富数科技

两类产品，一类是授权类产品，比如“**斑马合约**”“**隐像合约**”“**存证合约**”等，可以在自身数据不出门的前提下，查询逾期黑产、团队骗贷、多头负债等。同时也可以应用于用户核验、用户画像、精准营销等场景。另外一类则是**联合建模**产品，采用富数安全多方计算平台进行联合建模，各自的样本数据保存在本地，不需要透露给对方，通过加密计算进行分布式的算法训练建模，保护了用户隐私数据和模型成果，更加合法合规。

- 19年获得近亿元 Pre-B 轮融资
- 官网https://www.fudata.cn
- 官网github地址是 ud数链 https://github.com/unitedata-org-public
- 富数科技安全计算首席专家 **卞阳** （上海交大）

  UD数链开源项目创始人。

  早年从事语音识别和人工智能的成果转化，之后开发智能硬件及安全相关产品，用于智能电网和物　联网。然后，发现了区块链与自己在研究生阶段的研究课题分布式的数字微支付网络密切相关，于 是开始逐渐关注并研究，发起了Unitedata开源项目，一个致力于保护私有数据并实现数据价值流通 的网络。

  数纽科技

  数纽科技落地运营的开源项目-->ud数链
- 挖财、富数科技等金融科技企业，联合上海交通大学密码学实验室、浙江大数据交易中心进行研究和建设的Unitedata Open Source Project(UD数链开源项目)
- ud数链帮助中心https://help.unitedata.link/ 有斑马项目指南 并无安全多方计算指南
- 搜到 **富数科技安全计算平台Avatar** 外宣 官网完全没有Avatar任何信息
- 搜到一篇**富数fmpc**（联邦学习）与 我行fate 实战对比

  https://zhuanlan.zhihu.com/p/128467630

  总结，通过上面的两家平台性能评测，我们可以对比看出
  总体效率
  FMPC较FATE提升3-5倍，其中在大样本集训练上增速明显。
  总体准确度
  FMPC与FATE精确度基本一致

  算法丰富度
  FATE新增多款联邦推荐算法

  产品易用性
  FATE可扩展性强，但学习成本高；FMPC界面操作简单，上手快
  其他信息
  FATE目前不支持多个任务同时运行，可以同时建立多个任务，但同一时间只能运行一个算法任务；
- **FMPC**具有4个产品模块

  https://mp.weixin.qq.com/s/btYjf9wHhSKMZlPEdKJnOQ

  1）联邦学习：
  原始数据不出门，参与各方本地建模；没有敏感数据流通，交互中间计算结果；参与方只有自己模型参数，
  整个模型被保护；私有化部署；开放API快速开发；支持主流机器学习算法；LR, DT, RF,

