2020 WEST LAKE CYBERSECURITY CONFERENCE ON LINE

西湖论剑·网络安全线上峰会

之江实验室 ZHEJIANG LAB

数治安全 智理未来

DIGITALLY GOVERNED SECURITY INTELLIGENTLY MANAGED FUTURE

2020 WEST LAKE CYBERSECURITY CONFERENCE ON LINE
西湖论剑·网络安全线上峰会
之江实验室 ZHEJIANG LAB

智慧金融时代的数据隐私保护算法研究

那崇宁

Contents 目录

01 智慧金融与数据要素
02 数据安全与隐私保护
03 隐私计算技术方案
04 隐私计算与机器学习
05 隐私计算与数据共享
06 金融隐私计算框架

Part 01

智慧金融与数据要素

数据是智慧金融的核心要素

鼓励数据共享与跨机构跨行业金融生态的搭建

01《金融科技发展规划（2019-2021）》

指出大数据作为基础性战略资源的核心价值，并强调机构间需加强数据共享以发挥金融大数据的集聚和增值作用。

02《关于进一步加快推进上海国际金融中心建设和金融支持长三角一体化发展的意见》

建立健全长三角金融政策协调和信息共享机制。

03《浙江省新兴金融中心建设行动方案》

将以数据、技术、服务为内容的金融大数据创新企业和平台，探索金融与互联网、创新创业、人工智能、数据科技等融合发展的“金融+”创新模式为工作重点之一。

关键生产要素

- 土地
- 劳动力
- 资本
- 技术
- 数据

智慧金融中的数据价值挖掘

DIKW模型

电子计算机：
数字化、信息化

人工智能、大数据：
知识化，智能化

互联网、移动互联网，5G：
网络化，规模化

云计算、区块链：
协同化，生态化

Part 02

数据安全与隐私保护

金融隐私泄露事件

2017 年 9 月，**美国信用机构Equifax**遭到黑客攻 击，导致约 1.43 亿信用和信息服务用户数据遭到泄露，事件曝光后，Equifax 股票暴跌 30%。

2018年11月8日，**汇丰银行**宣布其客户账户在10月4日至10月14日期间遭到攻击，约1%的美国客户的姓名、出生日期、电话号码、电子邮箱等信息被泄露。

2019 年 6 月Quest Diagnostics 表示，**帐单收集供应商**的在线支付页面可能存在数据泄露问题，导致患者的财务和医疗信息被泄露。

2019年10月安莎社网站报道，意大利银行业巨头**裕信银行**文件包数据外泄，涉及300万意大利客户信息。

2020年1月西澳大利亚州最大的**银行P&N Bank**在服务器升级期间遭遇了网络攻击，发生数据泄露，其客户关系管理系统中的个人信息和敏感的帐户信息被暴露。可能已影响十万西澳大利亚人。

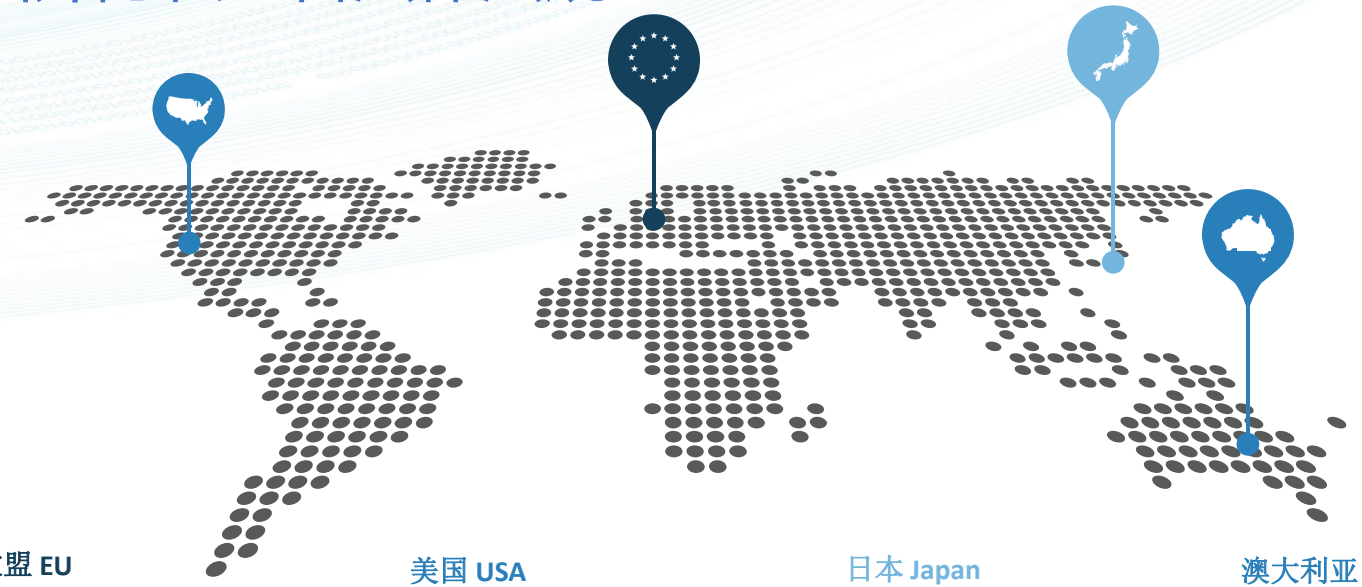
2017 年 12 月，**PayPal**公司收购的支付管理公司 TIO Networks 遭遇网络攻击。攻击者访问了 160 万用 户存储信息的服务器。

