

密码技术与金融科技

Cryptography & Fintech

李江涛

网络空间安全实验室

什么是密码学



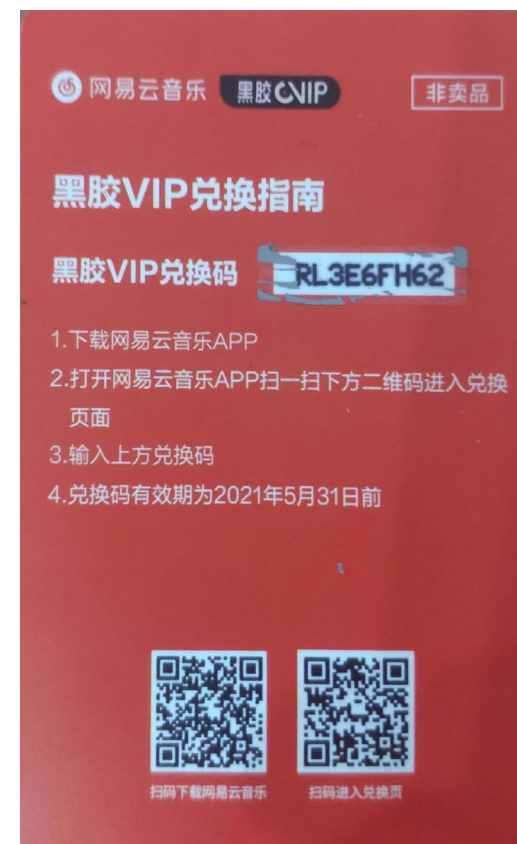
- 密码 (Cryptography) v.s. 口令(Password, PIN)
- 密码是指采用特定变换的方法对信息等进行**加密**保护、安全**认证**的技术、产品和服务。-- 《中华人民共和国密码法》
- 密码技术是指在被称为**敌手**的第三方在场的情况下进行安全通信的技术实践与研究。-- Wikipedia
- Kerckhoff 原则：算法公开；仅密钥保密

问题一：兑换码生成

- 腾讯的一道面试题：四亿个兑换码，兑换码由13个字符组成，字符选择为24个大写字母(I和O易跟数字混淆所以除外)。要求给出生成/验证算法，高效、安全、防爆刷、防重复兑换。

- 初步分析：

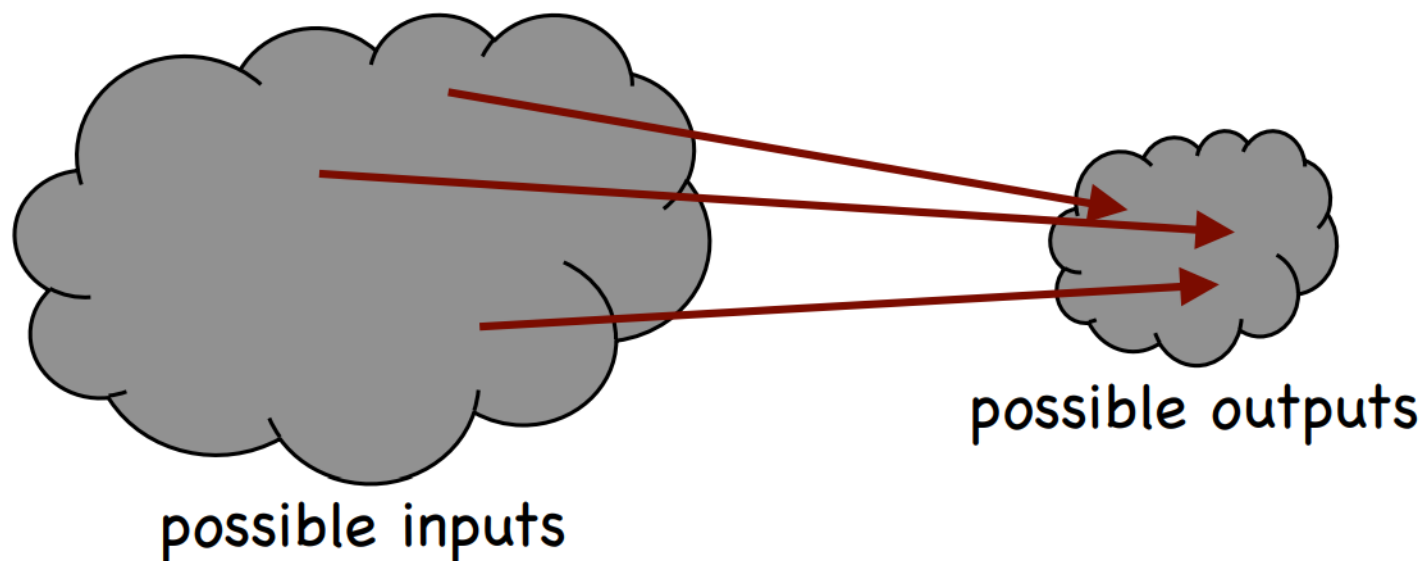
- ① 13个字符可以携带的信息量： $\log_2(24^{13}) = 59.6bits$
- ② 编号：需要编码的激活码上限为4亿 约等于 $\log_2(4亿) = 28.6bits$ 接近29位；
- ③ Payload：具有认证功能的编码，可用30bits



