DATAFUNCON

2020大数据 AI的最新技术实践

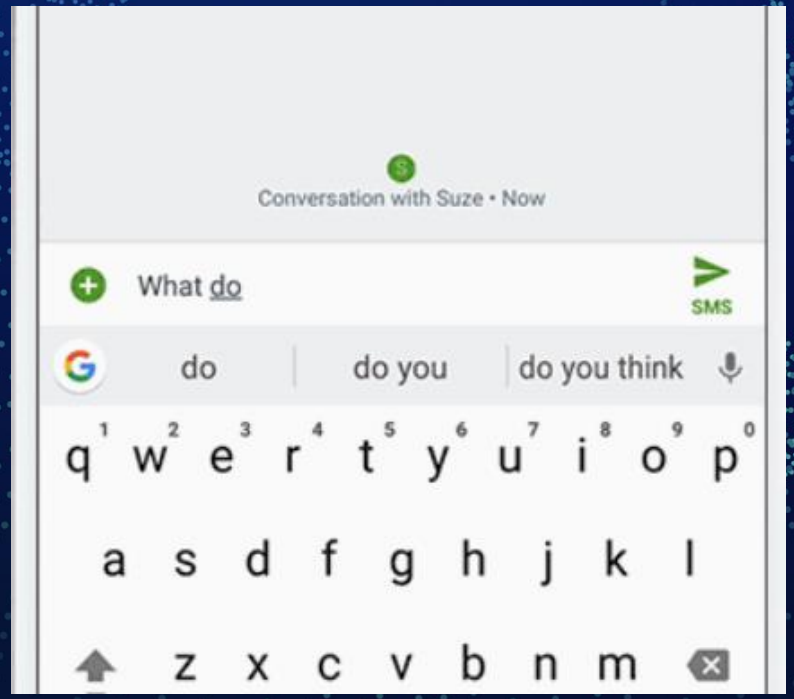
阿里安全 ALIBABA SECURITY

联邦学习与安全多方计算

洪澄 阿里安全 双子座实验室

- 联邦学习的发展变化
- 联邦学习面临的安全挑战
- 安全多方计算解决方案简介

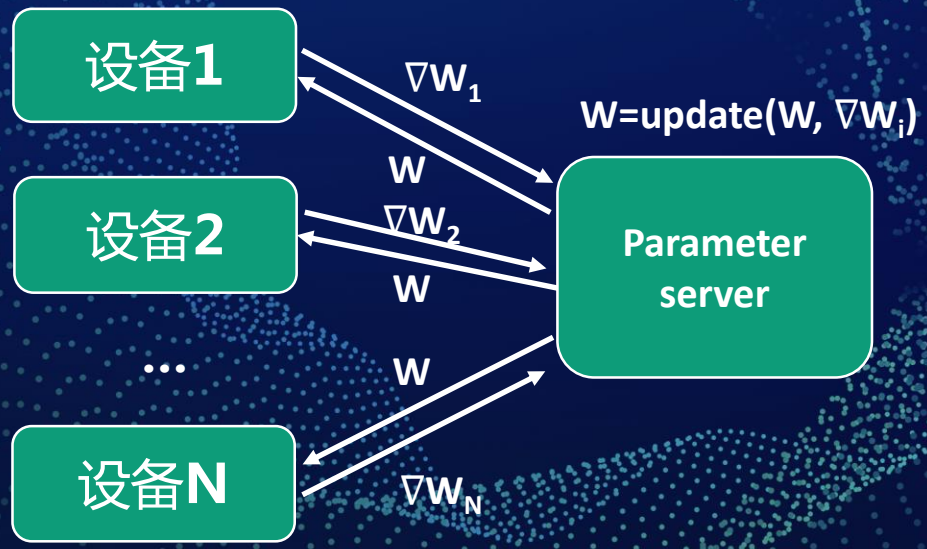
- 联邦学习（Federated learning，FL）由Google于2016年提出
  - 初衷是用于解决多个移动设备的分布式建模问题