2018年5月，据加拿大媒体报道，该国两家大型**银行Bank of Montreal**和**Simplii Financial**遭到黑客袭击，约9万名客户信息被盗。

2019 年 7 月，Capital One 透露，黑客已经窃取了美国和 加拿大约 1.06 亿**信用卡**申请人和客户的个人信息

2020年1月，**加密货币交易所Poloniex**通过电子邮件向用户发送电子邮件，称用户该网站的的用户名和密码可能已经泄露在Twitter上，攻击者可能会被这些泄露的用户名和密码登陆Poloniex帐户。

国外隐私监管法律法规



欧盟 EU

《通用数据保护条例》

美国 USA

《加州消费者隐私法案》

日本 Japan

《个人信息保护法》

澳大利亚 Australia

《数据泄露通报法案》

国内隐私监管法律法规

《中华人民共和国信息保护法》

2017年3月，第十二届全国人民代表大会第五次会议上提出议案，建议加快制定个人信息保护法，同时将《中华人民共和国个人信息保护法(草案)》作为附件提交。

1、强调了个人信息保护的基本原则；

2、明确了个人信息主体的基本权利；

3、分类规范信息处理主体相关活动。

《个人金融信息保护技术规范》

2020年2月13日，中国人民银行正式发布《个人金融信息保护技术规范》。该规范由中国人民银行提出，全国金融标准化技术委员会归口管理，由中国人民银行　科技司提出并负责起草，多家单位参与起草。

Part 03

隐私计算技术方案

隐私保护技术解决方法

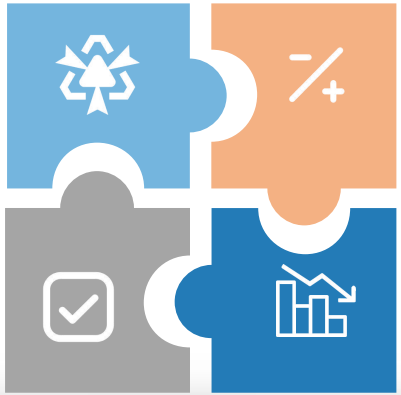
目前主流的通用数据隐私保护方法包括:

- 差分隐私
- 同态加密
- 多方安全计算等

隐私保护算法的要求:

