数据共享开放与隐私保护

AI Time 第四期

主办单位：AI Time
北京智源人工智能研究院

关于AI Time

AI Time是一群关注人工智能发展，并有思想情怀的青年人创办的圈子。AI Time旨在发扬科学思辨精神，邀请各界人士对人工智能理论、算法、场景、应用的本质问题进行探索，加强思想碰撞，打造成为北京乃至全国人工智能知识分享的策源地和聚集地。

往期回顾

第1期：人工智能安全与伦理

第2期：自动机器学习和可解释机器学习

第3期：知识图谱——知识赋能智能与智能产生知识

AI Time 4

数据共享开放与隐私保护

吴信东

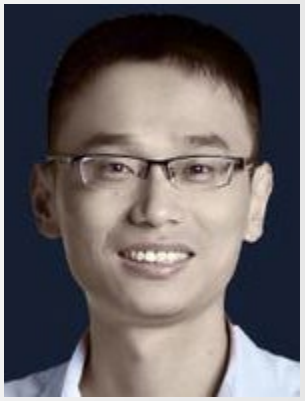
明略科技

朱小燕

清华大学

徐　葳

清华大学



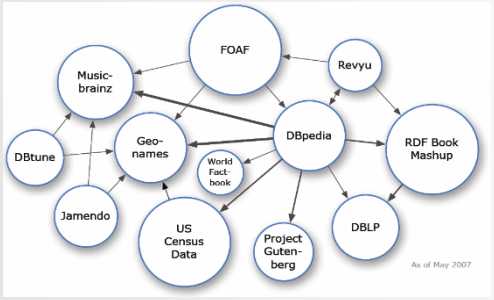
吴海山

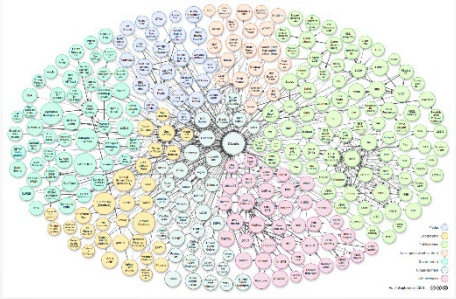
微众银行

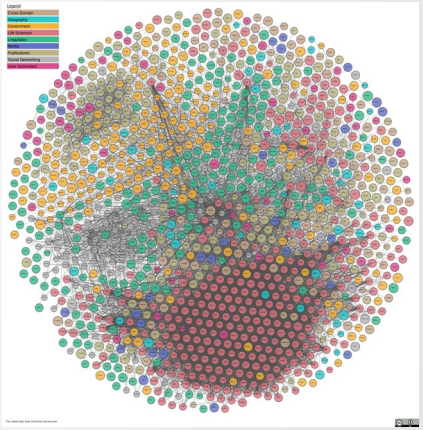
群满后加学术君微信“AMiner308”备注“AI Time 4”入群

数据开放共享

- 数据开放共享是大数据竞争的战略核心和突破点
- 互联网之父Tim Berners-Lee倡导了W3C链接开放数据计划







2007 2011 2019

W3C链接开放数据计划

嘉宾讨论

1 目前国内外有哪些影响力大的数据共享开放计划或平台?

2 数据共享开放主要涉及哪些关键技术?

3 数据共享开放在技术上的挑战主要有哪些?

4 目前国内外出台了哪些数据共享开放方面的政策?

5 数据共享开放在政策上的挑战主要有哪些?

数据隐私保护

- 大数据的使用必须面对隐私数据保护的责任与义务
- 保护隐私数据和防止敏感信息泄露成为目前的严重挑战

Facebook的数据隐私保护存在问题

Google的数据隐私保护存在问题

嘉宾讨论

6 您认为隐私数据主要分为几大类?

7 数据隐私保护主要涉及哪些关键技术?

8 现有的技术能有效保护用户隐私数据吗?

9 隐私保护面临的挑战?

