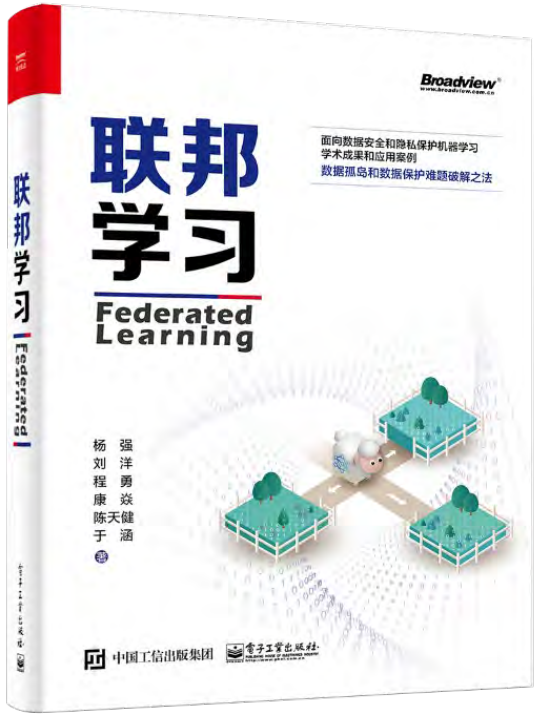
WeBank

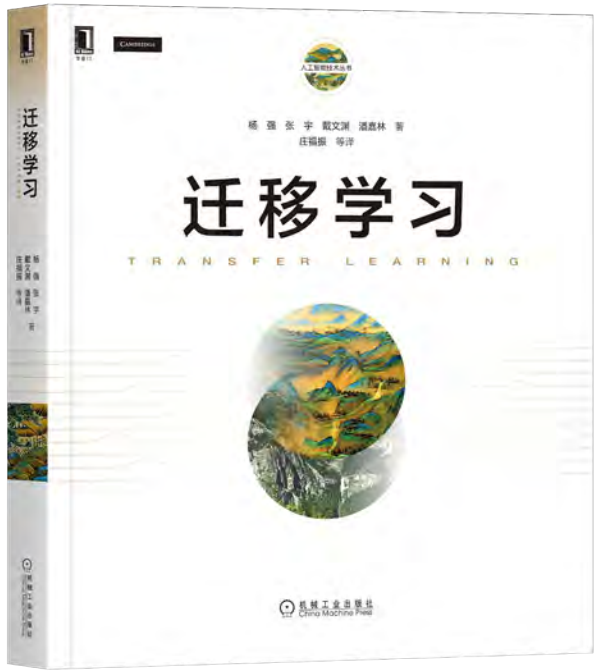
用户隐私、数据孤岛和联邦迁移学习

杨强

微众银行CAIO，香港科技大学讲席教授

2020年10月





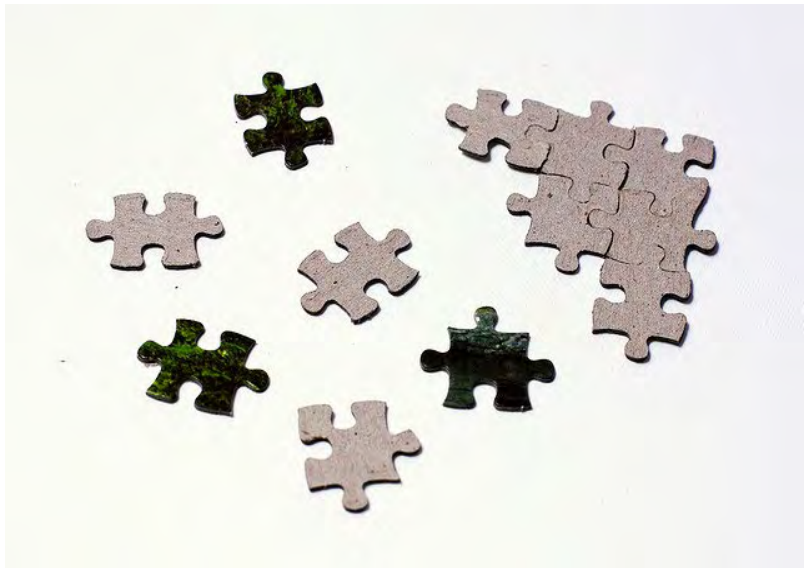
（1）大数据迁移到小数据（2）分散数据集的联邦

- **Small Data**

Transfer Learning from source task/domains to target tasks/domains

- **Fragmented Data**

Federated learning involving many parties collaboratively build models



Often, these two problems occur together

问题

能不能把小数据聚合起来，成为大数据呢？

个人隐私与数据法规： 欧盟的 GDPR

- 《通用数据保护条例》（General Data Protection Regulation，简称GDPR）为欧盟于2018年5月25日出台的条例。
- 对违法企业的罚金最高可达2000万欧元（约合1.5亿元人民币）或者其全球营业额的4%，以高者为准。
- 网站经营者必须事先向客户说明会自动记录客户的搜索和购物记录,企业不能再使用模糊、难以理解的语言，或冗长的隐私政策来从用户处获取数据使用许可。
- 明文规定了用户的“被遗忘权”（right to be forgotten），即用户个人可以要求责任方删除关于自己的数据记录。

2018年5月28日报道：

Facebook和谷歌等美国企业成为GDPR法案下第一批被告。

GDPR下，IT巨头纷纷被罚

French regulator fines Google $57 million for GDPR violations

Share on Facebook Share on Twitter +

Google hasn't transparently implemented GDPR rules, French regulator claims.

1 . France's National Data Protection Commission (CNIL) found that Google provided information to users in a non-transparent way.

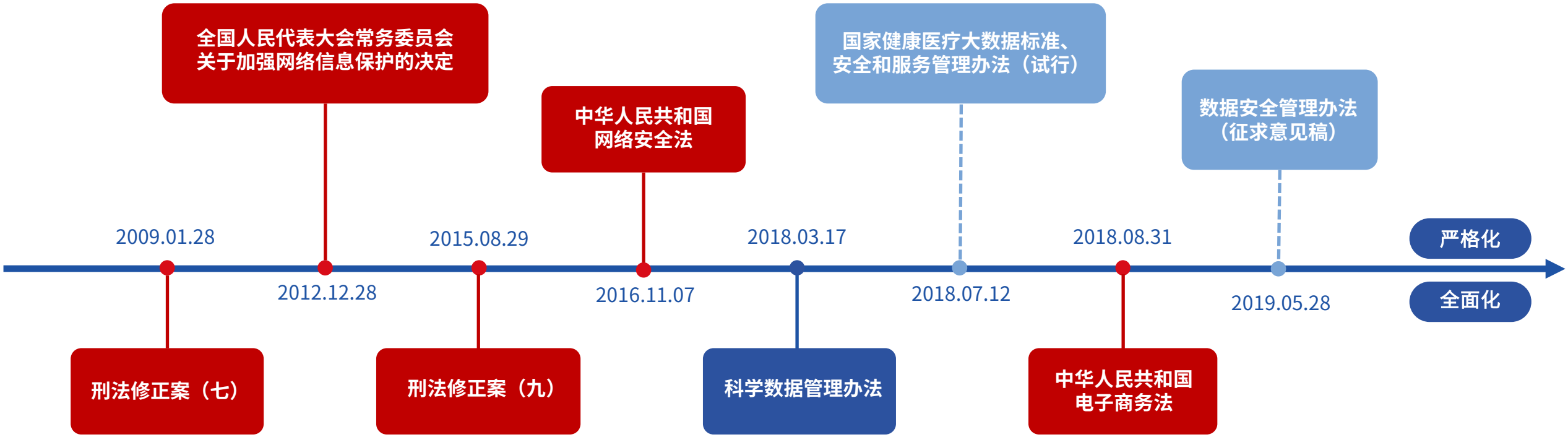
"The relevant information is accessible after several steps only, implying sometimes up to 5 or 6 actions"

- CNIL said.

2. The users' consent, CNIL claims, "is not sufficiently informed," and it's "neither 'specific' nor 'unambiguous'."

To date, this is the largest fine issued against a company since GDPR came into effect last year.

国内的数据监管法律趋严



严格化：数据控制方责任明确，刑罚到自然人

全面化：各领域数据管理细则密集出台，用户授权+监管部门审批

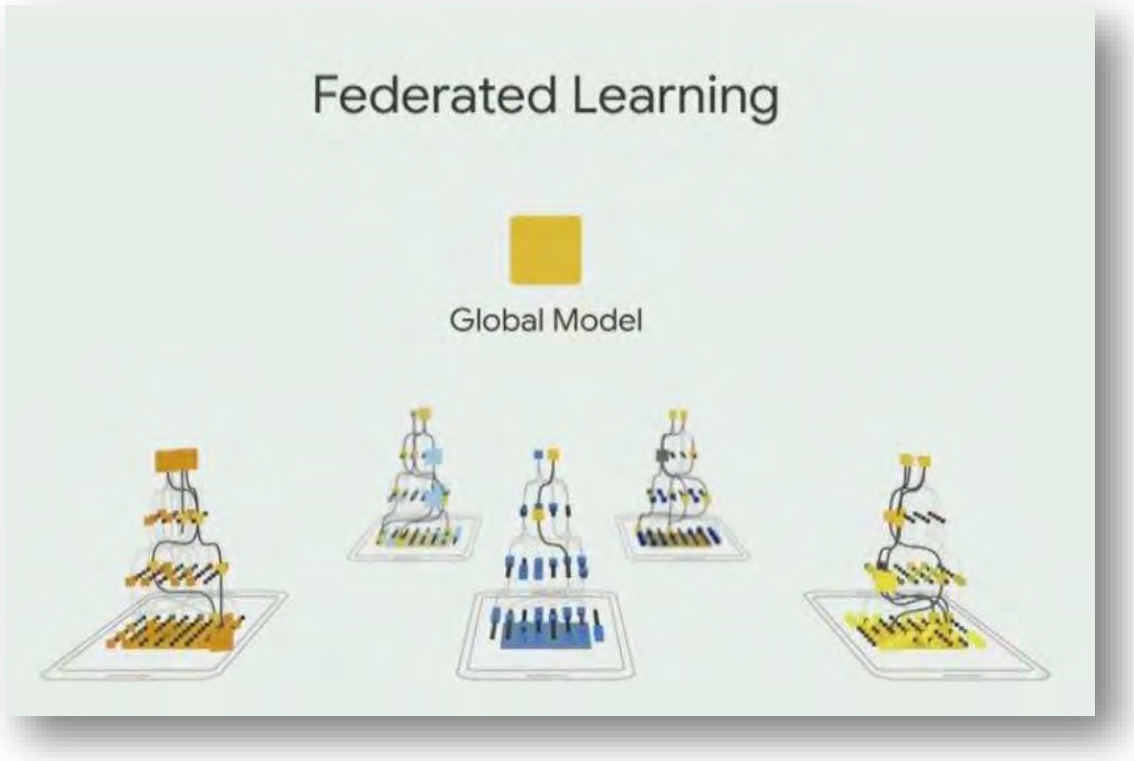
01

什么是联邦学习（Federated Learning）

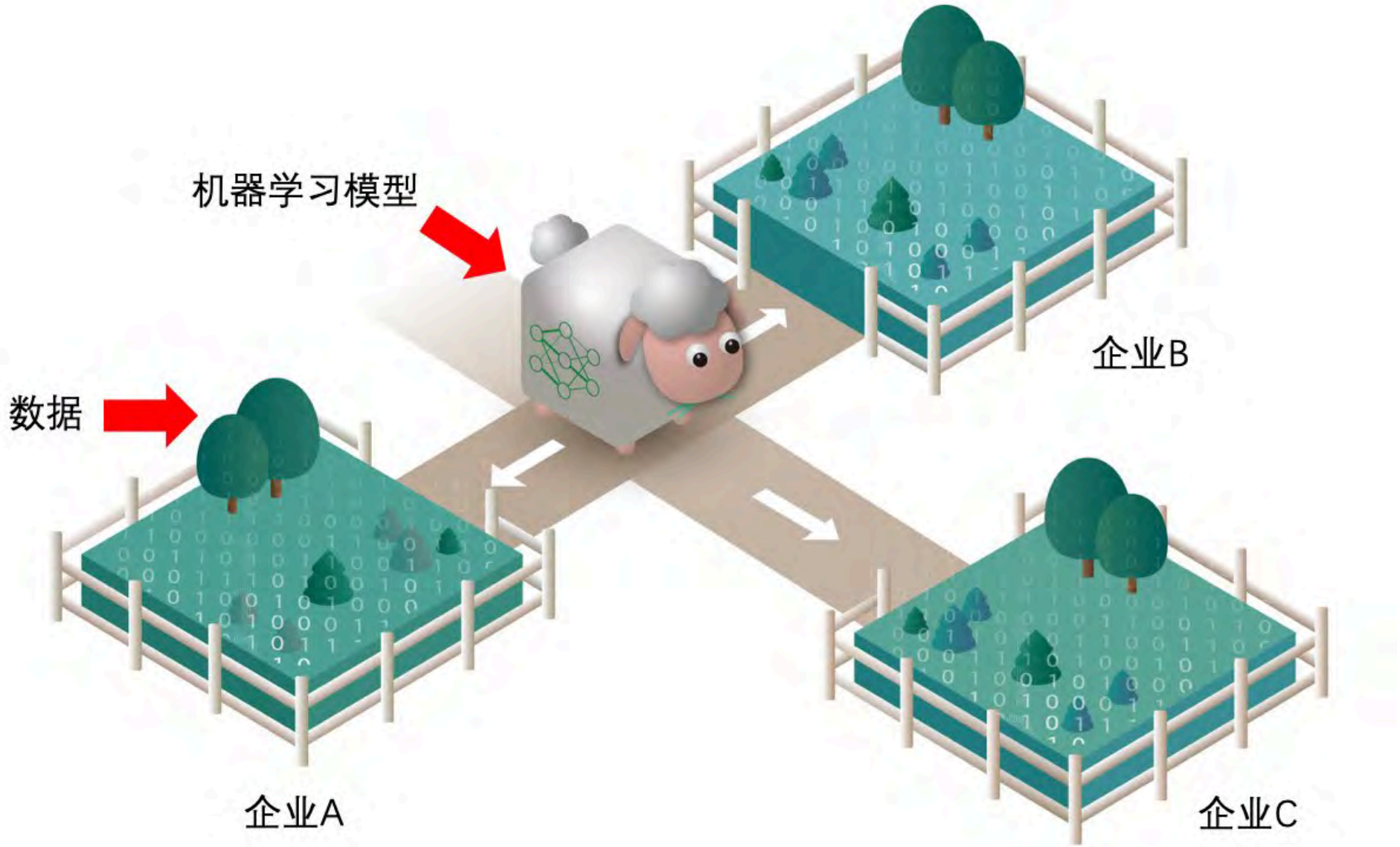
数据不动 模型动

联邦学习（Federated Learning）

1. **数据隐私保护**
2. **模型参数保护**
3. **建模能力效果更好**
   - A方有A模型
   - B方有B模型
   - A和B模型都比单独建模好



