研究方向介绍

陈 宇

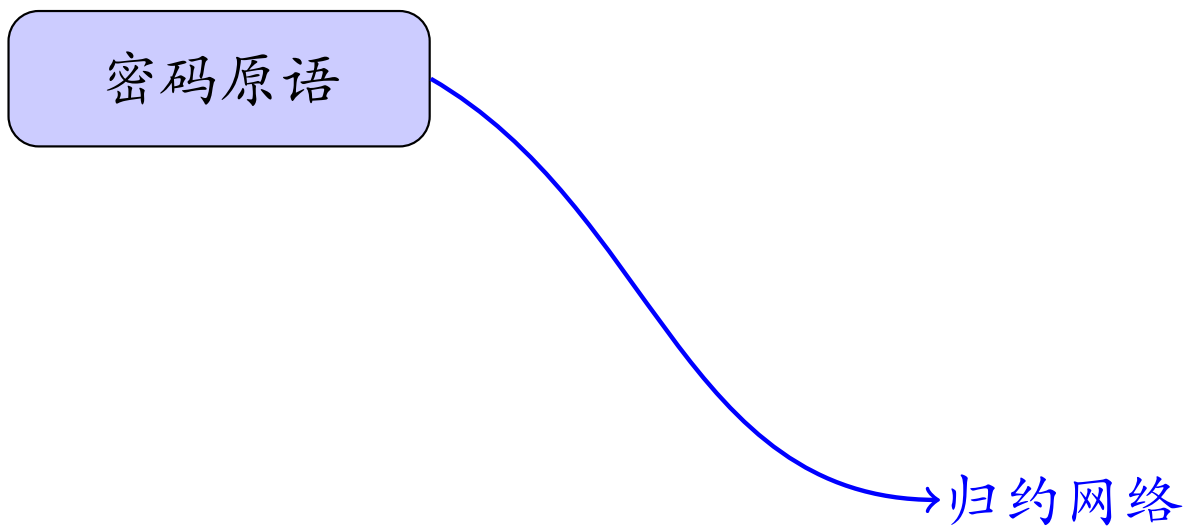
山东大学 网络空间安全学院

提纲

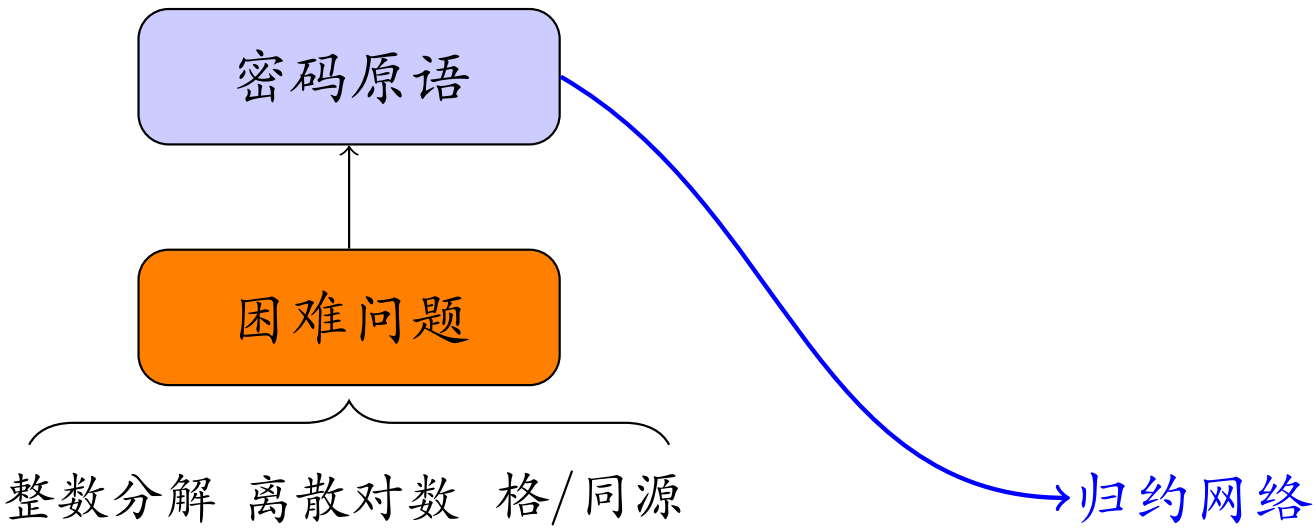
密码学科体系


密码应用
网络认证协议 (SSL, IPSec, SSH), 隐私保护计算...
密码方案/协议
加密, 签名, 密钥交换, 多方安全计算, 零知识证明...
密码原语/工具
(陷门) 单向函数, 伪随机函数, 程序混淆...
数学与复杂性基础
大整数分解类, 离散对数类, 格/同源; $\mathcal{P} =? \mathcal{NP}$

