数字货币和区块链 - 密码学（3）

山东大学网络空间安全学院

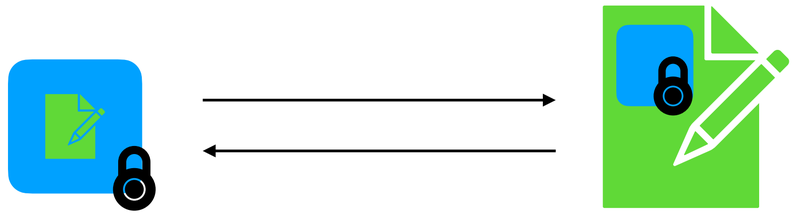
钱宸 2023年11月1日

密码学温故知新

- 哈希函数
- 零知识证明
- 签名
- 盲签名
- 加密算法

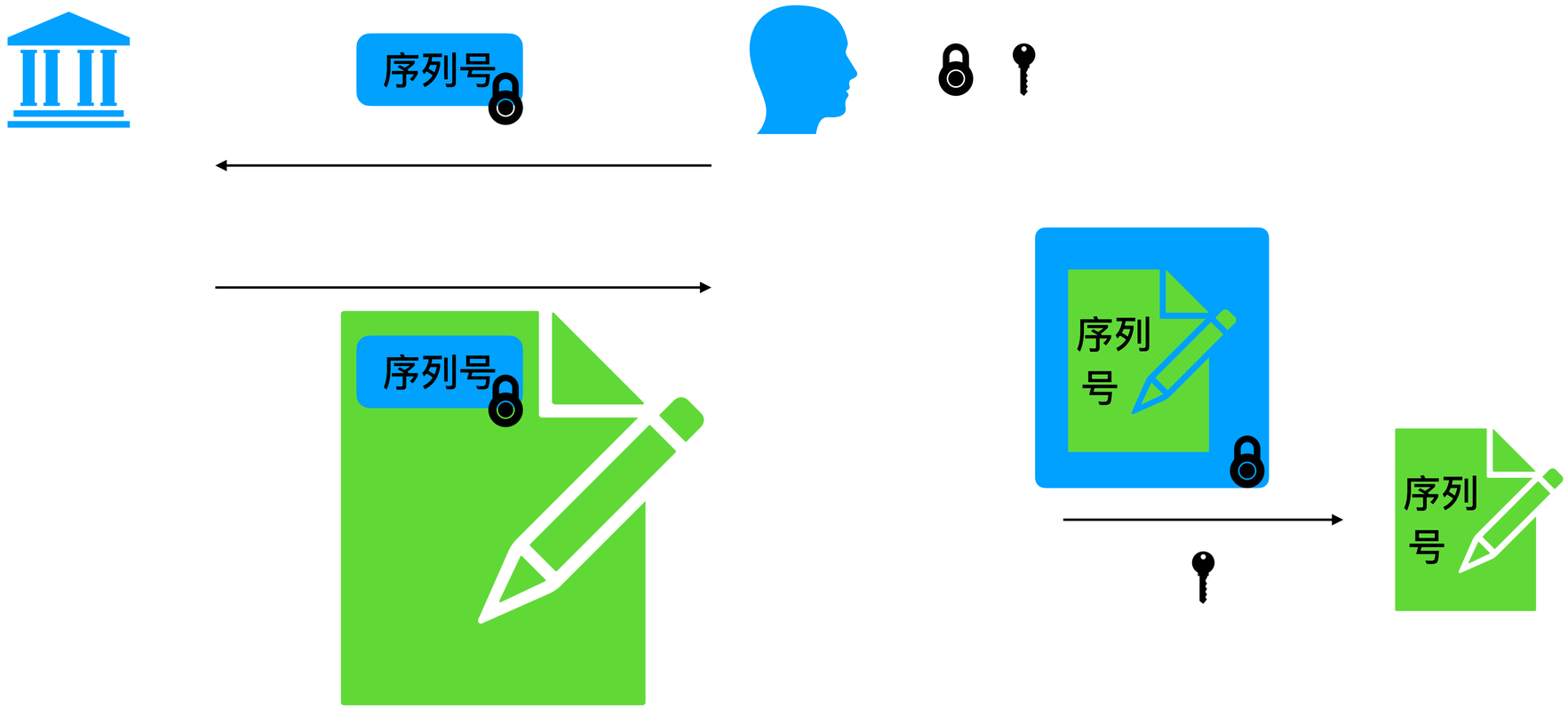