数据不动模型动

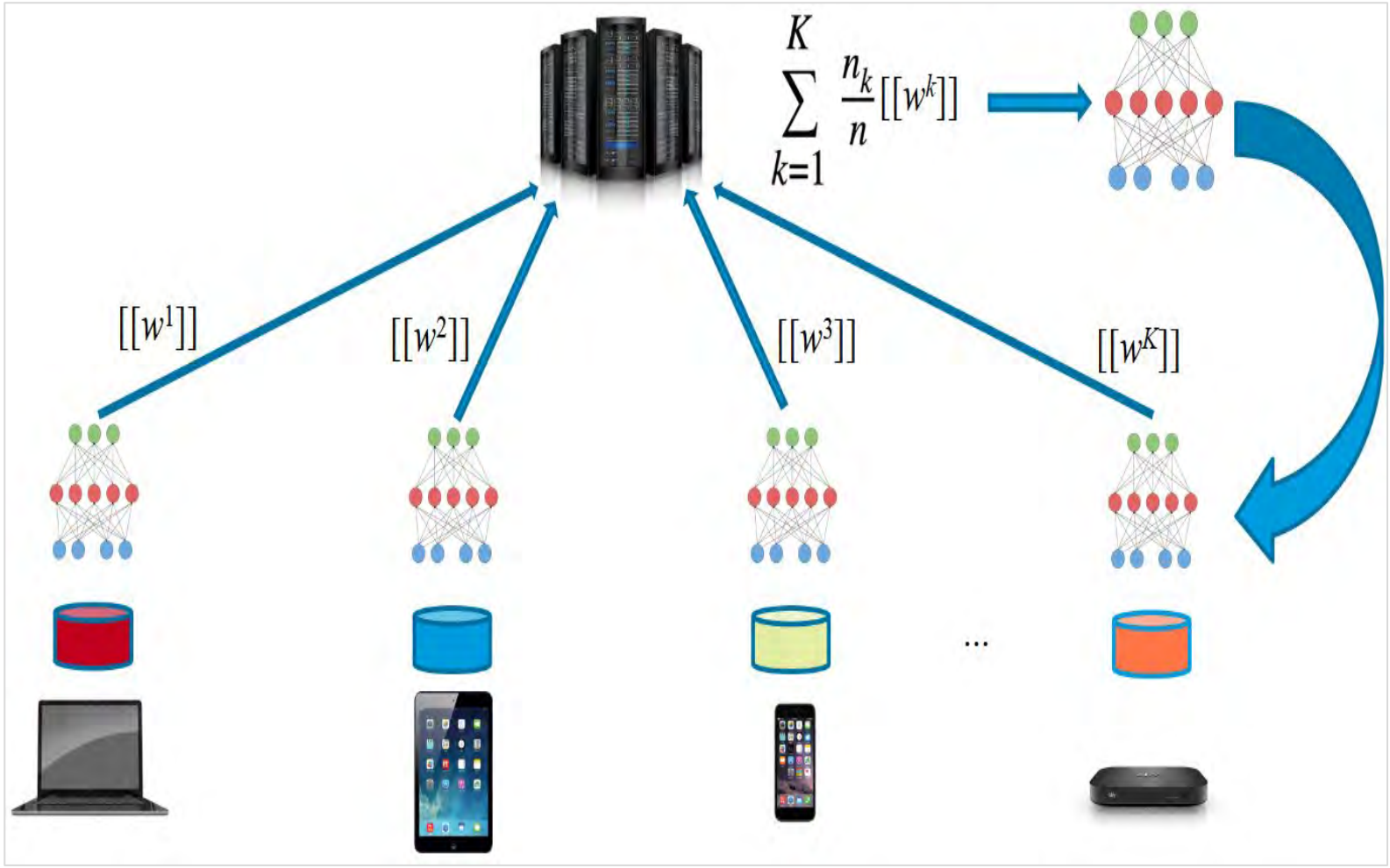

机器学习模型
数据
企业B
企业A
企业C

第一类联邦学习问题：按样本分割（横向切割数据）

ID	X1	X2	X3
U1	9	80	600
U2	4	50	550
U3	2	35	520
U4	10	100	600

ID	X1	X2	X3
U5	9	80	600
U6	4	50	550
U7	2	35	520
U8	10	100	600

ID	X1	X2	X3
U9	9	80	600
U10	4	50	550



联邦学习关键技术——加密/解密

- Step 1: 在各自本地建模： Wi
- Step 2: 在本地对模型Wi加密
  - [[Wi]]
- Step 3: 上传 本地加密的模型[[Wi]]
- Step 4: 在服务器端整合上传的加密的模型：W=F({[[Wi]], i=1,}) 2, …
- Step 5: 下传W到各个终端
- Step 6: 在各自本地，利用 W 对Wi更新

问题： 如何利用加密的参数进行模型更新?

- W=F({[[Wi]], i=1,}) ?

➢ 保护隐私的加密 （同态加密， Homomorphic Encryption (HE) ）

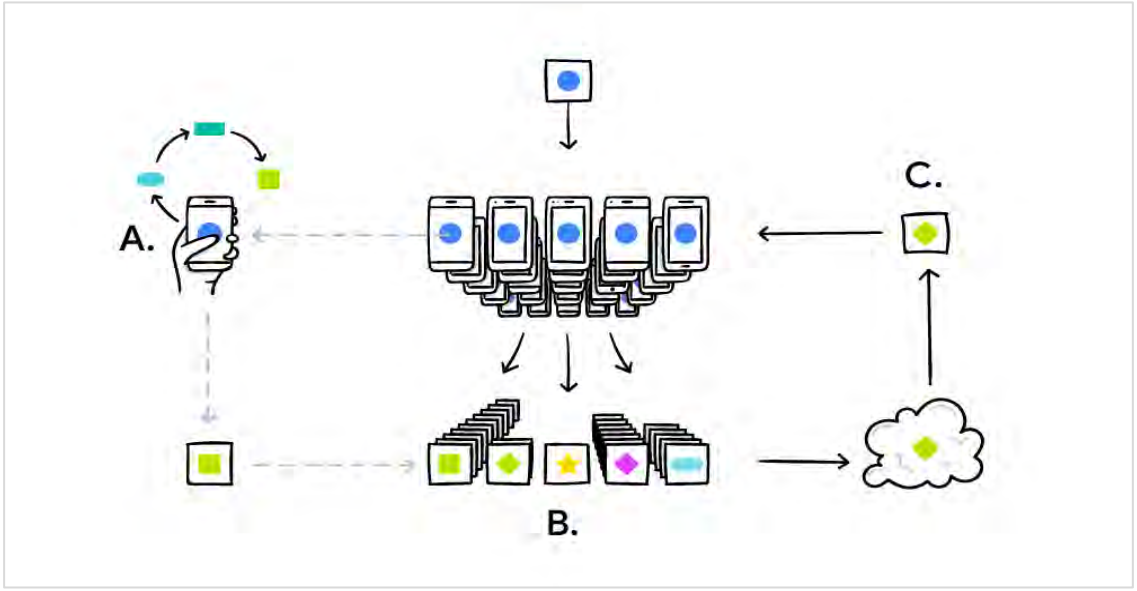
- **加法同态:**

$$\mathrm{Dec}_{\mathrm{sk}}([[u]] \oplus [[v]]) = \mathrm{Dec}_{\mathrm{sk}}([[u+v]])$$

- **标量乘法同态:**

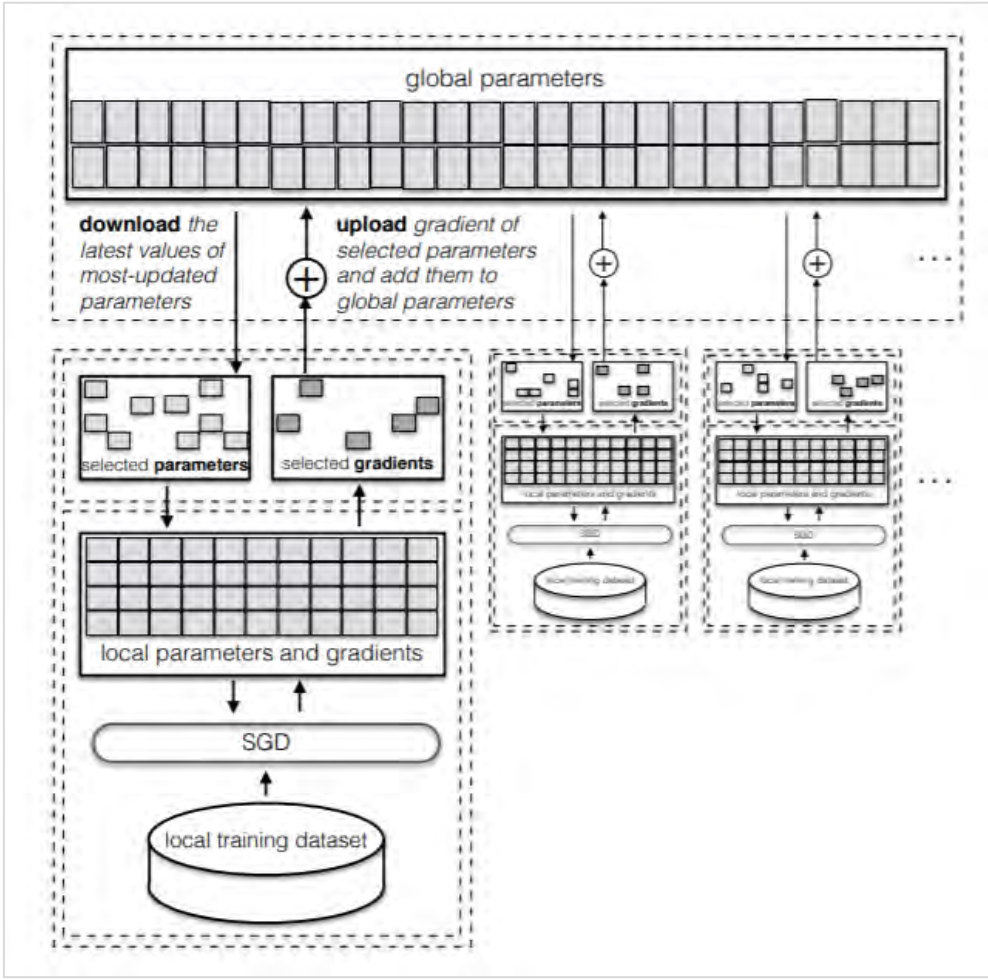
$$\mathrm{Dec}_{\mathrm{sk}}([[u]] \odot n) = \mathrm{Dec}_{\mathrm{sk}}([[u \cdot n]])$$

谷歌的横向联邦学习 （Federated Averaging）



H. Brendan McMahan et al, *Communication-Efficient Learning of Deep Networks from Decentralized Data*, Google, 2017

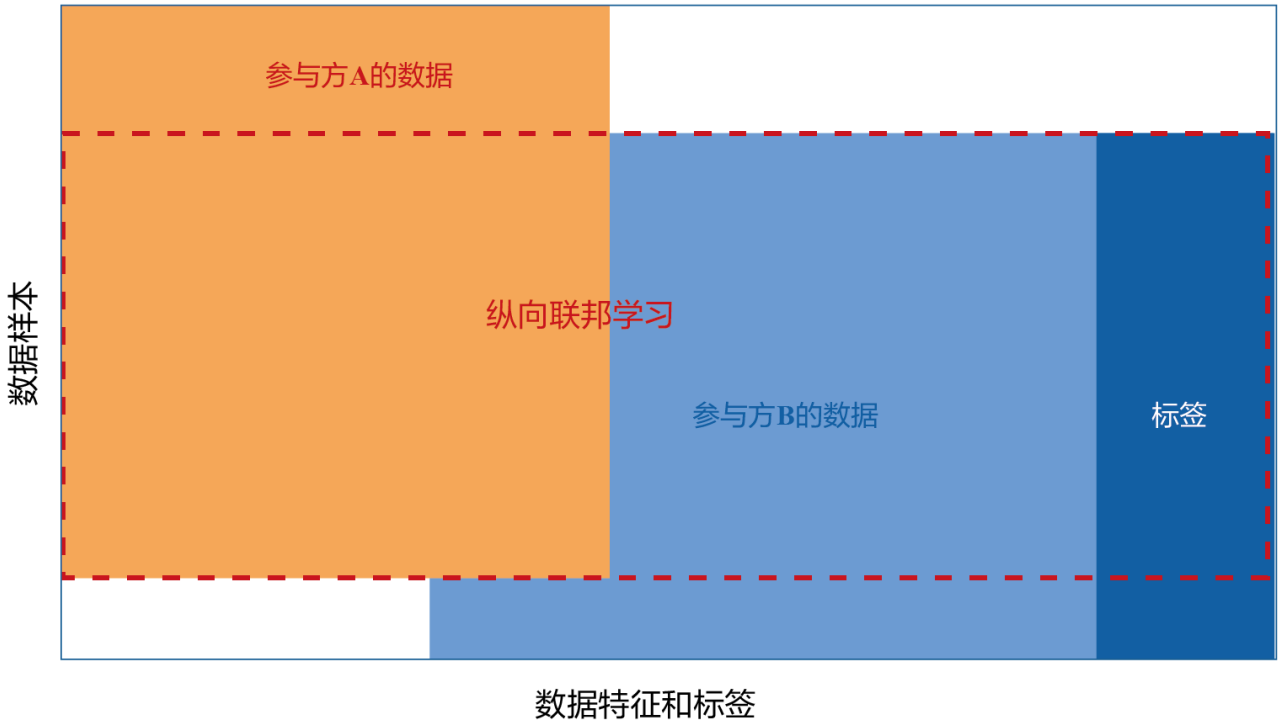
- 手机终端，多个用户，1个中心
- 所有数据特征维度相同
- 本地训练
- 选择用户训练

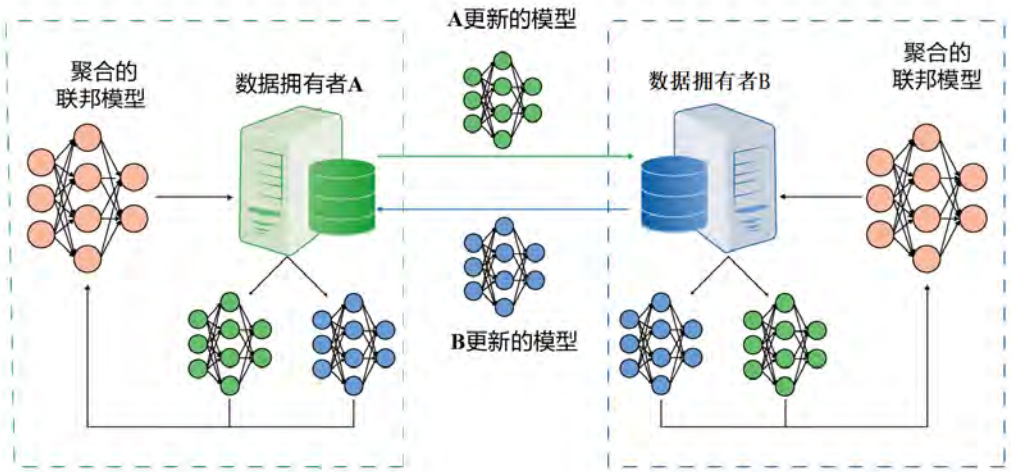


Reza Shokri and Vitaly Shmatikov. 2015. *Privacy-Preserving Deep Learning*. In Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security (CCS ' 15). ACM, New York, NY, USA, 1310–1321.

