3 月 11 日，由微众银行、百度联合举办的“视觉联邦框架直播公开课”圆满结束。本次直播课程吸引了超 3000 人次参与，众多 AI 从业者、联邦学习爱好者与专家展开了深入的探讨和交流。（点击“阅读原文”回顾本期圆桌会）

接下来，我们先回顾一下 FedVision 的基本信息，帮助计算机视觉应用开发者更好地掌握联邦学习。

**FedVision 介绍**

FedVision 是首个轻量级、模型可复用、架构可扩展的视觉横向联邦开源框架，内置 PaddleFL/PaddleDetection 插件，支持多种常用的视觉检测模型，助力视觉联邦场景快速落地。FedVision 是基于 Python 实现的，作为一个视觉横向联邦方向机器学习项目，已经在 GitHub（https://github.com/FederatedAI/FedVision） 上开源首个版本 FedVision v0.1。

FedVision 项目的主要目标是：

- 在学术场景下，助力实验人员快速验证相关的实验想法。
- 在实际生产环境中，助力视觉横向联邦项目进行快速落地。

为了快速实现最小可用版本，FedVision v0.1 版本借助 PaddleFL 项目的部分能力，实现视觉领域的横向联邦建模功能。由于借助了 Paddle 的丰富生态，经简单的调制适配，FedVision v0.1 即可直接使用 PaddleDetection 项目实现的几乎全部的视觉检测模型。

**圆桌会问答环节**

**想问一下 FedVision 大概什么时候能支持跨网多方部署?**

跨网多方部署应该不会支持。其实这个工具是给单方使用的，需要部署的组件都可以调整，也可以模拟多方参与的情况。如果是跨网的情况我默认为实际的多个用户？这种情况各方各自配置下部署配置文件执行部署命令即可。

**DH 可以用于多方么?**

基本协议是两方的，作为比较的话，多方的话需要考虑按什么顺序走一遍参与方。

- 本身的通讯跟两两进行没有差异。
- 协议流程更复杂。

**老师，请问多方横向联邦的话，一般会应用什么加密协议保障数据安全呢？（就是非仅支持 2 方的协议，求问支持多方并行的协议）**

简单理解一下，两方的话知道自己的和聚合的，不就知道另一方的了嘛。今天讲的协议需要多方参与的，如果两方的话，就不能是准确的，也许可以考虑 DP 查分隐私协议。

**您说的 DH 主要是两方协议，密码学我了解得不多，主要想请教您的其实是多方的场景。比如有 3~5 个组织想一起做横向建模，这种情况下用什么协议更能并行且安全呢?**

用今天讲的协议就行。今天讲的两方 DH 主要是用于开始时两两之间共享一份秘钥，之后一般作为随机数种子生成伪随机数来做随机混淆，简单来说秘钥交换这个其中一个步骤是两方的，但是训练流程是多方的。

**多方联邦中有一方机器挂死是整个任务结束吗?**

这个问题很好。一方机器挂死或者故障或者某种原因导致训练时间超出预期，都可能导致训练任务堵塞。横向联邦的一个策略是，允许只选取一部分模型参与聚会，抛弃剩余的部分。刚讲的协议后半部分我没展开，因为会比较复杂，短时间可能讲不清楚，后面 ppt 发给大家后可以看下参考文献。协议本身所用到的技巧很有意思，建议尝试去理解看看。

**老师您好，在网上看资料，大多通过同态加密算法，比如 Paillier 对梯度进行加密上传到服务器进行聚合，看到您讲到 DH 协议，这两者做的是一个事情吗?**

不完全一致。从结果上都可以达到目的，也有半同态加密实现横向联邦的方法。但是从技术实现上各有优劣，效率上 DH 会更高，但是用半同态可以实现一些比较奇怪的需求，比如让某一方连聚合的模型都拿不到。