- 如何平衡数据的可用性与隐私保护之间的关系
- 如何兼顾对个体隐私和数据自身稀缺性的有效保护

（eg.数据拼图是指数据使用者能够通过整合数据访问过程中多次获取的数据片段，利用数据片段之间的关联性，非法拼接还原出整个数据的全貌或者其中大量的涉及隐私的敏感数据。）

嘉宾讨论

10 目前国内外出台了哪些数据隐私保护方面的政策?

11 数据隐私保护在政策上的挑战主要有哪些?

12 您支持更严的隐私保护政策还是支持更开放的数据共享来促进技术进步?

It Is Your Turn

在信息大爆炸的时代，如果有这样一个APP：

（1）让有价值的、指定对象的信息被智能化地过滤出来。（老板的、重要客户的、女神男神的）

（2）跟踪消息历史记录，误删信息也可以找回来。银行卡消费了多少钱、航班临时改了登机口、快递送到了什么地方，这些信息还会以视觉化卡片的形式呈现。

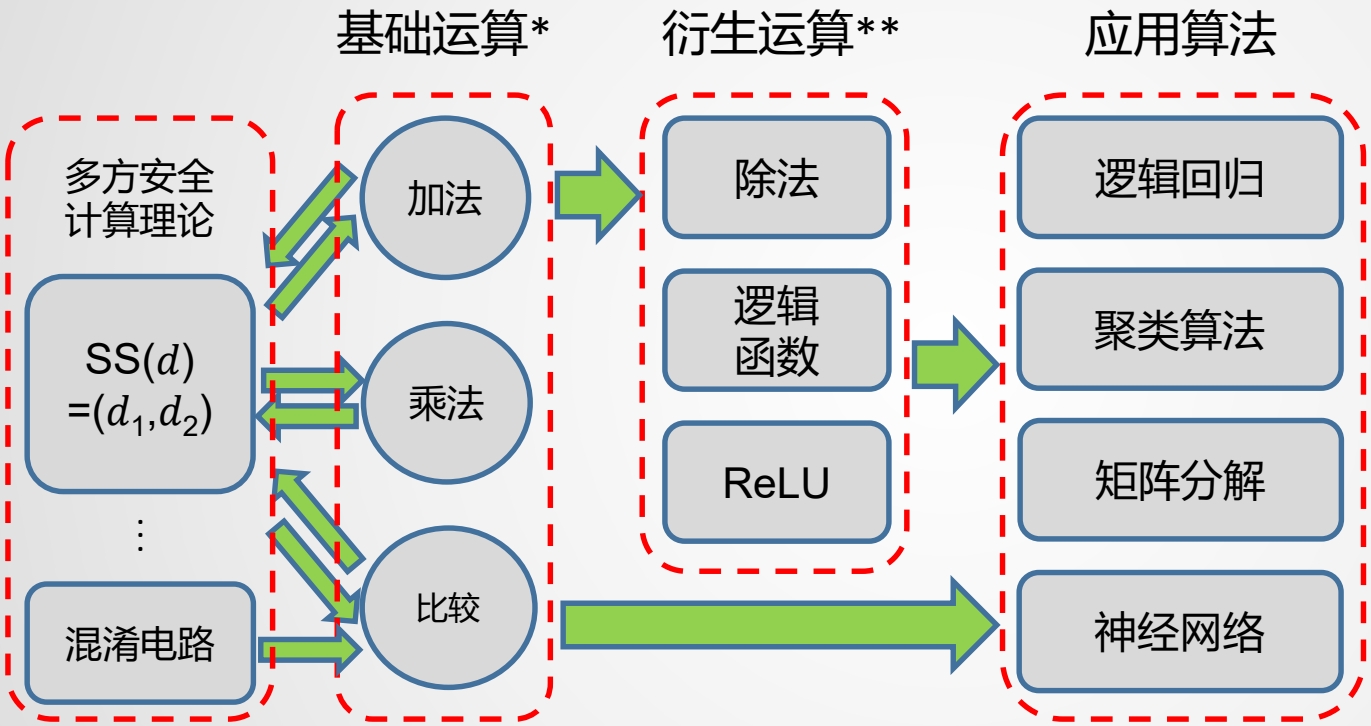
（3）符合GDPR审计，实现隐私保护。

你会使用吗？请扫码投票

如何保护隐私

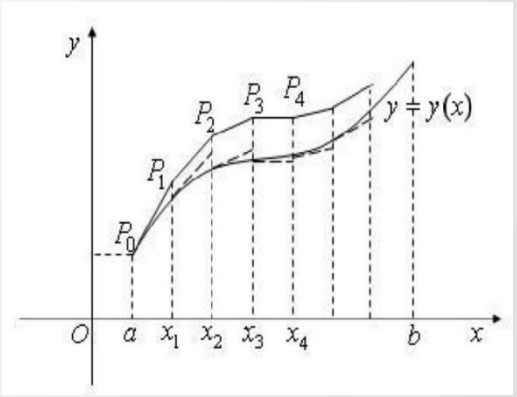
An image recovered using a new model inversion attack (left) and a training set image of the victim (right). The attacker is given only the person's name and access to a facial recognition system that returns a class confidence score. (Fredrikson et al., CCS 2015)

隐私保护计算技术原理



