新世纪加密术：基于和超越身份

王励成
wanglc2012@126.com

北京邮电大学网络空间安全学院

二零一八年一月

提纲

- 历史回顾：从私钥加密到公钥加密
- 基于身份加密（IBE）：Shamir的构思
- 超越身份加密：HIBE/FIBE/ABE/FE/SE/FHE
- 公钥认证框架可否基于区块链？

历史回顾：从私钥加密到公钥加密

- 私钥加密
  -
  -
  -
  -
- 公钥加密
  -
  -
  -
  -
  -

历史回顾：从私钥加密到公钥加密

- 私钥加密
  - 加密、解密用同一密钥
  -
  -
  -
- 公钥加密
  - 加密用公钥、解密用私钥
  -
  -
  -
  -

历史回顾：从私钥加密到公钥加密

- 私钥加密
  - 加密、解密用同一密钥
  - 安全信道：密钥经过“认证 + 保密”信道秘密传输
  -
  -
- 公钥加密
  - 加密用公钥、解密用私钥
  - 认证信道：公钥经过“认证”信道公开传输
    （私钥保密且无需传输）
  -
  -
  -

历史回顾：从私钥加密到公钥加密

- 私钥加密
  - 加密、解密用同一密钥
  - 安全信道：密钥经过“认证 + 保密”信道秘密传输
  - n 个用户之间实现两两保密通信：需要 $O(n^2)$ 密钥
  -
- 公钥加密
  - 加密用公钥、解密用私钥
  - 认证信道：公钥经过“认证”信道公开传输
    （私钥保密且无需传输）
  - n 个用户之间实现两两保密通信：需要 $O(n)$ 密钥
  -
  -

历史回顾：从私钥加密到公钥加密

- 私钥加密
  - 加密、解密用同一密钥
  - 安全信道：密钥经过“认证 + 保密”信道秘密传输
  - n 个用户之间实现两两保密通信：需要 $O(n^2)$ 密钥
  - 信任基础：发方、收方需要互相完全信任
- 公钥加密
  - 加密用公钥、解密用私钥
  - 认证信道：公钥经过“认证”信道公开传输
    （私钥保密且无需传输）
  - n 个用户之间实现两两保密通信：需要 $O(n)$ 密钥
  - 信任基础：发方只需要相信收发公钥的真实性——需要PKI

历史回顾：从私钥加密到公钥加密

- 私钥加密：密钥分发需要安全信道
  - 加密、解密用同一密钥
  - 安全信道：密钥经过“认证 + 保密”信道秘密传输
  - n 个用户之间实现两两保密通信：需要 $O(n^2)$ 密钥
  - 信任基础：发方、收方需要互相完全信任

- 公钥加密：密钥分发需要认证信道
  - 加密用公钥、解密用私钥
  - 认证信道：公钥经过“认证”信道公开传输
    （私钥保密且无需传输）
  - n 个用户之间实现两两保密通信：需要 $O(n)$ 密钥
  - 信任基础：发方只需要相信收发公钥的真实性——需要PKI

  - PKI：TTP，证书生成、发布、回收、维护

传统PKI的工作模式

- 理想三步曲
  - 1. 用户选择私钥 sk——随机数！
  - 2. $sk \xrightarrow{OW\ \ f} pk$
  - 3. $(pk, id) \xrightarrow{\sigma_{CA}} Cert$