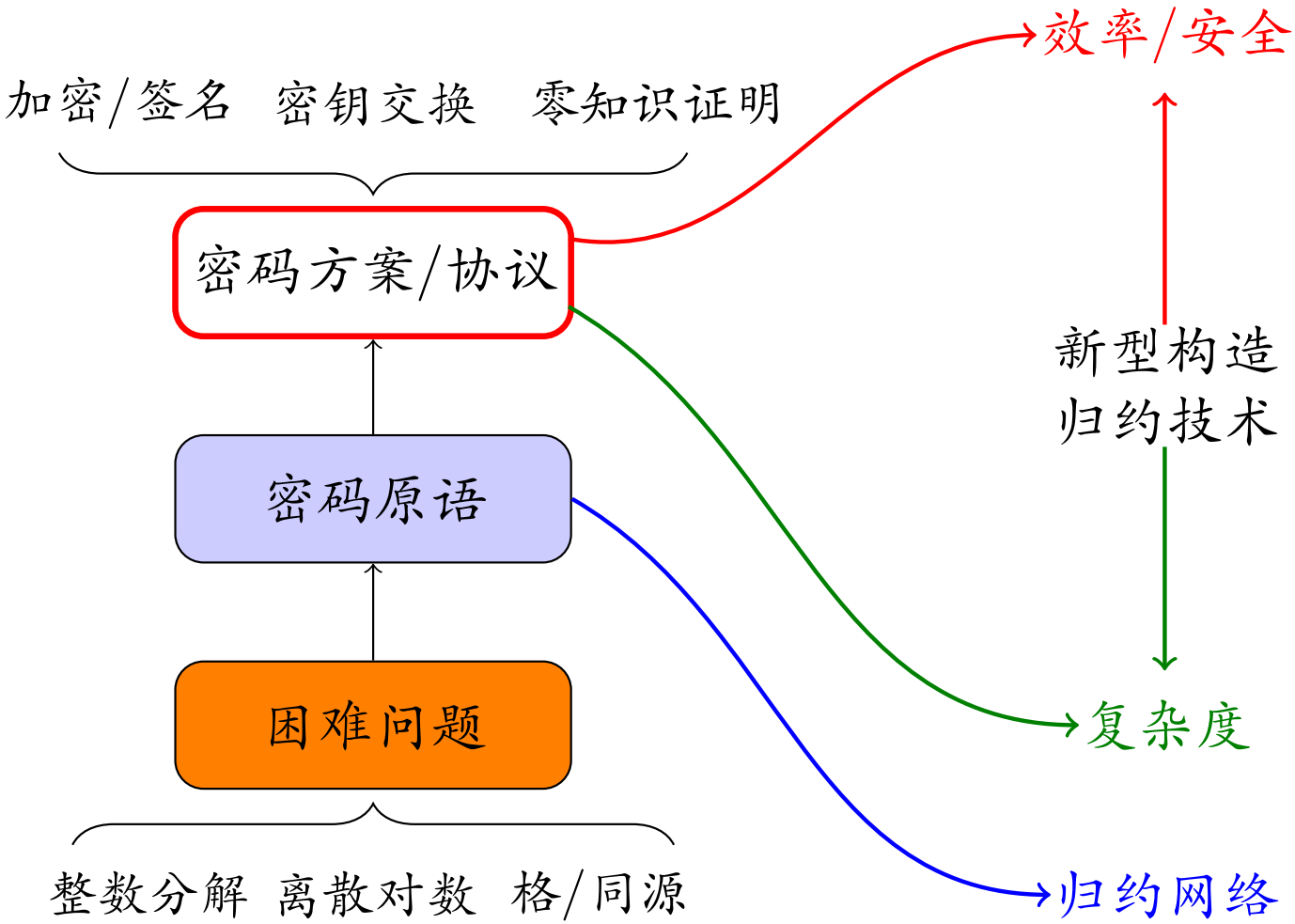
研究方向：理论密码学及应用



研究方向：理论密码学及应用



研究方向：理论密码学及应用



研究方向：理论密码学及应用

高功能 ⇒ 可用不可见

高安全 ⇒ 强安全保护




加密/签名　密钥交换　零知识证明

密码方案/协议

密码原语

困难问题

整数分解　离散对数　格/同源

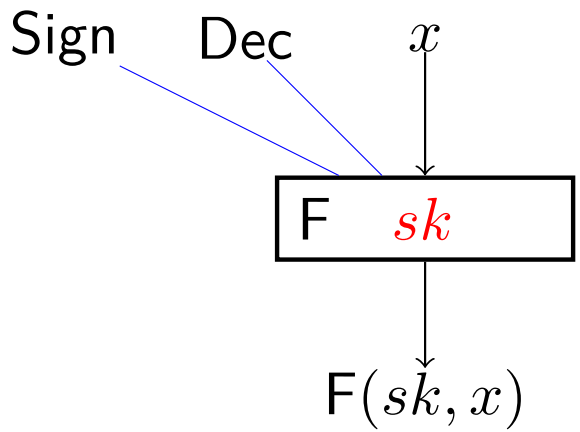
效率/安全

新型构造
归约技术

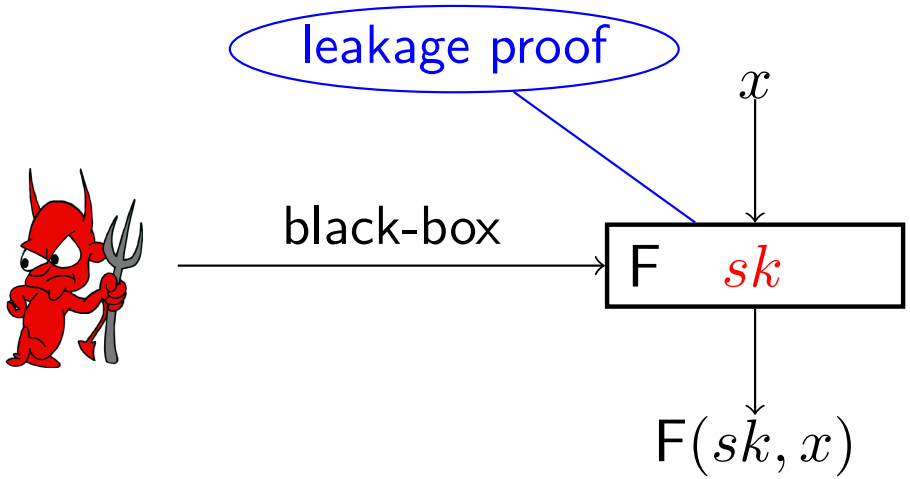
复杂度

归约网络

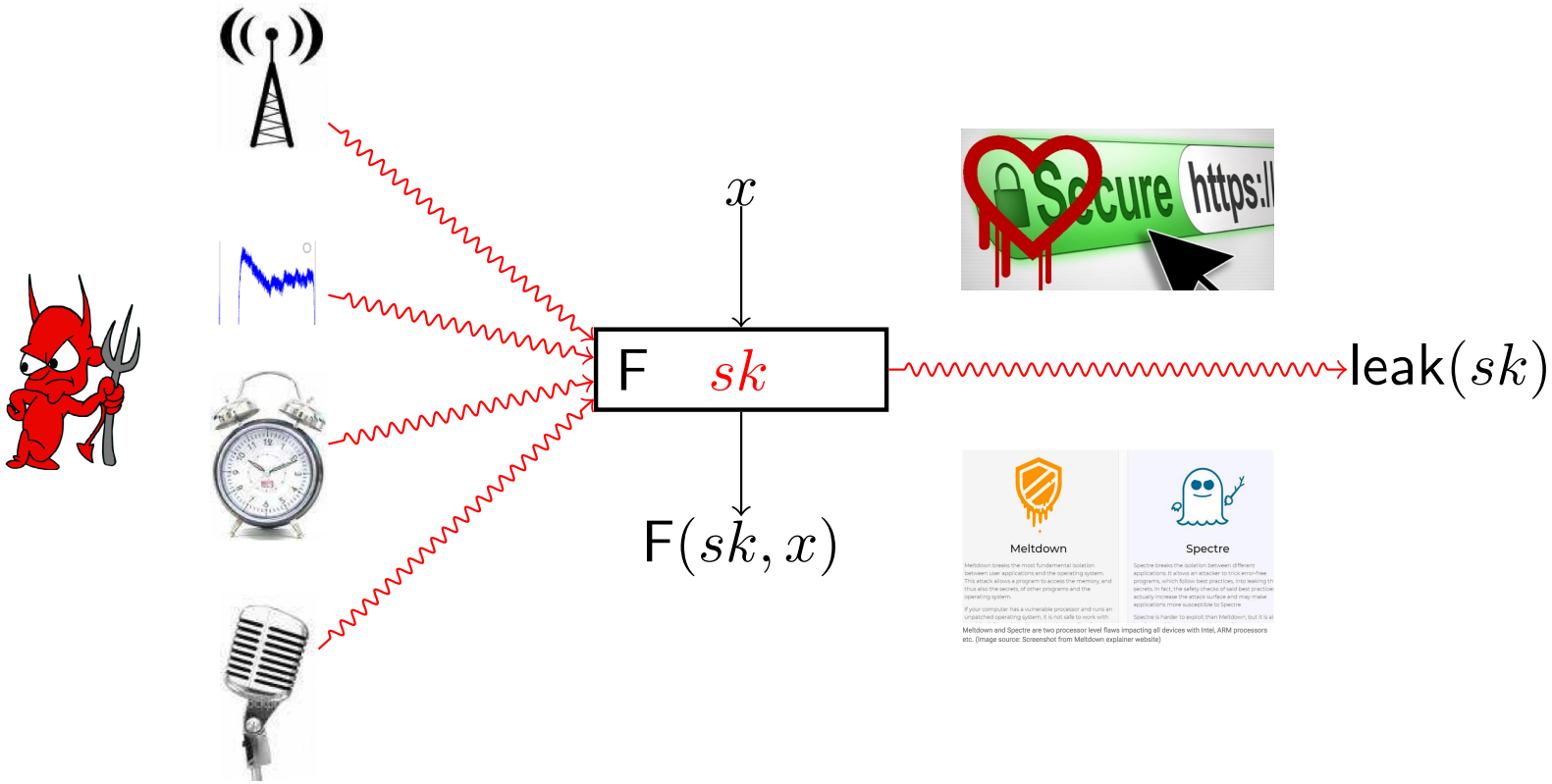
高安全的密码体制



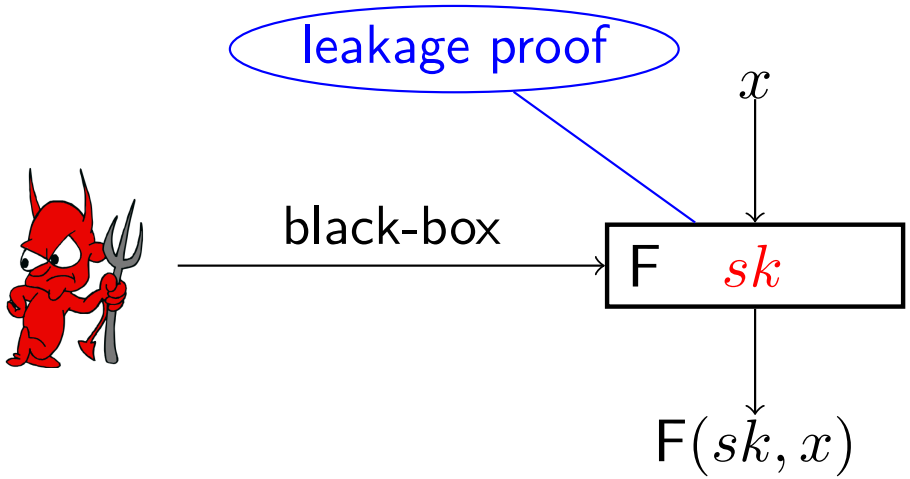
高安全的密码体制



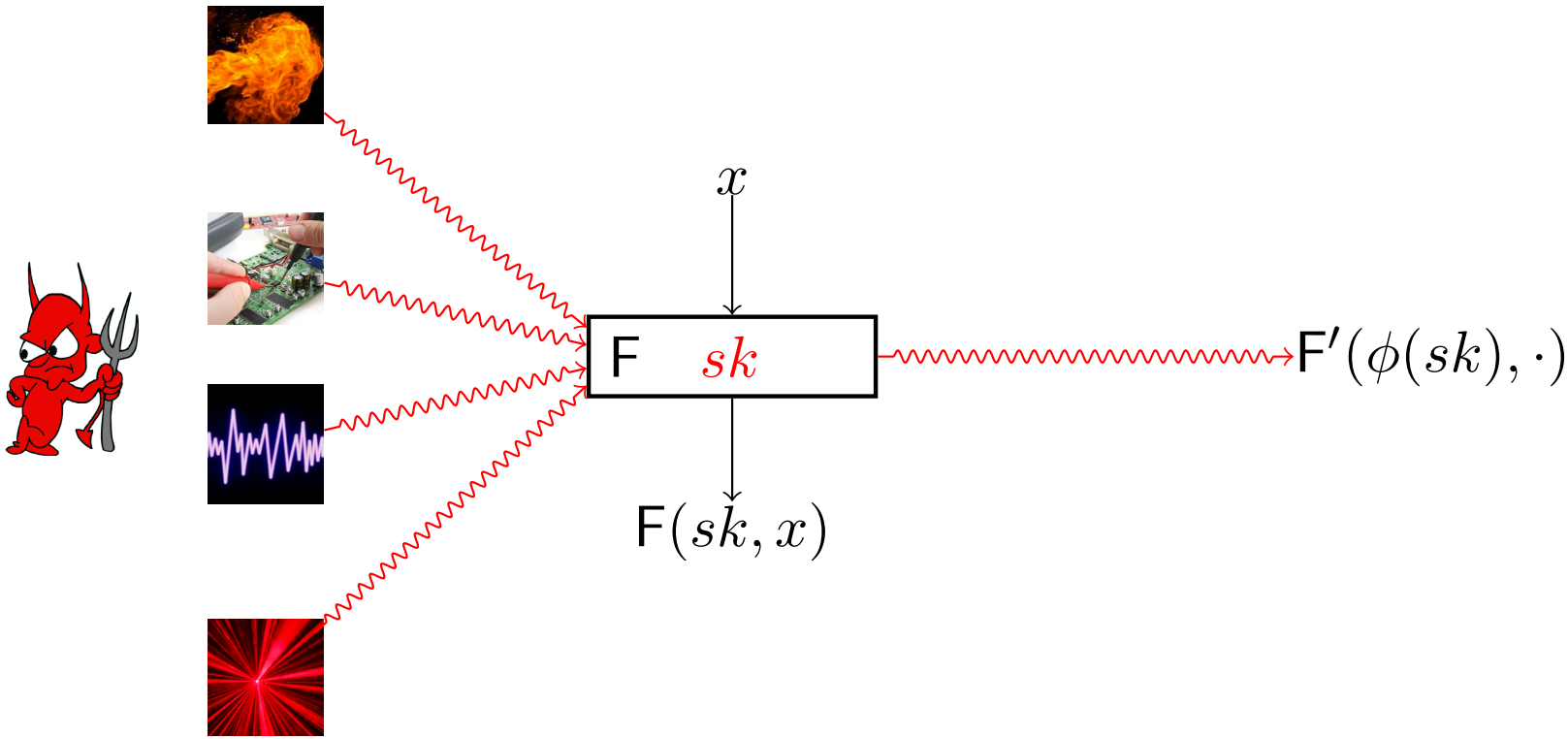
高安全的密码体制


x
F sk
$\mathsf{F}(sk, x)$
leak(sk)
Secure https://
Meltdown
Spectre
Meltdown and Spectre are two processor level flaws impacting all devices with Intel, ARM processors etc. (Image source: Screenshot from Meltdown explainer website)