** 衍生运算方法:

- 除法、Sigmoid、ReLu、其他函数: e^x, log(x), …



* 我们的隐私保护计算技术运用密码学/ 多方安全计算理论在计算机指令集和编译器层面用密文运算算替代了明文运算，建了密文数据编程系统，并极大地优化了计算性能。

k-anonymity

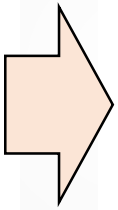
Voter Registration Data

Name	Age	Sex	Zipcode
Ahmed	25	Male	53711
Brooke	28	Female	55410
Claire	31	Female	90210
Dave	19	Male	02174
Evelyn	40	Female	02237

Patient Data

Age	Sex	Zipcode	Disease
25	Male	53711	Flu
25	Female	53712	Hepatitis
26	Male	53711	Brochitis
27	Male	53710	Broken Arm
27	Female	53712	AIDS
28	Male	53711	Hang Nail

Figure 1. Tables vulnerable to a joining attack



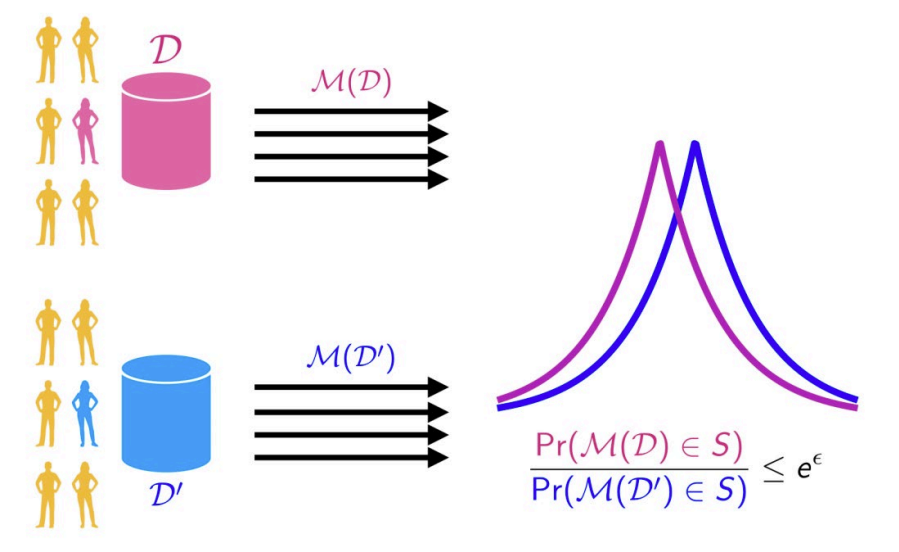
Age	Sex	Zipcode	Disease
[25-28]	Male	[53710-53711]	Flu
[25-28]	Female	53712	Hepatitis
[25-28]	Male	[53710-53711]	Brochitis
[25-28]	Male	[53710-53711]	Broken Arm
[25-28]	Female	53712	AIDS
[25-28]	Male	[53710-53711]	Hang Nail