- 选择参数更新

纵向联邦学习（特征不同，样本重叠）





Secureboost in VFL

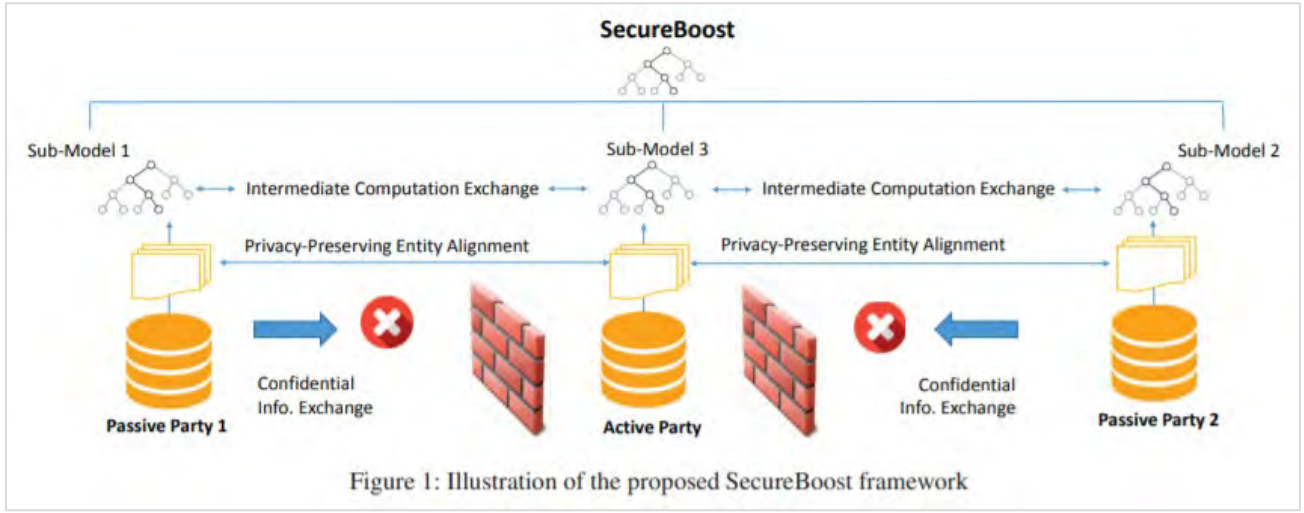
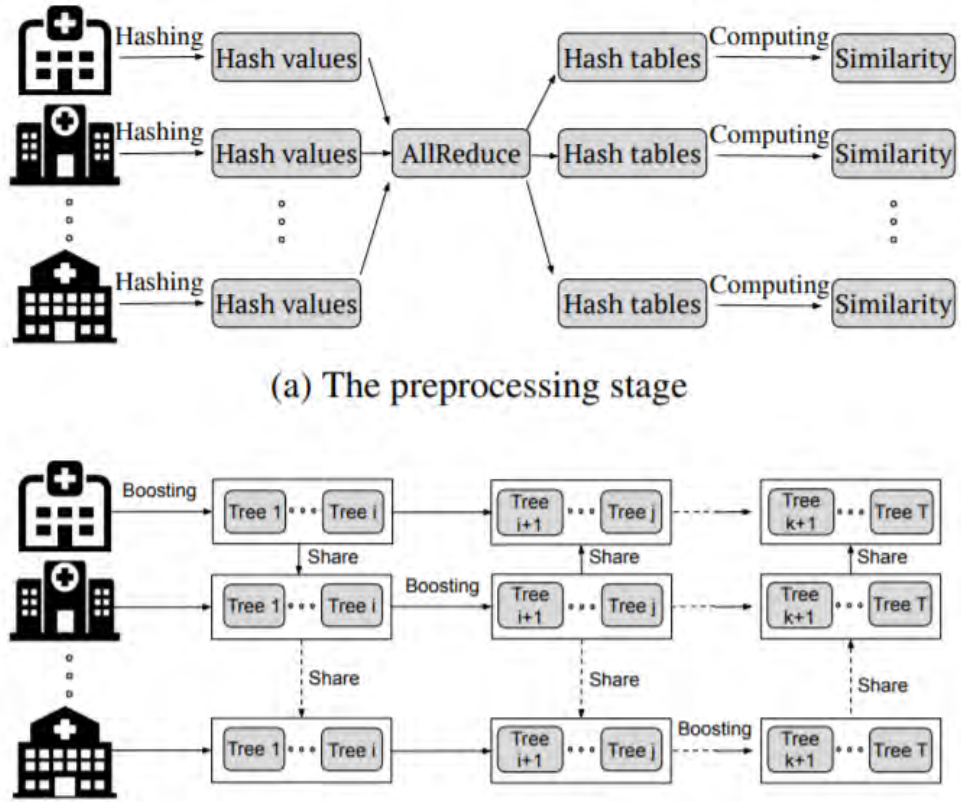


Figure 1: Illustration of the proposed SecureBoost framework

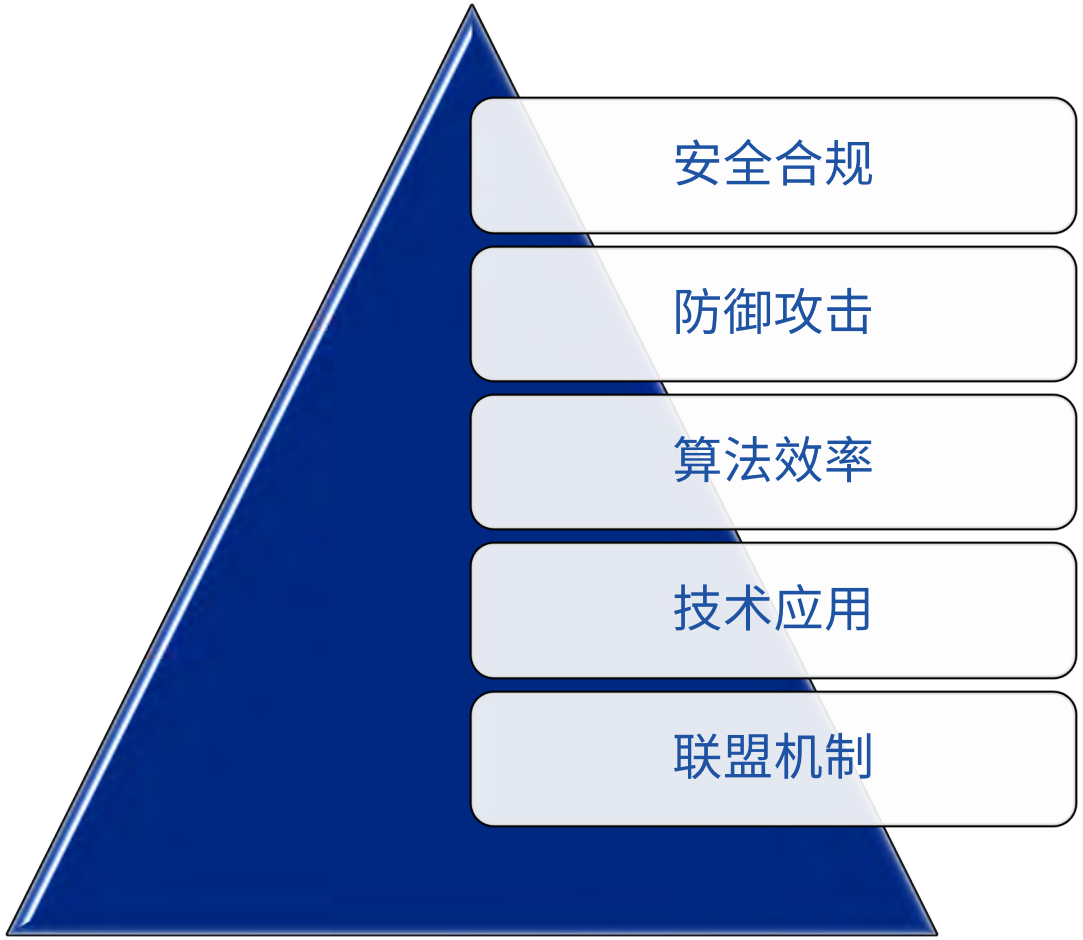
Kewei Cheng, Tao Fan, Yilun Jin, Yang Liu, Tianjian Chen, Qiang Yang, SecureBoost: A Lossless Federated Learning Framework, IEEE Intelligent Systems 2020

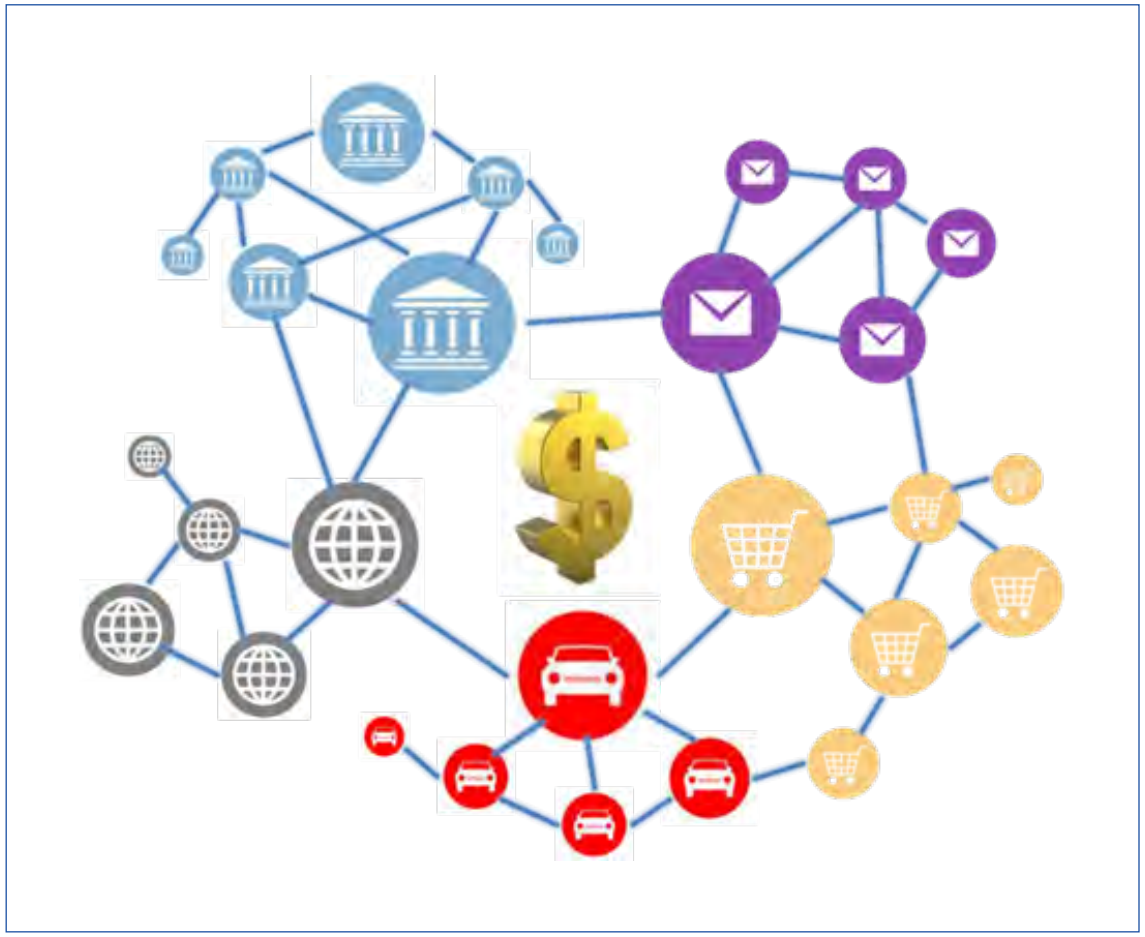
GBDT in HFL



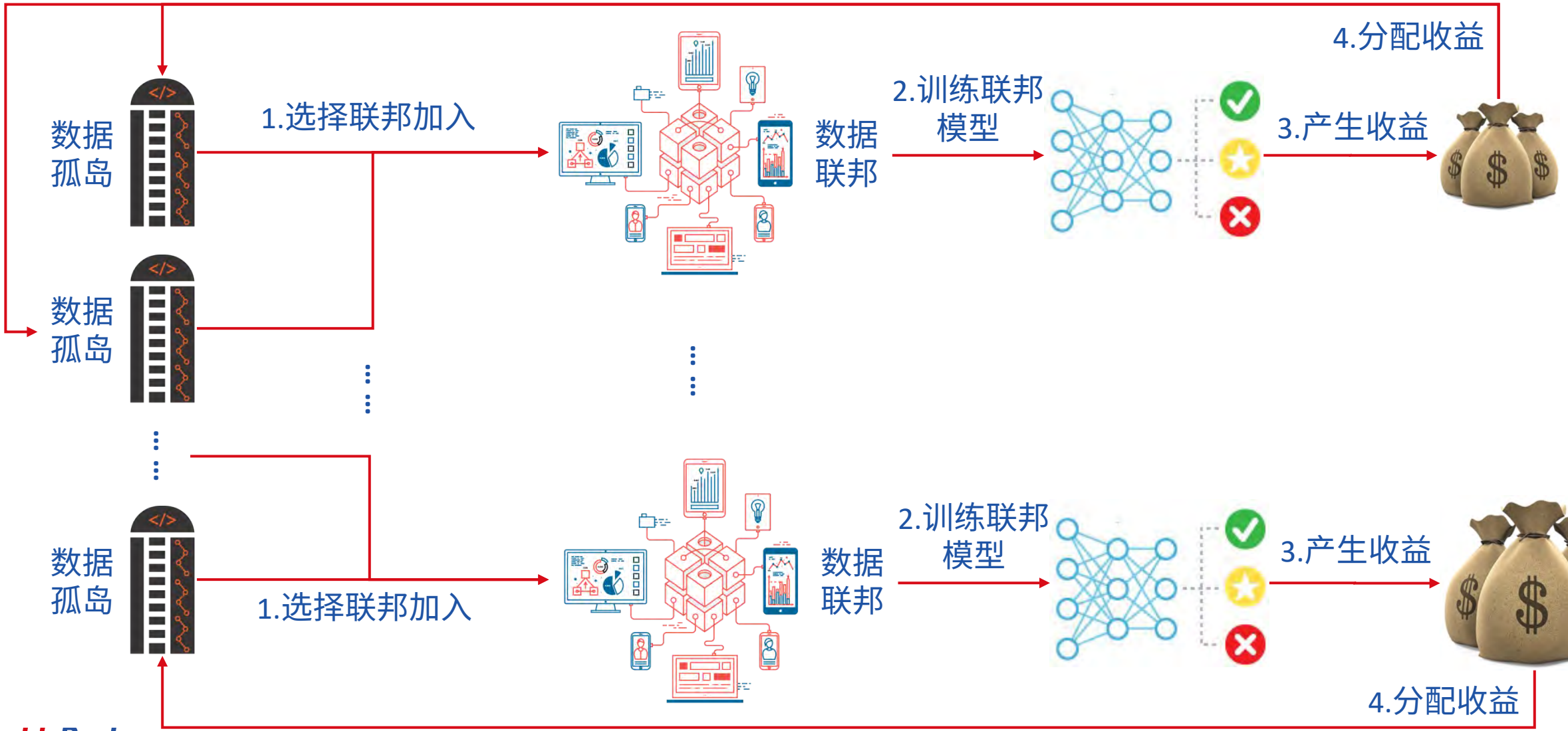
Qinbin Li, Zeyi Wen, Bingsheng He, Practical Federated Gradient Boosting Decision Trees, AAAI, 2019