盲签名算法回顾

- 1988年David Chaum提出利用盲签名的方式来同时解决匿名性和双支付攻击
- 盲签名的重要特性：



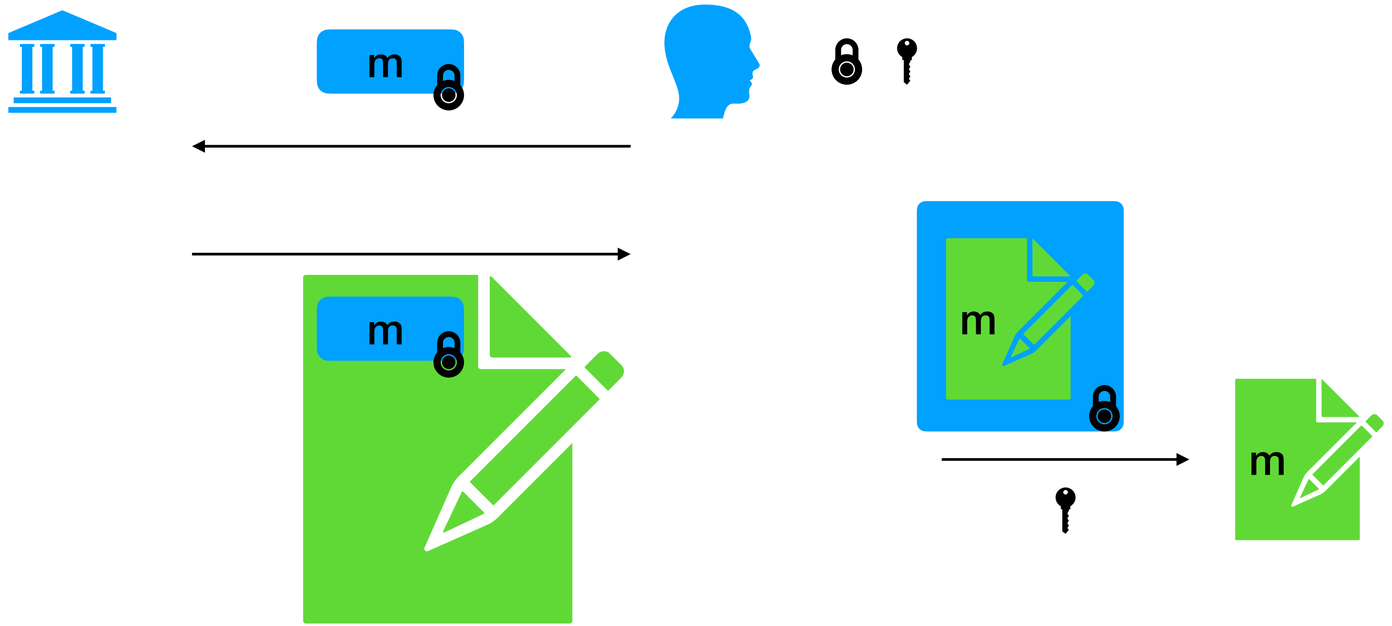
盲签名算法回顾

- 如何利用盲签名的性质设计数字现金?