Figure 2. Single-dimensional anonymization

Age	Sex	Zipcode	Disease
[25-26]	Male	53711	Flu
[25-27]	Female	53712	Hepatitis
[25-26]	Male	53711	Brochitis
[27-28]	Male	[53710-53711]	Broken Arm
[25-27]	Female	53712	AIDS
[27-28]	Male	[53710-53711]	Hang Nail

Figure 3. Multidimensional anonymization

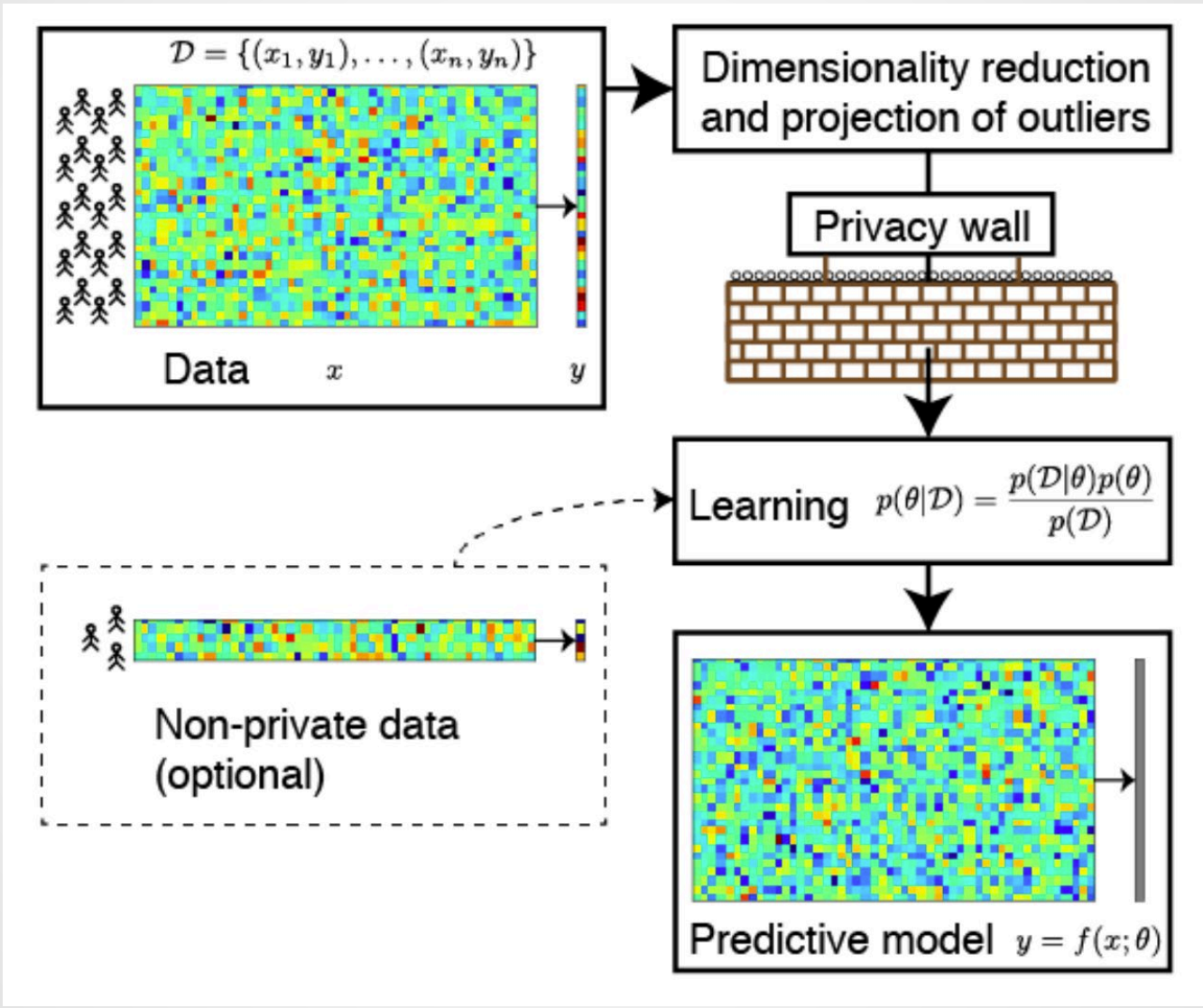
Differential privacy (Dwork et al., 2006)