01 能够适当假设攻击者拥有的背景知识，以应对各种类型的攻击

02 具有坚实的数学基础，对隐私保护有严格的定义和可靠的量化评估方法



03 在降低隐私泄露风险的同时，需考虑数据的可用性

04 尽可能降低计算代价

差分隐私

设计目标

数据的外部使用方对数据集D的任意一行的改动不会察觉，即单个ID的数据的存在与否以及正确与否不会影响到数据查询的结果

实现方法

对数据实施可参数化 ϵ 的扰动，如叠加拉普拉斯或高斯噪声。

- 参数ϵ为隐私预算，用以平衡数据查询结果的准确性vs数据隐私保护程度；
- 数据隐私保护程度与查询算法的敏感度（即数据集的改变对查询结果的扰动）相关

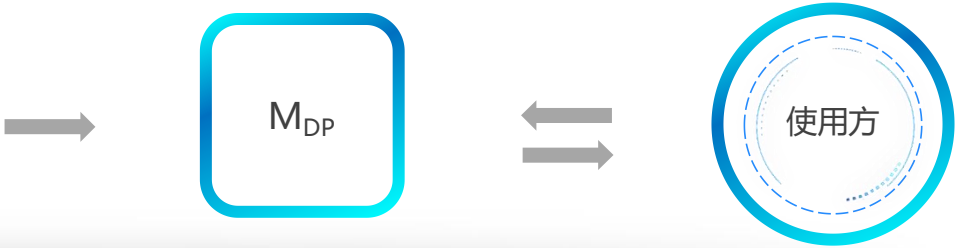
相关理论

ϵ-differential privacy, Dwork et. al. 2006

原始数据集D

ID	特征1	特征2	...	特征K	标签
1	$x_{1,1}$	$x_{1,2}$	···	$x_{1,K}$	y_1
2	$x_{2,1}$	$x_{2,2}$	···	$x_{2,K}$	y_2
...	...	...	...	...	...
N	$x_{N,1}$	$x_{N,2}$	···	$x_{N,K}$	y_N

数据保护机制



同态加密

同态加密计算实现对密文数据的计算，且确保解密后的计算结果等于相应的明文计算结果。

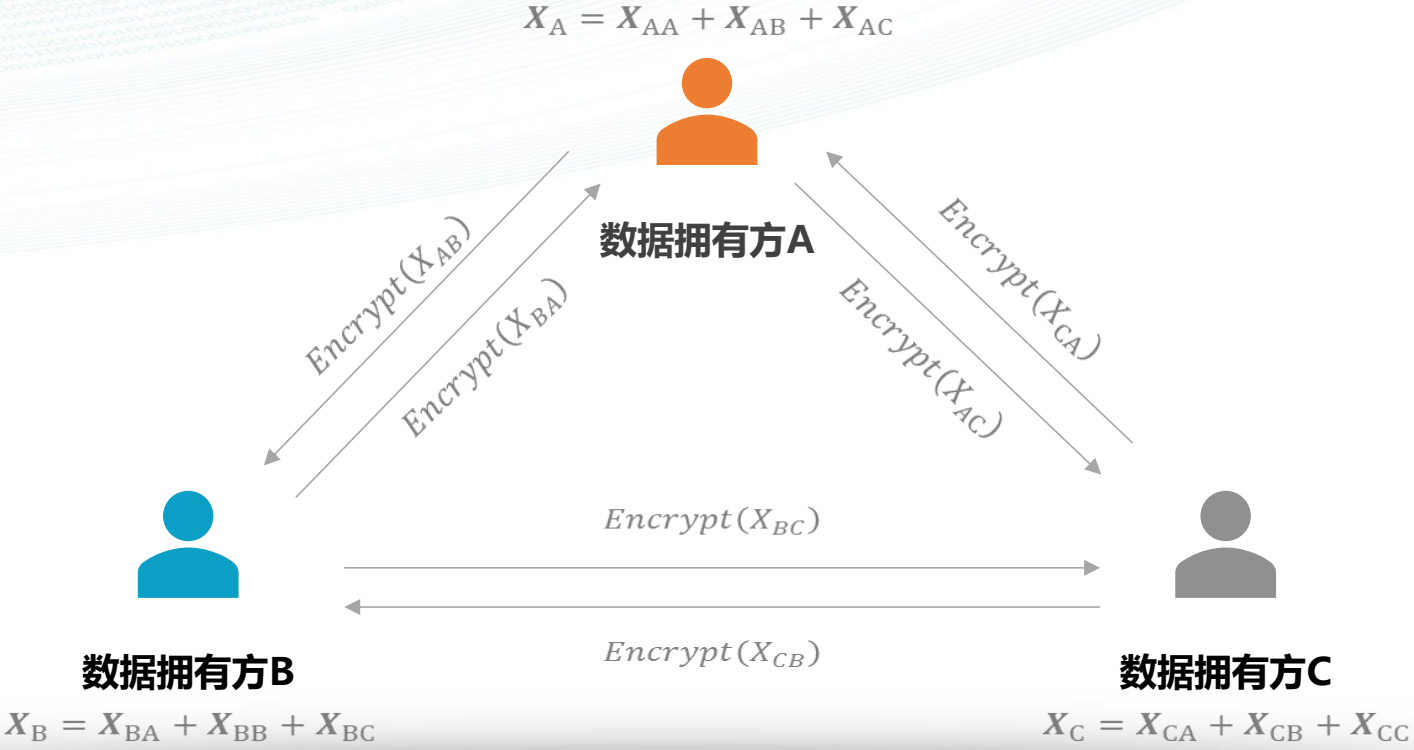
$$y = Decrypt_{SK}\left(Evaluate\left(f, Encrypt_{PK}(x)\right)\right) = f(x)$$