传统PKI的工作模式

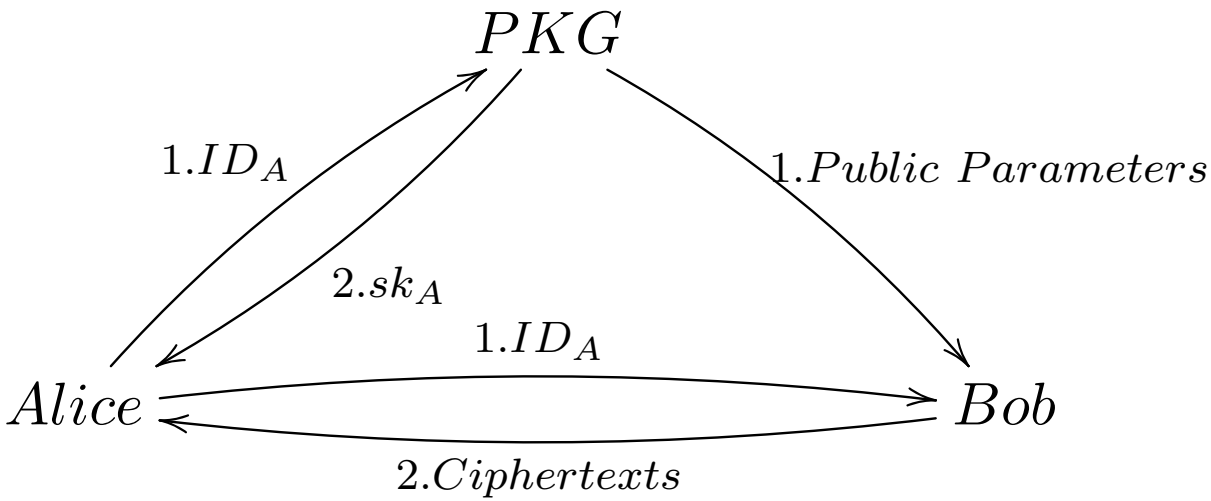
- 理想三步曲
  - 1. 用户选择私钥 sk——随机数！
  - 2. $sk \xrightarrow{OW\ \ f} pk$
  - 3. $(pk, id) \xrightarrow{\sigma_{CA}} Cert$
- 现实简化版
  - 1. CA 替用户选择私钥 sk——随机数！
  - 2. $sk \xrightarrow{OW\ \ f} pk$
  - 3. $(pk, id) \xrightarrow{\sigma_{CA}} Cert$