联邦学习（Federated Learning）的研究展望





联邦学习激励机制设立


数据孤岛
数据孤岛
数据孤岛
1.选择联邦加入
1.选择联邦加入
数据联邦
数据联邦
2.训练联邦模型
2.训练联邦模型
3.产生收益
3.产生收益
4.分配收益
4.分配收益

联邦学习激励机制研究

1. 如何能够让参与者受益，并激发它们持续参与到联邦训练中来?

2. 重要问题：

了解参与方在不同联邦收益分配机制下的行为反应
- 从而设计有效、合理的激励机制

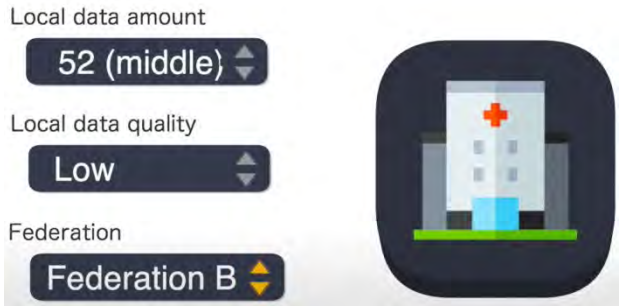
1. 平均主义分配方案
   - 平均分配
2. 边际收益分配方案
   1. 线性分配
   2. 工会分配(Labour Union)
   3. Shapley分配
3. 边际损失分配方案
   - 公平值分配
4. 多维度公平分配方案
   - Federated Learning Incentivizer

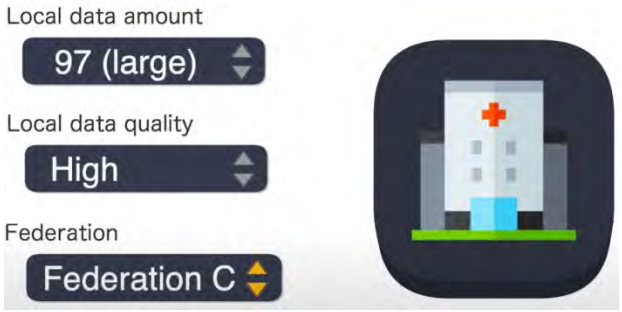
Yu, H., Liu, Z., Liu, Y., Chen, T., Cong, M., Weng, X., Niyato, D. & Yang, Q. A sustainable incentive scheme for federated learning. *IEEE Intelligent Systems*, vol. 35, no. 4, pp. 58–69, 2020.

FedGame：基于多人游戏的联邦学习激励机制研究平台

游戏流程：

1. 随机分配初始特征





2. 玩家选择联邦并设置自身策略

3. 系统根据玩家设置及联邦学习基本逻辑模拟本回合联邦学习模型训练

4. 系统根据模拟结果确定各个联邦的模型市场份额，以此分配总收益。个联邦根据自身的激励机制为各自的玩家分配收益

5. 开始下一回合

K. L. Ng, Z. Chen, Z. Liu, H. Yu, Y. Liu & Q. Yang, "A Multi-player Game for Studying Federated Learning Incentive Schemes," *IJCAI*, 2020.

FedGame：基于多人游戏的联邦学习激励机制研究平台

玩家选择联邦并设置自身策略

Ng, Z. Chen, Z. Liu, H. Yu, Y. Liu & Q. Yang, "A Multi-player Game for Studying Federated Learning Incentive Schemes," *IJCAI*, 2020.

纵向联邦推荐： 系统架构

Example: movie recommendation with data from two different groups of users

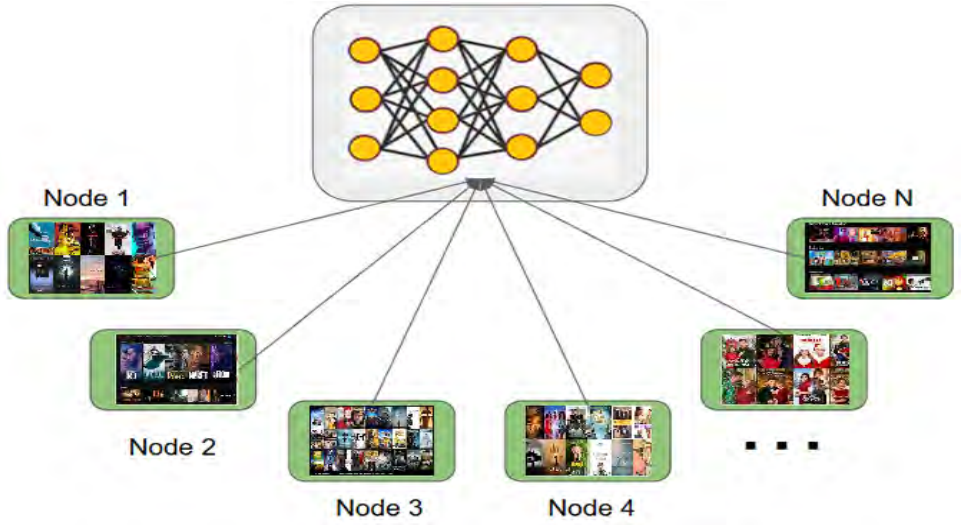
Party A

Party B

Solution to Case 2: Item profiles are securely aggregated by server, user profiles are locally updated by parties.

横向“联邦推荐”架构

Example: movie recommendation with data from individual users



Party A

No data exchange

Party B

Party C

02

联邦学习应用案例

FinTech, Insure-tech, IoT, Health Care, Education, Edge Computing

联邦学习应用于金融机构全面风险管理-信贷风控

多方数据本地建模 → 联邦建模 → 联邦评分

安全联合多方多维数据，提高AI模型精度

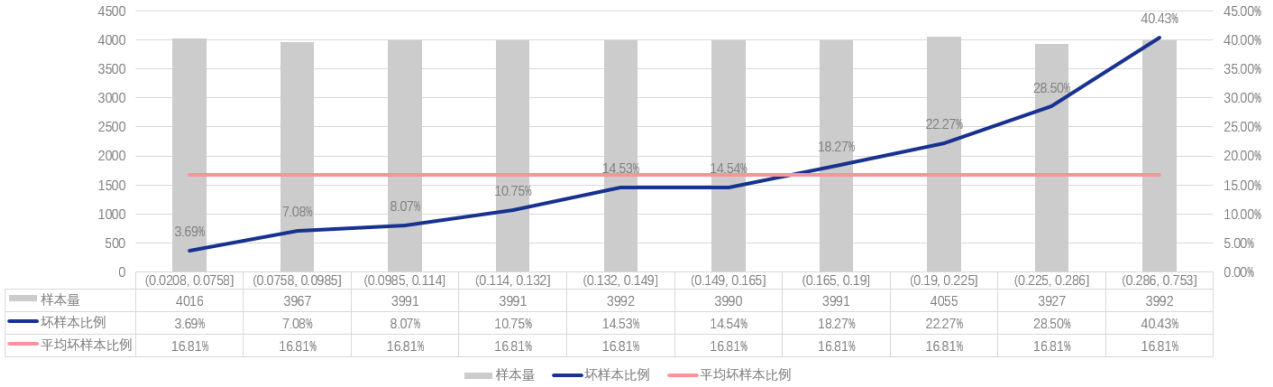
分数对应资质好坏

反欺诈/贷前评分/贷后监测

反欺诈评分举例

模型效果： AUC=0.70 KS=30，尾部分组坏样本比例是平均样本比例的2.4倍

使用方式：1）单一策略；2）入模变量；3）决策矩阵



	(0.0208, 0.0758]	(0.0758, 0.0985]	(0.0985, 0.114]	(0.114, 0.132]	(0.132, 0.149]	(0.149, 0.165]	(0.165, 0.19]	(0.19, 0.225]	(0.225, 0.286]	(0.286, 0.753]
样本量	4016	3967	3991	3991	3992	3990	3991	4055	3927	3992
坏样本比例	3.69%	7.08%	8.07%	10.75%	14.53%	14.54%	18.27%	22.27%	28.50%	40.43%
平均坏样本比例	16.81%	16.81%	16.81%	16.81%	16.81%	16.81%	16.81%	16.81%	16.81%	16.81%

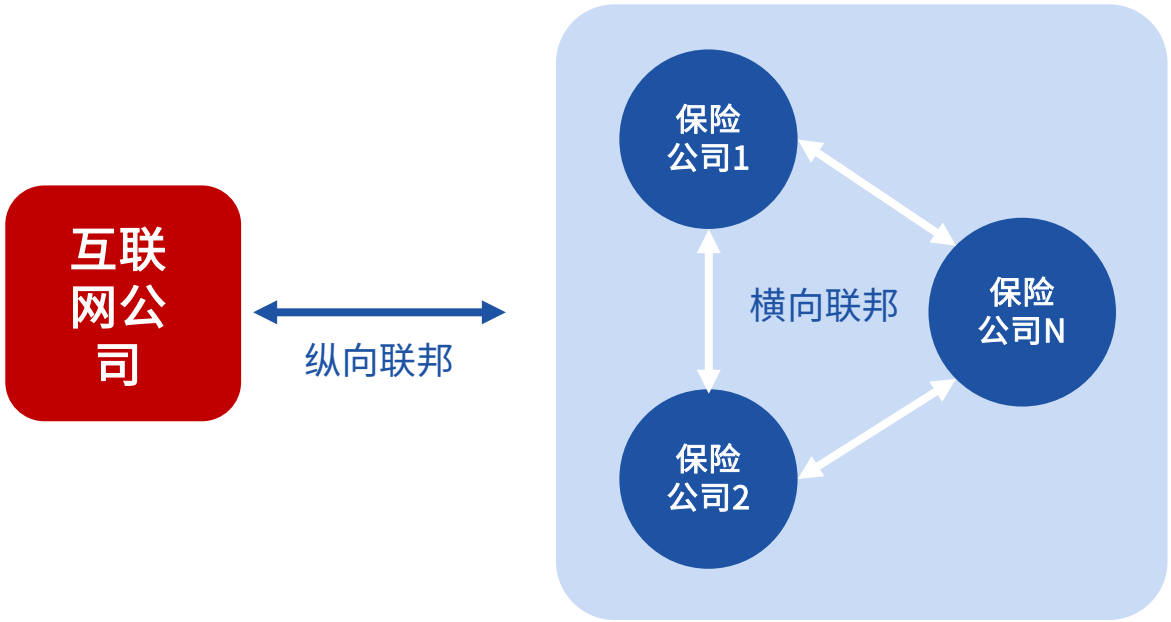
联邦学习应用于保险业

微众与瑞士再保险探索再保险商业创新 Swiss Re

协助再保公司建立承保人（保险公司）的车险索赔概率模型：纵向联邦引入和挖掘互联网大数据 “从人因子”，
横向联邦扩大承保人传统因子数据集规模，从而实现对车主进行精准画像和风险分析