1. 生成密钥对：公钥（PK），私钥（SK）
2. 原始数据加密：$m = Encrypt_{PK}(x)$
3. 发送加密数据 m
4. 发送计算函数 f
5. 执行同态计算：$r = Evaluate(f, m)$
6. 返回结果 r
7. 结果解密：$y = Decrypt_{SK}(r)$

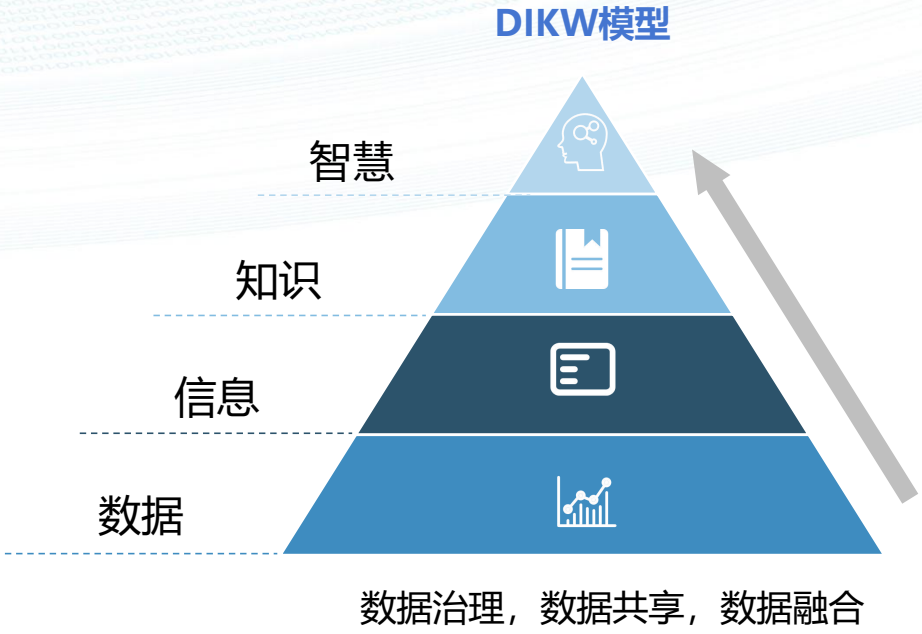
数据拥有方

函数计算方

多方安全计算


$X_A = X_{AA} + X_{AB} + X_{AC}$
数据拥有方A
$Encrypt(X_{AB})$
$Encrypt(X_{BA})$
$Encrypt(X_{CA})$
$Encrypt(X_{AC})$
$Encrypt(X_{BC})$
$Encrypt(X_{CB})$
数据拥有方B
$X_B = X_{BA} + X_{BB} + X_{BC}$
数据拥有方C
$X_C = X_{CA} + X_{CB} + X_{CC}$

智慧金融对隐私计算技术的进一步要求



2. 在多方数据共享的场景下实现隐私计算

1. 隐私计算与机器学习等复杂算法的融合

- 知识图谱
- 数据挖掘
- 机器学习
- 数据分析

Part 04

隐私计算与机器学习

机器学习任务

原始数据集 *D*

ID	特征1	特征2	…	特征*K*	标签
1	$x_{1,1}$	$x_{1,2}$	…	$x_{1,K}$	y_1
2	$x_{2,1}$	$x_{2,2}$	…	$x_{2,K}$	y_2
…	…	…	…	…	…
N	$x_{N,1}$	$x_{N,2}$	…	$x_{N,K}$	y_N