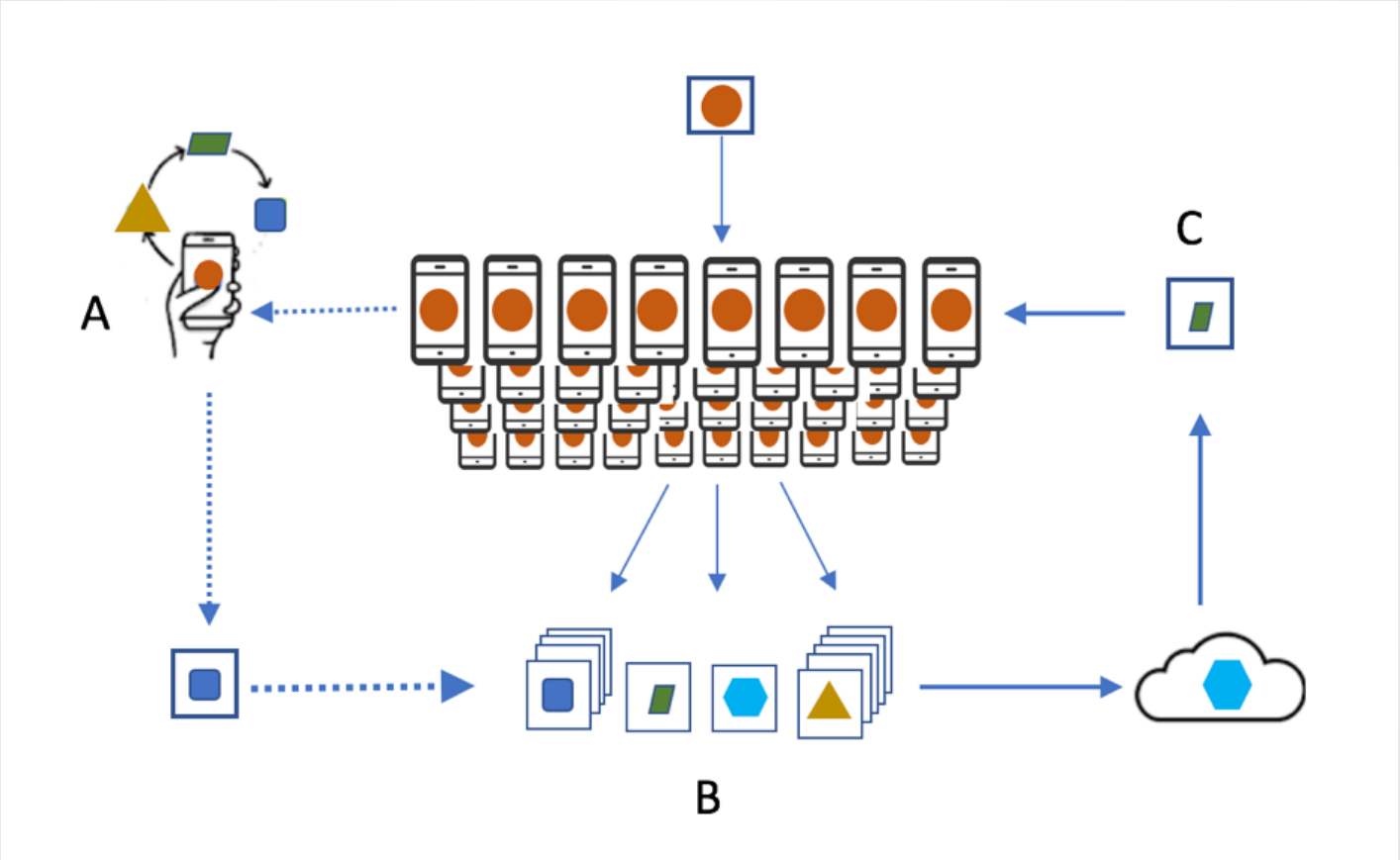
- 双随机法
  - 随机抛一个硬币
  - 如果tail则返回真值
  - 如果head，再次跑一个硬币，如果head则返回“Yes”，otherwise “No”
- Theory： $\epsilon = \ln 3, \epsilon$-DP