基于身份加密（IBE）：Shamir 的构思

- 目的：简化公钥证书管理
- 特点：任何标识串均可以作为公钥

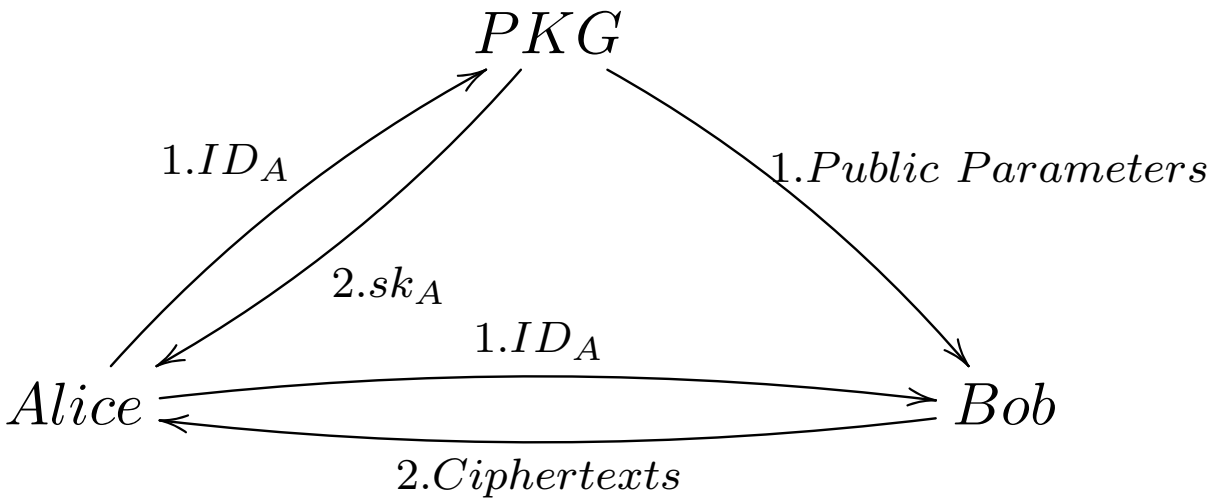
基于身份加密（IBE）：Shamir 的构思

- 目的：简化公钥证书管理
- 特点：任何标识串均可以作为公钥
- 基于身份加密（Identity-Based Encryption，IBE）的流程



基于身份加密（IBE）：Shamir 的构思

- 目的：简化公钥证书管理
- 特点：任何标识串均可以作为公钥
- 基于身份加密（Identity-Based Encryption，IBE）的流程



- 派生特性与应用：隐式证书、密钥演化、时间胶囊，等等

十七年的探索

- 实现IBE的难点
- 几乎被遗忘的探索
  - 1987: K. Koyama & K. Ohta, CRYPTO'87
  - 1989: G.G. Gunther, EUROCRYPT'89
  - 1989: E. Okamoto & Tanaka, JSAC'89
  - 1989: S. Tsujii & T. Itoh, JSAC'89
  - 1990: T. Okamoto & K. ohta, CRYPTO'90
  - 1991–1996: Maurer & Yacobi, EUROCRYPT'91'92,DCC'96
  - .....
- 1997: 南湘浩的CPK密码系统
- 破冰恰逢新世纪
  - 2000: Sakai, Ohgishi & Kasahara: ID-NIKD
  - 2001： Boneh & Franklin: 基于Weil配对的IBE
  - 2001： Cocks 基于二次剩余的IBE

实现IBE的难点

公私钥产生和认证流程发生改变：

- 传统PKI
  1. $sk \xrightarrow{OW \quad f} pk$：易
  2. $(pk, id) \xrightarrow{\sigma_{CA}} Cert$：易
  3. $dec(sk, enc(pk, m)) = m$：较容易，f 为单向陷门足以

实现IBE的难点

公私钥产生和认证流程发生改变：

- 传统PKI
  1. $sk \xrightarrow{OW\ \ f} pk$：易
  2. $(pk, id) \xrightarrow{\sigma_{CA}} Cert$：易
  3. $dec(sk, enc(pk, m)) = m$：较容易，f 为单向陷门足以

- IBE
  1. $id \xrightarrow{msk} sk_{id}$：易
  2. $\{sk_{id}\} \not\Rightarrow msk$：较易，但需谨慎
  3. $dec(sk_{id}, enc(id, m)) = m$：难！无陷门可利用

破冰恰逢新世纪：配对篇

- SOK00方案：基于身份的非交互式密钥分发
  - PKG设置：选择 s
  - PKG为用户提取私钥：$sk_{id_A} = sH_1(id_A), sk_{id_B} = sH_1(id_B)$
  - 两用户计算共享密钥：

$$K_{AB} = H_2(e(sk_{id_A}, H_1(id_B))) = H_2(e(sk_{id_B}, H_1(id_A))) = K_{BA}$$

破冰恰逢新世纪：配对篇

- SOK00方案：基于身份的非交互式密钥分发
  - PKG设置：选择 s
  - PKG为用户提取私钥：$sk_{id_A} = sH_1(id_A), sk_{id_B} = sH_1(id_B)$
  - 两用户计算共享密钥：

$$K_{AB} = H_2(e(sk_{id_A}, H_1(id_B))) = H_2(e(sk_{id_B}, H_1(id_A))) = K_{BA}$$

- BF01方案：基于身份的加密
  - PKG设置：选择 s 和 P，计算并公开 $P_{pub} = sP$
  - PKG为用户提取私钥：$sk_{id} = sH_1(id)$
  - 加密：$C_1 = rP, C_2 = m \oplus H_2(e(rH_1(id), P_{pub}))$
  - 解密：$m = H_2(e(sk_{id}, C_1)) \oplus C_2$

$$\text{SOK00} \overset{?}{\approx} \text{BF01}$$

破冰恰逢新世纪：二次剩余篇

C. Cocks @ CC01: An Identity-Based Encryption Based on Quadratic Residues.

- PKG设置：$n = pq$, 哈希函数 h
- PKG为用户提取私钥：$sk_{id}^2 = h(id)$ 或者$sk_{id}^2 = -h(id)$

破冰恰逢新世纪：二次剩余篇

C. Cocks @ CC01: An Identity-Based Encryption Based on Quadratic Residues.

- PKG设置：$n = pq$, 哈希函数 h
- PKG为用户提取私钥：$sk_{id}^2 = h(id)$ 或者$sk_{id}^2 = -h(id)$
- 加密：$c_1 = r_1 + h(id)/r_1, c_2 = r_2 - h(id)/r_2$,
  其中，$\left(\frac{r_1}{n}\right) = \left(\frac{r_2}{n}\right) = m \in \{1, -1\}$

