安全多方计算介绍

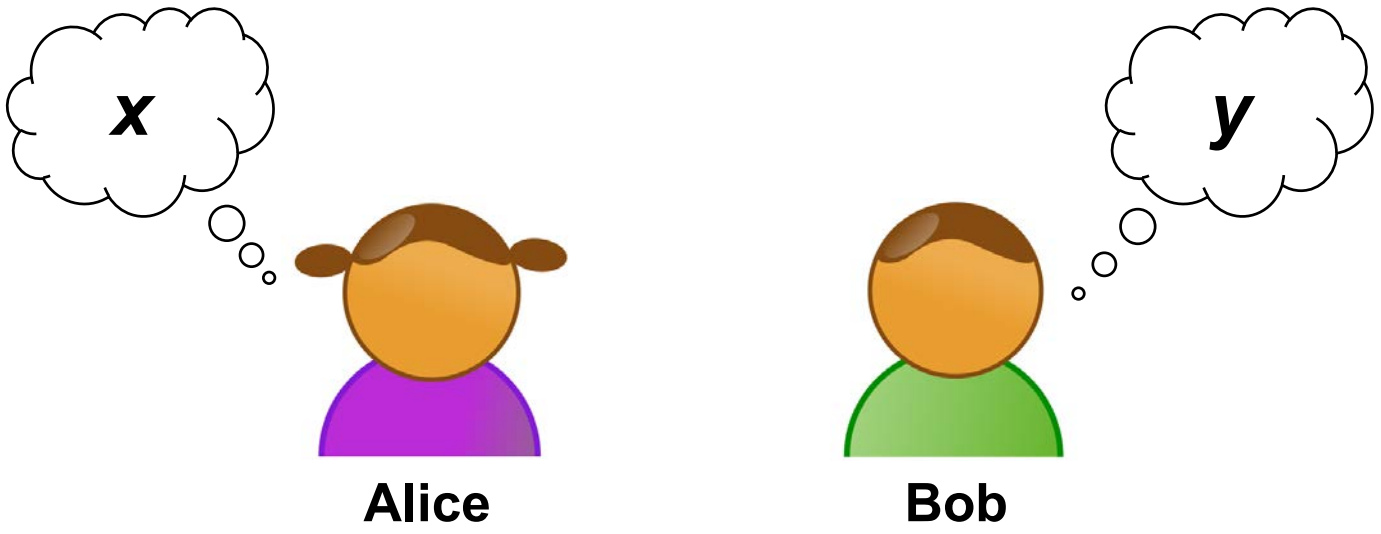
陆海宁

2018年7月26日

上海交通大學
SHANGHAI JIAO TONG UNIVERSITY

起源——Yao's Millionaires' Problem

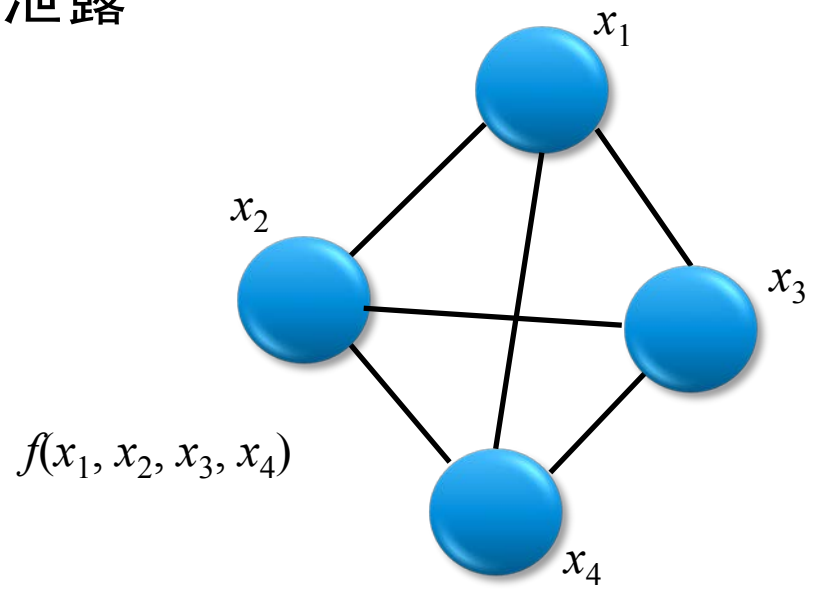
- 两个百万富翁想知道**谁更富有**，但不想公布自己具体有多少钱



x和y那个更大？

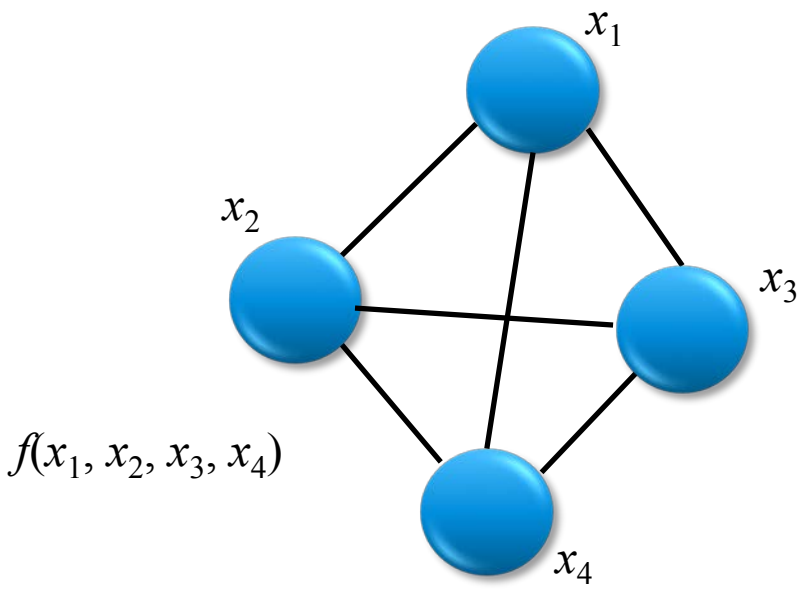
安全多方计算定义

- n个实体$p_1, p_2, \ldots, p_n$，每个实体拥有一个秘密数据，分别是$x_1, x_2, \ldots, x_n$
- 共同计算出一个公共函数$f(x_1, x_2, \ldots, x_n)$
- 实体的秘密数据不被泄露



安全多方计算的安全

- 在不超过t个恶意实体的情况下确保
  - 正确性：函数计算正确
  - 隐私性：$x_1, x_2, \ldots, x_n$不被他人知晓

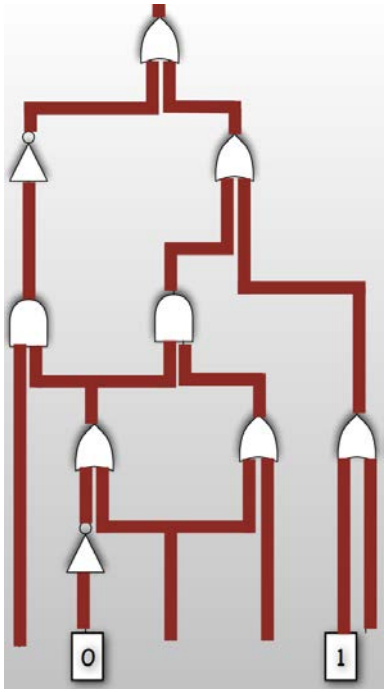


实际可行的*f*函数

- 理论上能写成程序的*f*函数都可以实现，问题是性能代价

```
program Millionaires {
    type int = Int<20>; // 20-bit integer
    type AliceInput = int;
    type BobInput = int;
    type AliceOutput = Boolean;
    type BobOutput = Boolean;
    type Output = struct {
        AliceOutput alice,
        BobOutput bob
    };
    type Input = struct {
        AliceInput alice,
        BobInput bob
    };

    function Output output(Input input) {
        output.alice = (input.alice > input.bob);
        output.bob = (input.bob > input.alice);
    }
}
```



