OWASP
Open Web Application Security Project

大数据全生命周期隐私问题探究

汇报人：刘雪峰

西安电子科技大学
网络与信息安全学院

数据隐私

数据隐私是什么?

攻击者通过某种途径，获取超出权限之外的数据或信息

数据隐私问题起因

为什么会产生数据隐私泄露？

OWASP
Open Web Application Security Project

大数据全生命周期

数据采集阶段隐私

- 用户与服务器是否**同一个信任域**？

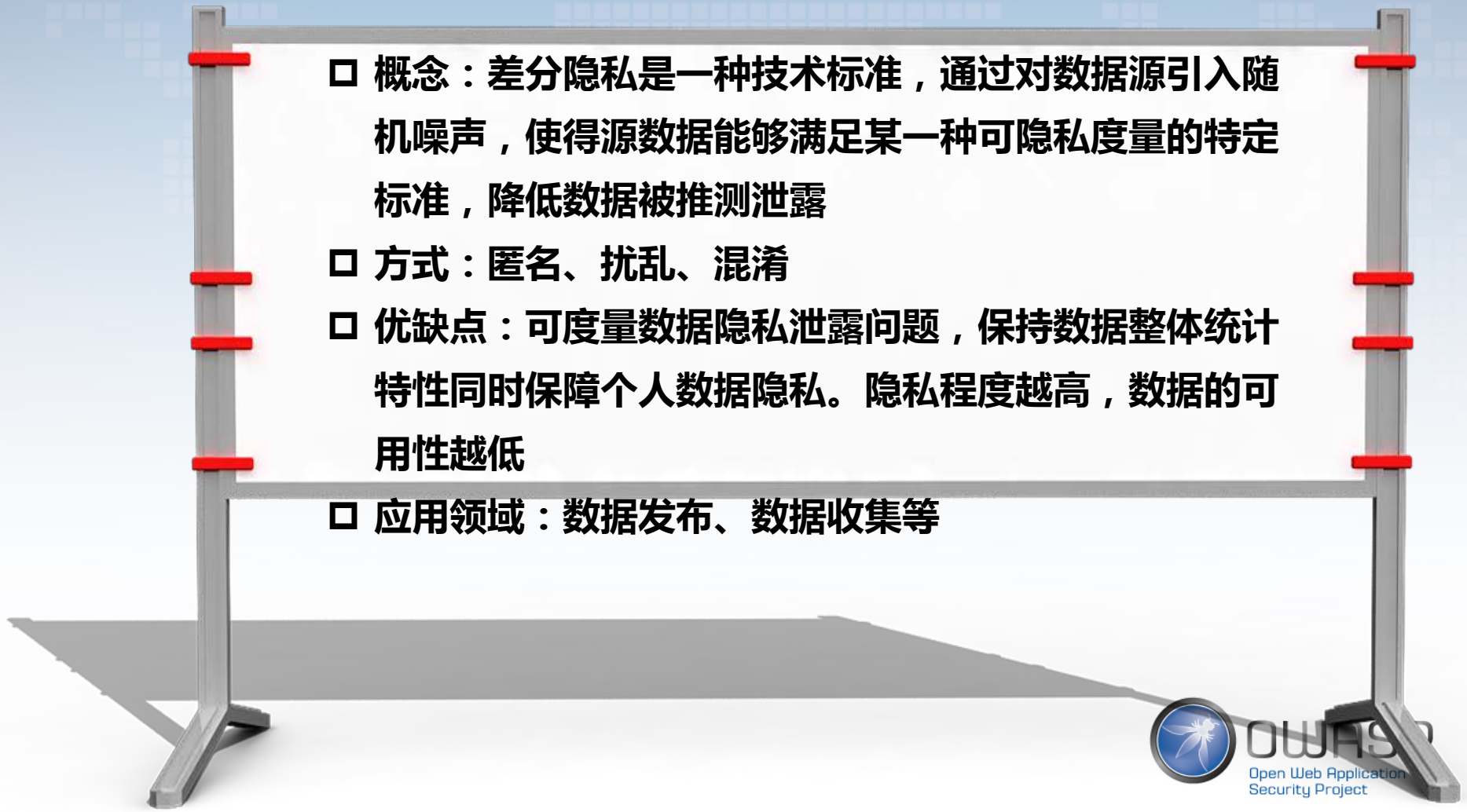
数据采集阶段隐私典型保护方法