盲签名算法

- 盲签名算法的步骤
- Setup(1^λ) → (ek, svk, ssk)
- Blind(ek, m) → $\bar{m}$
- Sig(ssk, $\bar{m}$) = $\bar{\sigma}$
- UnBlind(ek, $\bar{\sigma}$) → σ



盲签名算法

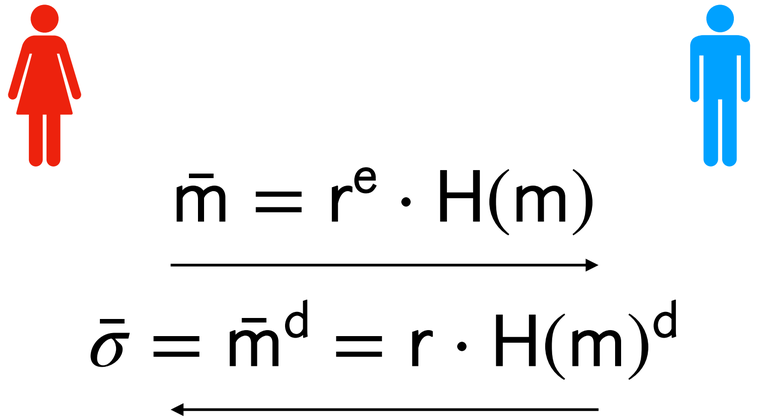
- 盲签名算法所要满足的性质：
  - 正确性（Correctness）： 正确的签名可以被验证
  - 盲化（Blindness）： 签名者不知道具体信息
  - 不可伪造性（Unforgeability）： 无法伪造新的签名

盲签名算法

- 基础算法回顾：
  - RSA-FDH:
    - PK $= N, e$, SK $= d$
    - $\sigma = \mathrm{H}(m)^d$
  - 一次一密One-Time Pad
    - SK $= K$, ct $= K \cdot m$

盲签名算法

- 最简单的盲签名算法（Chaum-RSA-FDH）
- Setup(1^λ) $\rightarrow$ (ek, svk, ssk)
  - ek $=$ K, svk $=$ N, e, ssk $=$ d
- Blind(ek, m) $\rightarrow \bar{m}$
  - $\bar{m} = r^e \cdot H(m)$
- Sig(ssk, $\bar{m}$) $= \bar{\sigma}$
  - $\bar{\sigma} = \bar{m}^d = r \cdot H(m)^d$
- UnBlind(ek, $\bar{\sigma}$) $\rightarrow \sigma : \sigma = \bar{\sigma} \cdot r^{-1}$



盲签名算法

- 盲化属性（Blindness）？
  - $\bar{m} = r^e \cdot H(m)$
  - 签名者Bob不知道(m,r)
    - 给定任意m'，存在$r' = \bar{m}^d \cdot H(m)^{-1}$，使得$\bar{m} = (r')^e \cdot H(m')$
    - 所以Bob没办法知道m的任何信息

盲签名算法

- 不可伪造性（Unforgeability）？
  - 在攻击者获得k个签名的情况下，仍然无法生成新的签名。
  - One-More RSA假设：给定一个寓言机$\mathcal{O}(x) = x^d$，攻击者在询问多项式次数以后，对于随机生成的$m \in \mathbb{Z}_N$，且$m \neq p \wedge m \neq q$，则找到m^d是困难的。
  - 想法：
    - 利用寓言机生成盲化后信息的签名
    - 如果攻击者生成了新的签名，则攻击了One-More RSA假设