例：Google Gboard安卓输入法预测

- 为了智能预测下一个词，需要针对大量用户的输入历史数据进行训练
- 设计目标：避免直接收集用户的输入历史，尽量在端上训练

- 联邦学习用于多移动终端分布式建模
  - 设计优点：设备只上传传输梯度∇W ，并不直接上传本地输入历史

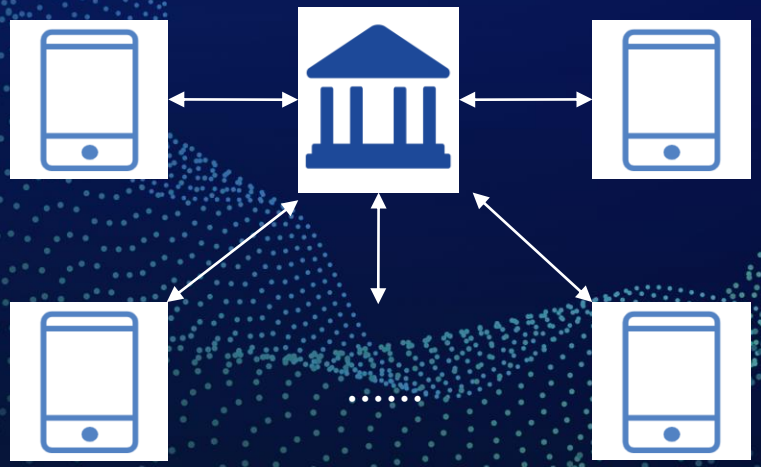


Step 1. 设备基于本地数据训练得到梯度∇W
Step 2. 设备将∇W发给Parameter server
Step 3. Parameter server更新全局模型W
Step 4. Parameter server把W发回给各个Client

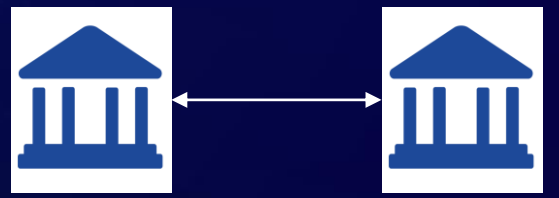
重复迭代N轮

- 2018年国内开始引入Federated learning概念，主要区别1：

Google FL：主要面向
海量（百万+）移动设备的合作



国内主要是cross silo FL：
少量（如2个）机构之间的合作



- 2018年国内开始引入Federated learning概念，主要区别2：

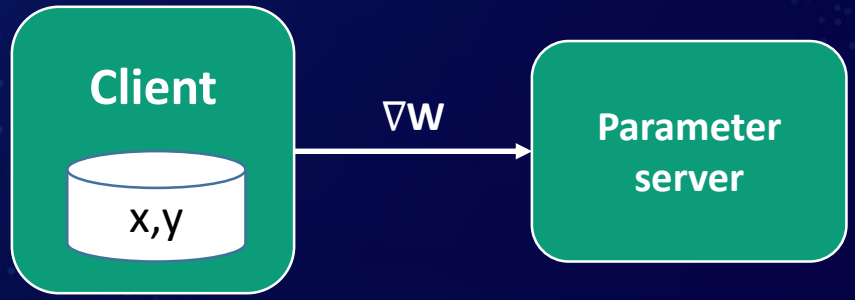
Google FL：主要面向数据的横向分割

国内FL：主要面向数据的纵向分割

- 联邦学习的发展历史
- 联邦学习面临的安全挑战
  - 联邦学习的共性问题
  - 联邦学习应用面临的新安全挑战
- 安全多方计算简介

- 梯度与原始数据的关系
  - 梯度∇w的定义：本质上是一个函数

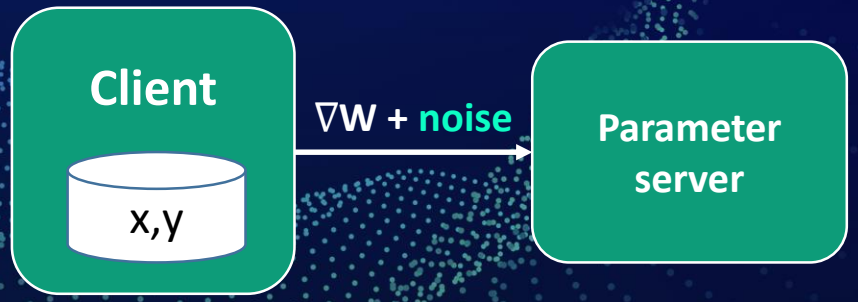
$$\nabla W_{t,i} = \frac{\partial \ell(F(\mathbf{x}_{t,i}, W_t), \mathbf{y}_{t,i})}{\partial W_t}$$