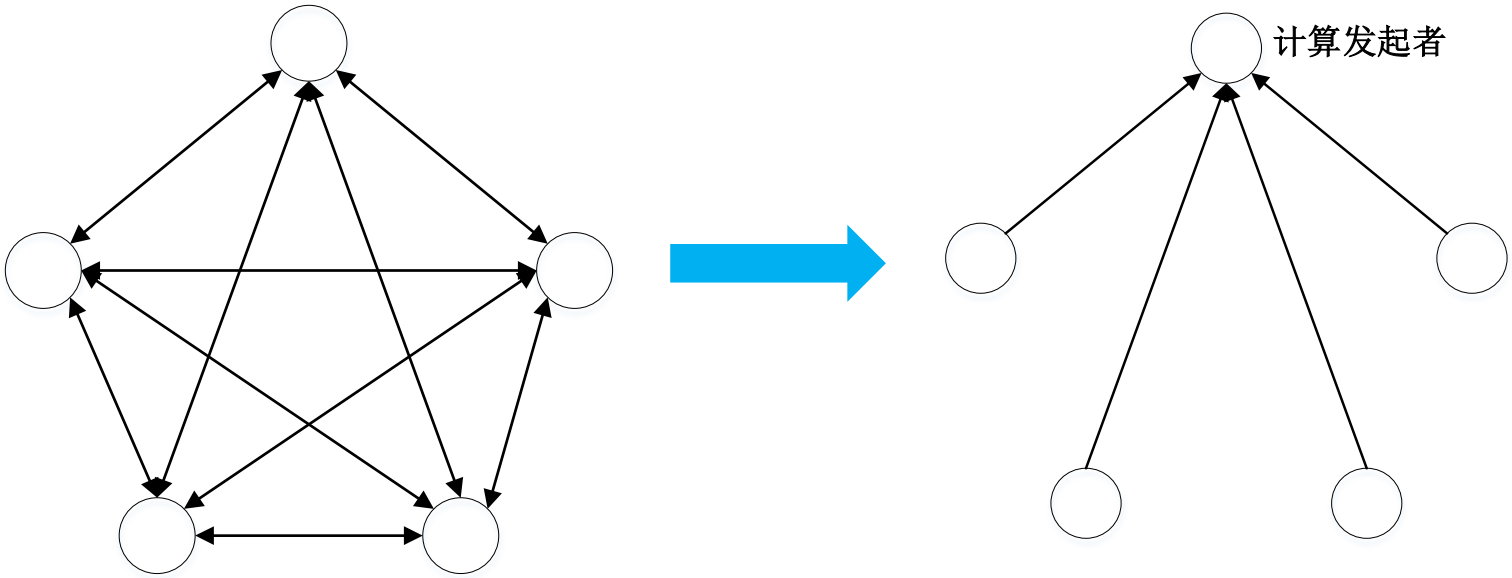
Yao's Millionaires' Problem & Garbled Circuit

实际可行的*f*函数

- **一次多项式：** $f(x_1, x_2, \ldots, x_n) = c_1x_1 + c_2x_2 + \ldots + c_nx_n$
- **在*n*等于2的情况下：**
  - $f(x_1, x_2) = x_1 * x_2$
  - $f(x_1, x_2) = x_1 \text{ XOR } x_2$
  - $f(x_1, x_2) = max(x_1, x_2)$
  - ….
- **……**