密码学温故知新

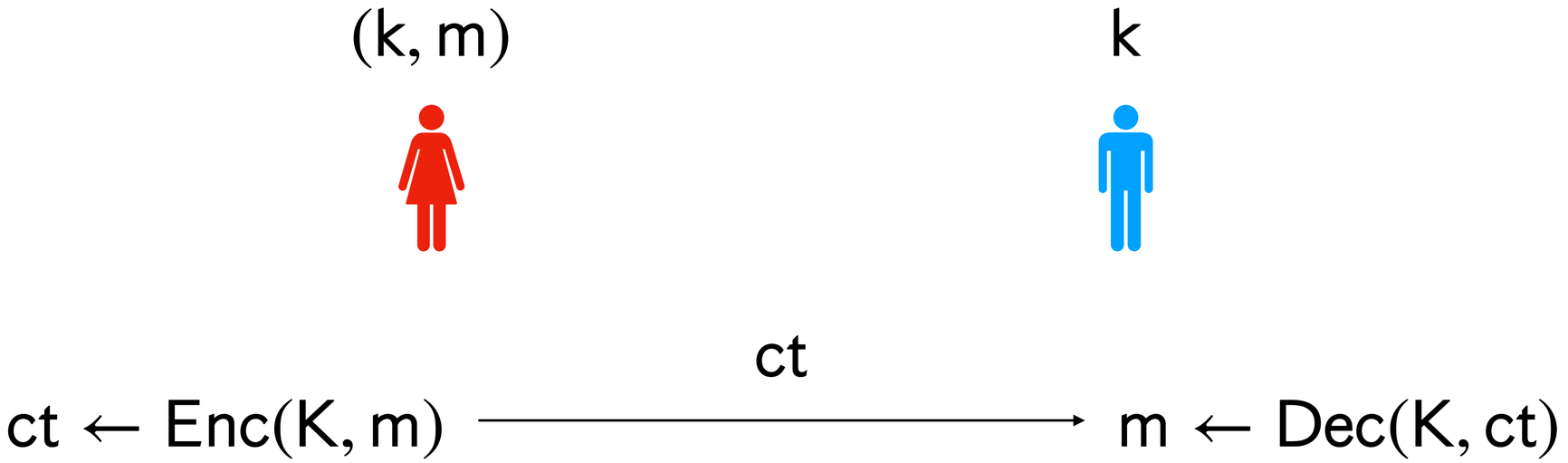
- 哈希函数
- 零知识证明
- 签名
- 盲签名
- 加密算法

加密算法

- 加密算法历史很悠久。。
- 对称加密算法
  - One-Time Pad
    - $ct = K \oplus m$，证明?
  - DES（1977，美国标准），AES（2001，美国标准），SM4（2012， 中国标准）