$$\frac{\Pr(Yes \mid Yes)}{\Pr(Yes \mid No)} = \frac{3/4}{1/4} = \frac{\Pr(No \mid No)}{\Pr(No \mid Yes)} = 3.$$

DP Machine Learning

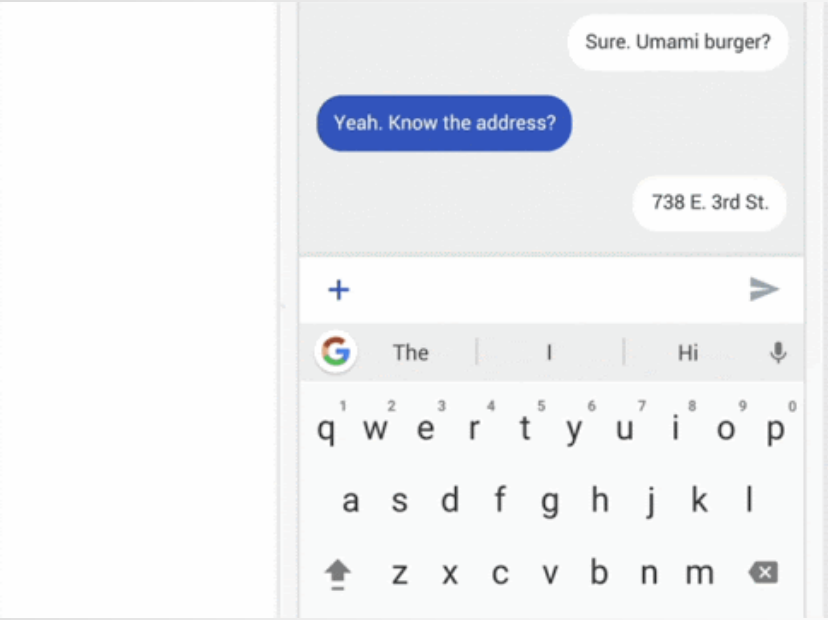


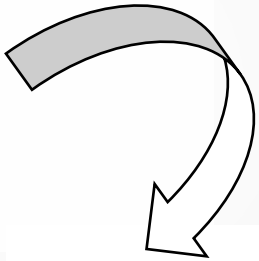
联邦学习

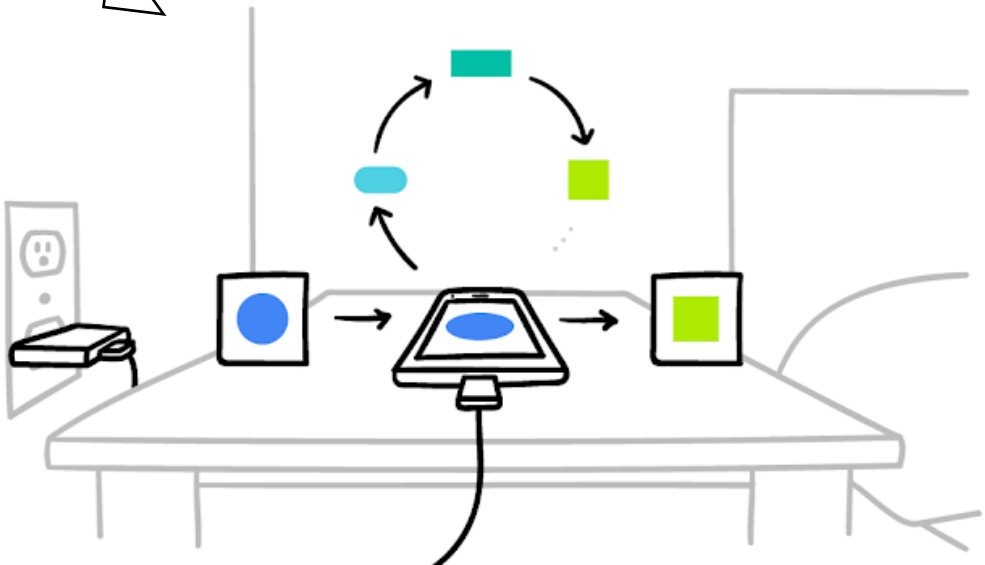


Federated Learning model development. Figure 2: A user's phone personalizes the model locally, based on her usage (A). Many users' updates are then aggregated (B) to form a consensus change © to the shared model. This process is then repeated