Xgboost...；建模速度快3倍；密文训练精度误差<1%

2）多方安全计算：

落地应用计算量1.1万+次/天；支持多方数据安全求交；支持一次多项式；支持多方归因统计分析；支持多方多维数据钻取分析；私有化部署

3）匿踪查询：

支持100亿+条记录；秒级响应时间；查询授权存证；甲方查询信息不泄露；加密隧道避免中间留存；私有化部署。

4）联盟区块链：

联盟节点30+；高性能扩展1万TPS；合约调用20万次/天；电子存证和智能合约；隐私保护协议；快捷部署场景应用；开源开发社区

洞见智慧

官网：https://www.insightone.cn/

INSIGHTONE——洞见安全多方数据智能平台

主要业务 政务数据智能 金融数据智能 医疗数据智能

中诚信征信有限公司 投资孵化 洞见科技

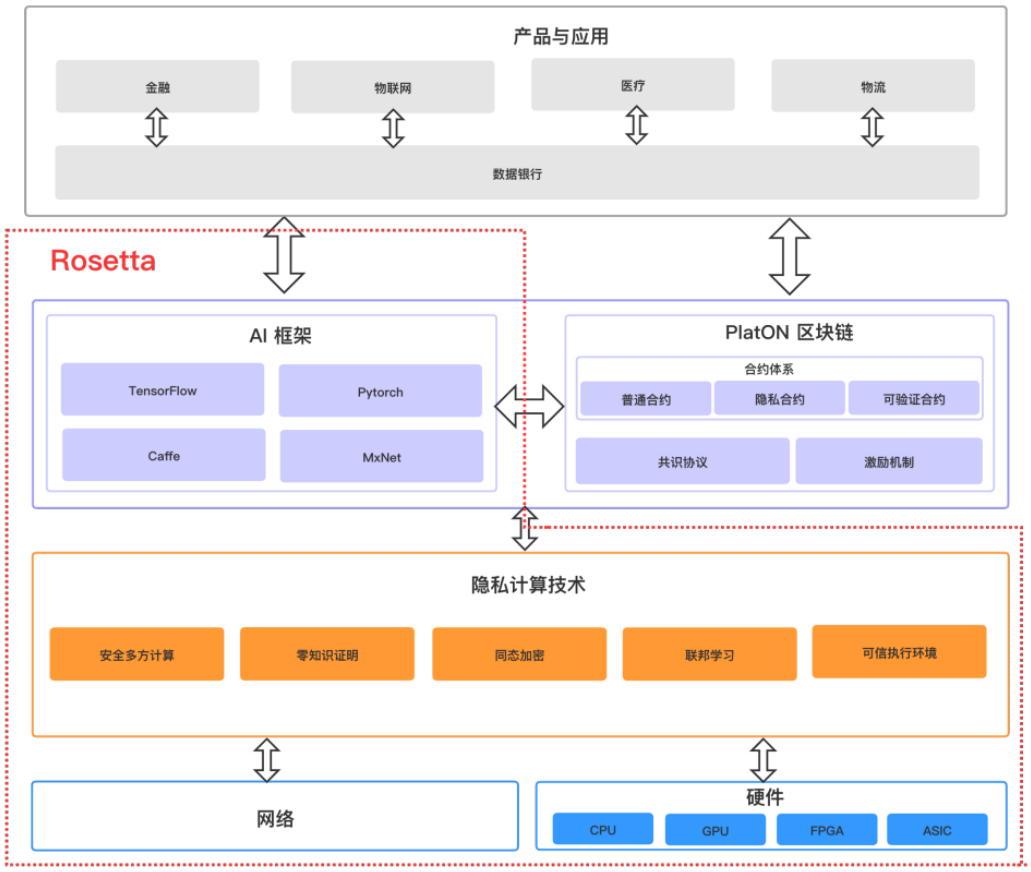
中诚信cto姚明 管理 洞见科技

中诚信和洞见 联合打造 **见智安全计算平台** --只有新闻稿

矩阵元Rosetta

- 官网 https://www.juzix.net/
- 矩阵元算法科学家 谢翔
- 矩阵元白皮书关键信息：

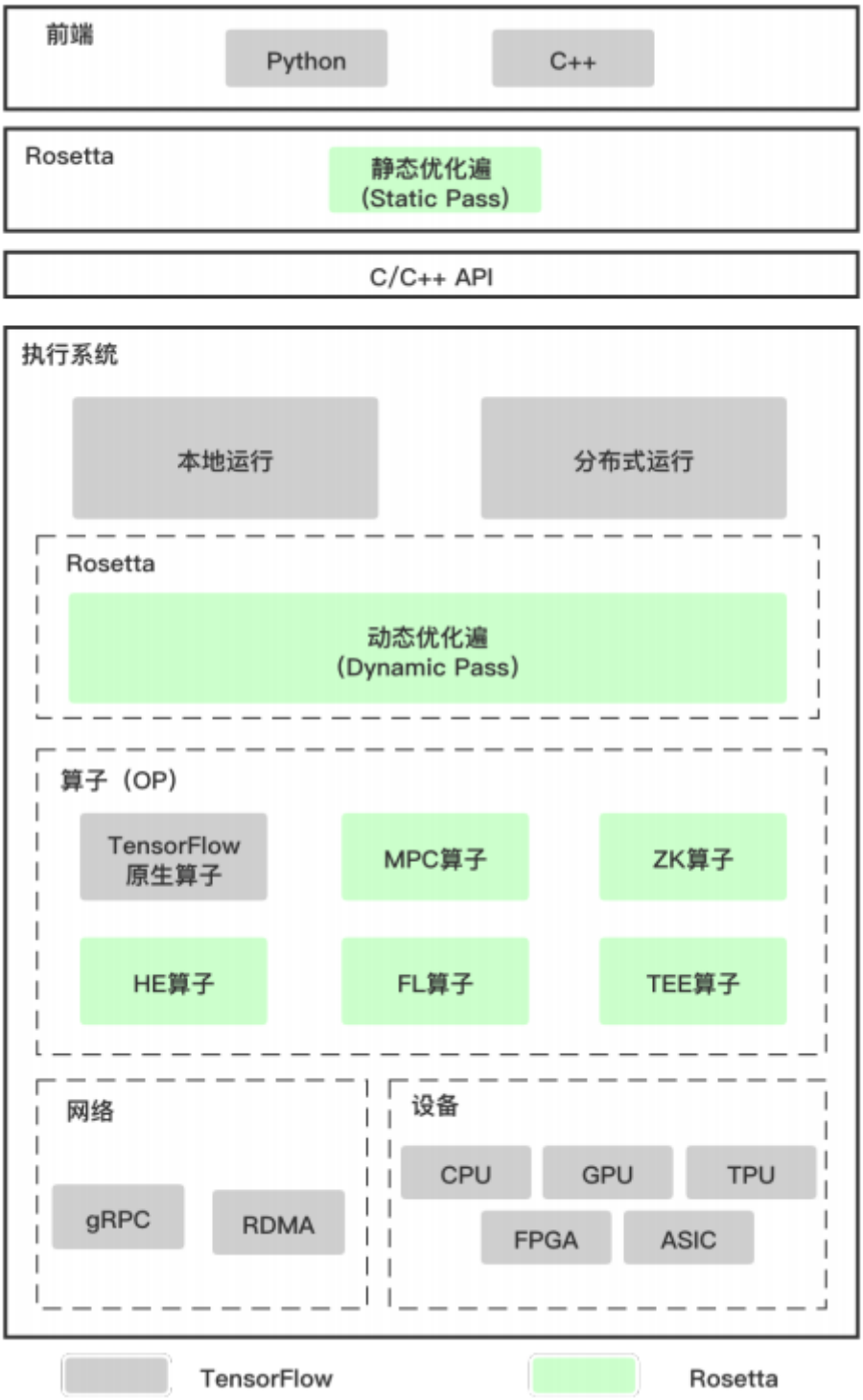
  架构图：



TensorFlow有高的扩展性，可以自定义和注册新的操作，以及不同的实现方式。