密码学哈希函数

- 输入任意长度的字符串，产生一个固定长度的输出（例如 256bit）。
- 一个密码学哈希函数需要满足以下两个性质：
 - 1) 可计算性：给定 x ，计算 $H(x)$ 是容易的。
 - 2) 抗碰撞性：给定 $x, H(x)$ ，找到 $y \neq x$ ，使得 $H(y) = H(x)$ ，是困难的。

密码学哈希函数——抗碰撞性



- 对于输出长度为256bits 的任意哈希函数，尝试 2^{130} 次，那么出现碰撞的概率为99.8%
- 计算时间太长

密码学哈希函数——抗碰撞性

是否存在更快的方式可以找到哈希碰撞？



- 2004 年我国密码学家王小云在国际密码讨论年会（CRYPTO）上展示了 MD5 算法的碰撞并给出了第一个实例。
- 2017年，荷兰CWI 研究所和 Google 公司的研究人员发布了世界上第一例公开的 SHA-1 哈希碰撞实例。

1. Collisions for hash functions MD4, MD5, HAVAL-128 and RIPEMD, rump session of CRYPTO 2004 2.
<https://security.googleblog.com/2017/02/announcing-first-sha1-collision.html>

SHA-1 碰撞实例展示

SHAttered

The first concrete collision attack against SHA-1
<https://shattered.io>





Marc Stevens
Pierre Karpman

Elie Bursztein
Ange Albertini
Yarik Markov

SHAttered

The first concrete collision attack against SHA-1
<https://shattered.io>



Marc Stevens
Pierre Karpman

Elie Bursztein
Ange Albertini
Yarik Markov

```
└─ sha1sum *.pdf
38762cf7f55934b34d179ae6a4c80cadccbb7f0a 1.pdf
38762cf7f55934b34d179ae6a4c80cadccbb7f0a 2.pdf
└─ /tmp/sha1
└─ sha256sum *.pdf
2bb787a73e37352f92383abe7e2902936d1059ad9f1ba6daaa9c1e58ee6970d0 1.pdf
d4488775d29bdef7993367d541064dbdda50d383f89f0aa13a6ff2e0894ba5ff 2.pdf
```

0.64G 8-11h

目前安全的哈希算法

- SHA-2家族： SHA-256, SHA-512等
- SHA-3算法： Keccak （2015年8月， NIST批准）
- 国密： SM3 （2010年12月）

消息认证码

- 消息认证码方案包含三个算法：
- Gen: 根据安全参数, 生成密钥 k 。
- Mac: 输入消息 m 和密钥 k 生成标签 t 。
- Verify: 输入标签 t 和消息 m , 输出true/false表示标签是合法/非法的。

解决兑换码生成问题

- 消息认证码 (Message Authentication Code)

$MAC_k(m) = H(k||m)$, 其中k是一个随机生成的密钥。

- 具体过程:
- 兑换码生成流程:
 - 1) 生成随机密钥k
 - 2) 生成兑换编号id, 计算 $MAC_k(id) = H(k||id)$, 并截取 $MAC_k(id)$ 前30bit, 记为 $\widetilde{MAC_k(id)}$ 。
 - 3) 兑换码为 $id||\widetilde{MAC_k(id)}$