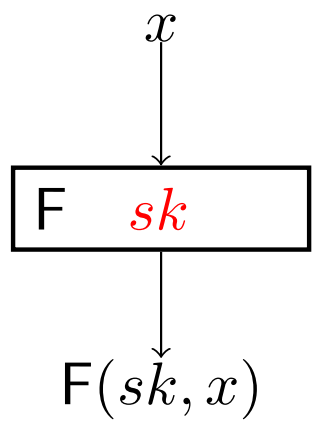
高安全的密码体制



高安全的密码体制



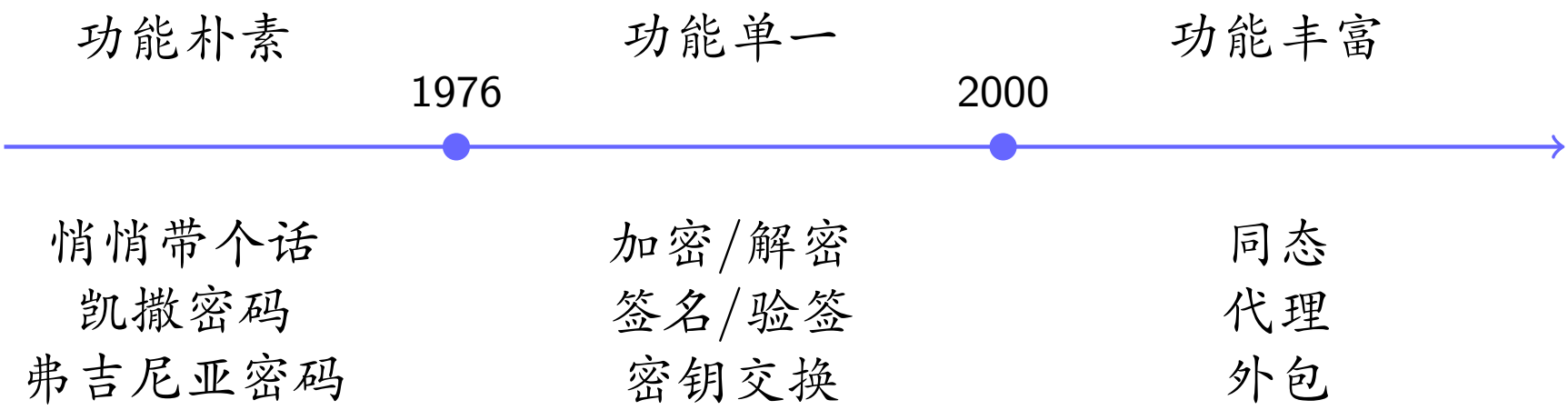
高安全的密码体制



可证明安全的

抗泄漏、抗篡改密钥体制

高功能的密码体制


功能朴素
功能单一
功能丰富
1976
2000
悄悄带个话
凯撒密码
弗吉尼亚密码
加密/解密
签名/验签
密钥交换
同态
代理
外包

高功能的密码体制

功能朴素	功能单一	功能丰富
	1976	2000
悄悄带个话	加密/解密	同态
凯撒密码	签名/验签	代理
弗吉尼亚密码	密钥交换	外包

通信技术发展 $\rightsquigarrow$ 距离变远 (man or dog)

容易建立信任	难以建立信任	很难建立信任

数据的价值在于
计算和流通

高功能的密码体制

功能朴素 | 功能单一 | 功能丰富

1976 | 2000

悄悄带个话 | 加密/解密 | 同态
凯撒密码 | 签名/验签 | 代理
弗吉尼亚密码 | 密钥交换 | 外包

通信技术发展 $\rightsquigarrow$ 距离变远 (man or dog)

容易建立信任 | 难以建立信任 | 很难建立信任

数据的价值在于
计算和流通

高功能密码体制建立可信计算模式 $\Rightarrow$ 数据可用不可见

隐私保护计算

client $\leftrightarrow$ server
client 拥有数据
但计算资源有限

隐私保护计算

黑科技中的黑科技

密态计算

同态加密

函数加密

多方地位对等
各自拥有秘密数据

安全多方计算

全同态加密 (Fully Homomorphic Encryption)

FHE: 对密态数据进行任意计算, 计算结果仍为密态

全同态加密 (Fully Homomorphic Encryption)

FHE: 对密态数据进行任意计算, 计算结果仍为密态

(pk, sk)

全同态加密 (Fully Homomorphic Encryption)

FHE: 对密态数据进行任意计算, 计算结果仍为密态

(pk, sk)

$m_i \longrightarrow$ $c_i = \mathsf{Enc}(pk, m_i)$

全同态加密 (Fully Homomorphic Encryption)

FHE: 对密态数据进行任意计算, 计算结果仍为密态

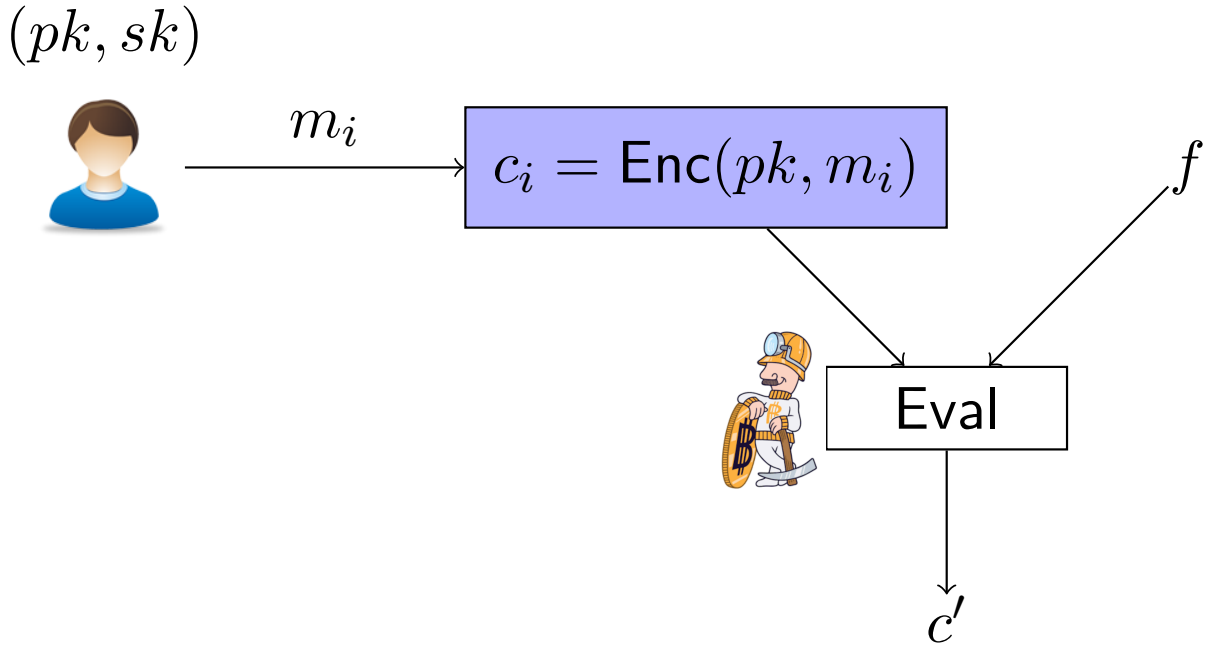
(pk, sk)

m_i → $c_i = \mathsf{Enc}(pk, m_i)$

f

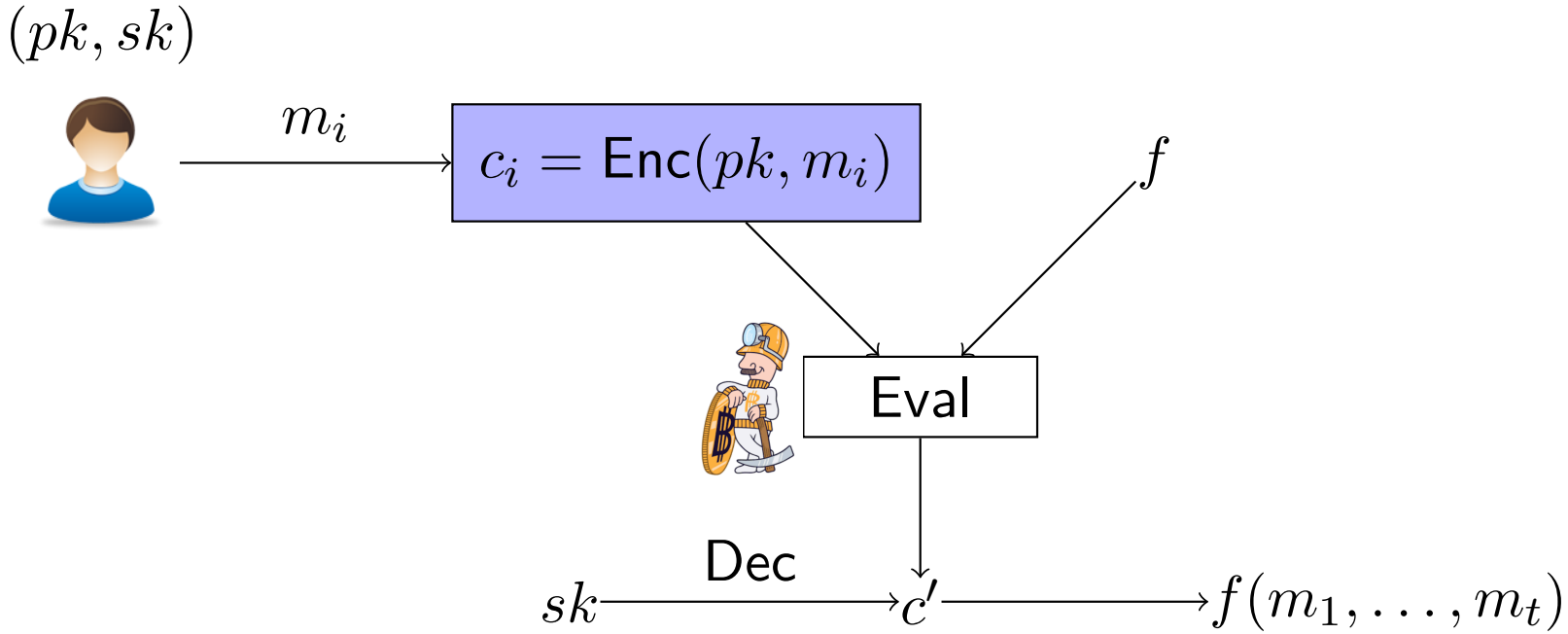
全同态加密 (Fully Homomorphic Encryption)