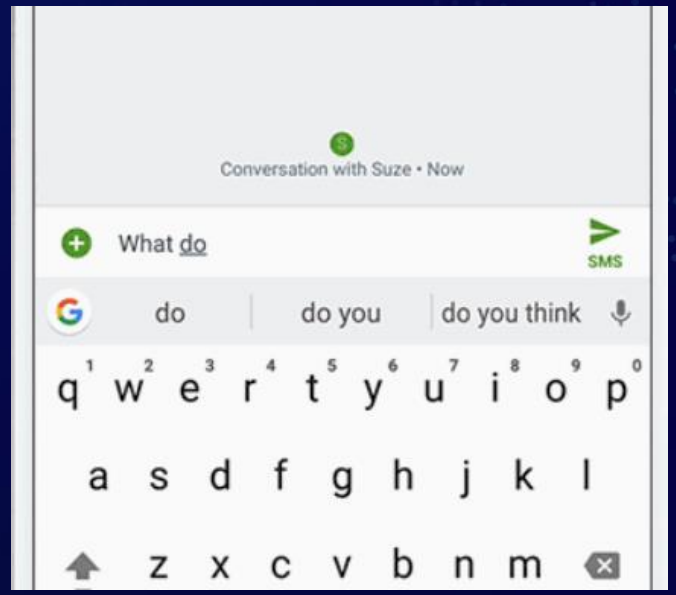


- 已知梯度，如何求原始数据？
  - 攻击方法1：对于简单的F（如Logistic regression），可以直接解方程组 (LHCH19)
  - 攻击方法2：对于复杂的F（如CNN），可以用ML方法求近似解 (MSCS19, ZLH19)

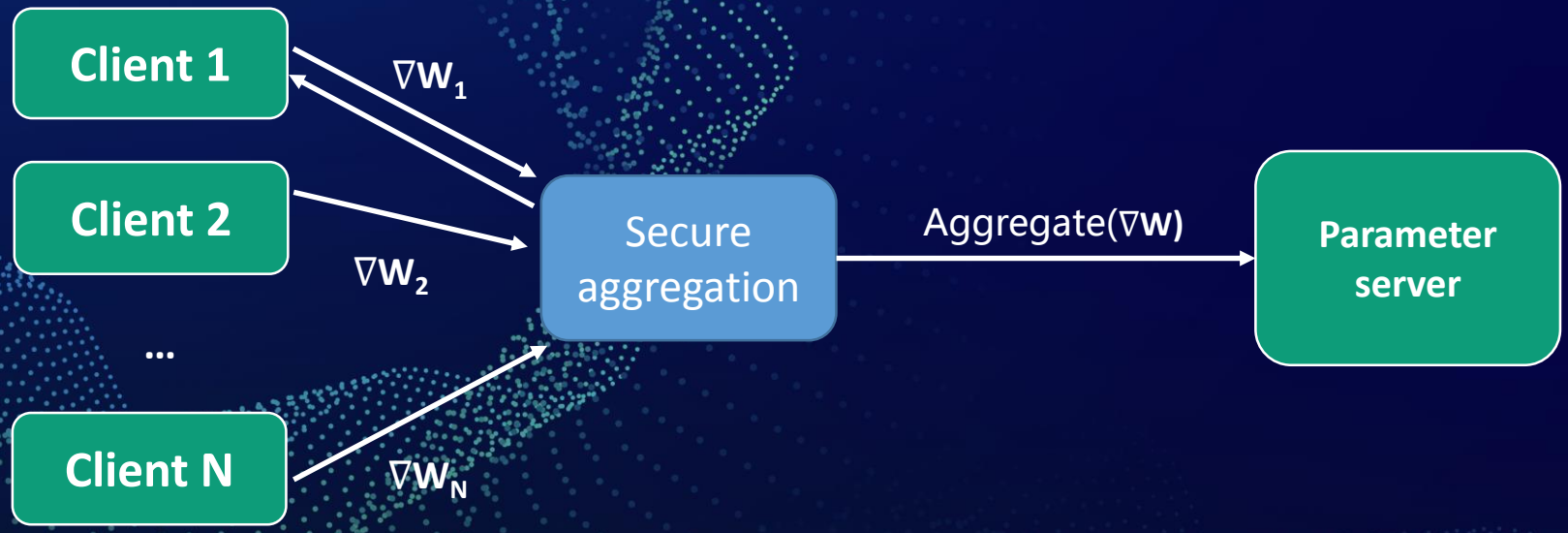
- MSCS19: Luca Melis, Congzheng Song, Emiliano De Cristofaro, and Vitaly Shmatikov. Exploiting unintended feature leakage in collaborative learning, S&P 2019
- ZLH19: Ligeng Zhu, Zhijian Liu, and Song Han. Deep leakage from gradients, NIPS 2019
- LHCH19: Zhaorui Li, Zhicong Huang, Chaochao Chen and Cheng Hong. Quantification of the Leakage in Federated Learning, FL-NeurIPS 2019