TensorFlow可以将定义和执行分开，所以开发者只需要编写模型即可，而不需要编写训练过程中的反向传播。自动求导?

Rosetta 的整体架构复用了 TensorFlow 的特性，基本的模式为利用 C/C++ 实现基本的算子以及梯度，然后将 TensorFlow 的算子按需转换成为隐私算子，最后进行隐私算子的执行。详细架构图如图 所示。



该版本中采用 Secure NN 的算法，并将在后续支持更多的 MPC 算法。

secure NN论文 19th Privacy Enhancing Technologies Symposium (PETS 2019)

https://eprint.iacr.org/2018/442

是一个三方模型的多方安全计算，增加了一个服务节点去分配随机数（三元组）。主要有三个突破

1. 准确率的提高。他们的技术能够在MNIST数据集上产生大于99%的推理准确率。而当时18年安全神经网络训练的最新技术SecureML准确率只有93.4%
2. 性能上的。SecureNN比以往的这种在两个到三个服务器上方案，例如SecureML, MiniONN, Chameleon, 还有Gazelle 有6-113倍的提高
3. 安全性。以往的协议只支持半成实敌手，这个不仅是半诚实安全，还**多了一个恶意敌手**安全可确保恶意服务器即使从协议中任意偏离，也无法了解诚实客户端的输入或输出的任何信息(只要没有向敌手透露计算的输出)。

