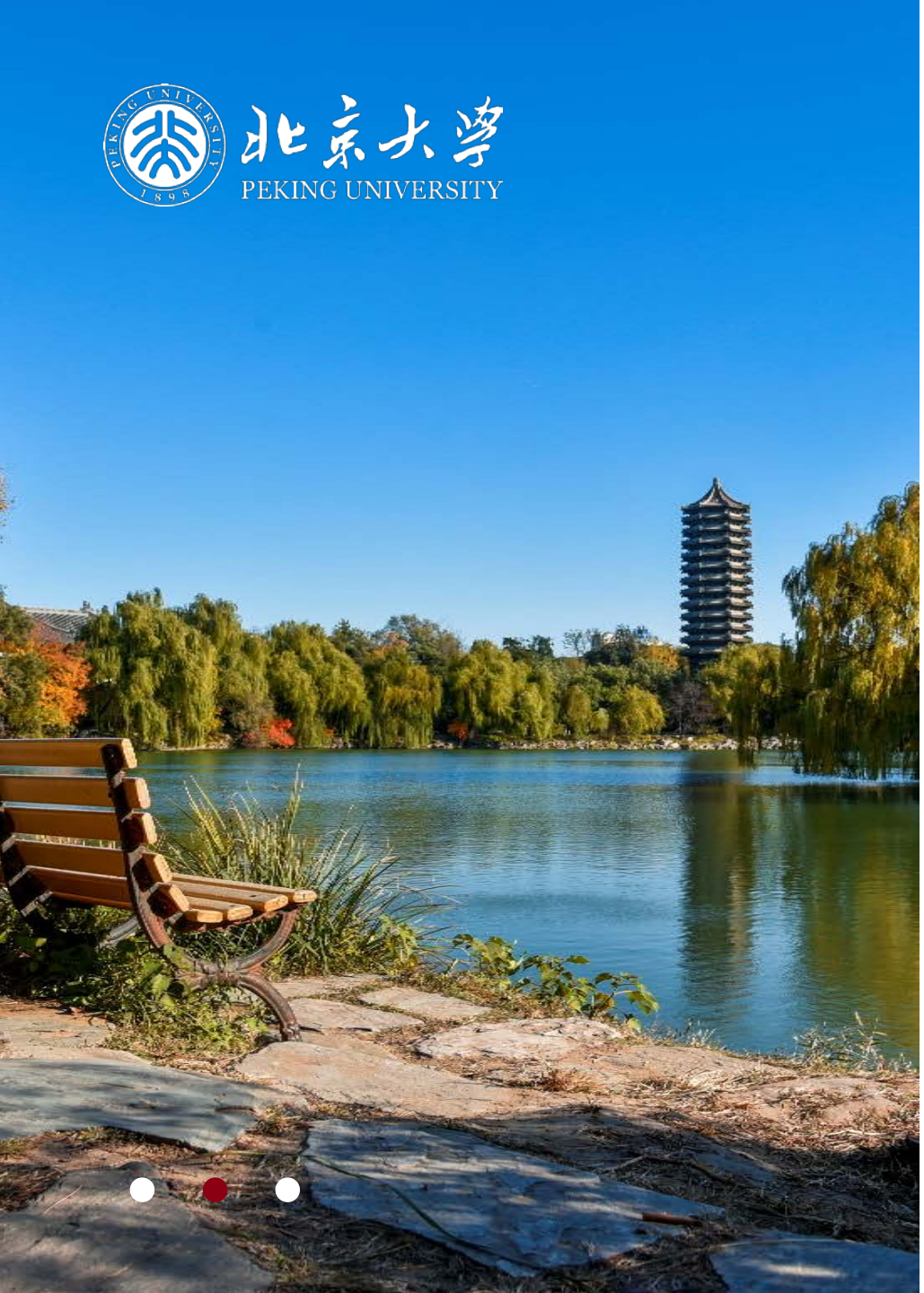
北京大学
PEKING UNIVERSITY

同态加密的综述

叶明聪 1901210694
刘华兴 1901210446



CONTENT

目 录

01

同态加密的背景

同态加密的背景

同态加密

同态加密是一类具有特殊自然属性的加密方法，此概念是Rivest等人在20世纪70年代首先提出的，与一般加密算法相比，同态加密除了能实现基本的加密操作之外，还能实现密文间的多种计算功能，即先计算后解密可等价于先解密后计算。

