1. 期刊，会议，实验室
    a. 期刊：
        i. https://ieeexplore.ieee.org/xpl/RecentIssue.jsp?punumber=10206
            1. early access :
            2. all access:
        ii. https://ieeexplore.ieee.org/xpl/RecentIssue.jsp?punumber=8858
    b. 会议：
        i. https://iacr.org/
            1. 侧重理论(美密、亚密、欧密)的三个会议
            2. https://crypto.iacr.org/2019/acceptedpapers.html
            3. 会议日程安排也会有paper
            4. https://eprint.iacr.org/2018/
                a. https://eprint.iacr.org/2019/
                b. 这个数据库有这篇文章
        ii. PKC
        iii. acmCCS
            1. http://www.sigsac.org/ccs/CCS2018/
            2. 应用密码学领域
            3. accepted
                a. mpc
                b. 同态加密
                c. 安全外包矩阵计算
                d. PSI(隐私保护求交集)
                e. 深度学习，机器学习
        iv. 另外两个会议
            1. https://esorics2019.uni.lu/
                a. conference-> accepted paper
            2. https://infocom2019.ieee-infocom.org/main-technical-program
                a. 大会议：隐私保护

b. 关键字搜索

c. 著名实验室：

i. https://dblp.uni-trier.de/

1. 新加坡 Robert h dblp
2. kui ren
3. rongxing lu
4. yi mu

d. 推荐会议的网站

i. https://www.ccf.org.cn/xspj/wlyxxaq/

1. 数据方面的会议
2. 近三年的paper

e. 谷歌学术搜索

i. privacy preserving machine learning

ii. https://dblp.uni-trier.de/

1. kui ren
2. rongxing lu
3. yi mu

2. 安全外包计算和多方计算

a. 多项式的外包计算

b. 多元多项式的外包计算（公钥同态加密）密文长度、计算开销

c. 两个工作：加法聚合，加法与乘法的聚合，多元多项式

3. 多用户多数据，数据并非来自同一个用户，不同用户之间的数据要保密

a. 每个用户加密自己的数据时，采用不同的加密算法

b. 集中式问题变成分布式问题，单用户变成多用户，单方变成多方

c. 雾计算：实时处理数据，减少延迟

i. 输入拆开，函数拆开，结果综合返回给用户

d. 实例：电子医疗

i. 输入：患者

ii. 输出：病人，授权医生（多方返回）

e. 解密：私钥解密

        i. 私钥
    f. 从功能上改进
4. 从安全上改进
    a. 随机模型
    b. 标准模型
5. 机器学习算法外包给服务器
    a. 把训练的数据加密
    b. 是服务器在密文上进行计算
    c. 恶意行为的检测
    d. 投毒攻击：训练数据的投毒，样本投毒，后面训练的数据可能不对
    e. 人工智能的安全检测
6. 1
7. 文件的查新
    a. 524.pdf efficient
        i. 单用户多数据
        ii. 机器学习 连邦学习 分布式学习
    b. 599
    c. ML
    d. po
    e. icc
    f. lppa
        i. 摘要 引言
8. 前面提到的两个技术
    a. 单用户多输入：老师主页
        i. [3] Zhou J., Cao Z., Dong X., Lin X., EVOC: More efficient verifiable outsourced computation from any one-way trapdoor function. IEEE ICC 2015, IEEE: 7444-7449,2015.
    b. 多用户多输入
9.
10. 1

11. 1
12. 1
13. 1
14.