- 如何防止从梯度反推原始数据
  - 方法1：加差分隐私，但是准确率会下降
    - 对于输入法这类产品来说或许可以接受
    - 但不适用于准确率是关键因素的产品



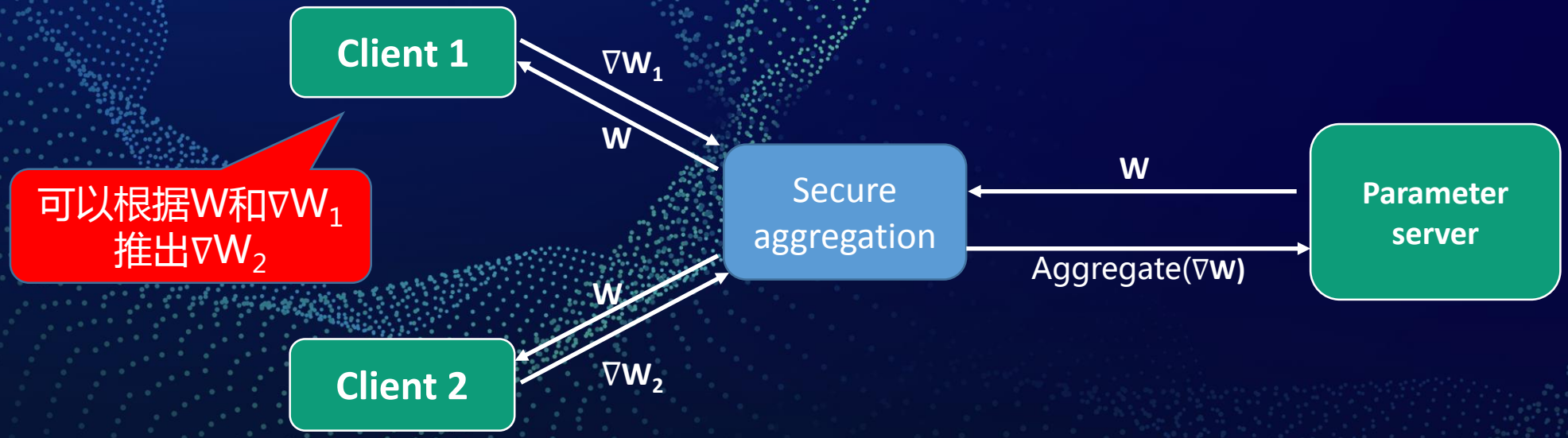


- 如何防止从梯度反推原始数据
  - 方法2：Secure Aggregation
    - Server只能看到聚合之后的梯度，无法了解具体某个client的梯度



但是 Secure aggregation 只适用于Client数目较多的场景

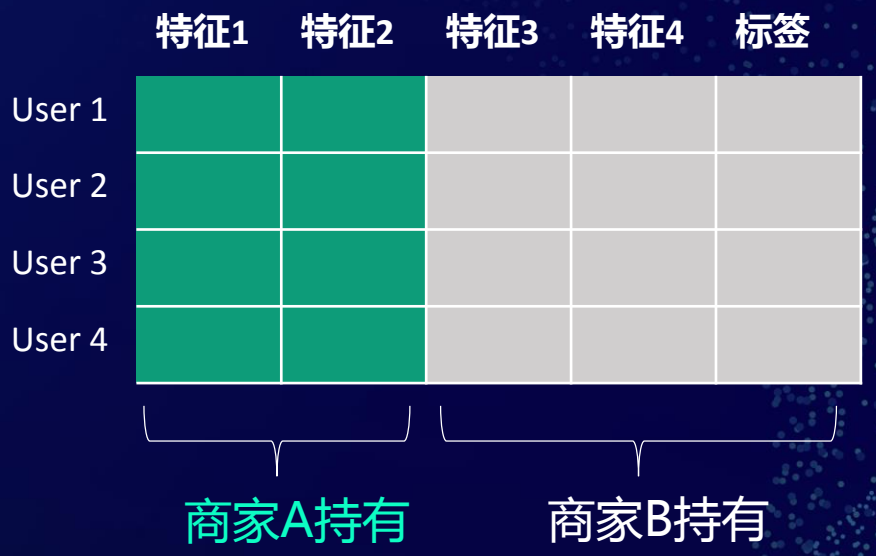
- Secure aggregation的局限性
  - 如果参与方过少（例如2个），Secure aggregation并不能保护梯度
  - Client 1拿到新一轮的W，减去自己的梯度就可以推出Client 2的梯度了