加密算法

- 对称加密算法

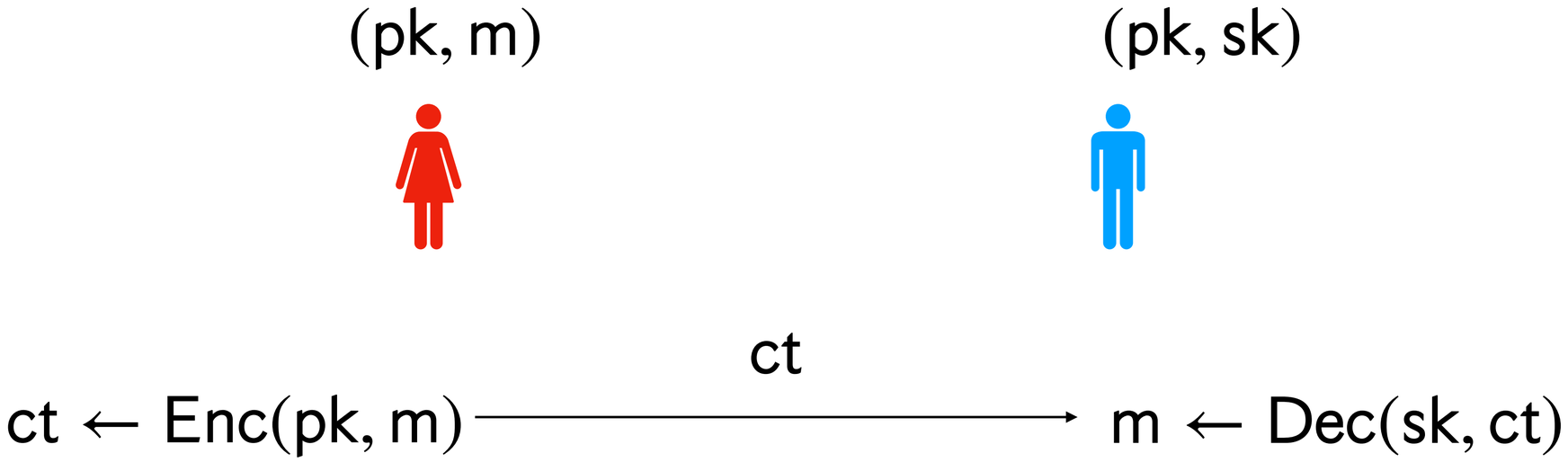


加密算法：对称到非对称

- 类似于从哈希函数到签名算法
- 我们对于对称加密算法也进行一些哲学思考：
  - 私钥（秘密）：定义了个人的身份
  - 加密过程：很多人向一个人传递信息的过程
  - 加密者：加密者并不需要证明自己的身份（不需要私钥）
  - 解密者：解密者是指定的（需要私钥）
  - 非对称加密

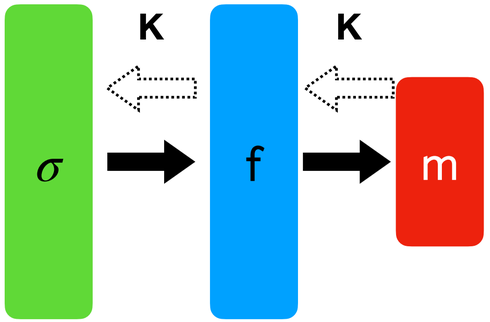
加密算法：非对称加密算法

- 对称加密算法



非对称加密算法

- 需要哪些性质呢?
  - 加密的时候：明文计算密文→简单
  - 攻击者：密文计算明文（没有私钥）→困难
  - 解密的时候：密文计算明文（有私钥）→简单
  - 解密正确性：密文对应一个明文→ 一一对应
- 联想：陷门单项函数（置换）！