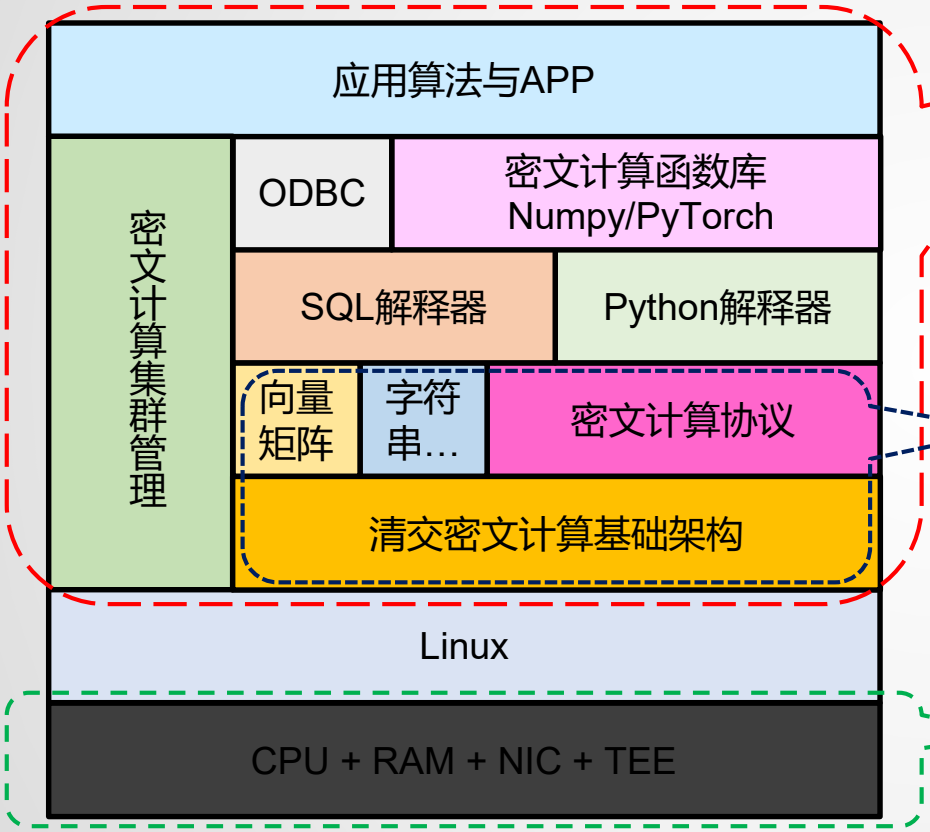
联邦学习


Sure. Umami burger?
Yeah. Know the address?
738 E. 3rd St.
The
I
Hi
q w e r t y u i o p
a s d f g h j k l
z x c v b n m





数据加密



- **安全计算平台软件栈**
  - ✓ 强调通用性、易用性
  - ✓ 兼容Python和SQL的密文计算编程接口
  - ✓ 兼容 Numpy 和 PyTorch 等函数库
  - ✓ 端到端：从协议到APP产品的原型
- **高效率多方安全计算协议**
  - ✓ 自主研发
  - ✓ 理论正确性保证
- **针对现有硬件设备的深度优化**
  - ✓ 定制化内核
  - ✓ 未来计划针对芯片、网络等进行优化