FHE: 对密态数据进行任意计算, 计算结果仍为密态



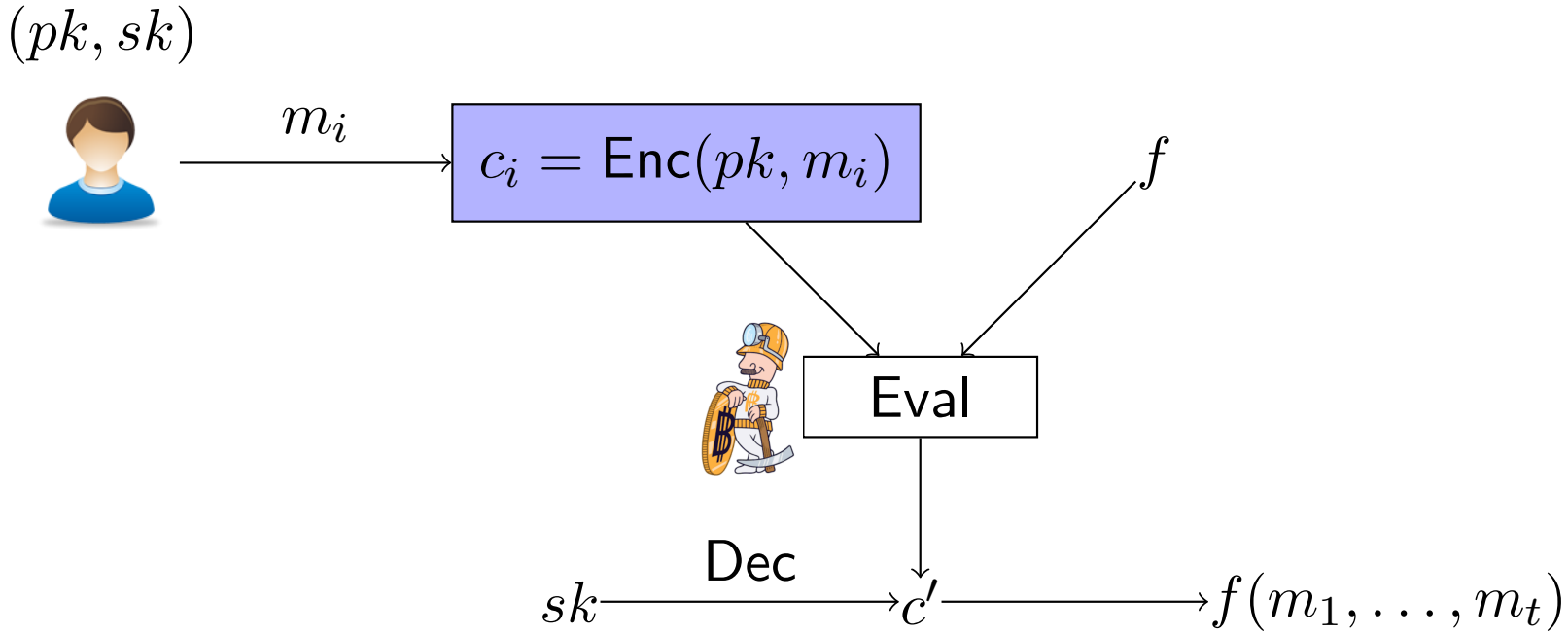
全同态加密 (Fully Homomorphic Encryption)

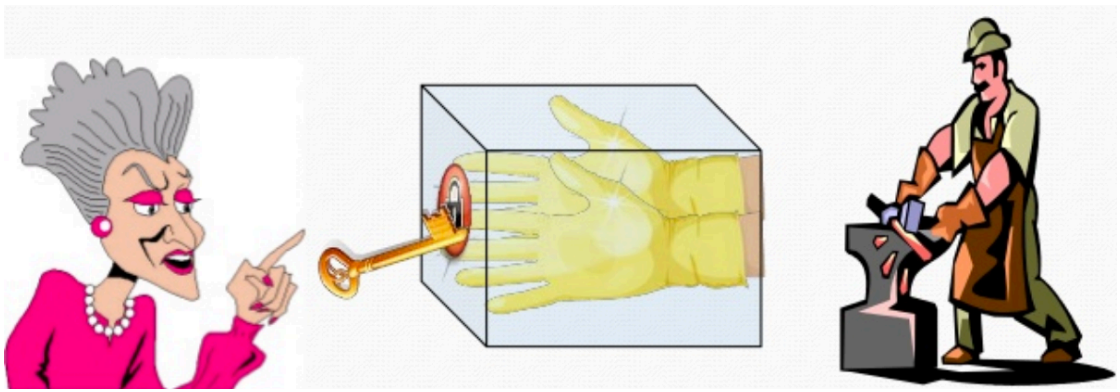
FHE: 对密态数据进行任意计算, 计算结果仍为密态



全同态加密 (Fully Homomorphic Encryption)

FHE: 对密态数据进行任意计算, 计算结果仍为密态





密态计算场景 1

服务器仅完成计算: 计算的输入和输出均为密态

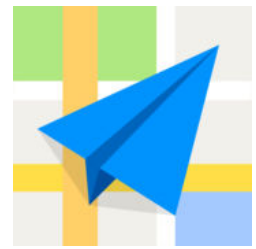
密态计算场景 1

服务器仅完成计算: 计算的输入和输出均为密态

x

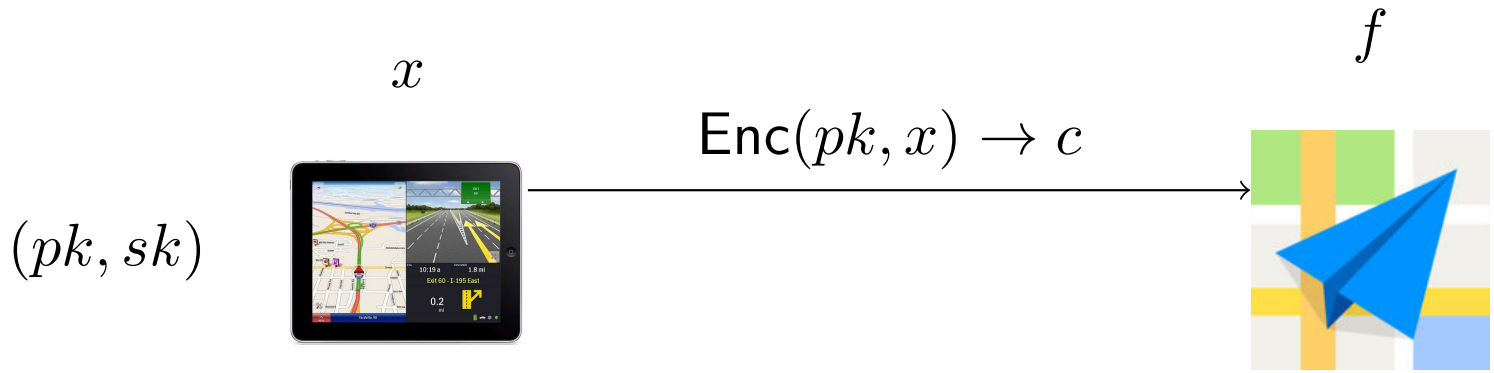
f

(pk, sk)