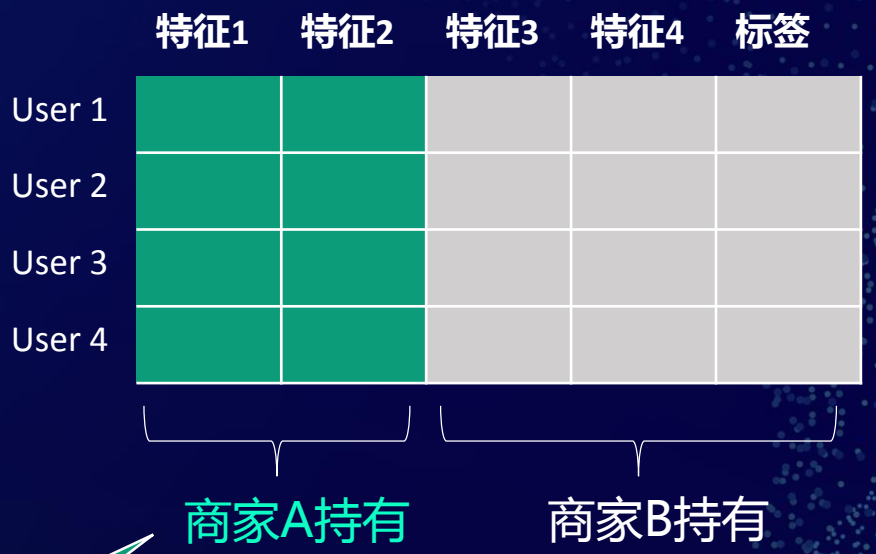
- 联邦学习的发展历史
- 联邦学习面临的安全挑战
  - 联邦学习的共性问题
  - 联邦学习应用面临的新安全挑战
- 安全多方计算解决方案简介

- 参与方过少（例如两方合作）带来的问题 – 续
  - 半同态加密保护参数：只能实现单向保护

- 纵向FL带来的问题-1
  - 为了实现纵向FL，需要首先按id对齐数据
  - 对齐过程是否符合隐私政策？
    - 即使用PSI（隐私求交）技术，也只能保护“不在交集内的用户身份”，但是在交集内的用户身份**必然泄露**
  - 例： 商家A知道了“用户1也在商家B那注册了”
    - 用户1未必同意这个信息被A知晓



- 纵向FL带来的问题-2
  - 纵向FL必然存在无标签方，而无标签方难以进行特征工程
  - 如何让无标签方进行特征工程又能保护数据隐私 ？
    - 已经脱离联邦学习的范畴
    - **需要定制化的安全解决方案**



没有标签，怎么做特征工程？

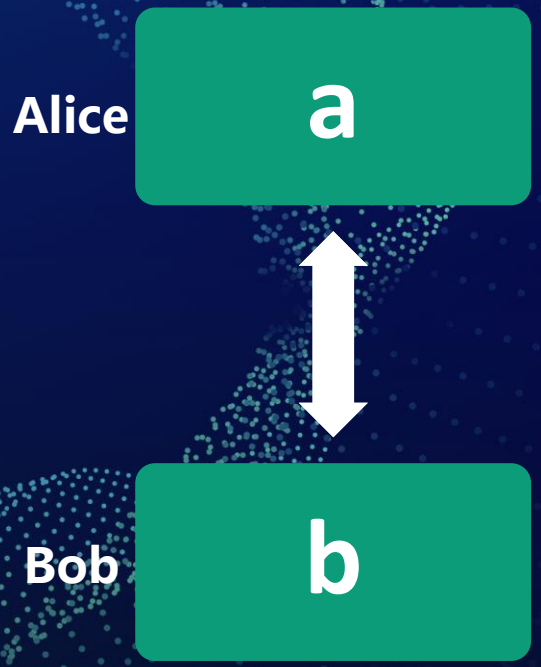
- 举例：计算WOE（Weight of Evidence）
  - WOE定义：某个特征箱体内的 ln(反例总占比/正例总占比)
  - 若拥有“年龄”一方不拥有标签（样本是正还是负），则难以正常计算WOE