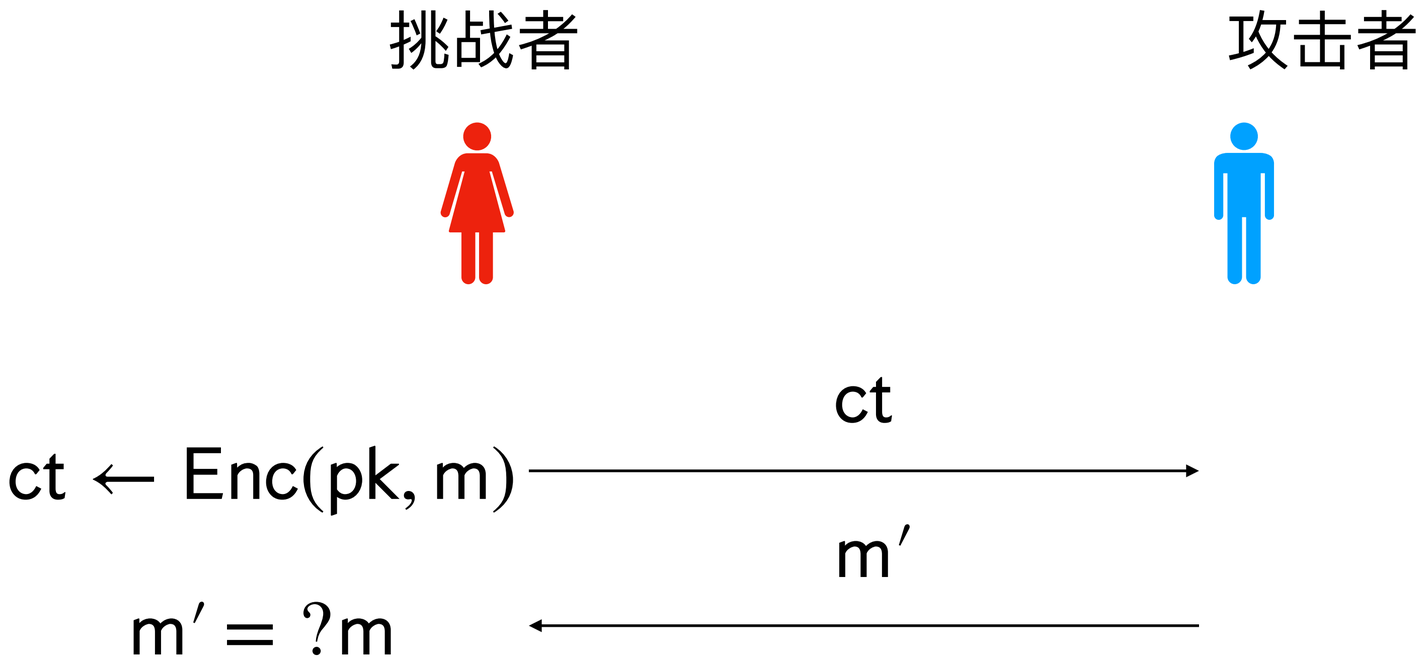


非对称加密算法

- 陷门单项置换！
  - 恰巧RSA陷门单向函数就是一个置换：$f_{\mathrm{RSA}}(x) = x^e$
  - f_{ISIS}虽然是一个陷门单向函数，但是并不是置换。
- RSA加密
  - $\mathrm{pk} = \mathrm{N}, \mathrm{e}, \mathrm{sk} = \mathrm{d}$
  - $\mathrm{ct} = \mathrm{m}^{\mathrm{e}}$

