学家Paillier发表于1999年欧密——Paillier密码算法

Paillier算法的同态性质

- 密文加法
  - $c_1 = g^{m_1} r_1^n \ mod\ n^2, \quad c_2 = g^{m_2} r_2^n \ mod\ n^2$
  - $c_1 \oplus c_2 = c_1 \cdot c_2 = g^{m_1+m_2}(r_1 r_2)^n \ mod\ n^2$
  - 等价于$c_1 + c_2$的密文
- 密文与明文的乘法
  - $c = g^m r^n \ mod\ n^2$
  - $c \otimes m' = c^{m'} = g^{mm'} r^{nm'} \ mod\ n^2$，等价于$mm'$的密文
- 可以在密文上计算任意一次多项式$ax + b$

半同态加密技术

法国密码学家Paillier发表于1999年欧密——Paillier密码算法

Paillier算法的安全性

- 公钥无法推出私钥$\lambda = lcm(p-1, q-1)$：大整数分解难题
- 语义安全
  - A，B已知m_0, m_1；B随机选择$m_{b|b\in\{0,1\}}$进行加密，发给A猜m_b是m_0还是m_1
  - 如果存在A，猜对的概率大于50%说明算法不安全；反之说明满足语义安全
- Paillier算法满足语义安全
  - 设存在这样的A，可以大概率识别c是m_0的密文：$c = g^{m_0} r_0^n \ mod\ n^2$，等价于$c \cdot g^{-m_0}$是一个$n$次幂（在$mod\ n^2$ 上）
  - 判别一个数是不是n次幂（在$mod\ n^2$ 上）是一个困难问题，难度接近于分解n


感谢聆听!
THANK YOU FOR YOUR ATTENTION!