破冰恰逢新世纪：二次剩余篇

C. Cocks @ CC01: An Identity-Based Encryption Based on Quadratic Residues.

- PKG设置：$n = pq$, 哈希函数 h
- PKG为用户提取私钥：$sk_{id}^2 = h(id)$ 或者 $sk_{id}^2 = -h(id)$
- 加密：$c_1 = r_1 + h(id)/r_1, c_2 = r_2 - h(id)/r_2$,
  其中，$\left(\frac{r_1}{n}\right) = \left(\frac{r_2}{n}\right) = m \in \{1, -1\}$
- 解密：$m \leftarrow \left(\frac{c+2\cdot sk_{id}}{n}\right)$,
  其中，$c = c_1$ 如果 $sk_{id}^2 = h(id)$；否则，$c = c_2$.

破冰恰逢新世纪：二次剩余篇

C. Cocks @ CC01: An Identity-Based Encryption Based on Quadratic Residues.

- PKG设置：$n = pq$, 哈希函数 h
- PKG为用户提取私钥：$sk_{id}^2 = h(id)$ 或者 $sk_{id}^2 = -h(id)$
- 加密：$c_1 = r_1 + h(id)/r_1, c_2 = r_2 - h(id)/r_2$,
  其中，$\left(\frac{r_1}{n}\right) = \left(\frac{r_2}{n}\right) = m \in \{1, -1\}$
- 解密：$m \leftarrow \left(\frac{c+2\cdot sk_{id}}{n}\right)$,
  其中，$c = c_1$ 如果 $sk_{id}^2 = h(id)$；否则，$c = c_2$.
- 特点：逐比特加密，密文扩展因子大：$\ell \mapsto 2\ell \cdot \log N$

破冰恰逢新世纪：二次剩余篇

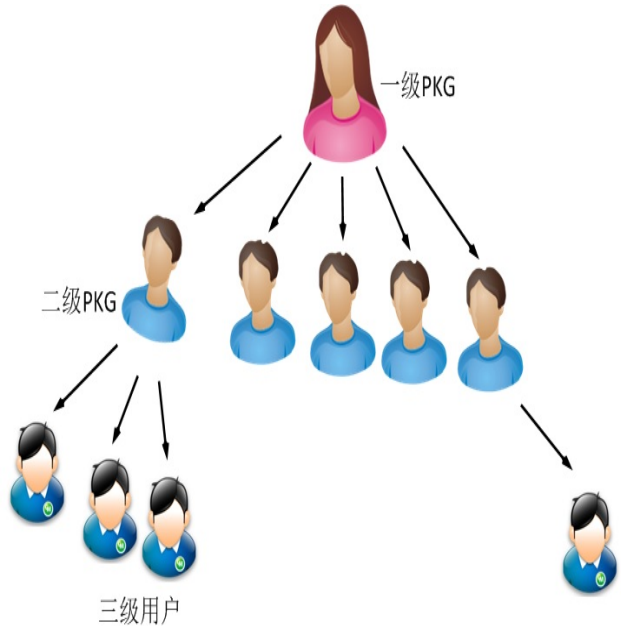
C. Cocks @ CC01: An Identity-Based Encryption Based on Quadratic Residues.

- PKG设置：$n = pq$, 哈希函数 h
- PKG为用户提取私钥：$sk_{id}^2 = h(id)$ 或者 $sk_{id}^2 = -h(id)$
- 加密：$c_1 = r_1 + h(id)/r_1, c_2 = r_2 - h(id)/r_2$,
  其中，$\left(\frac{r_1}{n}\right) = \left(\frac{r_2}{n}\right) = m \in \{1, -1\}$
- 解密：$m \leftarrow \left(\frac{c+2\cdot sk_{id}}{n}\right)$,
  其中，$c = c_1$ 如果 $sk_{id}^2 = h(id)$；否则，$c = c_2$.
- 特点：逐比特加密，密文扩展因子大：$\ell \mapsto 2\ell \cdot \log N$