意义：

1 先计算之后再解密，减少计算代价

2 实现无密钥方对密文的计算

3 解密方只能获知最后的结果，而无法获得每一个密文的消息

同态加密的背景

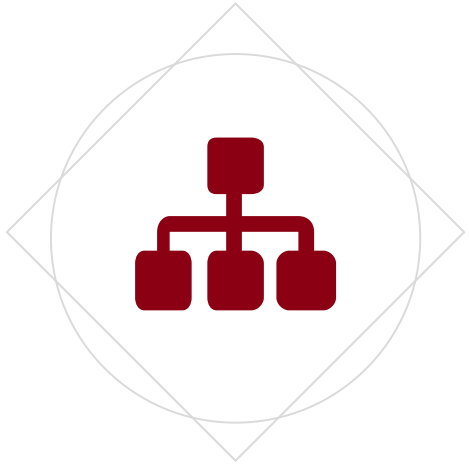
推动发展的因素

云计算

如何保护数据的私密性?

多方计算

如何分布计算却不泄露各方私有数据?



电子投票

如何不知道投票者投票内容，对投票结果进行统计?

02

同态加密的简介

同态加密的原理

同态的定义：

直观定义：A way to delegate processing of your data, without giving away access to it.

定义1 同态性：

对于加密算法ε和明文域 P_ε上的运算。,若$\forall p_1, p_2, \dots, p_n \in P_\varepsilon$都满足式(1):

$$Dec_\varepsilon(key, Cal_\varepsilon((c_1, \dots, c_n),。)) = (P_1, \dots, P_n)。 \quad (1)$$

其中， Cal_ε为密文运算算法， *key*为密钥;

定义2 部分同态加密算法：

对于加密算法ε和明文域 P_ε上的运算(+,*),若$\forall p_1, p_2, \dots, p_n \in P_\varepsilon$仅满足加法或者乘法运算在式(1)中成立,则称加密算法ε为满足部分同态的加密算法

同态加密的原理

同态加密算法的组成：

一个同态加密算法ε包括四个部分：

密钥生成算法Gen_ε、加密算法Enc_ε、解密算法Dec_ε、密文运算算法Cal_ε.

(1)密钥生成算法Gen_ε: $U \to Key$表示用户通过输入参数U生成密钥*key*;

(2)加密、解密算法:$Enc_\varepsilon: (key, P_\varepsilon) \to C_\varepsilon, Dec_\varepsilon: (key, C_\varepsilon) \to P_\varepsilon$,$P_\varepsilon$为明文空间，$C_\varepsilon$为密文空间;

(3)计算算法 :Cal_ε: $(P_\varepsilon, F_\varepsilon) \to (C_\varepsilon, F_\varepsilon), \circ \in F_\varepsilon, (P_1, P_2, \ldots., P_n) \in P_\varepsilon$,$F_\varepsilon$是$P_\varepsilon$上的运算集合,

对$\circ \in F_\varepsilon, (P_1, P_2, \ldots. P_n) \in P_\varepsilon$,$Cal_\varepsilon$将$P_\varepsilon$上进行的运算$\circ$转化为$C_\varepsilon$上运算再进行计算,结果是等价

Paillier 加密方案

密钥生成过程$Gen_{Paillier}$ 如下:

随机选取p、q 两个大素数以及$g \in Z_{n^2}$ 令$n = pq, \lambda = (p-1)(q-1)$, 设函数 $l(u) = \frac{u-1}{n}$, 且g、n 满足:

$$gcd(l(g^{\lambda} mod n^2), n) = 1 \quad (2)$$

这里,公钥为 $pk = (n, g)$,私钥 $sk = \lambda$.

加密算法$Enc_{Paillier}$:随机选取整数$r \in z_{n^2}^*$, 对于明文$m \in Z_n$, 加密后的密文 c 为

$$c = g^m r^n \, mod \, n^2 \quad (3)$$

式(3)中,$c \in z_{n^2}^*, z_{n^2}^*$为小于 n^2 且与 n^2 互素的正整数集合.