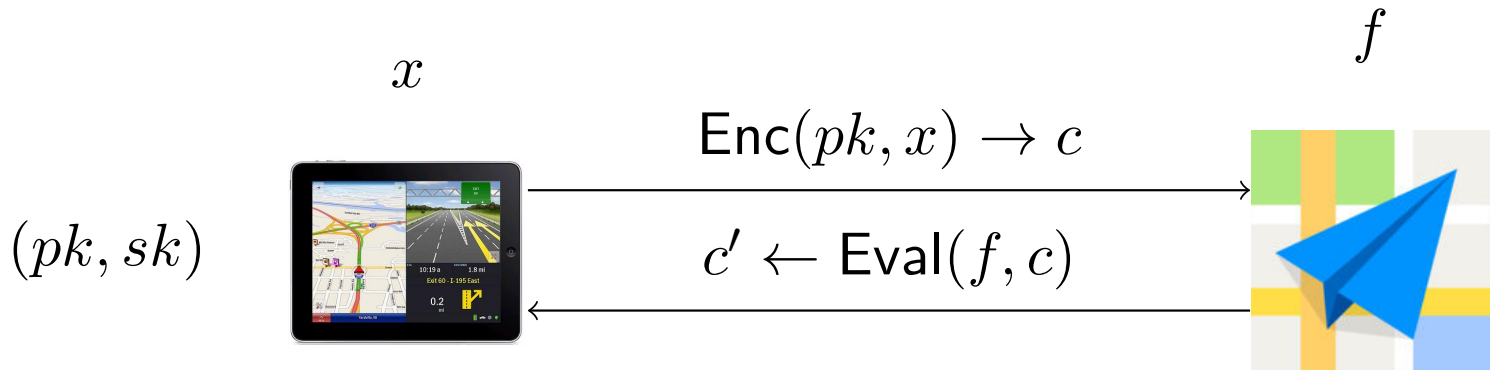
密态计算场景 1

服务器仅完成计算: 计算的输入和输出均为密态



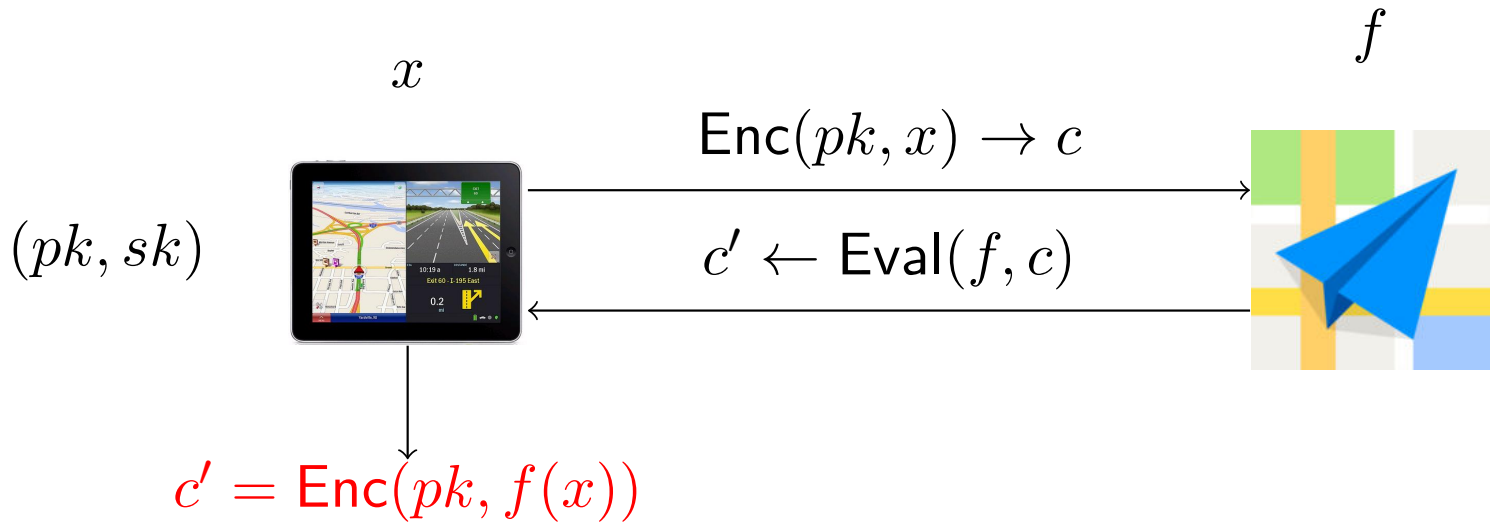
密态计算场景 1

服务器仅完成计算: 计算的输入和输出均为密态



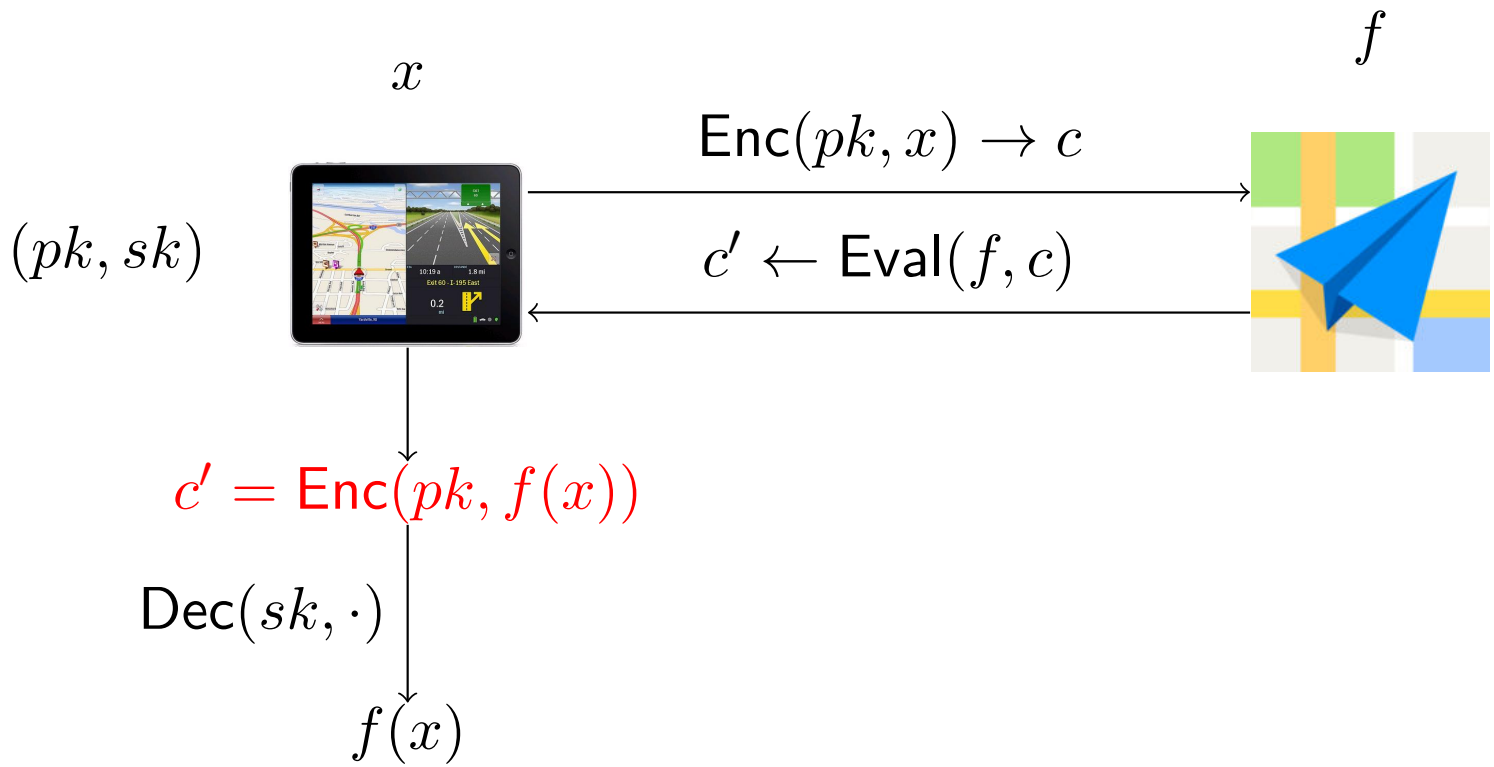
密态计算场景 1

服务器仅完成计算: 计算的输入和输出均为密态



密态计算场景 1

服务器仅完成计算: 计算的输入和输出均为密态



函数加密 (Function Encryption)

FE: 对密态数据进行授权计算, 计算结果为明文

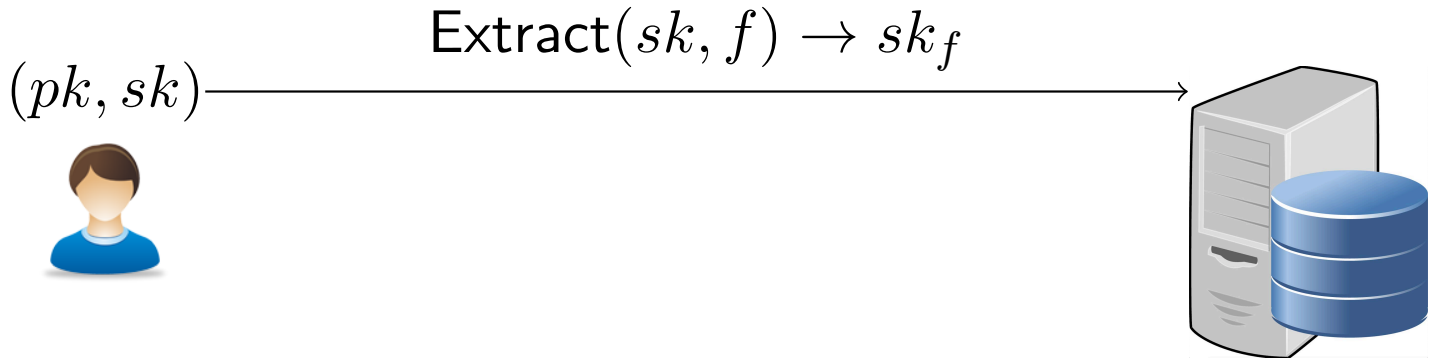
函数加密 (Function Encryption)

FE: 对密态数据进行授权计算, 计算结果为明文

(pk, sk)

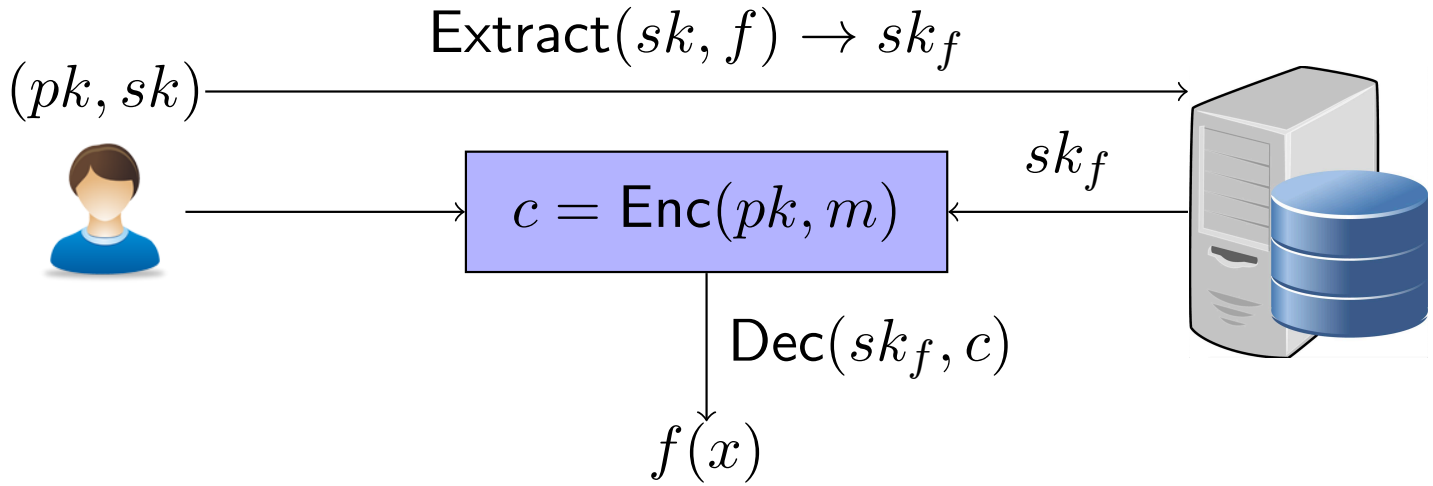
函数加密 (Function Encryption)

FE: 对密态数据进行授权计算, 计算结果为明文



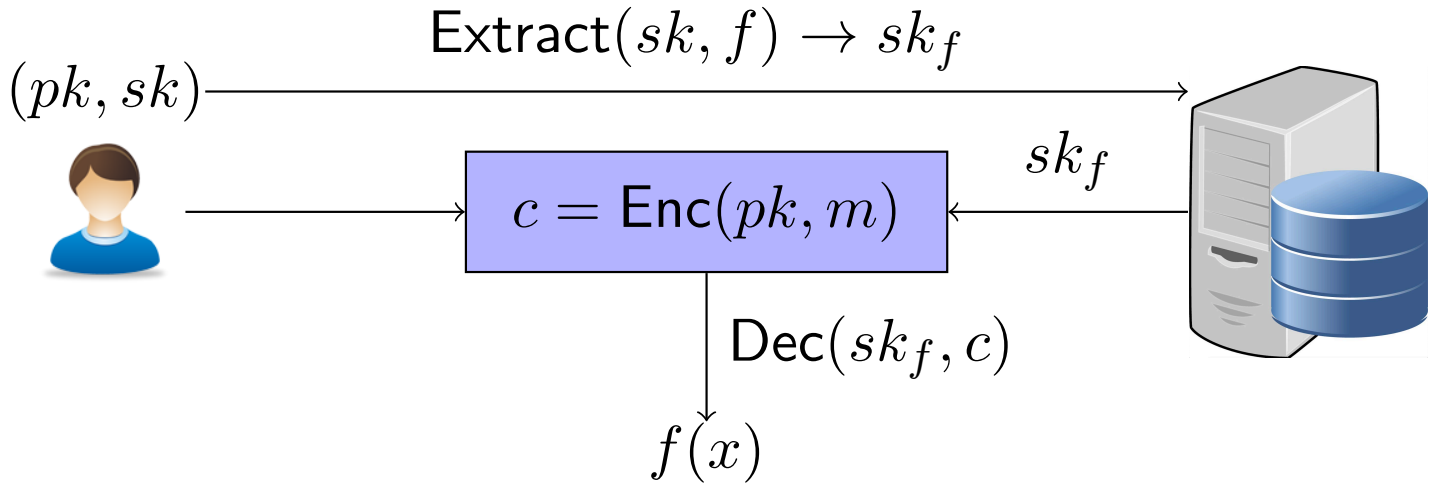
函数加密 (Function Encryption)