安全多方计算应用1

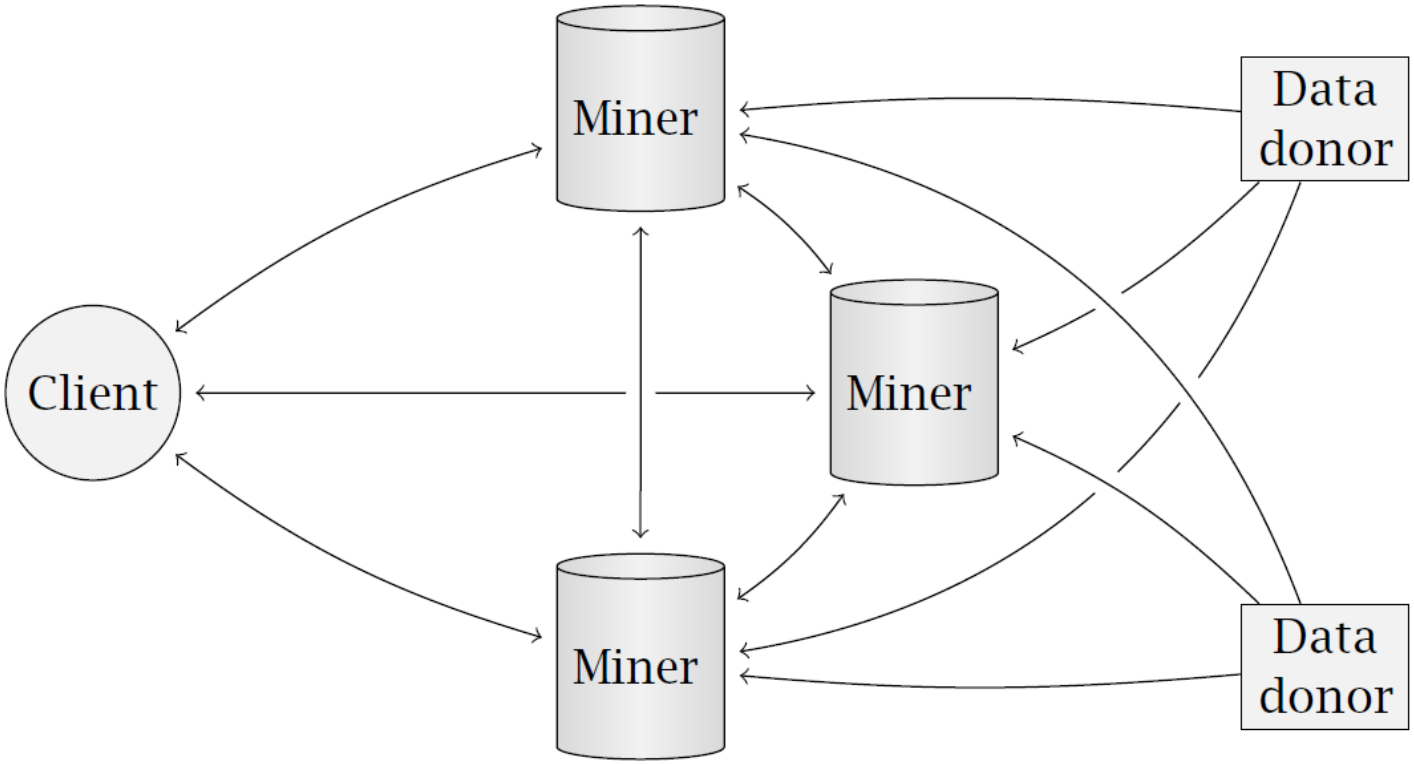
- 仅发起者需要获得计算结果
- 利用Shamir的秘密分享方案



秘密分享　　函数计算

安全多方计算应用2

- 数据市场（Sharemind architecture）



上海交通大学密码与计算机安全实验室

- 主任： 谷大武 教授
- 定位： 现代密码学，网络空间安全
- 成立于2003年，是上海交通大学重点支持的核心科研团队和优势平台，华东高校最大的密码学科研中心

LoCCS 密码与计算机安全实验室
Lab of Cryptology and Computer Security

LoCCS代表性成果——密码算法设计分析与实现

分组密码的分析与设计

密码分析中的关键问题

- 主流分析方法的联系
- 新型分析方法的提出
- 主流算法的安全性评估

主流算法的安全性评估：

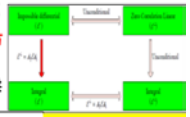
已分析的主流算法包括：

- ISO/IEC标准算法Camellia
- 国际标准算法Rijndael
- 美国NSA提出的算法SIMON
- 韩国标准算法ARIA
- 我国标准算法SM4