- **谷歌的RAPPOR**：利用本地化差分隐私保护技术从Chrome浏览器每天采集超过1400万用户行为统计数据

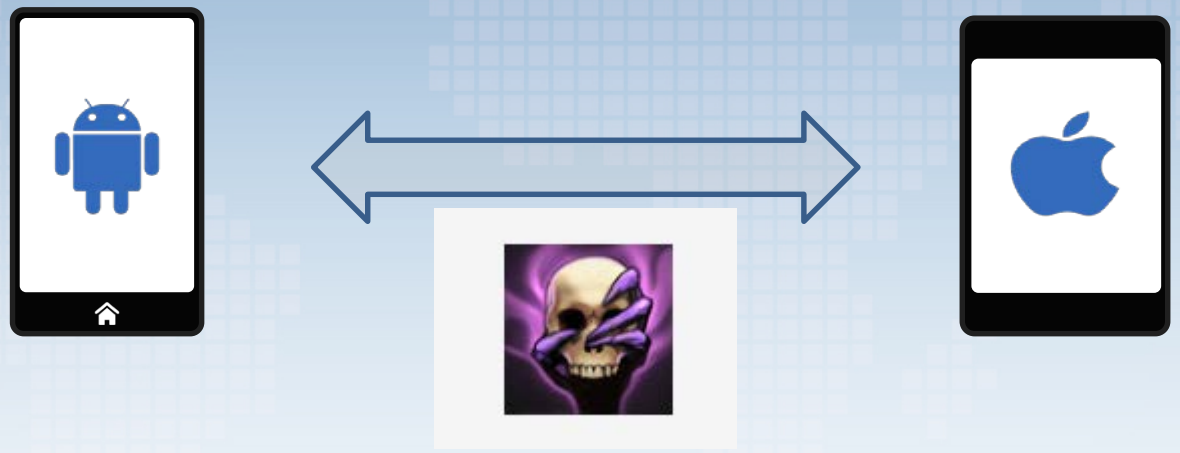
- **苹果的CMS**：使用差分隐私算法从iPhone收集行为统计数据

差分隐私

- 概念：差分隐私是一种技术标准，通过对数据源引入随机噪声，使得源数据能够满足某一种可隐私度量的特定标准，降低数据被推测泄露
- 方式：匿名、扰乱、混淆
- 优缺点：可度量数据隐私泄露问题，保持数据整体统计特性同时保障个人数据隐私。隐私程度越高，数据的可用性越低
- 应用领域：数据发布、数据收集等