非对称加密 - 单向安全性

- 上述我们所介绍的安全性期望：密文↛明文
  - 可以被严格定义为单向安全性



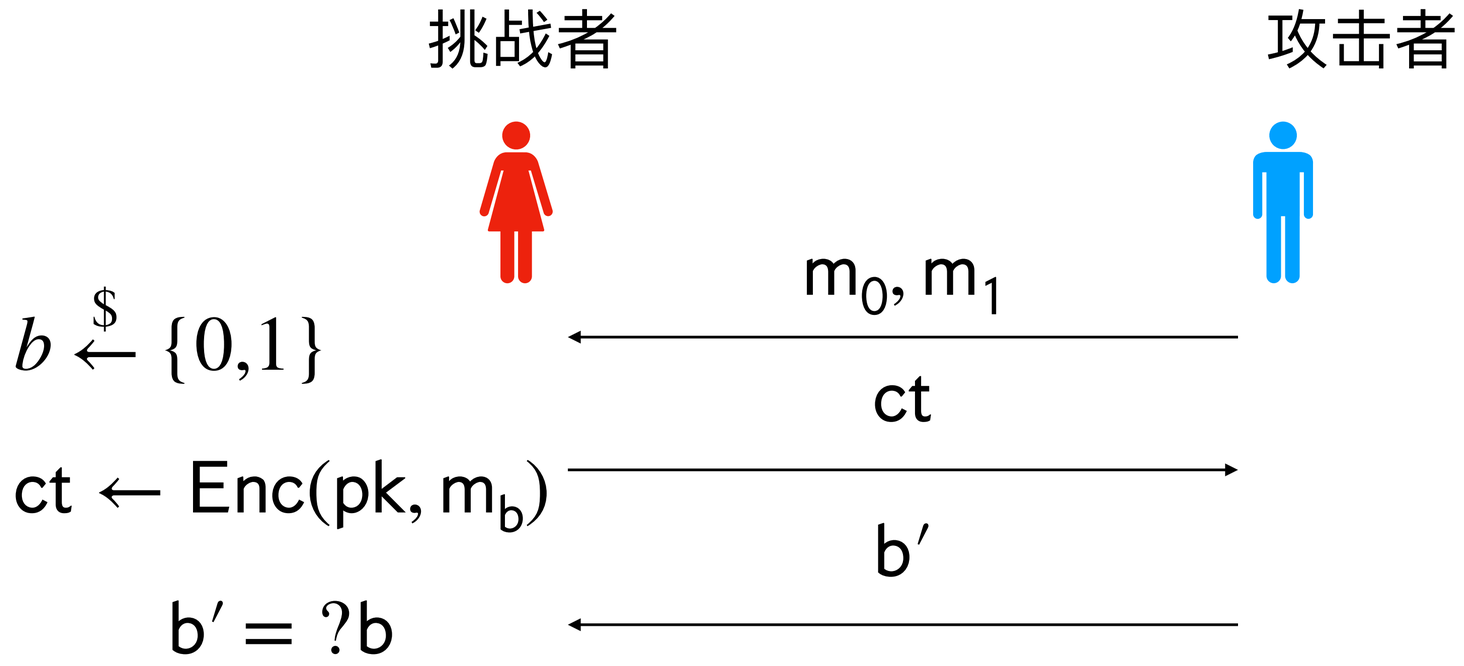
非对称加密 - 单向安全性

- 单向安全性足够么?
- 给定一个单向安全的加密算法
  - $ct' = ct \| m_{[:4]}$，其中$m_{[:4]}$表示消息的最后四位。
  - ct′仍然保证单向安全性
  - $m =$ ”打开山洞保险箱宝藏的口令是阿里巴巴”
  - $ct' =$ qbbsdfkkjxcklhfsd; flkwe阿里巴巴
  - 好像不是很安全。。。

非对称加密 - 语义安全性（sementic security）

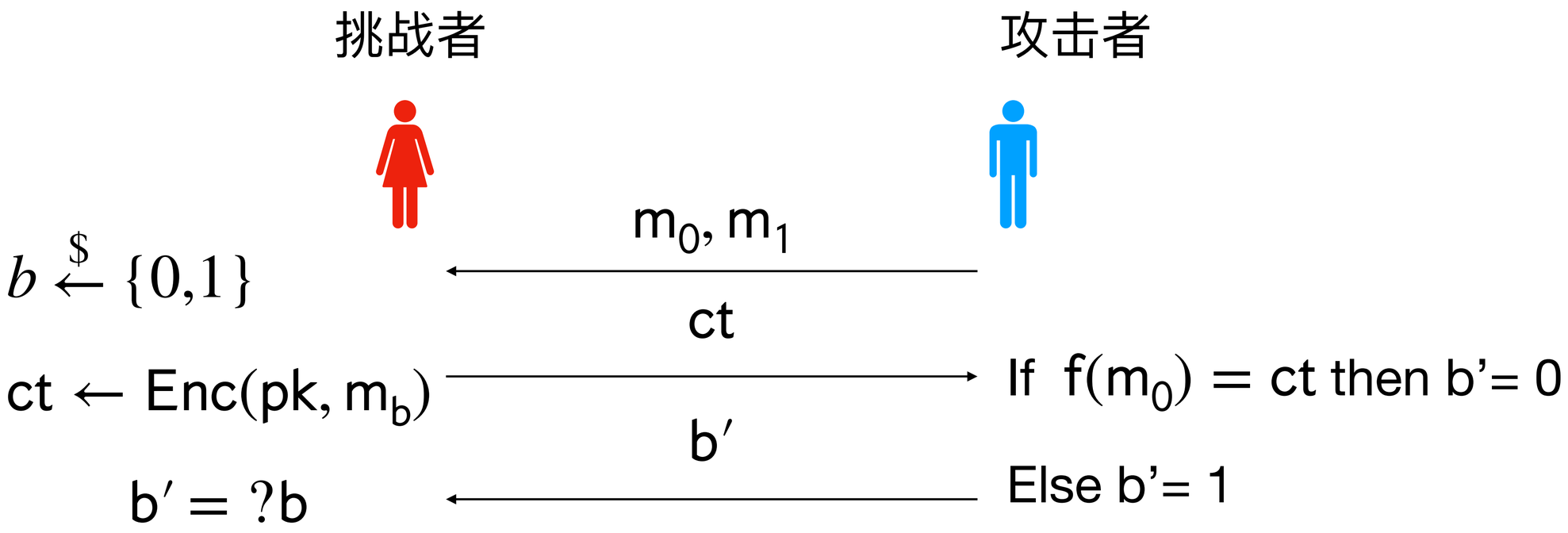
- $\forall \mathcal{A} \in$ PPT. $\mathcal{A}$不能通过ct_m获得除了 m 以外的关于m的任何信息。（Goldwasser，Micali 1982）