互联网行为数据

- ✓ 出行数据
- ✓ 消费数据
- ✓ 信息偏好
- ✓ 车辆违章数据
- ✓ ……



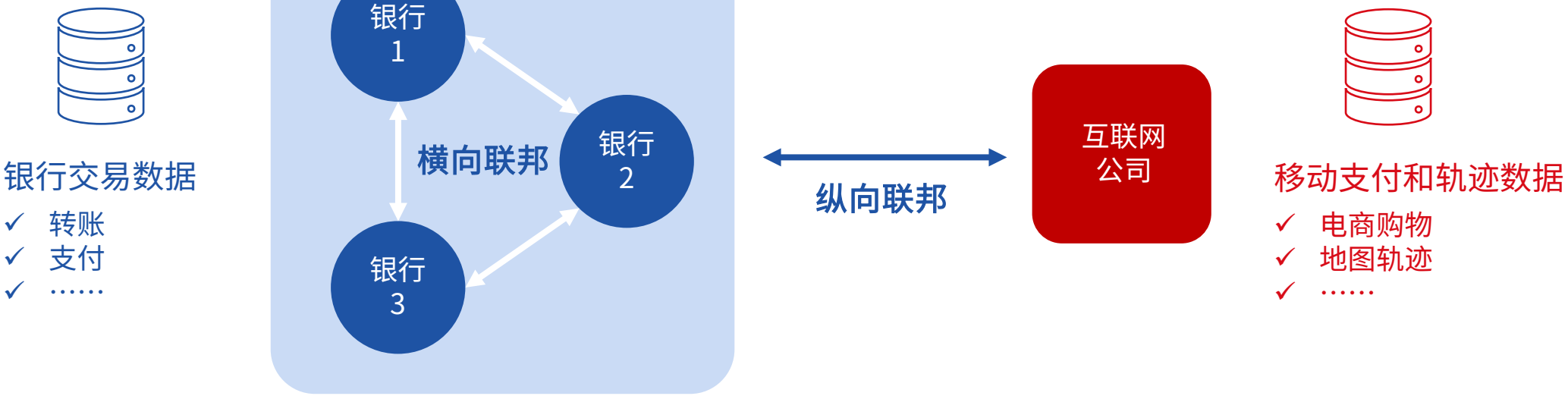
保险公司数据

- ✓ 承保数据
- ✓ 理赔数据
- ✓ 车联网数据
- ✓ ……

联邦学习应用于反洗钱

微众与人民银行深圳支行探索监管创新

因数据安全要求，银行和保险等金融机构在本地对数据进行建模，使用联邦学习，各个机构的模型联合起来，能打破数据之间的壁垒，提高反洗钱系统的准确度和审查人员的效率。



通过横向联邦扩充反洗钱样本，构建基础反洗钱模型 → 通过纵向联邦扩充客户特征维度，进一步优化模型效果

联邦学习应用于营销推荐: 联邦推荐

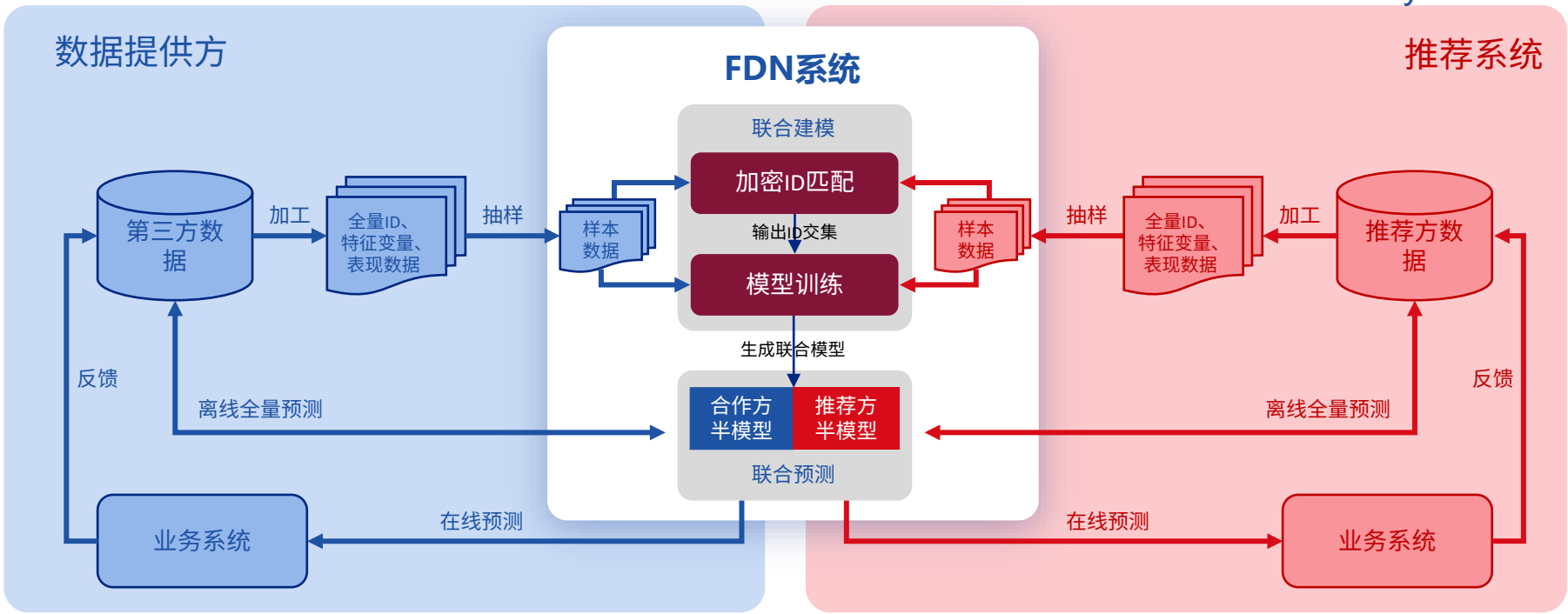
Example: movie and book recommendation with data from two different data sources

豆瓣读书

Party A

Party B

联合建模、预测示意图 —— 安全合规的数据合作过程



注：客户ID包括但不限于客户身份证号码、手机号、设备ID（imei）等； 联合建模过程由拥有Y（表现数据）的一方发起；

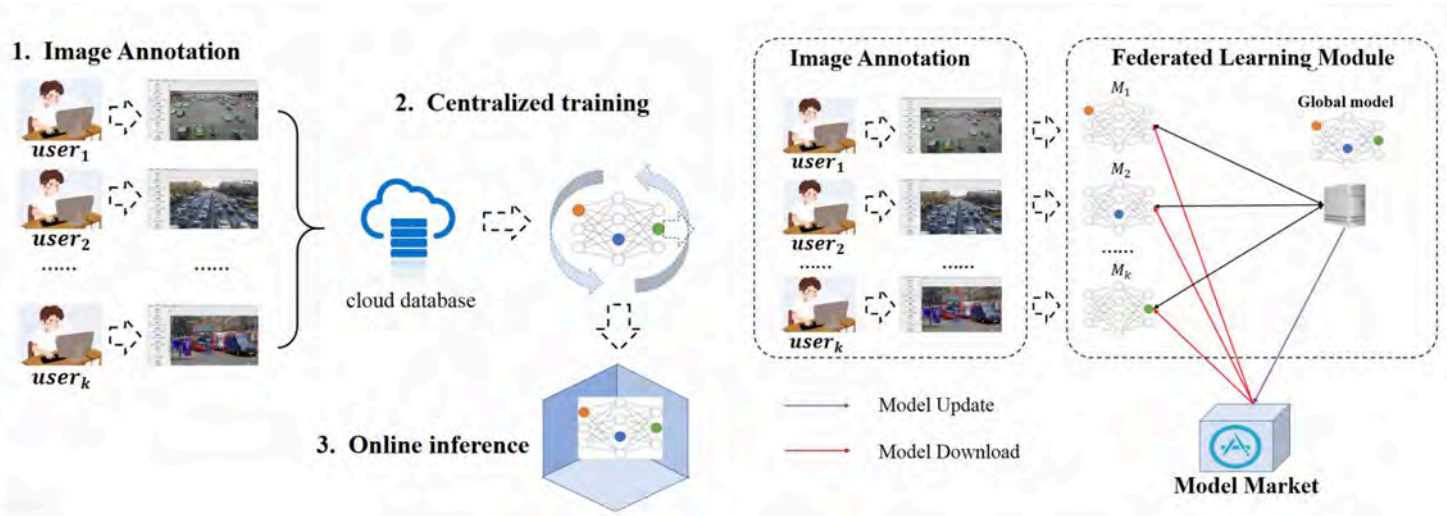
联邦学习用于计算机视觉

装备制造业、物联网AIOT、智慧安防等行业，依托联邦学习，进行视觉市场的场景拓宽

优势：

- 相对于本地建模进一步提升算法准确率
- 形成网络效应，降低长尾应用成本，提升视觉业务总体利润率

FedVision –由联邦学习提供支持的在线视觉对象检测平台



行人检测
出行检测
区域检测
设备异常检测
安全帽检测
火焰检测
烟雾检测
.....

智慧制造

智慧安防

智慧城市

在联邦视觉系统中，依托本地建模，在保证各方数据不出本地的情况下，即可提升AI算法准确率。

在联邦视觉系统项目中，通过联邦学习技术，整体模型的性能提升了15%，且模型效果无损失，极大地提升了建模效率

联邦学习应用于语音识别引擎

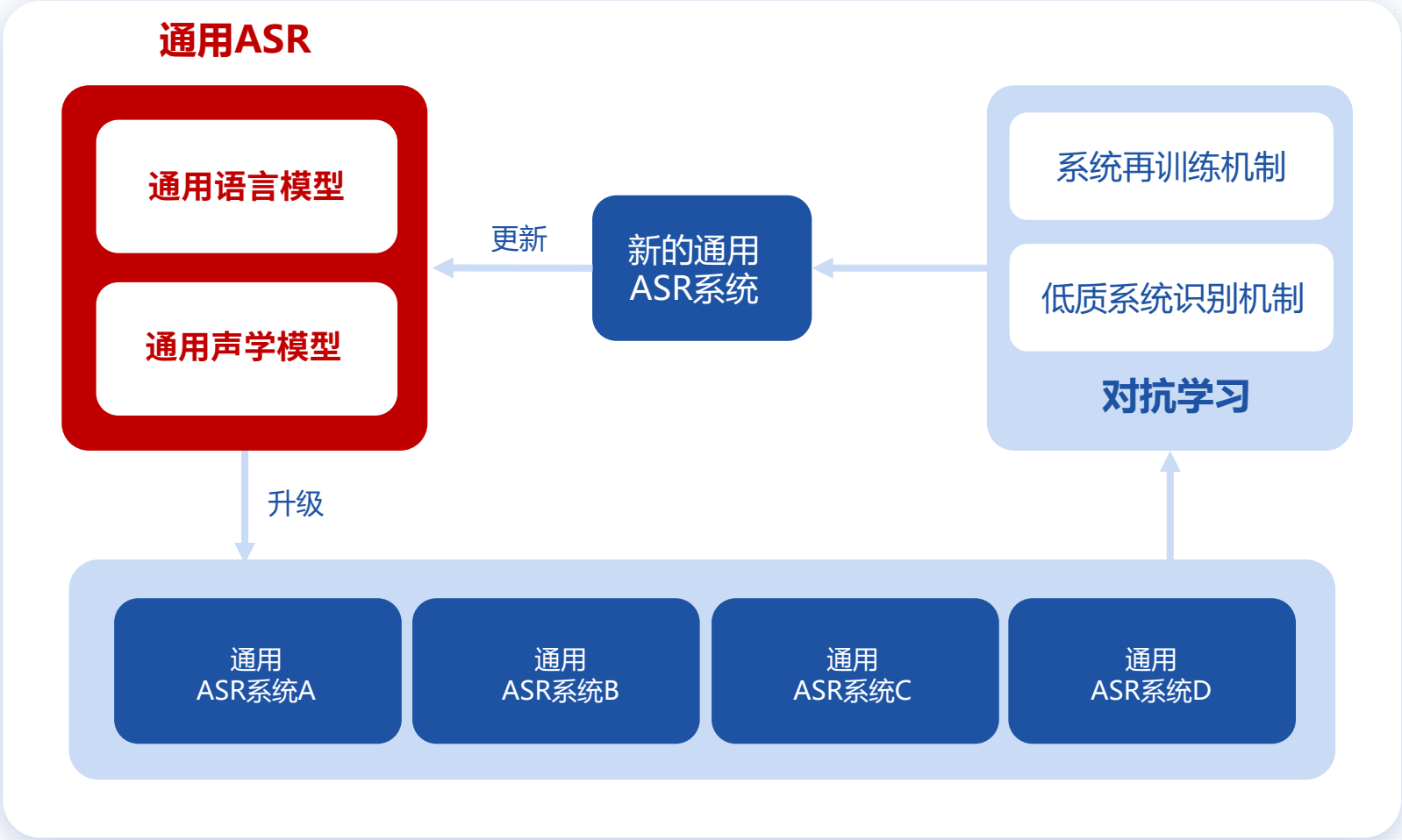
微众AI 基于“联邦对抗学习”的解决方案

语音识别联邦学习方案

- 业界常态目前为技术提供方到应用方的单向信息流动
- 我们的方案实现了技术提供方和应用方**共生共赢的生态闭环**

语音识别对抗学习方案

- 利用群体智能优胜略汰
- **减少对数据标注的依赖**



联邦学习应用于物联网

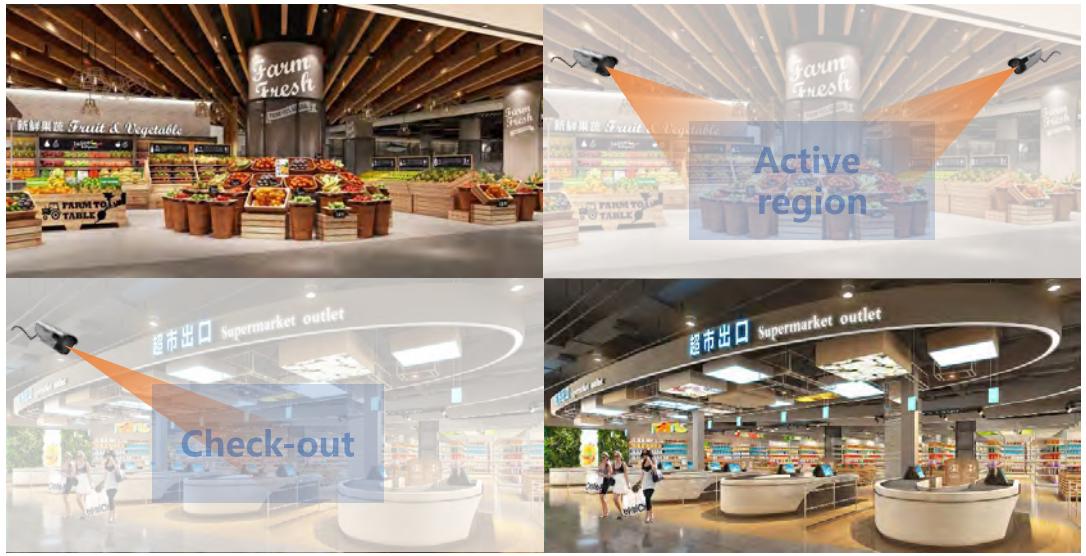
perception engine
analysis engine
recognition engine

Sensor & edge computing

Fog computing

Cloud computing

Client



联邦学习应用于医疗健康

微众银行携手腾讯天衍实验室成立
腾讯医疗健康-微众联合实验室

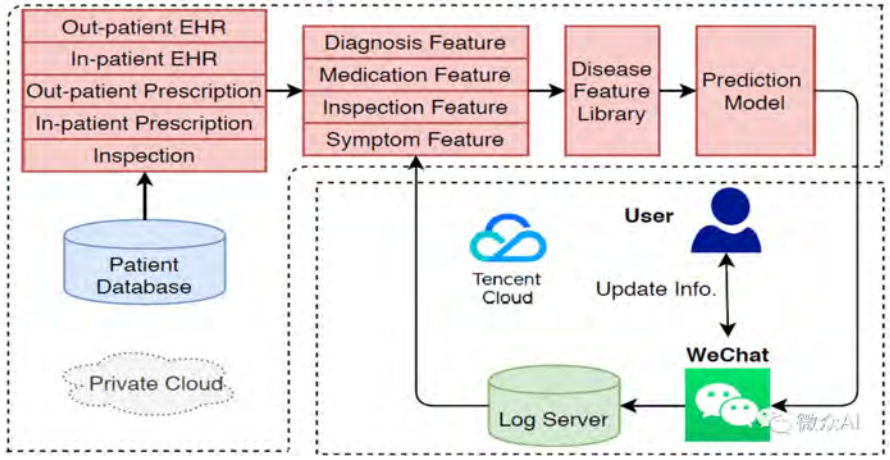
“脑卒中发病风险预测模型”准确率80%以上

小型医院模型预测指标提升了10-20%

研究论文被FL-IJCAI'20收录

Privacy-Preserving Technology to Help Millions of People: Federated Prediction Model for Stroke Prevention