- 刷新了上述算法的安全界限
- 对算法安全评估起到重要借鉴

主流分析方法之间的联系（对称密码困难问题）

- 部分解决了该困难问题
- 揭示了三种主流分析方法的本质联系
- 为算法评估与设计提供了便利



新型分析方法的提出：

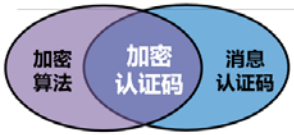
- 提出了三种新型分析方法
- 扩展了分组密码分析理论

CRYPTO 2015
INDOCRYPT 2014
FSE 2012/ACNS 2012
IET Inf. Sec./JSS/SCN …

新型密码算法的设计

- 设计了白盒分组密码算法
- 算法已提交解放军密码管理局进行评估

加密认证码设计



- 多功能密码算法
- 密码学未来发展的重要方向
- 设计理论不成熟：

现有标准算法GCM，EXPRIME被发现安全漏洞

SHELL加密认证码

- 申请人独立设计
- 强化安全性和强健性

	安全性	强健性
SHELL-AES	80-bit	55-bit
GCM-AES	64-bit	0

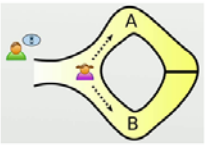
- 多平台之间效率平衡

	线性平台	并行平台
PX-MAC-AES	2.5cpb	0.8cpb
PMAC-AES	4.3cpb	0.6cpb
PC-MAC-AES	2.2cpb	2.2cpb

零知识证明

零知识证明是现代密码学中极为重要的领域，是构造加密、签名、安全多方计算等的基本工具。

- 构造了第一个常数轮精确零知识协议
- 构造了第一批精确时间与空间可模拟零知识证明和论证协议
- 构造满足不同要求、具有更少轮数的零知识协议



ICICS 2012
ProvSec 2011
ISC 2014
ICITS 2015 ……

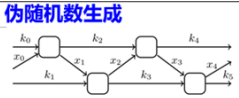
密码基础理论

密码学著名问题

如何基于单向函数

- 设计伪随机产生器
- 设计通用单向函数

伪随机数生成



- 基于规则单向函数 [ASIACRYPT 2013]
- 基于任意单向函数 [TCC 2013]

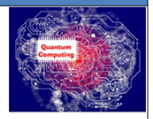
抗碰撞哈希函数

- 基于规则单向函数的最优设计
- 基于任意单向函数的目前最高效的设计 [CRYPTO 2015]

后量子密码

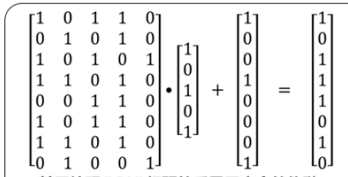
- 离散对数
- 大数分解(RSA)

量子不安全!



设计后量子安全的密码算法：

- 基于编码、学习困难问题
- 基于多变量、格困难问题



- 基于编码(LPN)问题的后量子安全的伪随机函数和分组加密 [EUROCRYPT 2016]
- 基于编码(LPN)问题的后量子安全的CCA安全公钥密码 [投稿中]

国密算法的实现

- 遵循10多份密码行业标准
  - GM/T 0002-2012 SM4分组密码算法
  - GM/T 0003.1-2012 SM2椭圆曲线公钥密码算法 第1部分：总则
  - GM/T 0015-2012 基于SM2密码算法的数字证书格式规范
  - ……
- 在多种语言上进行实现