- Boneh-Gentry-Hamburg（FOCS'07）的改进：$\ell \mapsto 1 + \ell + \log N$

超越身份

- 层次型IBE（HIBE）
  - 上级PKG可为下级PKG提取私钥
  - 适合层次型组织架构

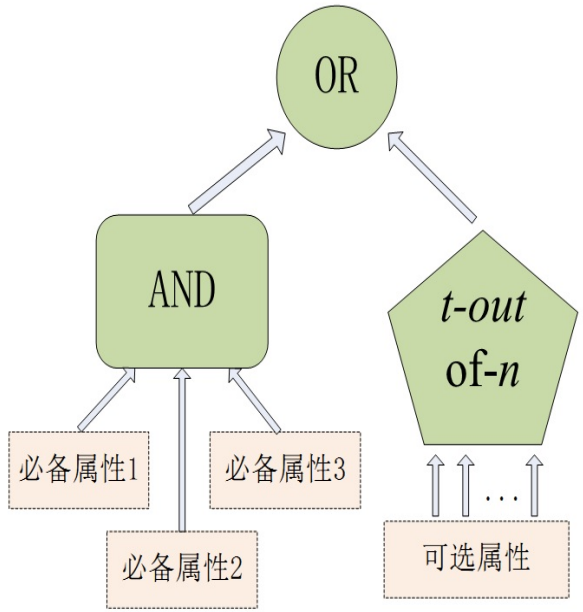


超越身份

- 模糊身份IBE（FIBE）
  - $dec(sk_{id}, enc(id', m)) = m$ 当且仅当 $id \approx id'$ （$|d - d'|_M < t$）
  - 适合以生物特征作为身份

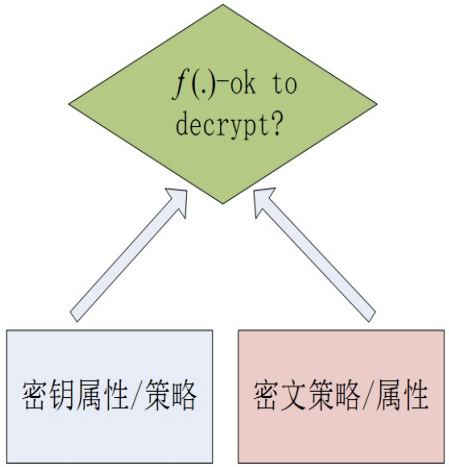
超越身份

- 属性基加密
  - $dec(sk, C) = m$ 当且仅当
    属性集 A 满足访问结构 S
    - 密钥策略：Key-Policy
      $KeyGen(S) \to sk$
      $Enc(m, A) \to C$
    - 密文策略：Ciphertext-Policy
      $KeyGen(A) \to sk$
      $Enc(m, S) \to C$
  - 细粒度访问控制结构



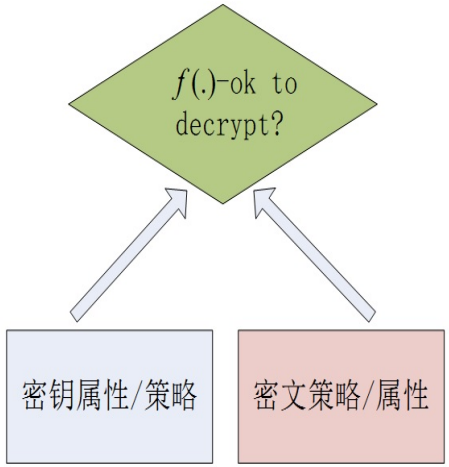
超越身份

- 函数加密
  - $dec(sk, C) = f(m)$
    当且仅当 属性集 A
    满足访问结构 S
  - 增强的隐私保护能力



超越身份

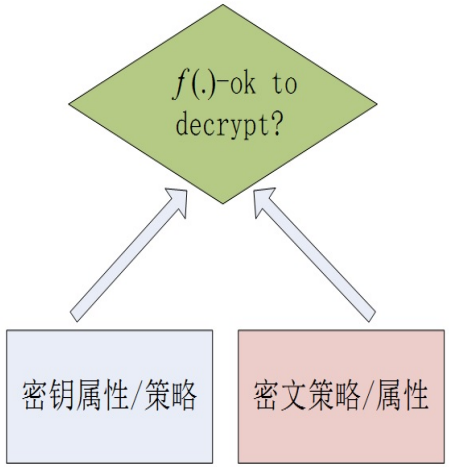
- 函数加密
  - $dec(sk, C) = f(m)$ 当且仅当 属性集 A 满足访问结构 S
  - 增强的隐私保护能力



Boneh-Sahai-Waters (2010)
FE supports a restrict key that enables a key holder to learn a specific function of encrypted data, but learn nothing else about the data.