	正样本数	负样本数	反例总占比	正例总占比	WOE
0-18岁	100	50	10%	10%	0
18-40岁	500	100	50%	20%	0.92
40-60岁	300	150	30%	30%	0
>60岁	100	200	10%	40%	-1.39
总数	1000	500			

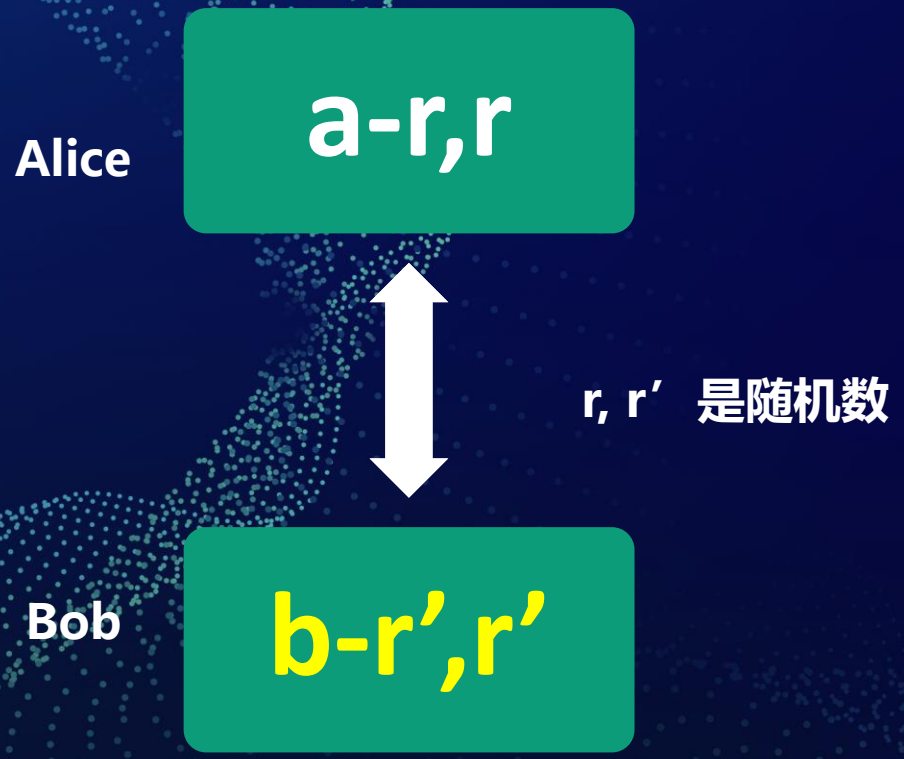
- 联邦学习的发展历史
- 联邦学习面临的安全挑战
- 安全多方计算解决方案简介

- 安全多方计算(Secure Multiparty Computation，MPC)
  - 可证明安全
    - 严格的安全定义：除最终的训练结果之外，不泄露任何数据内容
    - Semi-Honest model
    - Malicious model

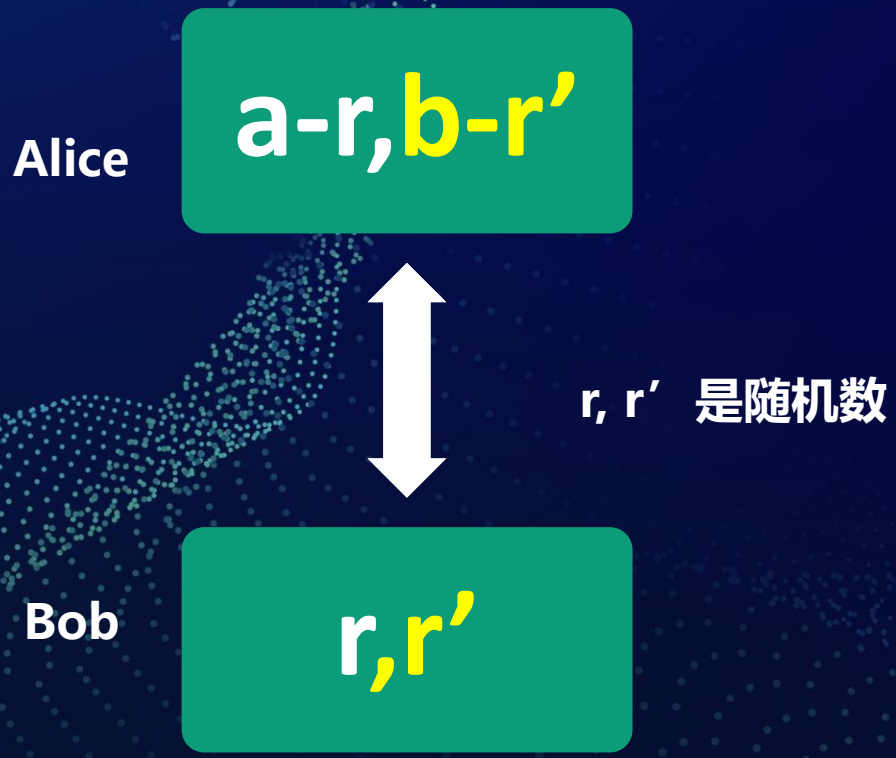
- 例：Alice和Bob分别拥有数据a,b，希望联合计算机器学习模型F(a,b)