**想问一下老师，FebVision 实际上是用横向联邦去解决视觉类的学习任务，而不是以可视化的方式去呈现横向联邦学习过程的吧?**

对，FebVision 不是可视化项目。不过你说的这一点其实很有意义，用可视化展示联邦学习过程无论从学习还是交互鉴权角度都蛮有意思的。

**老师您好，有抵抗客户端实施后门攻击的措施吗?**

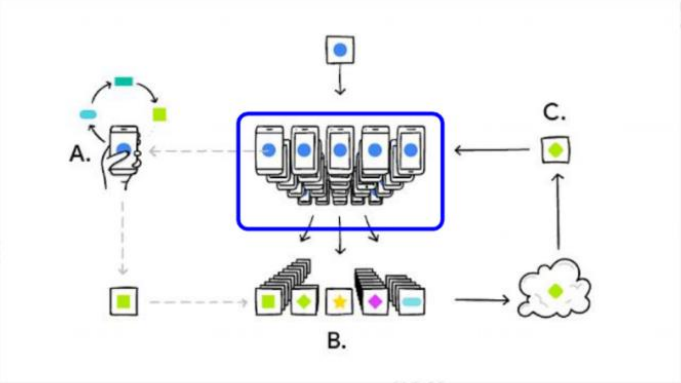
其实是有一些这方面的学术研究的。比如说，如果有客户端用“毒模型”去参与聚合，把模型拉偏怎么办？这就涉及到识别“有毒模型”，同时又要保护原始模型，可能需要做一定的权衡，具体的协议需要进一步去设计，可能并不简单。

今天所讲的协议直接使用应该是做不到的，当然实际情况还有技术之外的手段，比如商业合约等。

以下为本次圆桌会的部分内容介绍，添加小助手（FATEZS001）可获取详细资料:

## Google's Secure Aggregation

WeBank




(A) users' updates are aggregated (B) to form a consensus change (C) to the shared model, after which the procedure is repeated.Your phone personalizes the model locally, based on your usage (A). Many users' updates are aggregated (B) to form a consensus change (C) to the shared model, after which the procedure is repeated.(McMahan & Ramage, 2017)

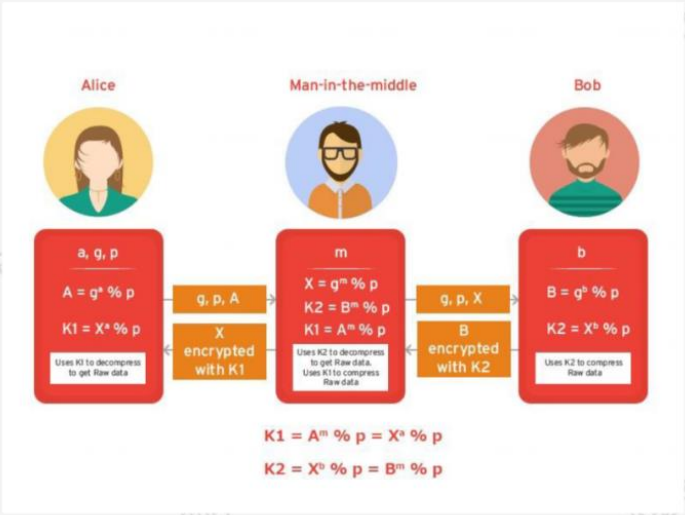
## Google's Secure Aggregation

WeBank

$$\underbrace{\begin{pmatrix} x_{1,1} \\ x_{1,2} \\ \vdots \\ x_{1,p} \end{pmatrix}}_{\text{model } 1} + \underbrace{\begin{pmatrix} x_{2,1} \\ x_{2,2} \\ \vdots \\ x_{2,p} \end{pmatrix}}_{\text{model } 2} + \cdots + \underbrace{\begin{pmatrix} x_{n,1} \\ x_{n,2} \\ \vdots \\ x_{n,p} \end{pmatrix}}_{\text{model } n} = \underbrace{\begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix}}_{\text{sum model}}$$

## Google's Secure Aggregation

WeBank




Diffie-Hellman Key Exchange. (Micro, 2015)

## 跟数据并行的分布式训练的关系与差异

WeBank

| 共同点 | 差异 |
| --- | --- |
| 主要流程都是模型（梯度）平均<br>都可能存在节点训练进度差异 都可以改进（？）为“ring reduce”都可以用剃度压缩技术<br>... | 联邦学习数据非单方掌握<br>联邦学习数据 non-iid<br>联邦学习应用环境一般网络稳定性、带宽较差<br>联邦学习还可能存在恶意（好奇）节点的可能性需要防范中心节点 |

Table: 与数据并行的分布式训练的比较


获取会议 PPT，或对圆桌会还有别的疑问？欢迎联系 FATE 开源社区助手获得帮助。

原文链接： https://mp.weixin.qq.com/s/41TVzaG6oBLhNYbGy6qtzw