关于隐私保护的公共政策

- GDPR
  - 前身是欧盟在1995年制定的《计算机数据保护法》
  - 2018年5月25日，欧洲联盟出台《通用数据保护条例》.
  - 合法性、脱敏与数据安全、限制使用、存储限制
- 《数字安全管理办法》（国内）
  - 用不到的信息不许强行收集
  - 拒绝大数据杀熟
  - 治理垃圾推送消息
  - 标注机器生成内容
  - 设立「数据安全负责人」职位
  - 对已有数据的保护
  - 强制「溯源」

GDPR更细、给予用户更多控制权；

关于隐私保护的公共政策

- GDPR
  - 前身是欧盟在1995年制定的《计算机数据保护法》
  - 2018年5月25日，欧洲联盟出台《通用数据保护条例》.
  - 合法性、脱敏与数据安全、限制使用、存储限制

英国信息专员办公室（Information Commissioner’s Office, ICO）决定，对去年英国航空50万用户信息泄露一事开出1.83亿英镑（约合人民币15.8亿元）的罚单——这是欧盟《通用数据保护条例》（GDPR）生效以来的最高金额罚单，约占英国航空2018年收入的1.5%。ICO调查发现，英国航空公司脆弱的安全防护措施是造成这起信息泄露的重要原因。

关于隐私保护的公共政策

- GDPR
- 《数字安全管理办法》

GDPR消耗公司资源

GDPR伤害欧洲科技创业公司

GDPR对欧盟经济产生负面影响

GDPR减少了数字广告行业的竞争

GDPR使企业实施起来过于复杂

GDPR未能增加用户之间的信任

GDPR对用户的在线访问产生负面影响

数据开放共享

- 虽然布满未知与挑战，研究人员依然热衷于继续保持研究所蕴含的全球分享文化（Nature，2019）

人工智能研究

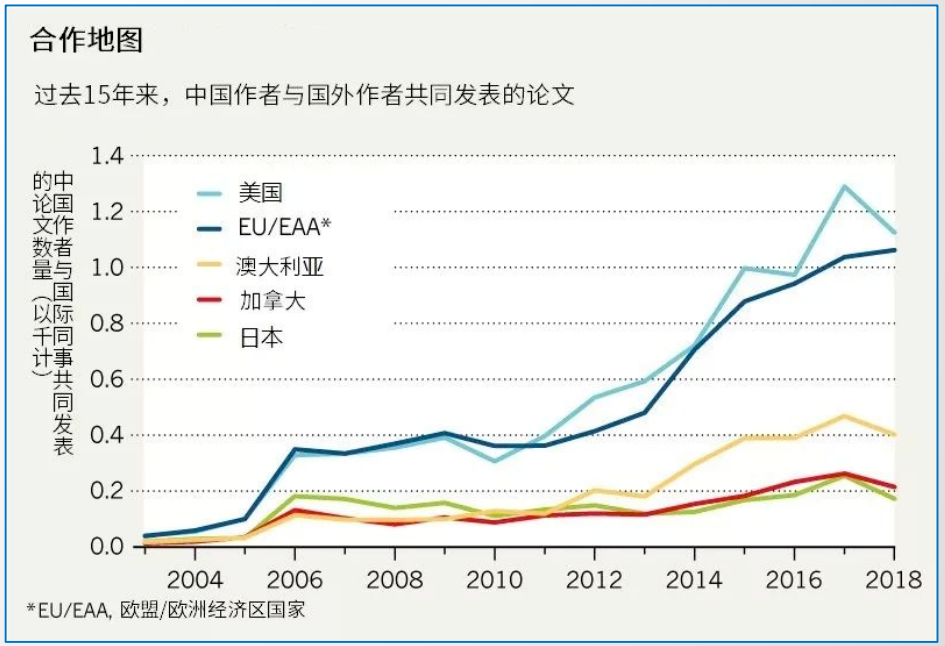
关乎

开放和速度。

如果你不与别人分享

你的成果，你的工作就

毫无意义。



谢谢大家

剧透7.26第五期AI Time：论道无人驾驶即将来临还是遥遥无期？
嘉宾：楼天成和邓志东等。