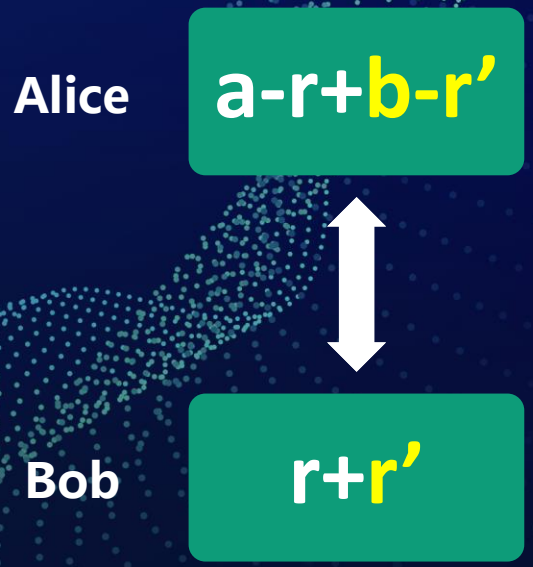
- Step 1：随机拆分



- Step 2：交换分量
  - 得到秘密分享状态的a和b
  - 单方视角下都是乱码，只有双方同意的情况下才能复原



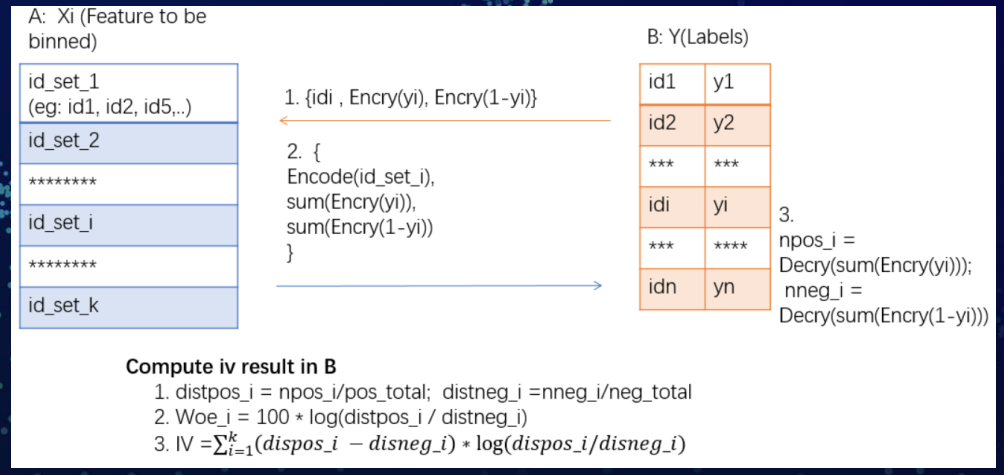
- Step 2：秘密分享状态下进行计算
  - 加法：A和B各自本地将“密文”相加即可得到a+b的“加密”版本
  - 其他操作：乘法、比较、除法 ...
  - {+, - , * , ...} 构成整个机器学习算法