数据传输阶段隐私

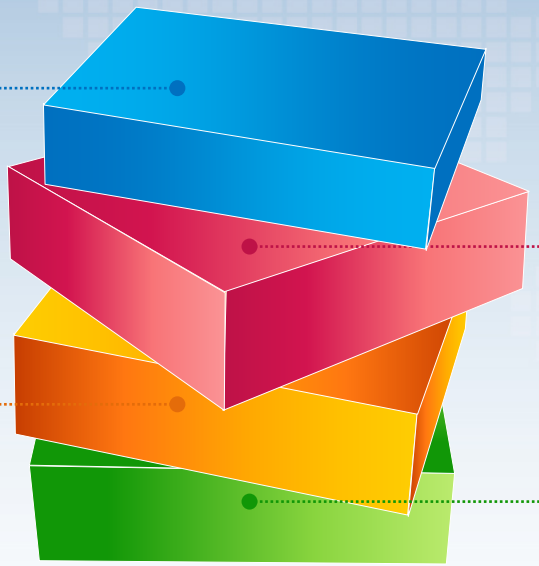


链路隐私安全

- **机密性**
  - 数据是加密的
- **完整性**
  - 数据是不可篡改的
- **方式**
  - HTTPS/SSL/TLS

数据处理阶段隐私

处理者是谁？

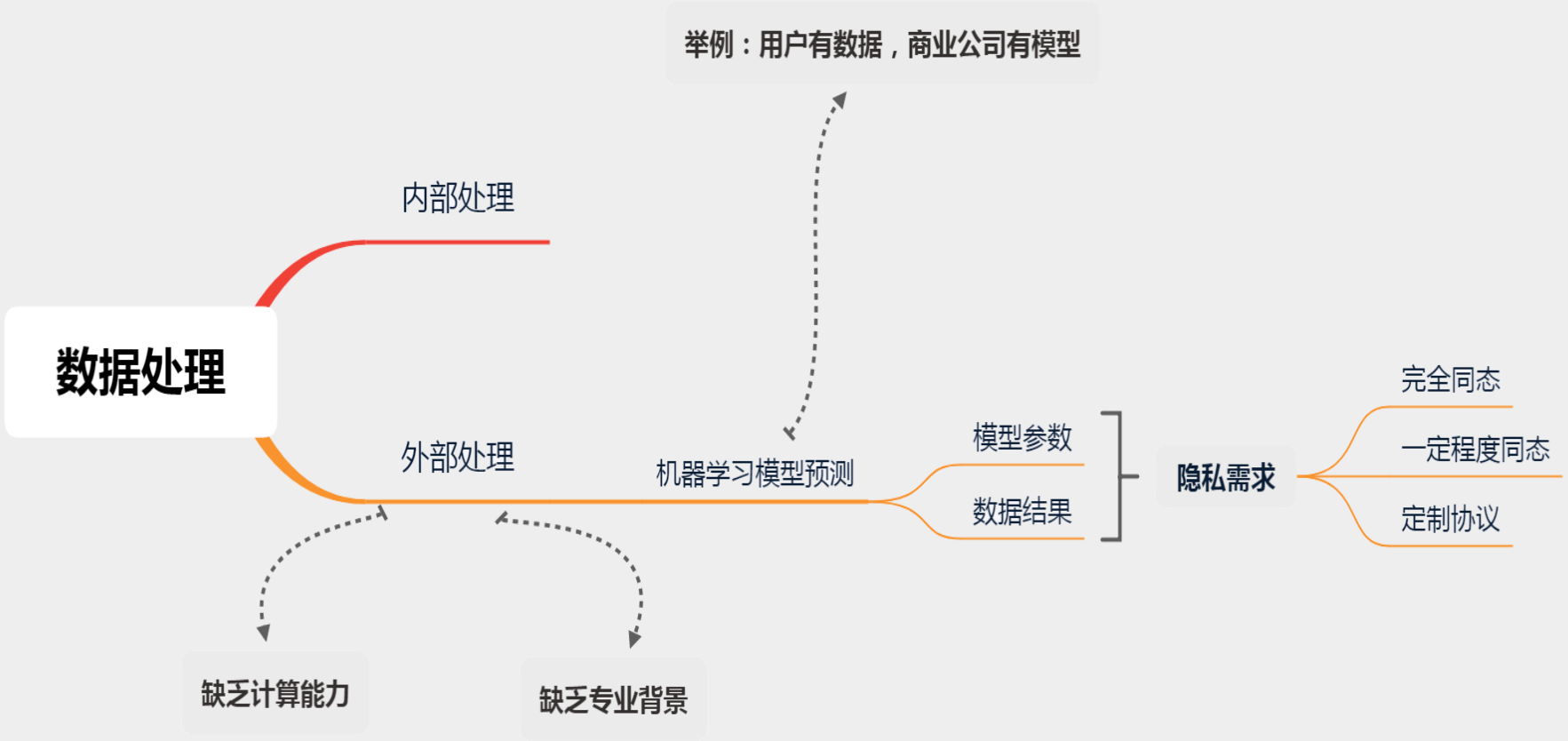


处理方式是什么？

隐私需求是什么

