# 会议纪要

**会议主题：**FL和PLS结合架构及其安全编码方案

**会议时间：** 2024年4月1日（星期一）19：00至21：00

**会议地点：** 西安电子科技大学北校区会议中心303-1会议室

**线下人员：** 孙瑞锦 尹志胜 贺靖超 王葳 沈京龙 王秀程 杨浩 张茹倩 马龙飞 周新阳 权赟昊 张玉洁 黄蕾 杨杰 胡陆莹 齐阁 傅连浩 侯毓真 邓川 李青壮 陈梦豪 朱煜朋

**线上人员：** 温瑶 王兆薇 邱子仪 方忠盛 祝馨平 朱煜朋 韩松明 尚佳瑶 贾昊燏 赵璇 郑雯馨 张智杰 孙兴栋 郑佩林 刘苏 解思舀 万佳林

**记 录 人：张玉洁**

**会议内容：**刘永红介绍FL和PLS结合架构及其安全编码方案

**提问**

* **尹志胜**：梯度信息怎么到安全编码？

**刘永红**：梯度信息经过本地差分隐私机制（LDP Mechanism）后在边缘服务器处进行聚合，边缘服务器进行安全编码。

* **尹志胜**：从终端到边缘服务器的任务有什么具体的描述？

**刘永红**：没有，主要是关注传输的方面。

* **孙瑞锦**：LDP是什么？

**刘永红**：本地差分隐私。

* **孙瑞锦**：你自己的工作是什么？

**刘永红**：采用无编码的物理层安全方法，通过功率控制和波束矩阵实现物理层安全，还没有改出来

* **尹志胜：**FL的安全性怎么评估？隐私保护有没有量化指标？都完成任务怎么衡量谁强？

**刘永红：**联邦学习的隐私要求设置是为了达成性能允许信息泄露

**沈京龙：**没有指标

**王秀程：**肯定得有吧，那差分隐私怎么衡量

* **尹志胜：**满足两个不等式就满足差分隐私的标准 也就是说所有差分隐私强弱都是一样吗？

**刘永红：**也不是，差分隐私的强弱不是根据不等式来判定的，实际需要靠后续训练的结果来考量

* **尹志胜：**物理层安全传的是加扰之后的梯度信息，梯度信息泄露又如何？已经用差分隐私保护了

**刘永红：**仿真结果看出来泄露还是有影响的，没有进行信道加密的窃听者误码率在0.25左右，证明其还是能获取一定的信息量

* **尹志胜：**没有分析合法系统性能有多好

**刘永红：**仿真图中红线分析了，红线是采用了LDPC编码的误码率

* **王秀程：**PLS加 FL之前有人做过吗？

**刘永红：**无编码做的很少，只有一篇magazine给出了结果，但是具体实现的明细没有描述。

**总结**

**尹志胜**：FL模型训练过程中的威胁调研不全，需要将FL模型训练过程中有关于窃听威胁具体的攻击模式调研清楚。例如窃听者根据泄露的信息能做些什么？为什么就带来了安全风险。

**尹志胜**：安全编码的问题没深入理解，安全编码目的是为了让系统的保密速率亦或保密容量达到或接近理想情况下的性能。

**尹志胜：**在更复杂的通信系统下，包括PLS或者波束赋形的方法选择的余地更多，应该把最基本的工作和逻辑厘清，先把现有的工作跑通，借鉴已有的优势做一些创新。先进行工程性的工作，多跑一些实例，有积累之后才能更好地结合，再进行创新性的工作。