Java　C/C++　JavaScript　GO

Bouncy Castle　OpenSSL

- 筹划在交大成立检测中心/研究院

LoCCS代表性成果——网络与金融安全

区块链 + 安全

涵盖平台、模块、监测加固和咨询的全面解决方案

- 顶层安全架构设计
- 抗量子攻击密码算法
- 数据的隐私保护
- 可监管性解决方案
- 新性共识机制
- 高安全性的终端设计
- 安全监测和加固

金融支付 + 安全

设计安全的网络支付机制

- 交易的完整性保护与不可抵赖
- 用户私钥和密码等信息的机密性保护
- 交易数据的保护传输与安全存储
- 支持PC端和移动终端支付

GM

中华人民共和国密码行业标准

云 + 安全

让不可信的云可信地存储与计算

- 确保用户云端数据的保密性，完整性和可用性
- 云端安全计算

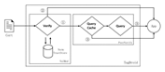
通信协议 + 安全

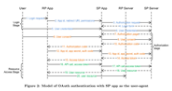
硬件层智能识别分析

- 自动化识别密码算法
- 自动化提取密钥
- 自动化分析参数

协议层智能识别分析平台

- 对SSL协议进行安全分析和加固
- 对Oauth协议进行安全分析





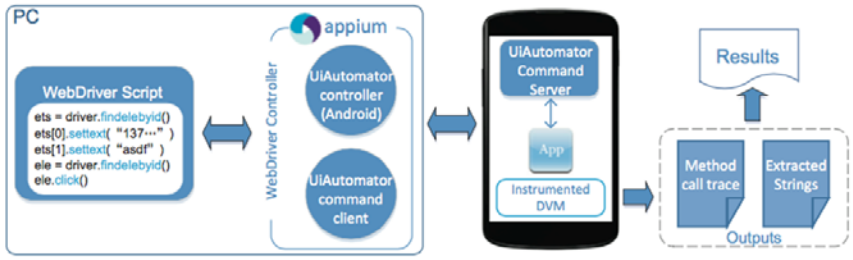
大数据 + 安全

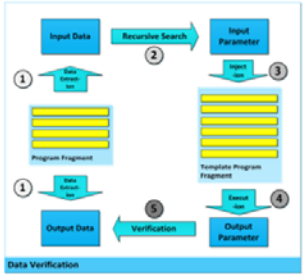
针对隐私的差异化和个性化需求，对隐私进行度量、计算和风险评估

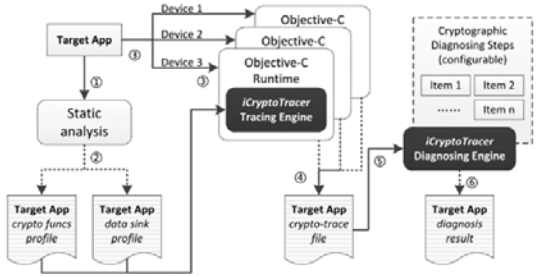
- 复杂大数据隐私泄露甄别与量化
- 敏感数据的分级分类
- 数据脱敏技术

LoCCS代表性成果——密码软件代码的分析测试技术

- 识别/提取应用软件中的密码算法、协议及秘密信息，发现隐藏代码/漏洞
- 支持Windows、Linux、Android、iOS和嵌入式OS
- 国家重大专项、科技支撑计划、重点研发计划支持
- 获全球DEF CON CTF 2016决赛亚军、世界CodeGate CTF 2015 冠军、Hack.lu CTF 2014 全球亚军







●终端类身份认证系统的渗透测试

- 安卓市场中下载量排名前300的Android应用程序
- 网络端被动监听、主动中间人攻击
- 测试结论：超过70%的应用程序没有能够恰当地保护用户的身份认证凭据信息

●密码程序分析综合系统：BaGua

- 一套跨平台、多架构的程序分析综合系统
- Android平台APP自动化脱壳和恶意代码清除
- iOS APP密码学误用问题分析检测
- 多种协议（SSL、OAuth、支付类）安全模型与分析

LoCCS代表性成果——密码硬件系统的攻防对抗技术

- **硬件旁路攻击技术平台**
  - 破解密码电路/芯片/嵌入式系统中的秘密参数
  - 发现和定位可疑的硬件木马电路
  - 适用于芯片、电路板、物联网节点、智能终端、工控设备

- **密码芯片电路旁路分析软硬件平台**
  - 支持ISO7816智能卡和USBKEY
  - 支持SM2、SM3、SM4国密算法的分析
  - 包含31个数据采集、预处理和密码分析模块

- 国家973计划、国家重大专项支持
- **国家科技进步二等奖**、上海市科技进步一等奖、中国密码学会密码创新一等奖

- **USIM芯片旁路攻击**
  - 发现3G/4G USIM芯片的重大安全问题，在30分钟内可提取12个秘密参数且完全复制
  - 引起沃达丰、联通、金雅拓等运营商和SIM卡制造商的关注

谢 谢!