解密算法$Dec_{Paillier}$**:** 对于密文c,其对应的明文m为

$$m = \frac{l(c^{\lambda} mod n^2)}{l(g^{\lambda} mod n^2)} \, mod \, n \quad (4)$$

同态属性分析:

由于$Enc(m_1)Enc(m_2) = (g^{m_1} r_1^n)(g^{m_2} r_2^n) = g^{m_1+m_2}(r_1 r_2)^n = Enc(m_1 + m_2) mod \, n^2$,即明文加法运算对应密文乘法运算,所以方案具备加法同态性:

$$Dec_{paillier}(key, Cal_{paillier}((c_1, \dots, c_n), x)) = (m_1, \dots, m_n) + \quad (5)$$

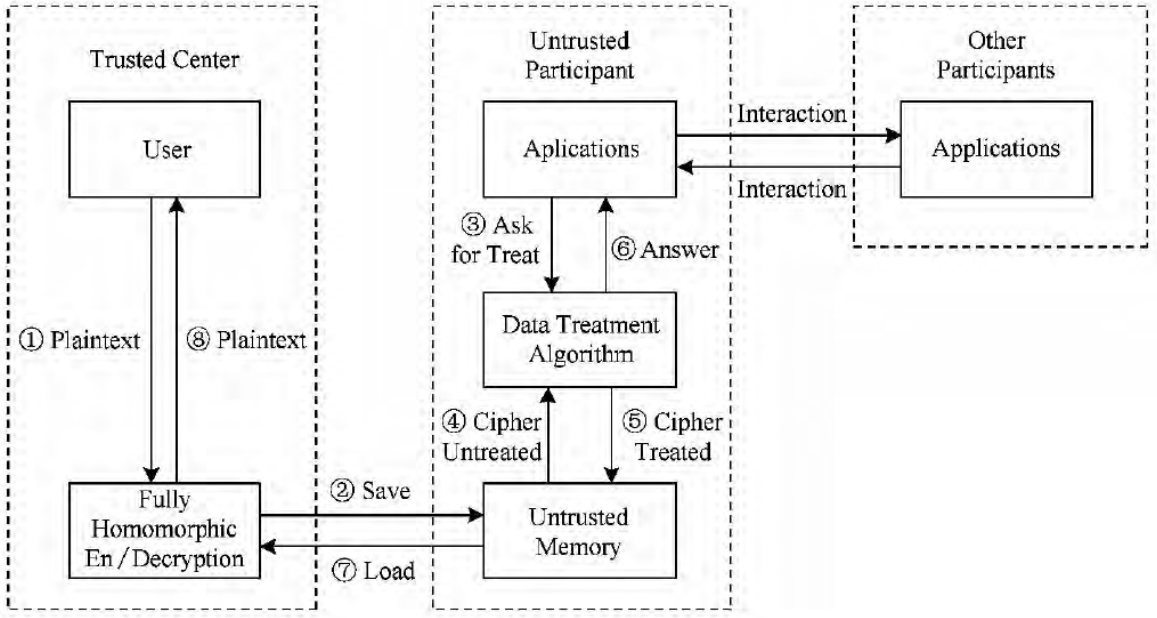
03

同态加密的应用

同态加密的应用

同态加密的一般性框架：

加密数据处理方法简述如下：假设存在同态加密函数$Enc_k(x)$，首先用户用自己的私钥k对需要处理的数据m进行同态加密$c = Enc_k(m)$，然后将加密数据c上传到云端服务器。服务器能够对加密数据 c 直接进行处理，得到$c' = f(c) = f(Enc_k(m))$,然后将处理后的密文 c' 返回给用户。用户收到$c' = f(c) = f(Enc_k(m)) = Enc_k(f(m))$后，利用自己的私钥 k 对其进行同态解密，得到已经处理好的明文数据$f(m)$。