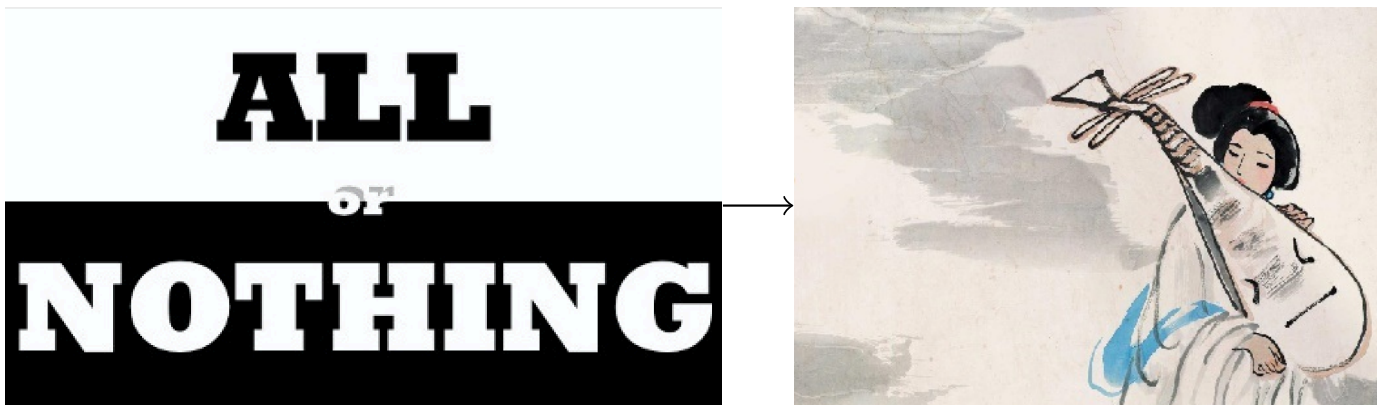
FE: 对密态数据进行授权计算, 计算结果为明文



函数加密 (Function Encryption)

FE: 对密态数据进行授权计算, 计算结果为明文





密态计算场景 2

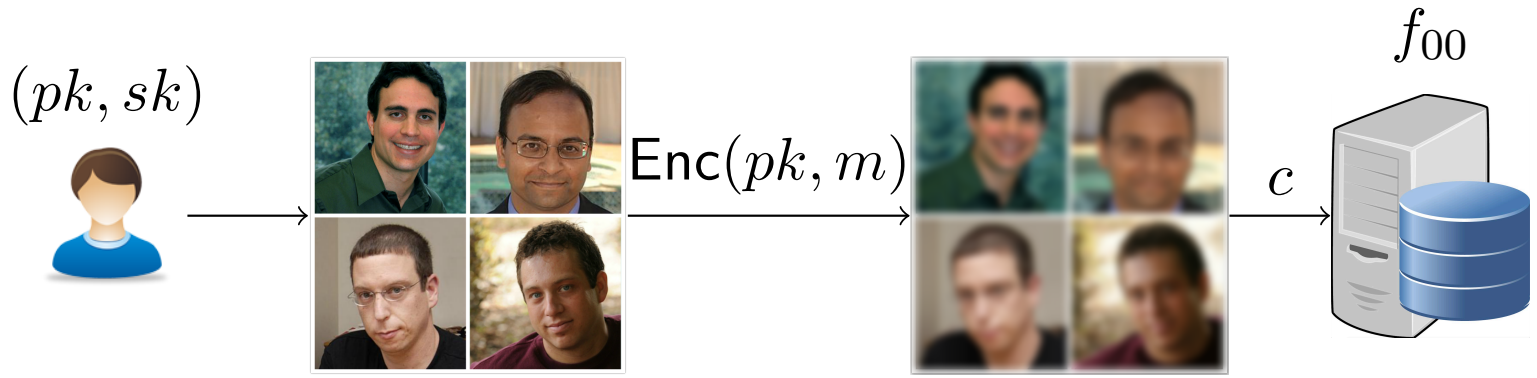
服务器完成计算后进一步根据计算结果进行后续操作: 计算的输入为密态, 输出为明文

(pk, sk)