模型训练

机器学习模型

M_L

模型预测

模型预测结果

$\hat{y}_{new} = M_L(\boldsymbol{X}_{new,1})$

构建模型

$$M_L(\boldsymbol{X}_i) = f(\theta_{opt}, \boldsymbol{X}_i)$$

构建目标函数

$$L(\theta) = \sum_{n=1}^{N} J(f(\theta, \boldsymbol{X}_n), y_n) + R(\theta)$$

参数优化
(梯度下降)

$$\theta_{j+1} = \theta_j - \nabla L(\theta_j)$$

参数输出

$$\theta_{opt} = \min_{\theta} L(\theta)$$

差分隐私机器学习

关键问题：差分预算的设计和参数选择；隐私保护 vs 算法性能

输入扰动	目标扰动	梯度扰动	输出扰动
$M_L(\boldsymbol{X}_i) = f(\theta_{opt}, \boldsymbol{X}_i')$ $\boldsymbol{X}_i' = \boldsymbol{X}_i + \beta_X(\epsilon)$	$L(\theta) = \sum_{n=1}^{N} J(f(\theta, \boldsymbol{X}_n), y_n) + R(\theta) + \beta_L(\epsilon)$	$\theta_{j+1} = \theta_j - \nabla L(\theta_j) + \beta_{\nabla L}(\epsilon)$	$\theta_{opt} = \min_{\theta} L(\theta) + \beta_\theta(\epsilon)$
⬆	⬆	⬆	⬆
构建模型	**构建目标函数**	**参数优化 (梯度下降)**	**参数输出**
$M_L(\boldsymbol{X}_i) = f(\theta_{opt}, \boldsymbol{X}_i)$	$L(\theta) = \sum_{n=1}^{N} J(f(\theta, \boldsymbol{X}_n), y_n) + R(\theta)$	$\theta_{j+1} = \theta_j - \nabla L(\theta_j)$	$\theta_{opt} = \min_{\theta} L(\theta)$

基于密文的机器学习

关键问题：同态加密的能力限制 vs 机器学习的计算需求

密文输入

$$M_L(\boldsymbol{X}_i) = f_{\mathrm{HE}}(\theta'_{opt}, \boldsymbol{X}'_i)$$

$$\boldsymbol{X}'_i = Encrypt(\boldsymbol{X}_i)$$

构建模型

$$M_L(\boldsymbol{X}_i) = f(\theta_{opt}, \boldsymbol{X}_i)$$

密文目标函数计算

$$L(\theta) = \sum_{n=1}^{N} J(f(\theta, \boldsymbol{X}'_n), y'_n) + R(\theta)$$

$$\boldsymbol{X}'_n = Encrypt(\boldsymbol{X}_n)$$

$$y'_n = Encrypt(y_n)$$

构建目标函数

$$L(\theta) = \sum_{n=1}^{N} J(f(\theta, \boldsymbol{X}_n), y_n) + R(\theta)$$

密文梯度更新

$$\theta_{j+1} = \theta_j - \nabla L'(\theta_j)$$

$$\nabla L'(\theta_j) = Encrypt\left(\nabla L(\theta_j)\right)$$

参数优化
(梯度下降)

$$\theta_{j+1} = \theta_j - \nabla L(\theta_j)$$

模型参数加密

$$\theta_{opt} = \min_{\theta} L(\theta)$$

$$\theta'_{opt} = Encrypt(\theta'_{opt})$$

参数输出

$$\theta_{opt} = \min_{\theta} L(\theta)$$

Part 05

隐私计算与数据共享

多方横向数据融合

特点

扩充特征的多样性，针对特定的跨域合作场景构建特定的特征集合和数据标签体系

适用场景

- 联合风控
- 跨域精准营销

隐私保护方案

- 差分隐私或同态加密 + 联邦学习
- 安全多方计算 + 机器学习

金融机构A

ID	特征 A-1	特征 A-2	…	特征 A-*K*	标签
A_1	$x_{1,1}$	$x_{1,2}$	…	$x_{1,K}$	y_1
A_2	$x_{2,1}$	$x_{2,2}$	…	$x_{2,K}$	y_2
…	…	…	…	…	…
A_N	$x_{N,1}$	$x_{N,2}$	…	$x_{N,K}$	y_N