同态加密的应用

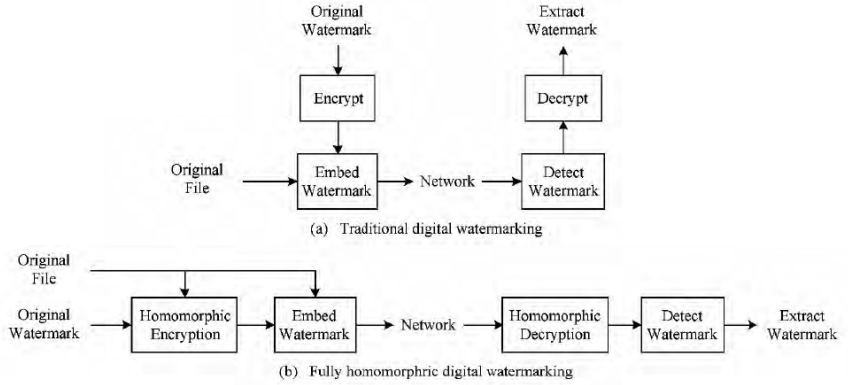
同态加密与机器学习：

同态加密可以在无需进行解密的情况下，直接计算加密数据。在训练图像数据中，用户可以将加密数据（例如图像）传递给云 API，以此运行机器学习模型，并返回加密的答案。整个过程中都没有解密用户数据，尤其是云服务商既不能访问原始图像，也不能解码计算得到的预测值，从而在保护隐私的情况下，达到目的。

同态加密的应用

数字水印：

数字水印技术是指用信号处理的方法在数字化的多媒体数据中嵌入隐蔽的标记，这种标记通常是不可见的，只有通过专用的检测器或阅读器才能提取．如何应对复杂网络环境下数据隐藏与数字水印系统的安全挑战，是目前需要迫切解决的问题。



传统数字水印与基于全同态加密的数字水印的区别

同态加密的应用

电子投票：

基于同态加密技术设计的电子选举方案，统计方可以在不知道投票者投票内容的前提下，对投票结果进行统计，既保证了投票者的隐私安全，有能够保证投票结果的公证。

简单的方案：

1）若有同态函数Enck(x1+x2)＝Enck(x1)*Enck(x2)，选民将自己的选票进行加密Ci＝Enck（Mi），其中Mi∈{0,1};

2)投票中心收集同态加密后的选民选票Ci；投票中心基于全同态加密方案的同态性质对加密后的选票Ci进行计票C=C1*C2*…*Cn，得到经过同态加密后的选举结果C＝Enck(M1+M2+…+Mn)；

3)只有拥有解密密钥的某个可信机构才能够对加密后的选举结果进行解密，公布选举结果.

同态加密的应用

安全云计算与委托计算：

同态技术在该方面的应用可以使得我们在云环境下，充分利用云服务器的计算能力，实现对明文信息的运算，而不会有损私有数据的私密性。

文件存储与密文检索：

用户可以将自己的数据加密后存储在一个不信任的远程服务器上，日后可以向远程服务器查询自己所需要的信息，存储与查询都使用密文数据，服务器将检索到的密文数据发回。用户可以解密得到自己需要的信息，而远程服务器却对存储和检索的信息一无所知。

04

同态加密的展望

同态加密的展望

(1) 对称密码体制同态加密方案

(2) 可验证的同态加密方案

(3) 无噪声FHE 方案

(4) 基于人工智能技术的FHE 方案

参考文献

[1]李宗育,桂小林,顾迎捷,李雪松,戴慧珺,张学军.同态加密技术及其在云计算隐私保护中的应用[J].软件学报,2018,29(07):1830-1851.

[2]刘明洁,王安.全同态加密研究动态及其应用概述[J].计算机研究与发展,2014,51(12):2593-2603.

[3]陈智罡,王箭,宋新霞.全同态加密研究[J].计算机应用研究,2014,31(06):1624-1631.

[4]Chen H, Gilad-Bachrach R, Han K, et al. Logistic regression over encrypted data from fully homomorphic encryption[J]. BMC medical genomics, 2018, 11(4): 81.

[5]Martins P, Sousa L, Mariano A. A survey on fully homomorphic encryption: An engineering perspective[J]. ACM Computing Surveys (CSUR), 2018, 50(6): 83.

[6]Armknecht F, Boyd C, Carr C, et al. A Guide to Fully Homomorphic Encryption[J]. IACR Cryptology ePrint Archive, 2015, 2015: 1192.

感谢您的观看

THANKS FOR WATCHING