代码没有跑起来的原因：

TensorFlow版本限制 Tensorflow (1.14.0=, cpu-only) 是一个19年7月的版本 最新版本2.3

源码编译安装Tensorflow 1.14.0 需要100G空间和超过6个小时编译时间

```
> TensorFlow source code is recommended to install more than 100GB of free disk space
```

```
**TensorFlow source code compilation**
 > Installation time will be long (about 6 hours), it is recommended to configure 8G+ memory
```

现在Rosetta可以实现的计算：

除了常用的加减乘除比较，还特地对机器学习用到的函数做了封装：矩阵乘法、Sigmoid、Relu等。

TensorFlow OP	MPC OP	MPC OP Gradient
Add	MpcAdd	MpcAddGrad
Sub	MpcSub	MpcSubGrad
Mul	MpcMul	MpcMulGrad
Div	MpcDiv	MpcDivGrad
TrueDiv	MpcTrueDiv	MpcTrueDivGrad
RealDiv	MpcRealDiv	MpcRealDivGrad
MatMul	MpcMatMul	MpcMatMulGrad
Sigmoid	MpcSigmoid	MpcSigmoidGrad
Log	MpcLog	MpcLogGrad
Log1p	MpcLog1p	MpcLog1pGrad
Pow	MpcPow	MpcPowGrad
Max	MpcMax	MpcMaxGrad
Mean	MpcMean	MpcMeanGrad
Relu	MpcRelu	MpcReluGrad
Equal	MpcEqual	-
Less	MpcLess	-
Greater	MpcGreater	-
LessEqual	MpcLessEqual	-
GreaterEqual	MpcGreaterEqual	-
SaveV2	MpcSaveV2	-
ApplyGradientDescentOp	MpcApplyGradientDescentOp	-

数牍科技

- 官网 https://www.sudoprivacy.com/#/home
- 应用场景 **个人风险评估 数据匿名查询 存量客户意向识别 广告优化投放 战略决策支撑 投保风险评估 反欺诈识别**
- 团队创始人&联合创始人 宋一民、蔡超超

  宋一民（Ethan）曾就职于 Facebook Ads 主导了基于隐私保护的数据协作项目。

  蔡超超 曾先后任职于 Amazon、Facebook。加州大学洛杉矶分校（UCLA）机器学习博士。
- 拿到红杉资本投资

  https://mp.weixin.qq.com/s/UYB8diH7-piFyJDpD5NhlA

  我们投了一个做隐私计算的公司叫数牍科技，两位创始人曾经是海外巨头企业的隐私计算部门非常核心的团队骨干。他们看到了隐私计算不止在海外有机会，在国内也有机会，而且相较于国内团队，他们的认知要领先一到两年时间。这一到两年对于创业团队来说是一个很不错的时间窗口，所以我觉得在一些技术领域还是存在这样打时间差的机会的。

上海柯橙

- 官网 https://k-orange.cn/ 官网附带微信公众号认证是上海柯橙信息技术有限公司 但是推送是广告
- 地址 上海市杨浦区霍山路398号12层08室 股东 沈筱微 余力 诸葛忠 **没有郭宇**

  企查查 https://www.qcc.com/firm/d7a7589710513f7784d5a25d072aaed4.html

其他

https://mp.weixin.qq.com/s/UuePObI3KNPEJRPl6pX7ZA

mpc

华控清交（Privpy）、蚂蚁金服（Morse）、富数科技（Avatar）、百度（点石）

联邦学习

微众银行（Fate）、蚂蚁金服（Morse）、富数科技（Avatar）、平安科技（蜂巢）、数牍科技

场景 **政务大数据 医疗科研 银行金融 保险营销与定价 基金管理 大数据增值服务 广告平台联合营销 供应链金融 高校科研 量化投资模型**