科技公司B

ID	特征 B-1	…	特征 B-*L*
A_1	$x_{1,1}$	…	$x_{1,L}$
A_2	$x_{2,1}$	…	$x_{2,L}$
…	…	…	…
A_N	$x_{N,1}$	…	$x_{N,L}$

垂直产业公司C

ID	特征 C-1	…	特征 C-*M*
A_1	$x_{1,1}$	…	$x_{1,L}$
A_2	$x_{2,1}$	…	$x_{2,L}$
…	…	…	…
A_N	$x_{N,1}$	…	$x_{N,L}$

多方纵向数据融合

金融机构A

ID	特征1	特征2	...	特征*K*	标签
A_1	$x_{1,1}$	$x_{1,2}$	···	$x_{1,K}$	y_1
A_2	$x_{2,1}$	$x_{2,2}$	···	$x_{2,K}$	y_2
...	...	...	...	...	...
A_N	$x_{N,1}$	$x_{N,2}$	···	$x_{N,K}$	y_N

金融机构B

ID	特征1	特征2	...	特征*K*	标签
B_1	$x_{1,1}$	$x_{1,2}$	···	$x_{1,K}$	y_1
B_2	$x_{2,1}$	$x_{2,2}$	···	$x_{2,K}$	y_2
...	...	...	...	...	...
B_M	$x_{N,1}$	$x_{N,2}$	···	$x_{N,K}$	y_N

特点

扩充训练数据样本量，提升模型精度和泛化能力

适用场景

各类AI建模场景

隐私保护方案

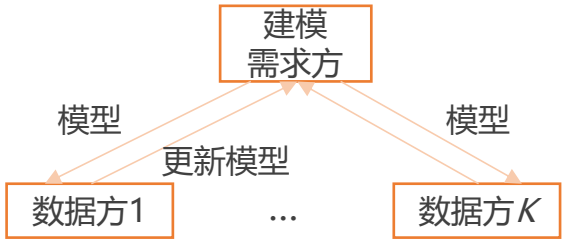
- 差分隐私或同态加密 + 联邦学习
- 安全多方计算 + 机器学习

多方参与的AI隐私计算

中心化无隐私保护模型训练，预测

从数据交互
到模型交互

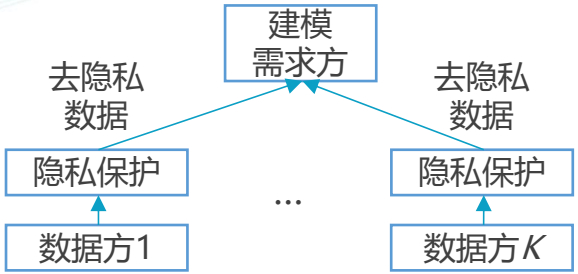
联邦学习 (Google 2018)



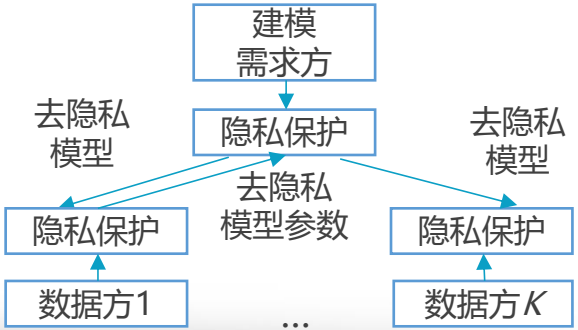
数据不动，模型动

从明文交互
到密文交互

中心化隐私保护模型训练，预测



强隐私保护联邦学习



Part 06

金融隐私计算框架

金融隐私计算系统架构


传统数据中台
隐私保护机制
应用层
业务应用
风险评估
金融产品推荐
智能客服
交互层
交互协议
传统分布式学习
联邦学习
MPC
网络结构
中心化
代理模式
去中心化
计算层
算法模型
神经网络模型
决策树模型
其他模型
中间层算子
损失函数运算
梯度运算
优化算子运算
统计运算
数学变换
底层算子
数学运算算子
逻辑运算算子
向量矩阵运算
数据层
特征数据
特征数据
标签数据
底层数据
金融数据
泛金融数据
隐私计算协议
安全多方计算
隐私联合建模
隐私计算算法
差分隐私
同态加密
秘密共享
混淆电路
数据隐私处理
数据脱敏
匿名化

谢谢！