隐私方式是什么？

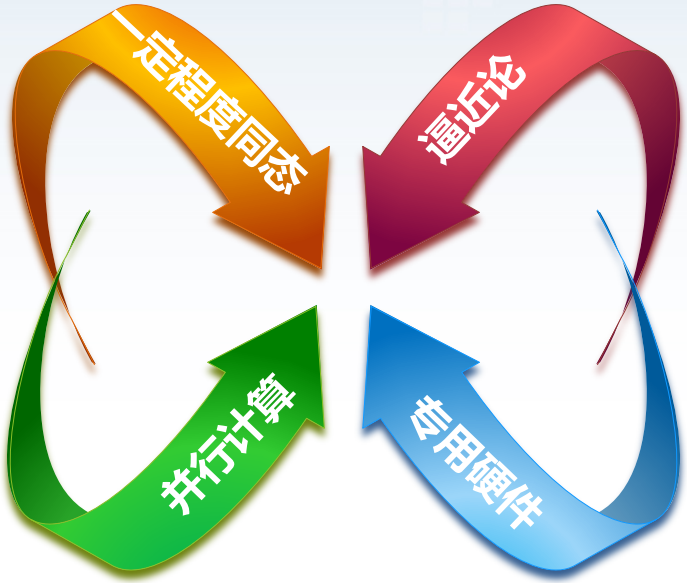
数据处理阶段隐私保护方式



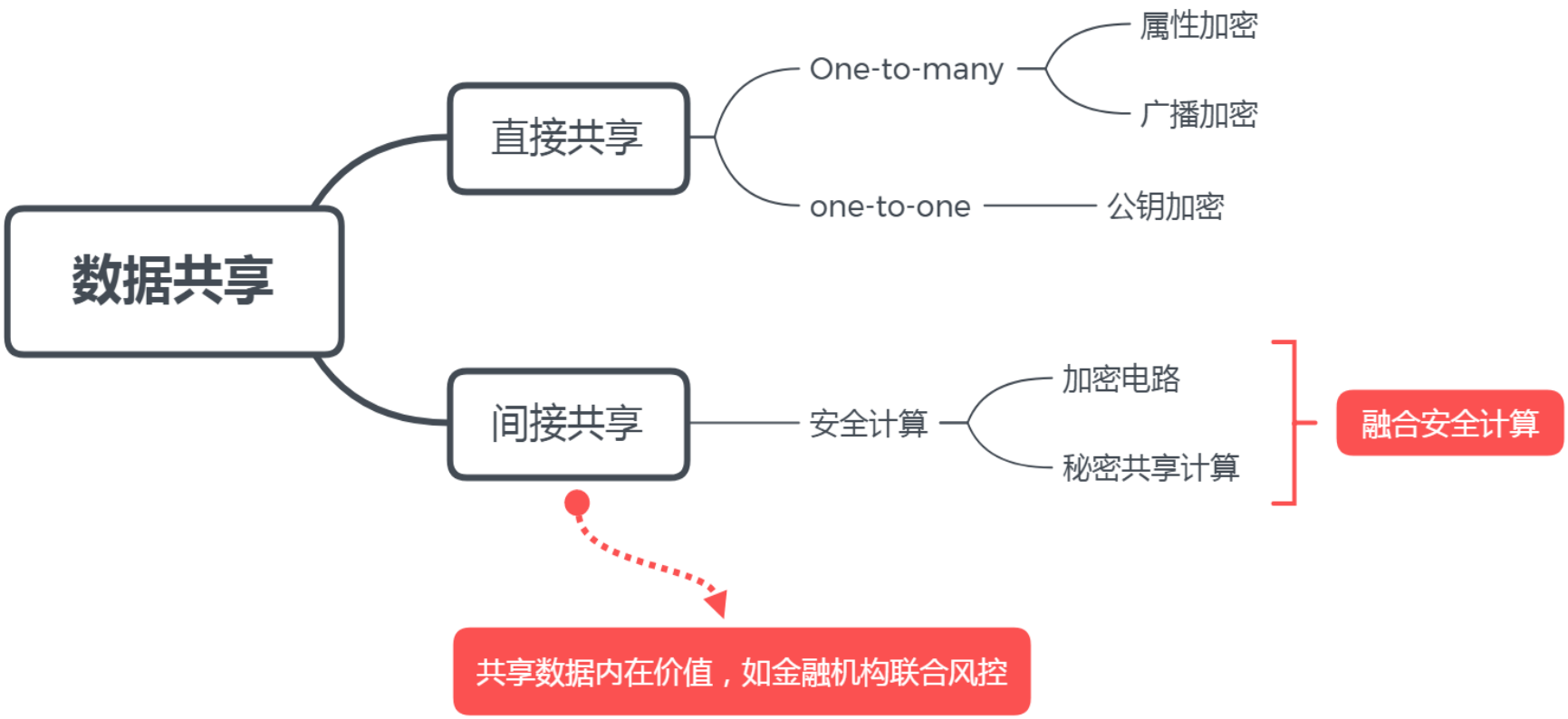
同态加密

完全同态：能够像明文一样处理密文，实用性差

一定程度同态：能够以较高效率处理低次多项式以及低深度电路。实际中数据处理，通常涉及到复杂的非线性函数，怎么办？



数据交换/共享阶段隐私