- 后续证明该定义于IND-CPA定义等价



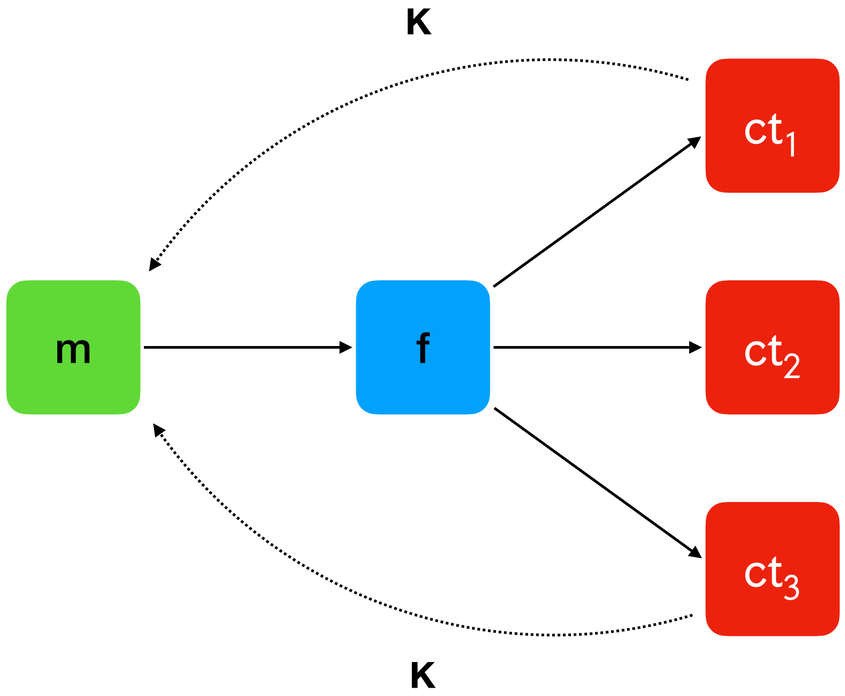
非对称加密 - IND-CPA

- 思考：基于陷门单向函数的加密满足IND-CPA么?
- 不满足：陷门单向函数f是确定性函数。



非对称加密 - IND-CPA

- 随机陷门单向函数



非对称加密 - IND-CPA

- 基于CDH假设$f_{g,h}(m; r) = (g^r, m \cdot h^r)$
  - 单向性：CDH假设$g, h, g^r \nrightarrow h^r$
  - 陷门：
    - $k = \log_g(h)$
    - $m = m \cdot h^r \cdot (g^r)^{-k}$

非对称加密 - IND-CPA

- DDH假设
  - $(f, g, f^r, g^r) \equiv_c (f, g, h, i)$，其中$f, g, h, i \xleftarrow{\$} \mathbb{G}, r \xleftarrow{\$} \mathbb{Z}_p$
- El-Gammal加密算法
  - $pk = y = g^x$，$sk = x$
  - $ct = (g^r, m \cdot g^{xr})$

非对称加密 - IND-CPA

- $(f, g, f^r, g^r) \equiv_c (f, g, h, i)$
- DDH假设→El-Gammal加密IND-CPA安全