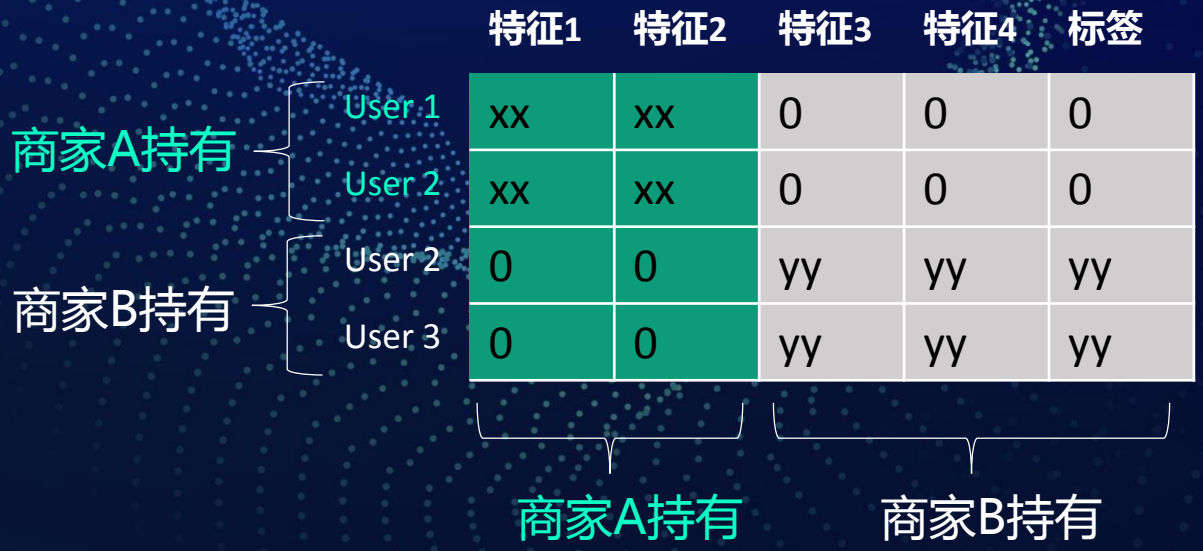
- 安全多方计算可以无泄露的计算WOE
  - 秘密共享状态下向量内积计算正负样本数
  - 秘密共享状态下计算除法得到WOE
    - 除WOE之外没有任何信息泄露

	正样本数	负样本数	反例总占比	正例总占比	WOE
0-18岁	100	50	10%	10%	0
18-40岁	500	100	50%	20%	0.92
40-60岁	300	150	30%	30%	0
>60岁	100	200	10%	40%	-1.39
总数	1000	500			

- 对比：使用半同态计算WOE的方案会泄露每个分箱的样本数目



- 安全多方计算不需要“对齐数据”就可以建模
  - 秘密共享状态下进行匹配，各机构不泄露自己的客户信息
  - 交集也是秘密共享状态，不泄露交集内的用户身份
- GDPR第5条(b)
  - 对个人数据的处理不应当违反最初收集该数据时的初始目的（对齐数据过程是存在风险的）
  - 若为统计用途，则可以超出该初始目的（可以建模）



MPC匹配，
谁都不知道匹配上的
是User 2

https://engineering.fb.com/open-source/private-matching/

- **在LR等模型方面，安全多方计算的性能完全可以满足业务需求**
  - 20000样本，100特征，LR建模耗时：秒级~分钟级

Team	Affiliation	Training time cost(s)		Accuracy(%)	
		BC-TCGA	GSE2034	BC-TCGA	GSE2034
Gene X	University of Washington	130.985	1161.29	100	测试结果有误
V for Victory	Alibaba security	37.61 (11.631+25.979)	21.82 (5.814+16.006)	100	76.087 70.492
Morse	Ant Financial Services Group	6.183	8.897	100	66.102
		13.231	16.129	100	61.017
		69.112	81.713	100	64.407

注：组委会复议时发现 University of Washington 的准确率有误，实际不到68%

- 国内流行的FL方案与Google的经典FL方案存在很大不同
  - 技术角度：国内FL多为纵向，Google FL为横向；
    国内FL多面向少量机构的合作，Google FL面向海量终端的合作
  - 风险角度：国内FL面临的安全挑战更多
- 在设计FL解决方案时，安全性上必须慎之又慎
  - 必须详细说明对各参与方提供了何种安全保障，存在何种信息泄露，能抵抗何种攻击
- 安全多方计算（MPC）解决方案有其独到的安全优势
  - 有广阔的应用前景

DATAFUNCON

2020大数据 AI的最新技术实践

阿里安全
ALIBABA SECURITY

THANKS

可用不可见
BLINDFOLDED COMPUTING