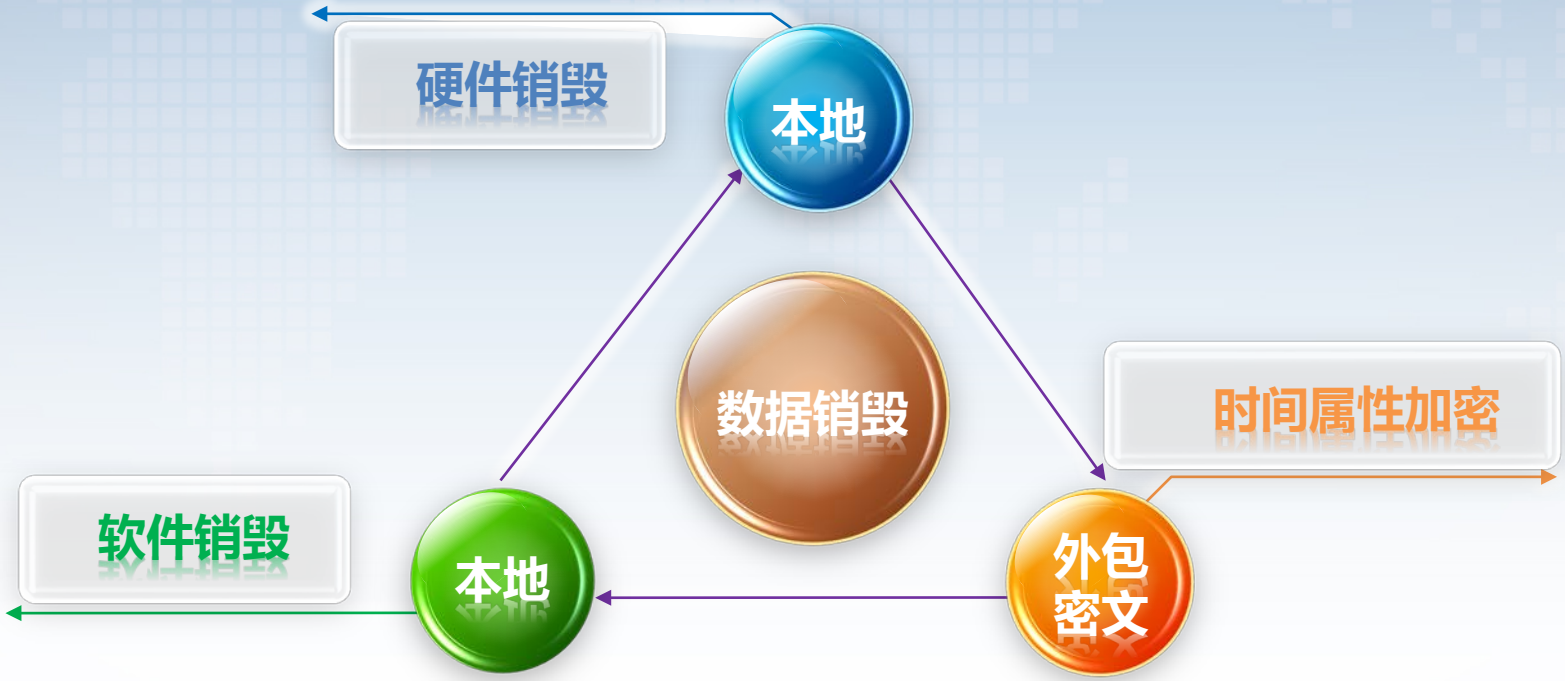

数据共享
直接共享
One-to-many
属性加密
广播加密
one-to-one
公钥加密
间接共享
安全计算
加密电路
秘密共享计算
融合安全计算
共享数据内在价值，如金融机构联合风控

加密电路与秘密共享计算

融合安全计算+逼近论+并行计算

OWASP
Open Web Application Security Project

数据销毁阶段隐私



谢谢！