f_{00}

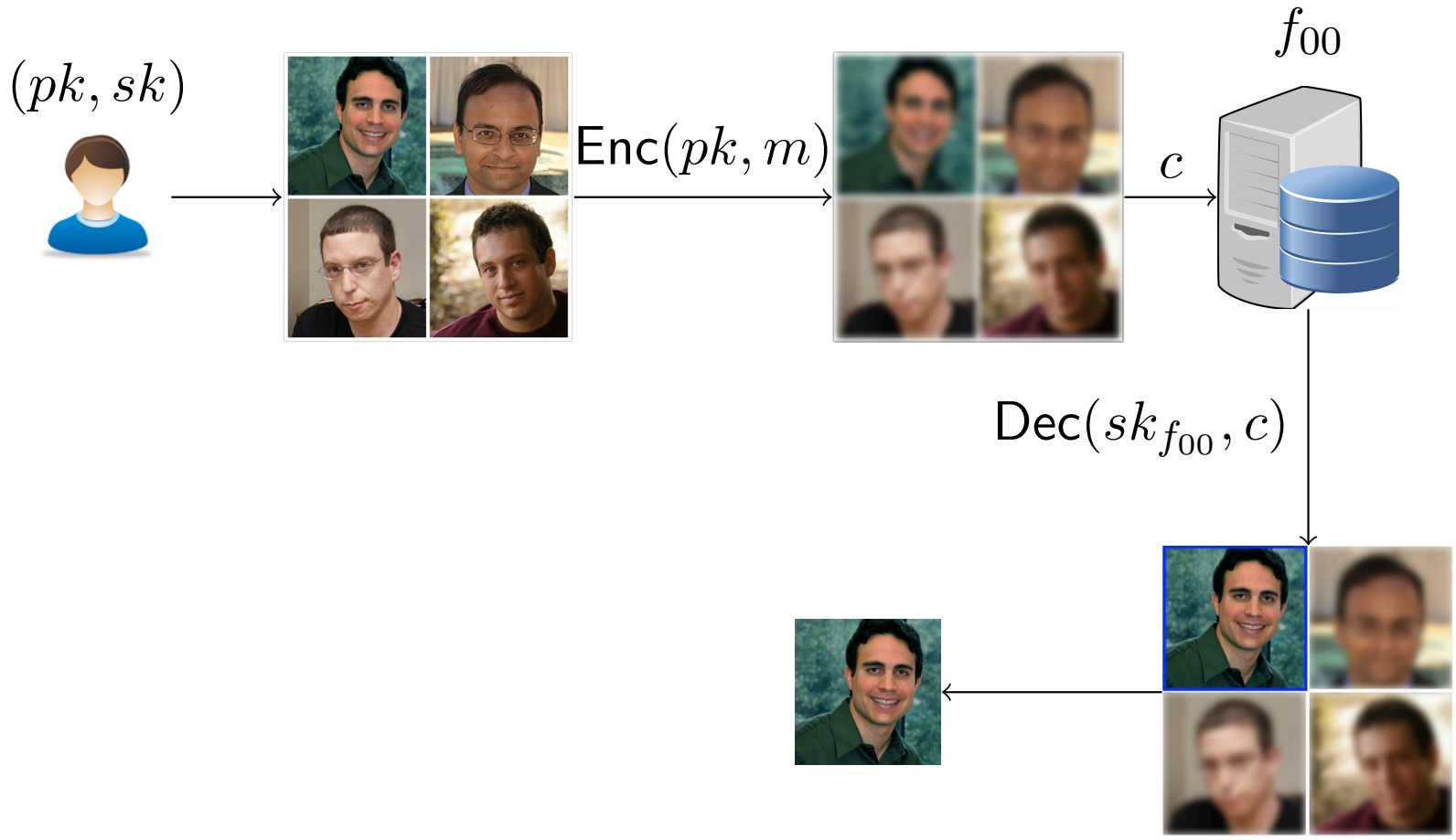
密态计算场景 2

服务器完成计算后进一步根据计算结果进行后续操作：计算的输入为密态，输出为明文



密态计算场景 2

服务器完成计算后进一步根据计算结果进行后续操作：计算的输入为密态，输出为明文



多方安全计算

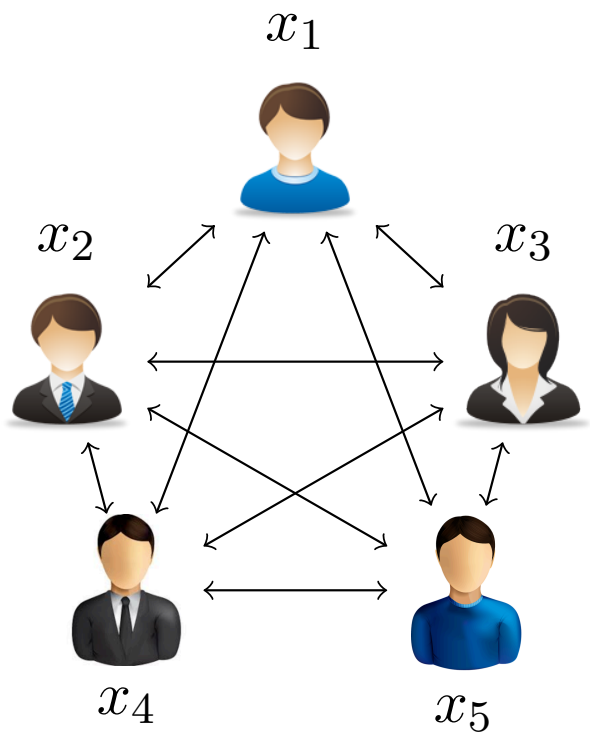
多方各持秘密输入，计算同一个函数；在计算完成后仅知道计算结果

$$f(x_1, \ldots, x_n) = y$$

多方安全计算

多方各持秘密输入，计算同一个函数；在计算完成后仅知道计算结果

$$f(x_1, \ldots, x_n) = y$$



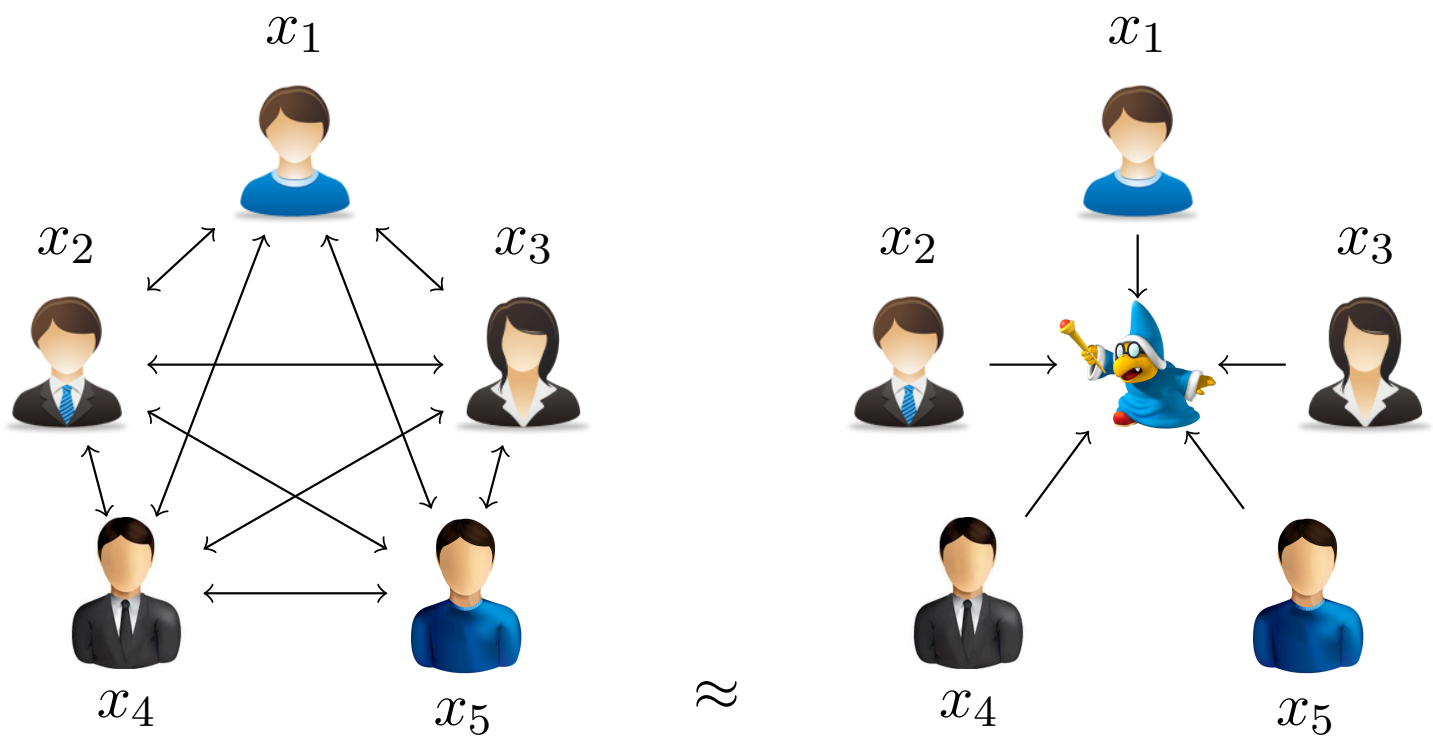
MPC

真实世界

多方安全计算

多方各持秘密输入，计算同一个函数；在计算完成后仅知道计算结果

$$f(x_1, \ldots, x_n) = y$$

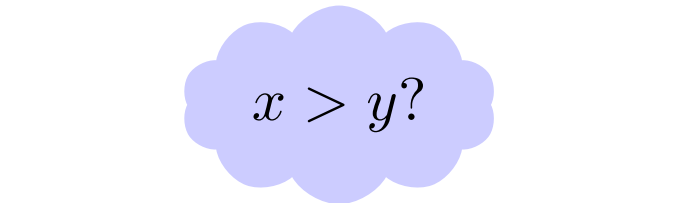


MPC
真实世界

可信第三方存在
理想世界

典型应用

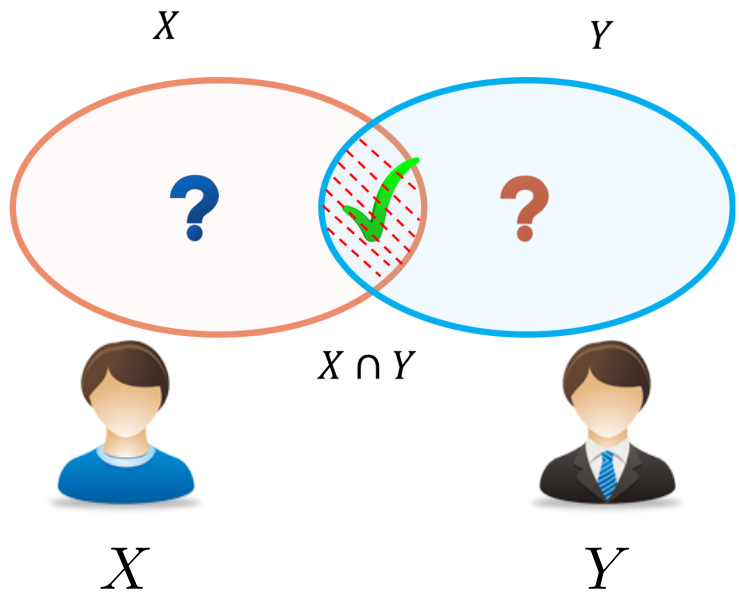
Yao (1982): 百万富翁问题



x

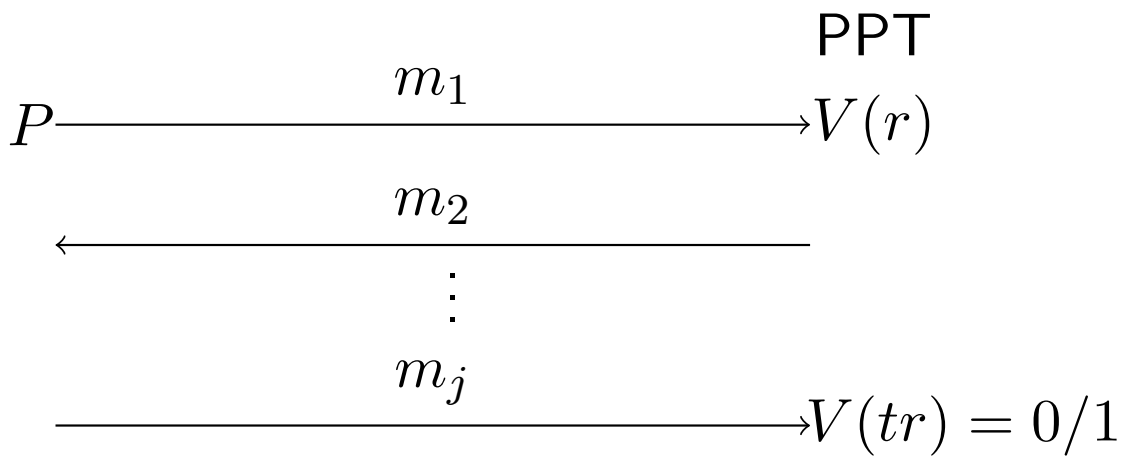
y

隐私集合求交



零知识证明

$$C(x) = y$$



- 完备性: $C(x) = y \Rightarrow \langle P, V \rangle = 1$
- 合理性: $C(x) \neq y \Rightarrow \Pr[\langle P, V \rangle = 1] \leq \mathsf{negl}(\lambda)$
- 零知识: $\langle P, V \rangle \approx S^V$

提纲

背景：区块链科技

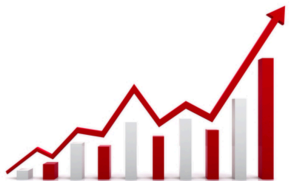
2008

分布式数据平台

核心技术	特性	价值潜力	应用前景
密码学	防篡改抵赖	低成本	数字货币
共识协议	分布式存储	高可信	存证溯源
经济博弈	智能可编程	高安全	供应链金融

重塑信息产业格局，促进信息互联网到价值互联网的演变

背景：区块链科技

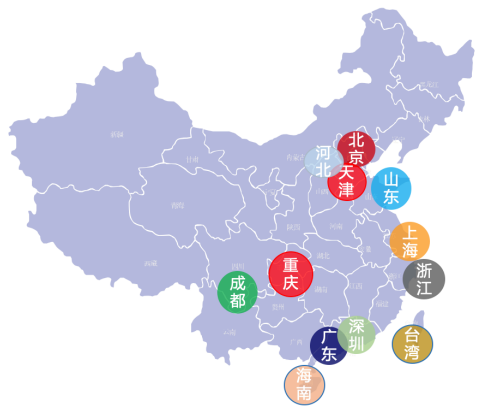


Gartner

连续两年全球
十大科技进展

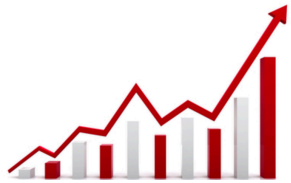
2008 — 2018

产业界	学术界	政府布局
IBM 蚂蚁金服 ANT FINANCIAL Google Baidu 百度 facebook Tencent	美、英、以色列等国顶尖高校成立研究组 + 初创公司 国内清北复交等实验室 + 研究院	100+ 央行开展研究



区块链逐步从概念走向应用，业务规模已达1000 亿美元左右

背景：区块链科技

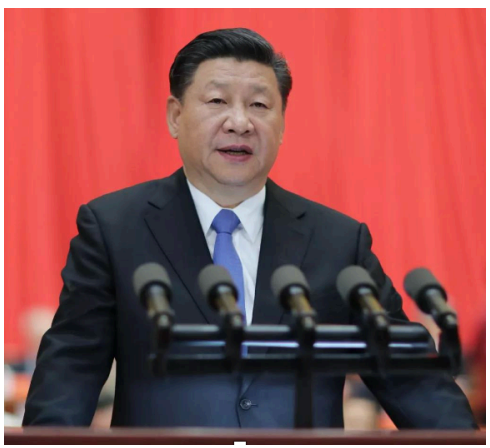


Gartner

连续两年全球
十大科技进展

习总书记
政治局讲话

2008 — 2018 — 2019.10



“区块链技术的集成应用在新的技术革新和产业变革中起着重要作用，要把区块链作为核心技术自主创新的重要突破口，明确主攻方向，加大投入力度，着力攻克一批关键核心技术，加快推动区块链技术和产业创新发展.”

区块链科技源于国家重大需求，是未来经济主战场.
有望成为下一代信息基础设施.