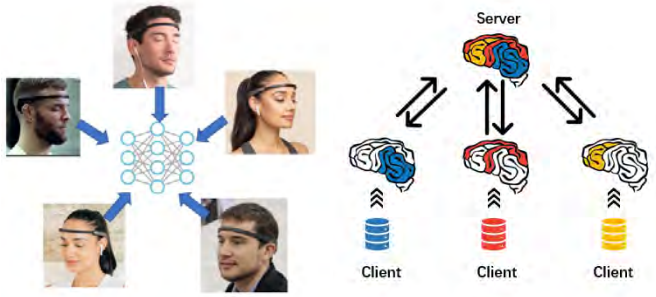
Ce Ju[1,*], Ruihui Zhao[2,*], Jichao Sun[2,*], Xiguang Wei[1,*], Bo Zhao[2], Yang Liu[1], Hongshan Li[3], Tianjian Chen[1], Xinwei Zhang[4], Dashan Gao[5,6], Ben Tan[1], Han Yu[7] and Yuan Jin[8]

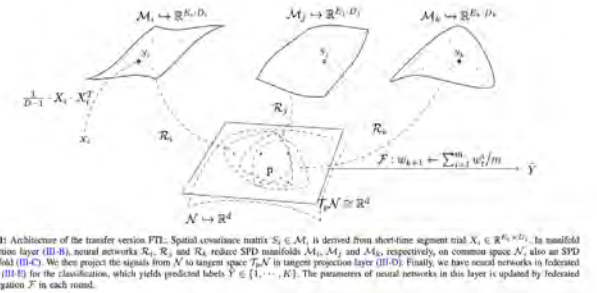


arXiv: https://arxiv.org/abs/2006.10517

微众银行携手顶尖学术机构
联邦学习技术在脑机接口领域应用

将不同研究机构、不同受试者的脑电图数据在不泄露隐私信息的情况下联合使用，为脑机接口大规模商用保驾护航。





研究论文被IEEE EMBC 2020收录

[Submitted on 26 Apr 2020 (v1), last revised 29 Jul 2020 (this version, v2)]

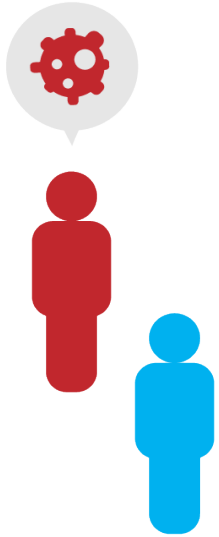
Federated Transfer Learning for EEG Signal Classification

Ce Ju, Dashan Gao, Ravikiran Mane, Ben Tan, Yang Liu, Cuntai Guan

The success of deep learning (DL) methods in the Brain-Computer Interfaces (BCI) field for classification of electroencephalographic (EEG) recordings has been restricted by the lack of large datasets. Privacy concerns associated with EEG signals limit the possibility of constructing a large EEG-BCI dataset by the conglomeration of multiple small ones for jointly training machine learning models. Hence, in this paper, we propose a novel privacy-preserving DL architecture named federated transfer learning (FTL) for EEG

arXiv: https://arxiv.org/abs/2004.12321
GitHub: https://github.com/DashanGao/Federated-Transfer-Learning-for-EEG

Federated Health Code：Defending COVID 19 with privacy

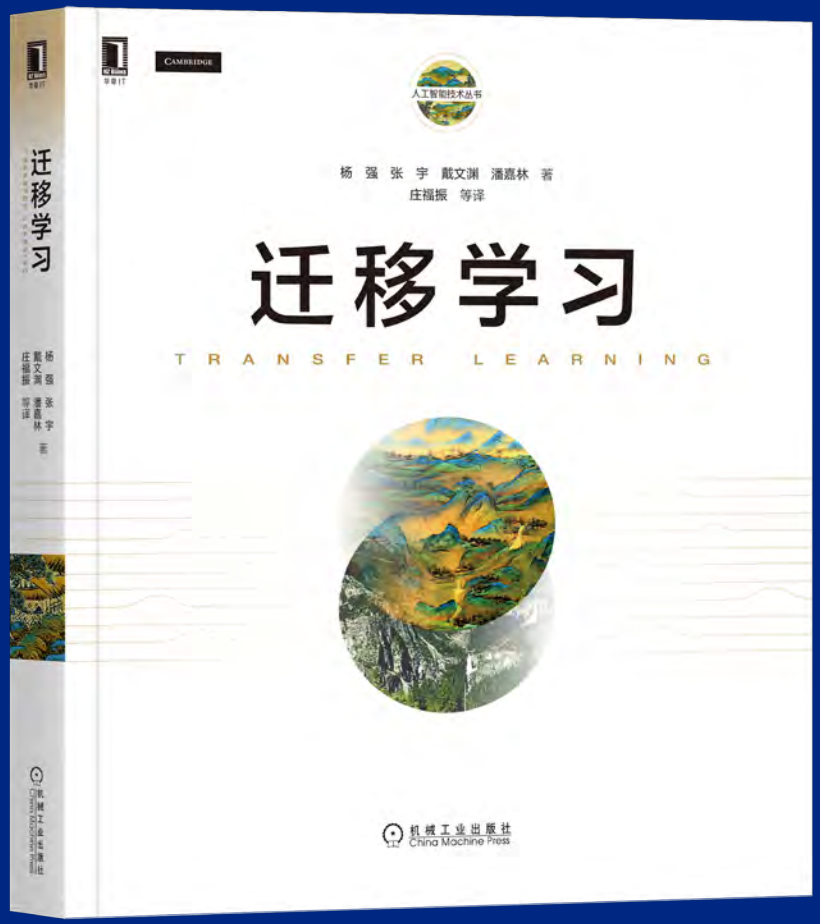


接触了病毒携带者

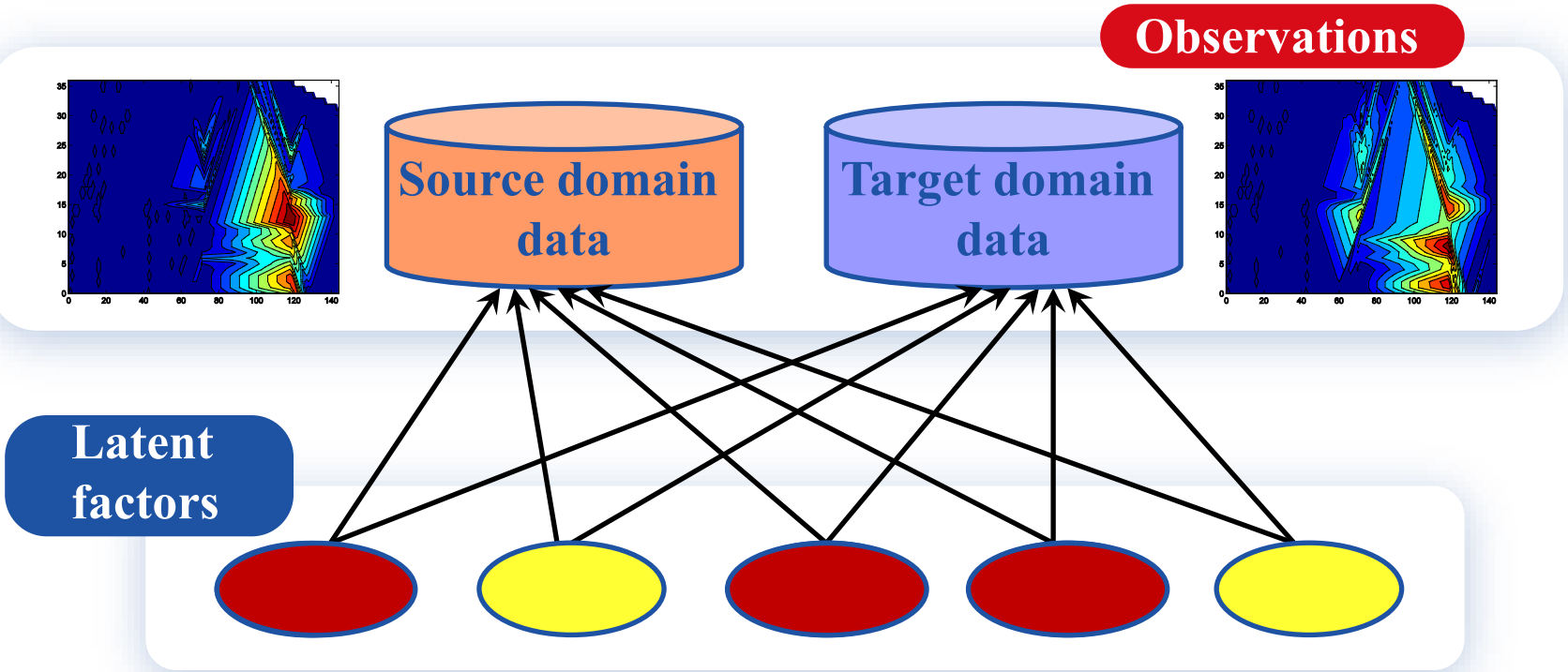
经过安检出示健康码

03

联邦学习 + 迁移学习

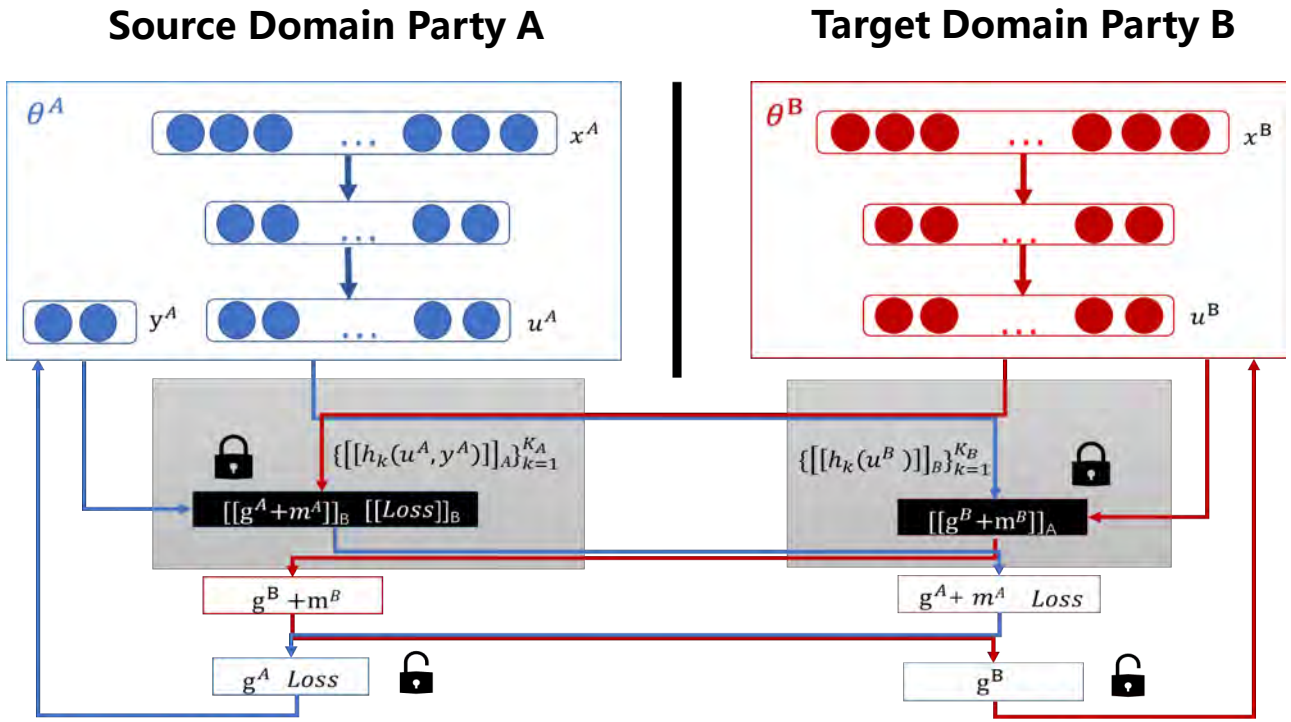

CAMBRIDGE
人工智能技术丛书
杨 强 张 宇 戴文渊 潘嘉林 著
庄福振 等译
迁移学习
TRANSFER LEARNING
机械工业出版社
China Machine Press