超越身份

- 函数加密
  - $dec(sk, C) = f(m)$ 当且仅当 属性集 A 满足访问结构 S
  - 增强的隐私保护能力



Boneh-Sahai-Waters (2010)
FE supports a restrict key that enables a key holder to learn a specific function of encrypted data, but learn nothing else about the data.

O'Neill (2010)

$$Eval(sk_f, Enc(pk, m)) \rightarrow f(m) :$$

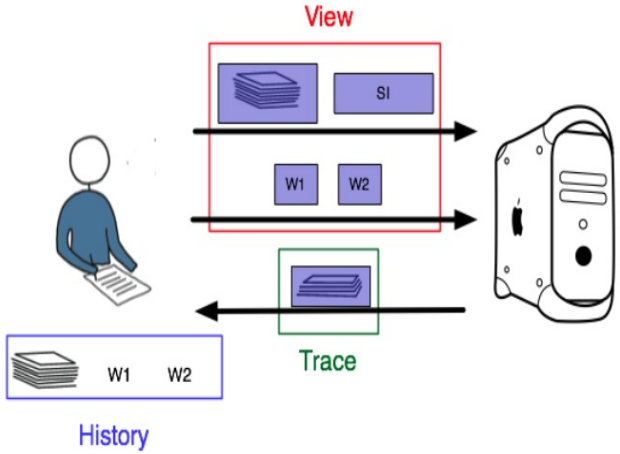
$$Setup(1^k) \rightarrow (pk, sk),\ KD(sk, f) \rightarrow sk_f$$

超越身份

- （全）同态加密
  - $dec(c_1 \odot c_2) = m_1 \star m_2$
  - 支持基于密文的数据融合和挖掘
  - 密码学的“圣杯”、云计算的理想工具

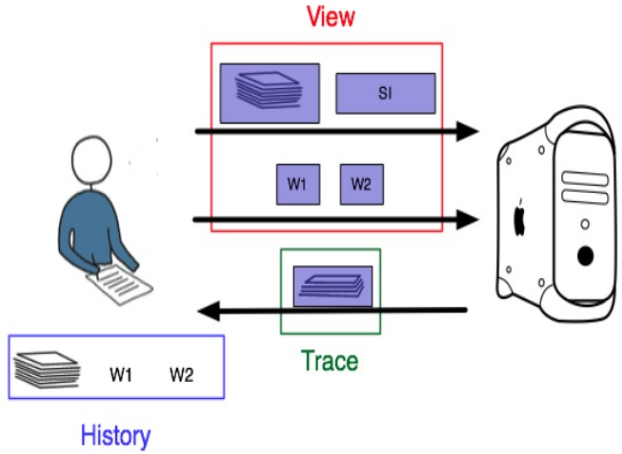
超越身份

- 可搜索加密
  - 支持基于密文的数据检索



超越身份

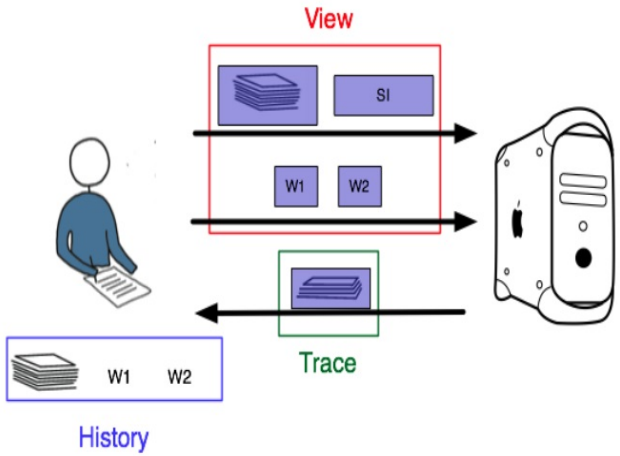
- 可搜索加密
  - 支持基于密文的数据检索



  - 哪些隐私可保护？
    - History: 文档、关键词
    - View: 加密的文档、索引、陷门
    - Trace: 文档长度、搜索结果、搜索模式