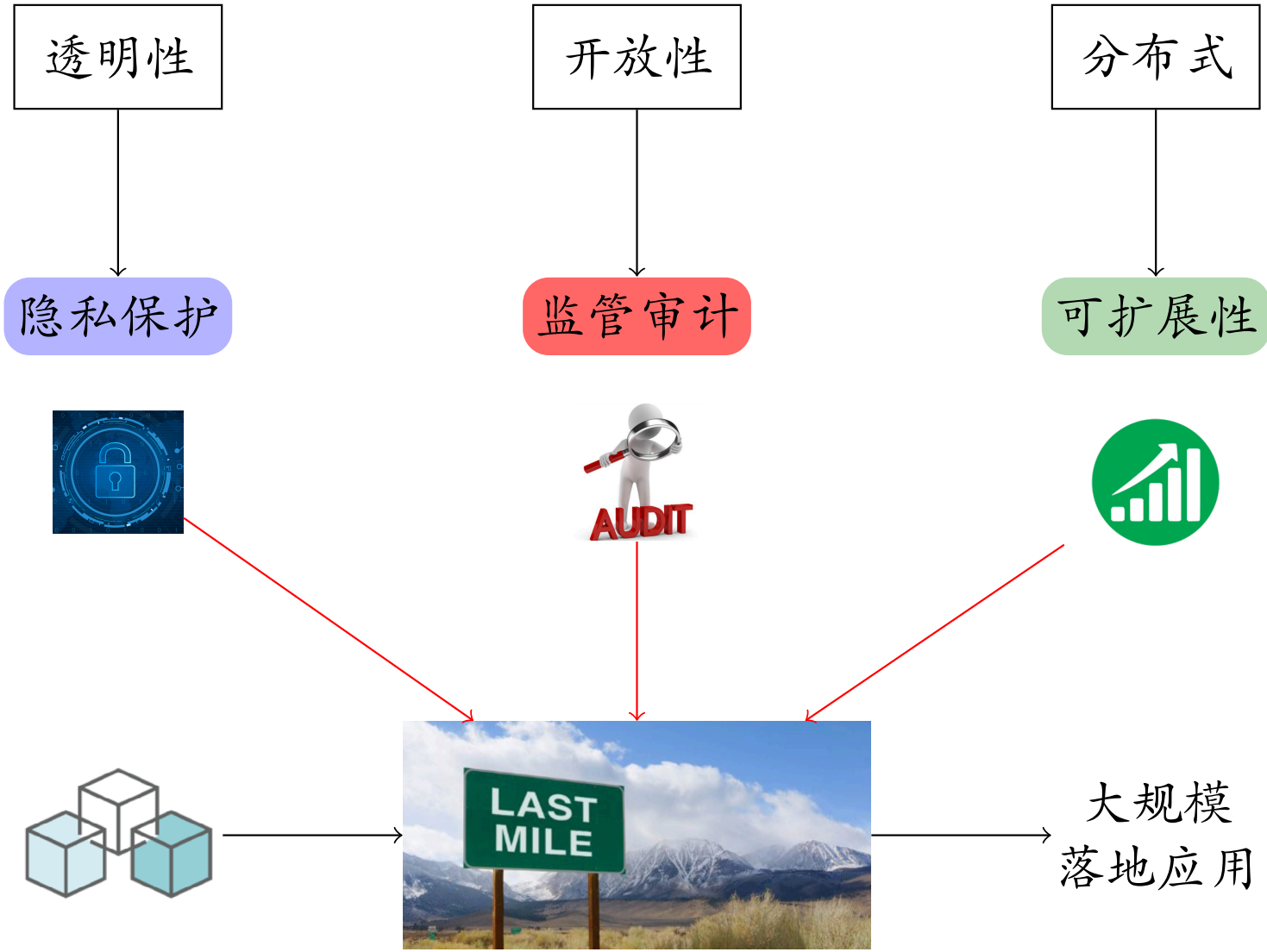
存在的问题

透明性 → 隐私保护

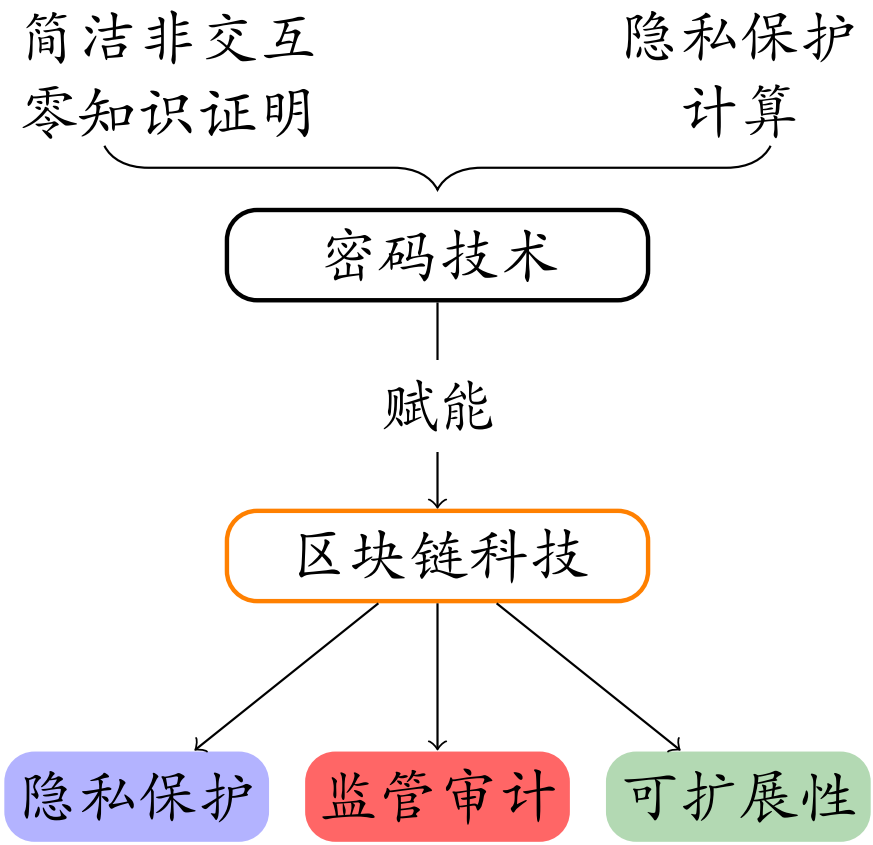
开放性 → 监管审计

分布式 → 可扩展性

存在的问题



研究思路



1. 为用户构建隐私保护层以保护敏感数据安全
2. 为监管方提供抓手接口以确保区块链应用可管可控
3. 为基础设施预设内蕴的扩容机制以支持大规模应用

围绕零知识证明工具链
构建密码组件库
形成“理论-应用”闭环

金融密码: 可监管审计的分布式机密交易系统

首次提出并设计 "可监管审计的分布式机密交易系统 (SDCT)"

- 强安全模型+通用构造框架 + 高效实例化 (C++ 算法库)

本系统 (目前惟一) 同时支持

合规性审计 ∧ 穿透式监管

为金融科技提供了隐私保护与监管审计的共性技术和理论基础

创新性

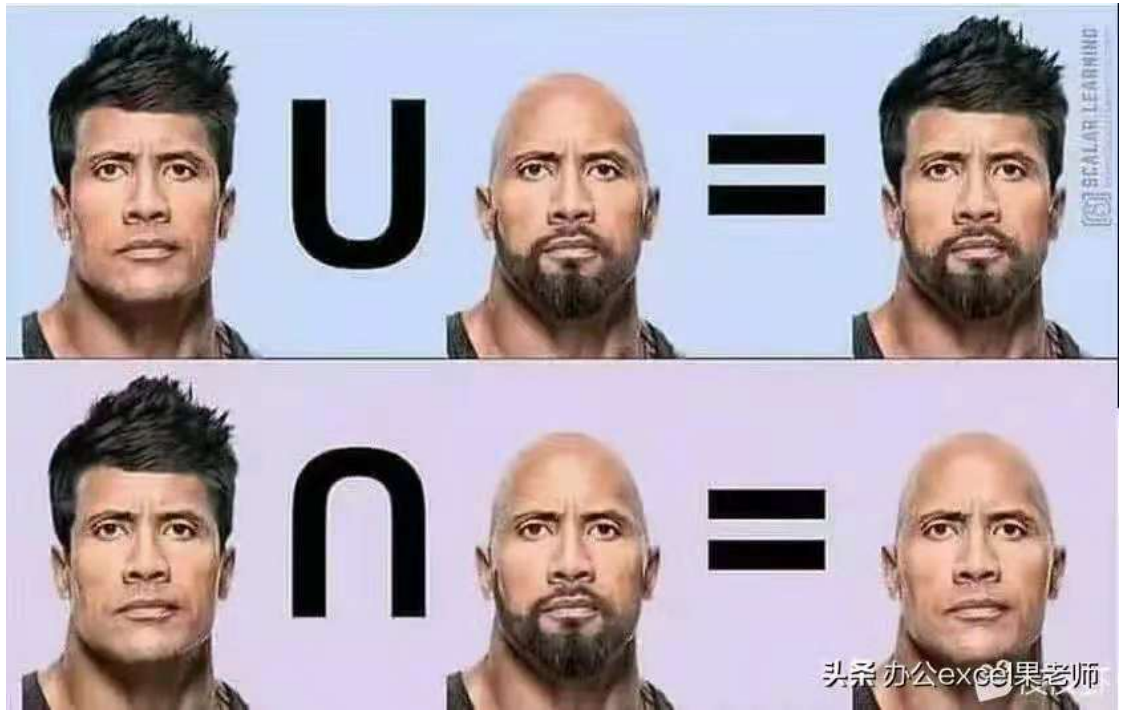
- 理论创新: 推广 Noar-Yung 双重加密范式为三重加密范式

  $\Rightarrow$ **隐私保护前提下实施 "穿透式监管" 的通用方法**

- 技术创新: 提出了零知识证明友好的新型同态加密算法 + 隐式签名技巧

全国 205 支队伍中脱颖而出，获得首届金融密码杯创新赛一等奖
(全国共 3 项)

隐私集合运算



阶段性进展

- 提出可交换弱伪随机性函数和批处理反向成员测试协议, 给出构造 PSO 协议的统一框架
- 同时给出了首个同时具备线性计算复杂度和线性通信复杂度的 PSU 协议.

欢迎加入

希望你

- 积极主动
- 思维严谨、善于思考
- 喜欢“理论 + 实践”
- 具有良好的数学素养

你将

- 具备坚实的理论密码学基础
- 了解真实业界应用，学以致用

涂昌苑 D 座 0324

https://yuchen1024.github.io