联邦学习和迁移学习的结合：联邦迁移学习



✓ 异构数据集：找到同分布子空间

Towards Secure and Efficient FTL

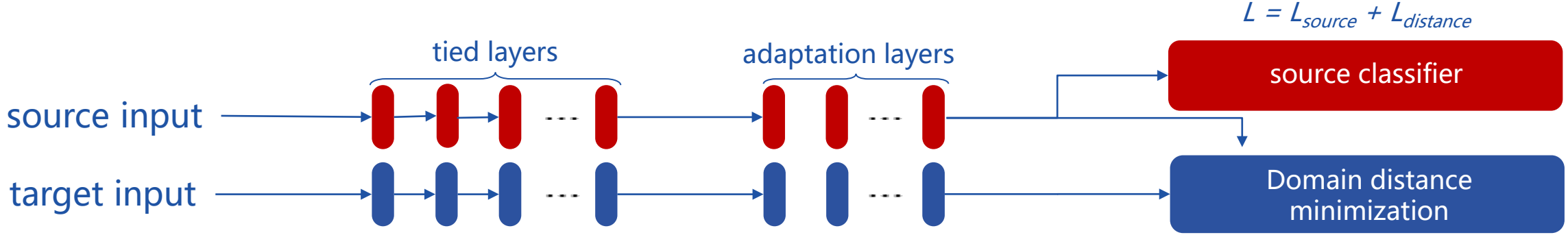


Step 1
Party A and B send public keys to each other

Step 2
Parties compute, encrypt and exchange intermediate results

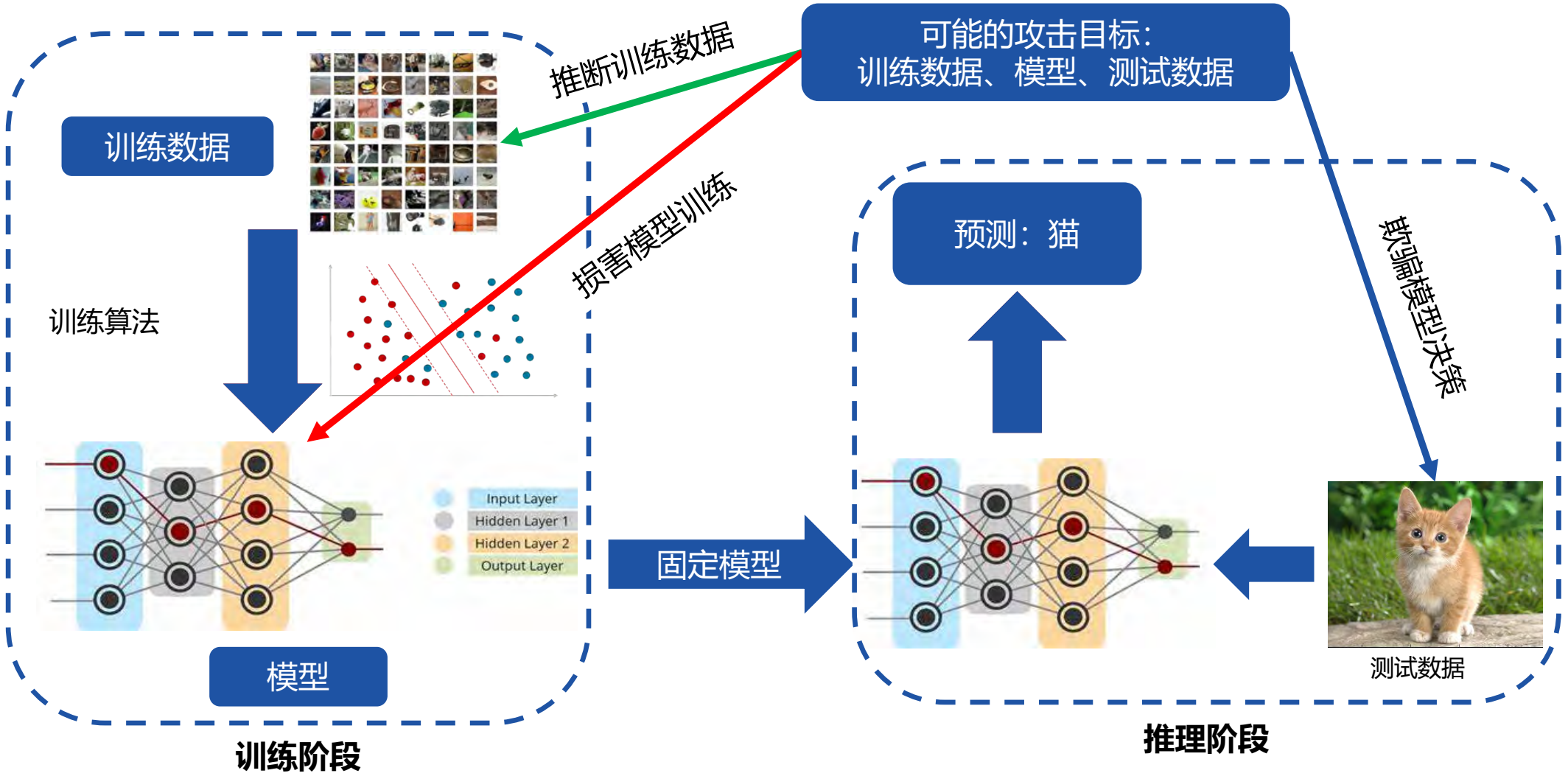
Step 3
Parties compute encrypted gradients, add masks and send to each other

Step 4
Parties decrypt gradients and exchange, unmask and update model locally



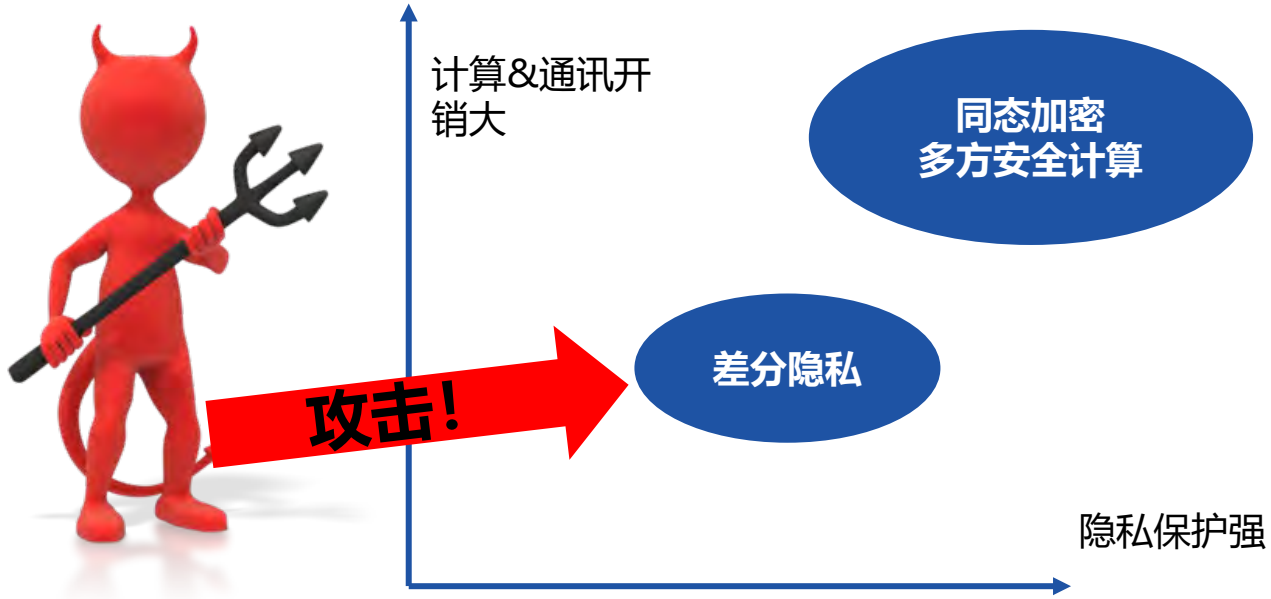
联邦学习：对抗攻击的应对

机器学习流程中的可攻击点



隐私攻击：防御攻击

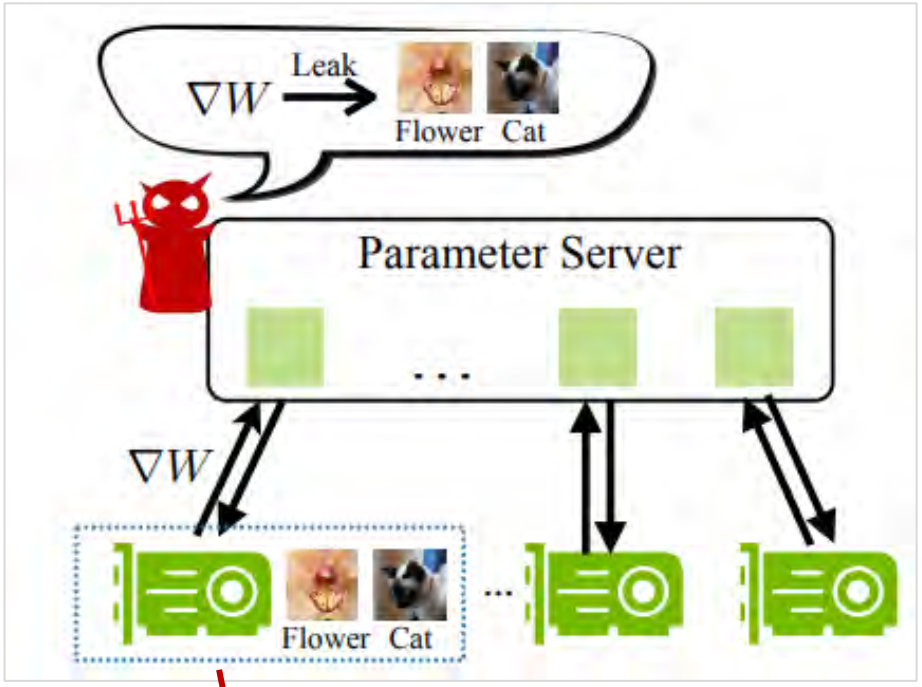
- 多方合作机器学习中的隐私防御工具：
  - 同态加密（HE）[1]、多方安全计算（MPC）[2]
    - 强隐私保护，不牺牲模型性能，但计算及通讯开销大
  - 差分隐私（DP）[3]
    - 计算/通讯开销小，效率高
    - 隐私保护与模型性能无法兼顾



[1] Le Trieu Pong, Yoshinori Aono, Takuya Hayashi, Lihua Wang, Shino Moriai. **Privacy-Preserving Deep Learning via Additively Homomorphic Encryption**. In IEEE Trans. On Information Forensics and Security, 2018.
[2] Payman Mohassel, Yupeng Zhang. **SecureML: A System for Scalable Privacy-Preserving Machine Learning**. In IEEE S&P, 2017.
[3] Martin Abadi, Andy Chu, Ian Goodfellow et al. **Deep Learning with Differential Privacy**, In ACM CCS 2016.

隐私攻击例子：深度泄漏攻击

MIT韩松教授团队设计了深度泄漏攻击，针对**差分隐私**的防御，对训练数据进行像素级别的提取



	Original	G-10^{-4}	G-10^{-3}	G-10^{-2}	G-10^{-1}
Accuracy	76.3%	75.6%	73.3%	45.3%	≤1%
Defendability	–	✗	✗	✓	✓
		L-10^{-4}	L-10^{-3}	L-10^{-2}	L-10^{-1}
Accuracy	–	75.6%	73.4%	46.2%	≤1%
Defendability	–	✗	✗	✓	✓

逐步提取训练数据

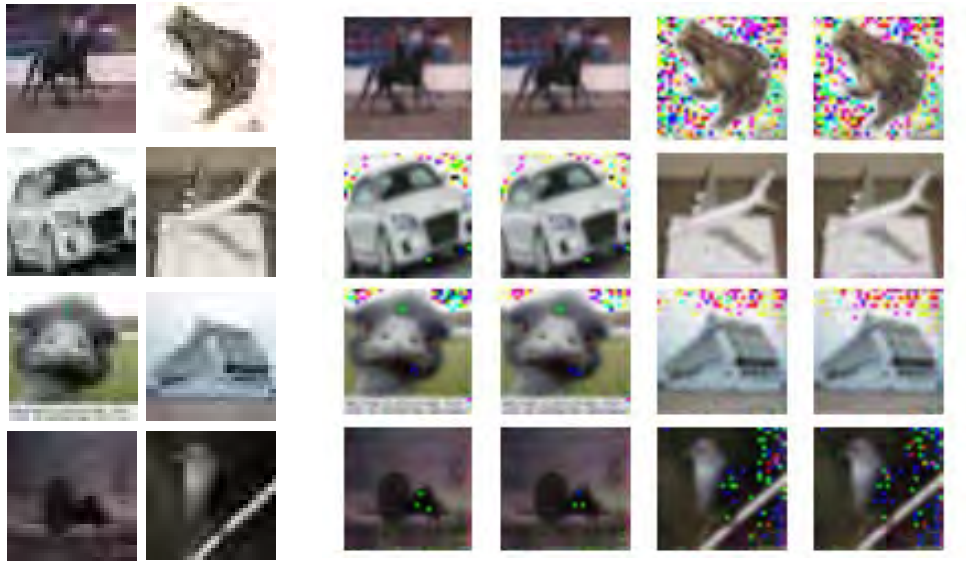
真实数据

Ligeng Zhu, Zhijian Liu, Song Han. **Deep Leakage from Gradients.** In NeurIPS, 2019.

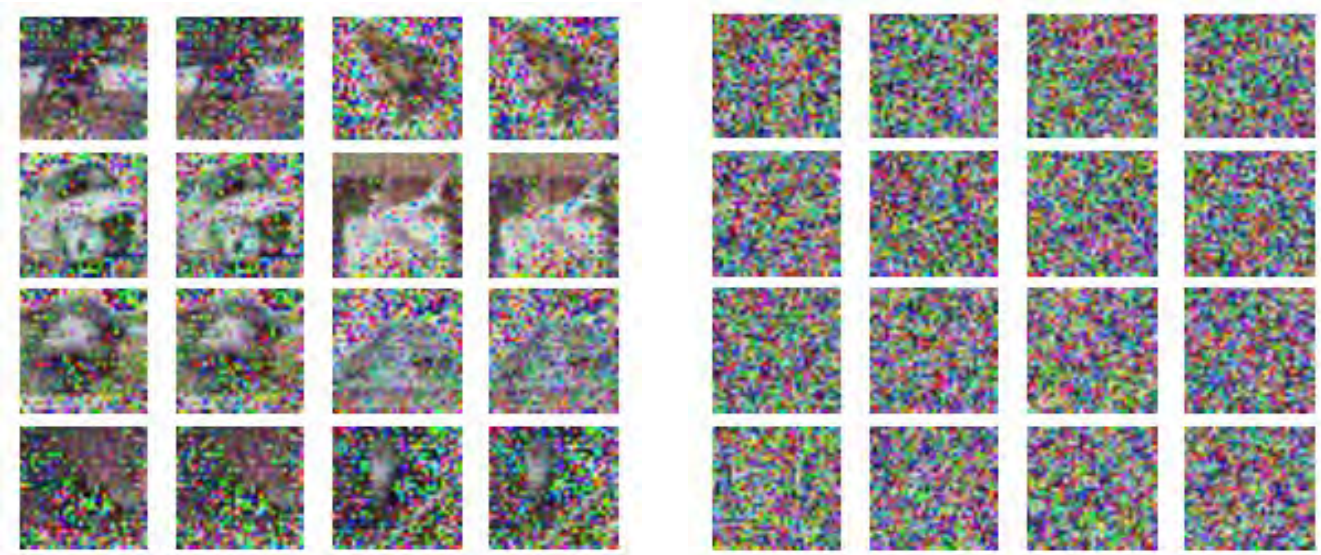
深度泄漏攻击：防御

- 微众银行团队从理论上证明了可以在不影响模型效果同时，完全防御深度泄漏攻击

隐私完全泄漏



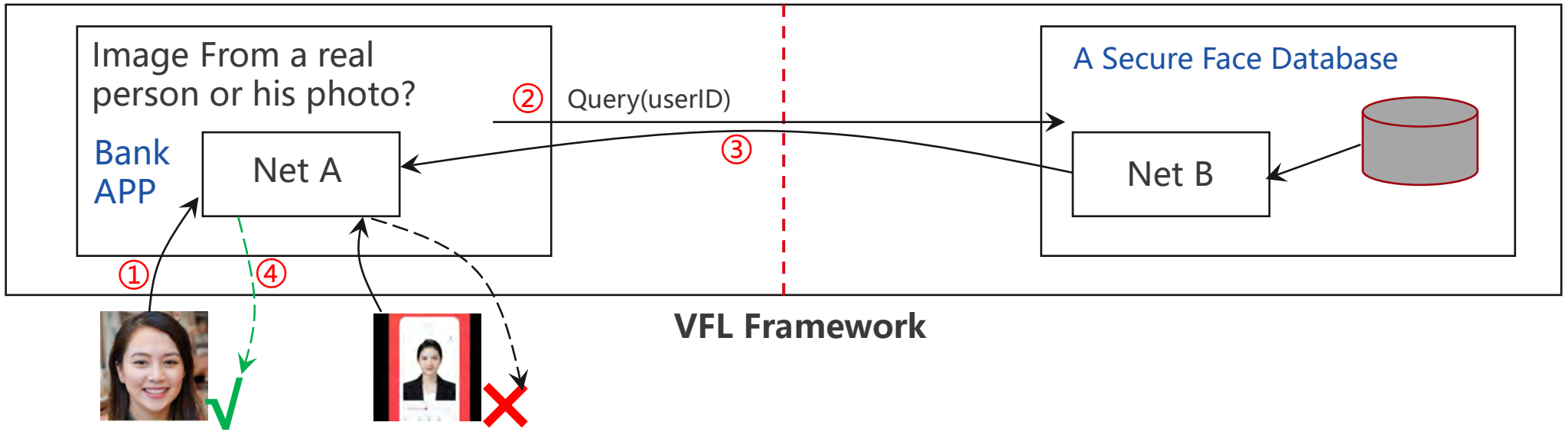
完全保证隐私



L. Fan, K. W. Ng, C. Ju et al. Rethinking Privacy Preserving Deep Learning: How to Evaluate and Thwart Privacy Attacks.
https://arxiv.org/abs/2006.11601