超越身份

- 可搜索加密
  - 支持基于密文的数据检索

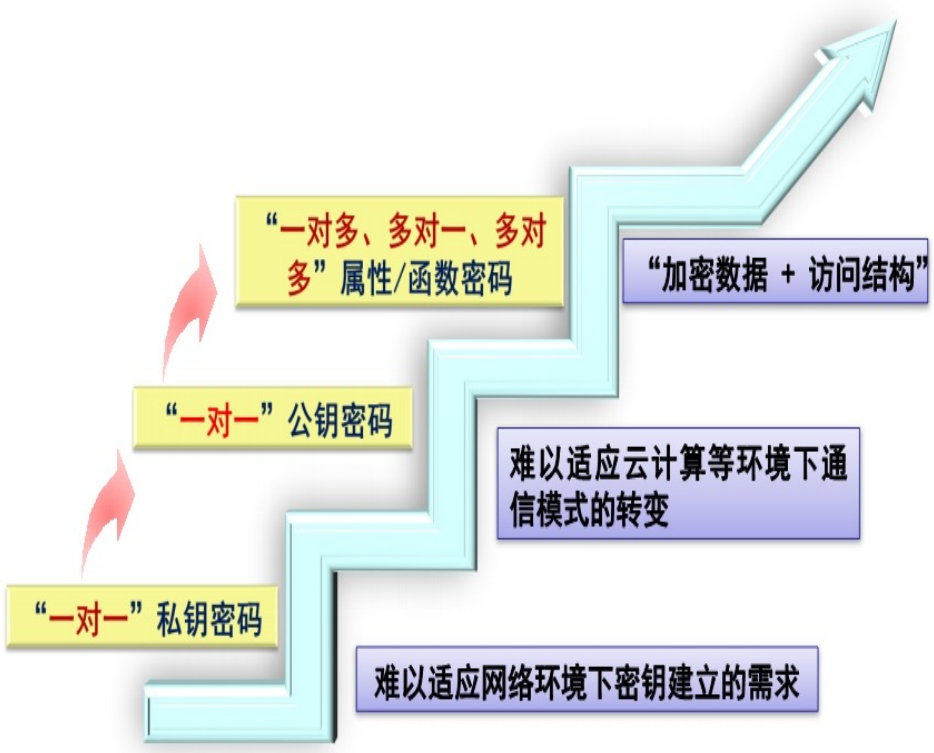


  - 哪些隐私可保护？
    - History: 文档、关键词
    - View: 加密的文档、索引、陷门
    - Trace: 文档长度、搜索结果、搜索模式

超越身份

小结：通信模式由点对点向一对多、多对一、多对多转变

- 由访问结构决定
- 动态、多变



基于区块链

- 基于区块链的公钥认证框架？
  - 可行性：分布式账本 $\leftrightarrow$ 证书列表？
  - 挑战：证书回收如何解决？

结束语

CRYPTO IS DEAD? (Rump Session, CRYPTO'12)

结束语

CRYPTO IS DEAD? (Rump Session, CRYPTO'12)

基于密码技术的区块链已经火起来了.....

$$\Downarrow$$

结束语

CRYPTO IS DEAD? (Rump Session, CRYPTO'12)

基于密码技术的区块链已经火起来了.....

基于区块链新型密码技术也来了.....

R. Goyal, V. Goyal @ TCC 2017: Overcoming cryptographic impossibility results using blockchains.

结束语

CRYPTO IS DEAD? (Rump Session, CRYPTO'12)

基于密码技术的区块链已经火起来了.....

$\Downarrow$

基于区块链新型密码技术也来了.....

R. Goyal, V. Goyal @ TCC 2017: Overcoming cryptographic impossibility results using blockchains.

欢迎批评指正！