联邦学习+AutoML

Vertical Federated Learning



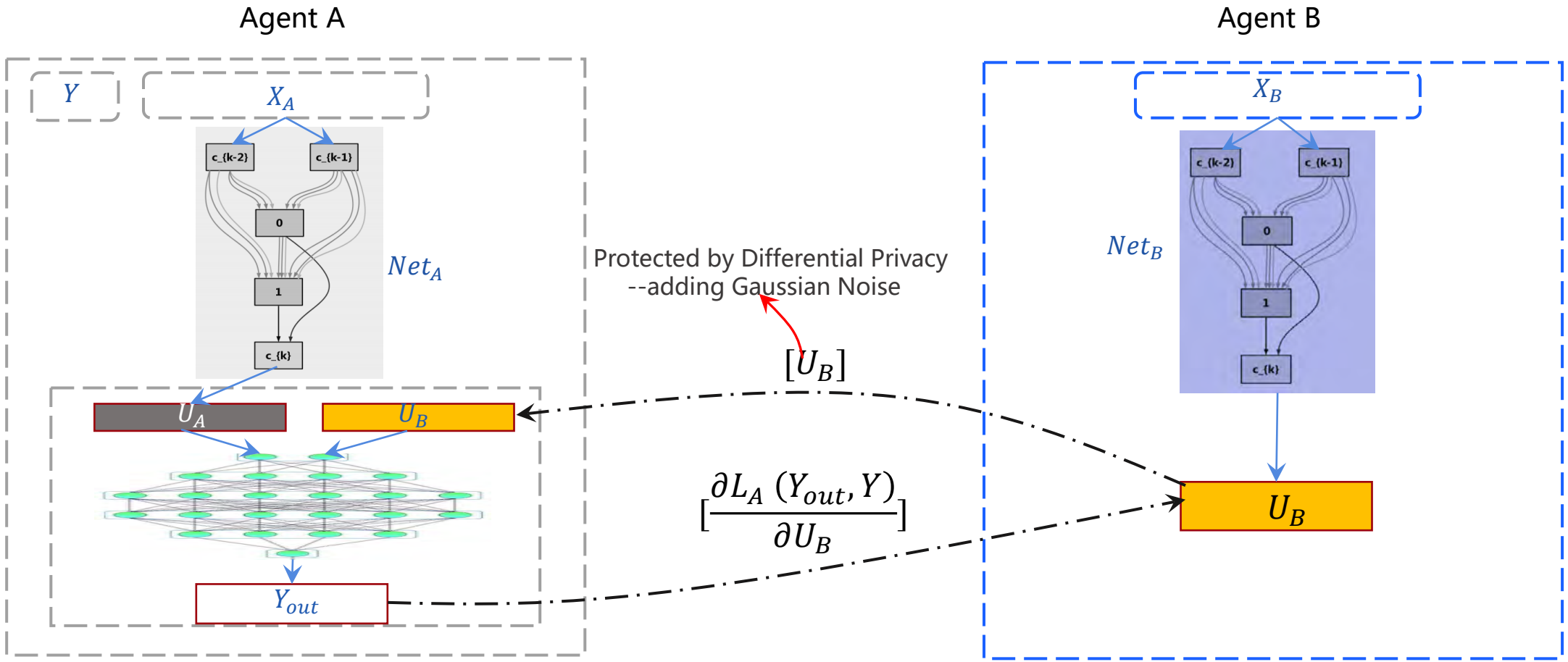
Banking Authentication:

1. Upload front camera photo: to judge whether an image is taken from a real person or his photo.
2. Bank A can cooperative with a **a Secure Face Database** with VFL;

What can AutoFL (Vertical) do:

To determine the learning architecture **automatically** and **locally** in a **communication-efficient manner** with **data protection**;

AutoFL with DARTS



1、Agent A update architecture and weights based on;

U_B

2、Agent B update architecture and weights based on gradients of;

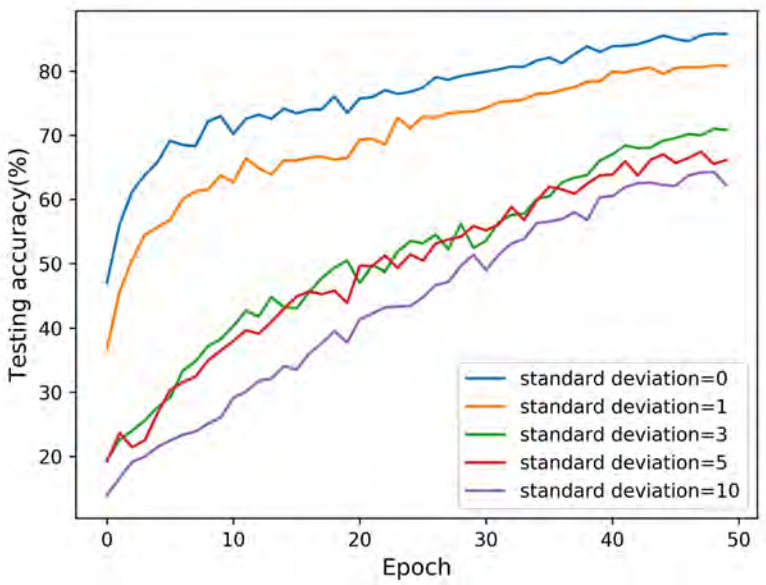
U_B

Experiment Results: Accuracy vs DP Noise

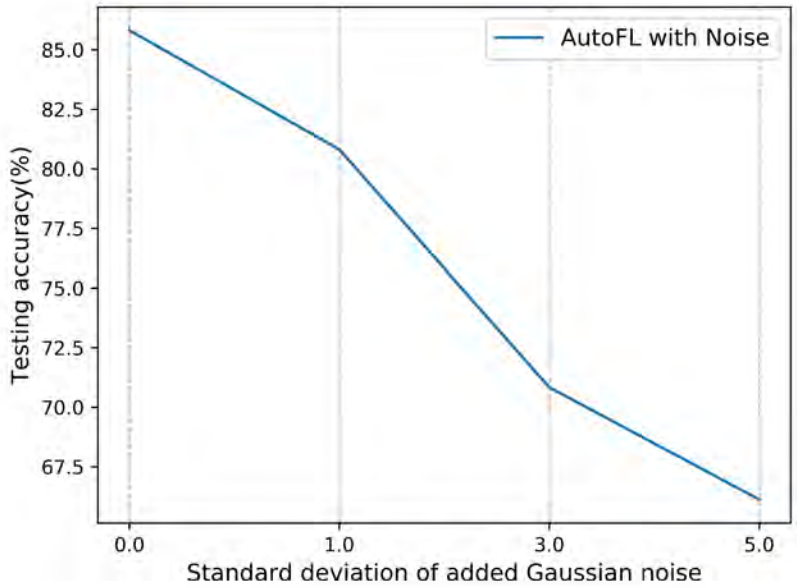
Dataset: ModelNet40

VFL settings:

- two VFL participants
- each holding a single view of one 3D object



Change of **Test Accuracy** on AutoFL with different DP noise level



Final **Test Accuracy** Comparison on AutoFL with different DP noise level

Conclusions:

1. AutoFL can achieve reasonable performance within acceptable time;
2. Trade-off exists between AutoFL performance and privacy;

04

联邦学习生态进展

生态，平台，标准，技术，课本

保护数据隐私安全的联邦学习技术开源平台

微众开源平台(FATE) https://FedAI.org

I. 工业级别联邦学习系统 。
II. 有效帮助多个机构在符合数据安全和政府法规前提下，进行数据使用和联合建模
III. 支持联邦学习产业生态联盟建设

设计原则

I. 支持多种主流算法：为机器学习、深度学习、迁移学习提供高性能联邦学习机制。
II. 支持多种多方安全计算协议：同态加密、秘密共享、哈希散列等。
III. 友好的跨域交互信息管理方案，解决了联邦学习信息安全审计难的问题。

FATE LINUX FOUNDATION

国内专利 135， 国内其他：200+

国际PCT18， 国际其他： 70+

130+ 家企业机构，150+ 所高校

3 个FATE社群1080人，1695 GitHub Star

联邦学习生态联盟, 24 家国内外单位加盟

Tencent UnionPay 银联 vmware 京东数科

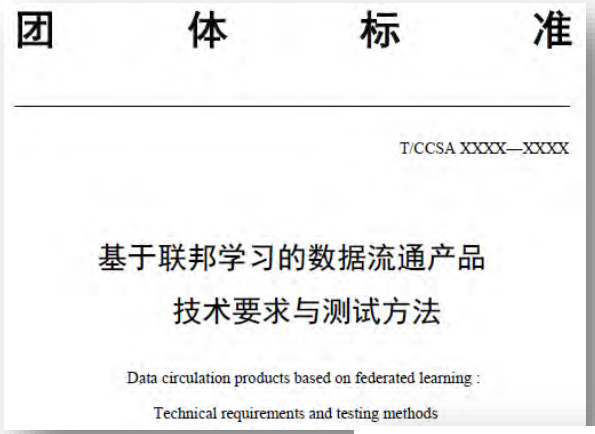
FedAI Ecosystem https://github.com/FederatedAI/

联邦学习技术标准建设

已发布标准

《基于联邦学习的数据流通产品 技术要求与测试方法》

- **7/9** 日于正式发布，**17**家参与单位
- 提供调度管理、数据处理能力、算法实现等方面的测试方法


团 体 标 准

T/CCSA XXXX—XXXX

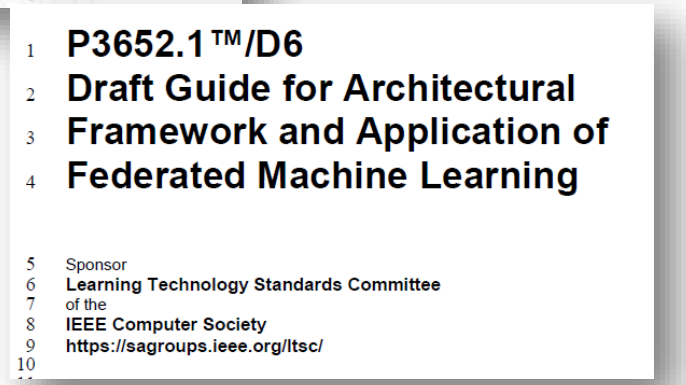
基于联邦学习的数据流通产品
技术要求与测试方法

Data circulation products based on federated learning :
Technical requirements and testing methods

制定中标准

《Guide for Architectural Framework and Application of Federated Machine Learning》

- 预计**2020年底**发布，全球**首个**联邦学习标准 **20家** 参与单位
- 召开工作组会议6次，提供 **10种** 联邦学习应用场景规范


P3652.1™/D6
Draft Guide for Architectural Framework and Application of Federated Machine Learning

Sponsor
Learning Technology Standards Committee
of the
IEEE Computer Society
https://sagroups.ieee.org/ltsc/

《Guide for an Architectural Framework for Explainable Artificial》

- 预计**2021年**发布
- 计划**7/24**召开第一次工作组会议 **14家** 参与单位
- 为人工智能模型落地应用提供，可解释性依据

标准参与主要单位

联邦学习产业生态发展联盟
(Alliance of Federated Learning Industrial Ecosystem Development)

- 推动以**人工智能**及**联邦学习**算法为核心的技术创新, 打造以提升数据价值及加强**信息隐私安全保护**为目的的产业生态系统
- **24 家会员单位来自: 金融行业、电商、能源、制造等行业及**国际国内标准化制定单位

标准研制与认证

研究制定数据信息相关标准，完善相关标准的制定与认证工作，推动相关系统和产品的认证工作。加强标准在企业的试点示范，促进推广应用，推动相关研究成果向国际、国家、行业或地方标准转化，通过加强国际合作与交流，推进数据信息安全国际标准化工作。

人才培养

促进联盟会员之间的校企合作、院所合作，建立满足会员单位所在国家法律法规要求的数据资源管理与治理、人工智能技能培训机构，助力提升相关人才能力培养。

政策建议

围绕提升数据价值与加强信息隐私安全保护的主题，组织开展市场调研、技术跟踪、政策研究和科研攻关，向有关部门反映企业需求，提供决策信息，研究提出促进数据信息产业发展的政策咨询建议。

评估咨询

开展跨行业、跨区域的数据安全、联邦学习、人工智能系统有关的评估和咨询工作。

交流合作

组织召开数据价值安全发展会议、培训、展览等交流活动，促进产、学、研、用各方深入协同合作，并积极开展国际交流合作。

WeBank

Dataset

The FedVision Project

This project is supported by WeBank AI group and ExtremeVision to boost the academic research and industrial applications of computer vision based on federated learning.

VIEW MORE

- Web: https://dataset.fedai.org/
- Github: https://github.com/FederatedAI/FATE
- Arxiv: Real-World Image Datasets for Federated Learning

WeBank

谢谢 THANKS

杨强

微众银行CAIO，香港科技大学讲席教授

2020年10月