1.当哈希函数H是一个随机预言机时, 该构造给了一个安全的消息认证码。但是对于MD结构哈希函数, 需要更加复杂的构造。

解决兑换码生成问题

- 兑换码生成流程:

- 1) 生成随机密钥 k

- 2) 生成兑换编号 id , 计算 $MAC_k(id) = H(k||id)$, 并截取 $MAC_k(id)$ 前30bit, 记为 $MAC_k(id)$ 。

- 3) 兑换码为 $id||\widetilde{MAC_k(id)}$, 转化成13个大写字母。

- 兑换码验证过程:

- 1) 将兑换码前29bit记为 $code1$, 后30bit记为 $code2$

- 2) 计算 $MAC_k(code1) = H(k||code1)$, 并验证 $MAC_k(code1)$ 前30bit 与 $code2$ 是否相等。

其它: 由于MAC安全性有一定的牺牲, 需要一定机制防止暴力破解。

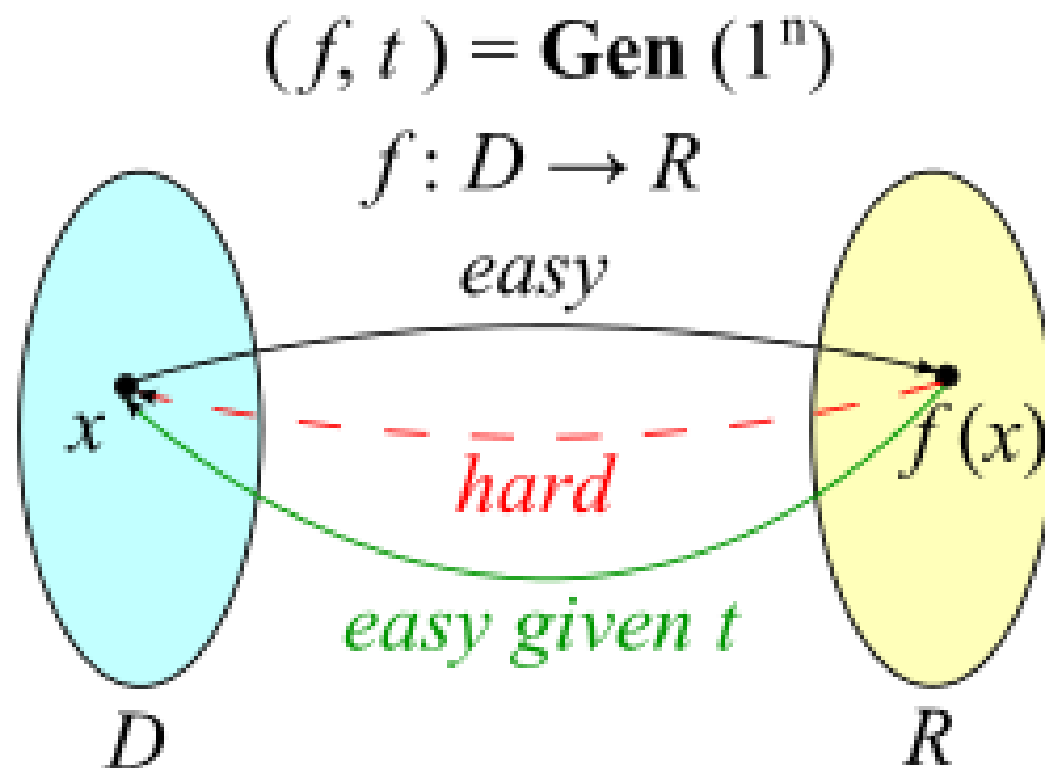
小结：MAC

- 消息认证码MAC可以实现：
 - 1) 身份认证：只有具有密钥 k 的用户才可以生成合法的MAC
 - 2) 消息完整性：篡改内容后，MAC无法通过验证

问题二：借条

- Alice要向Bob借100元，并承诺，下个月还102元。
- 如果利用MAC，假设Alice和Bob共享了密钥k，那么Alice可以使用k，对内容“Alice借款100元，下月还102元”生成一个消息认证码。Bob拿到消息认证码之后，可以确信，Alice说了这句话。
- 但是，如果Alice拿到钱以后抵赖怎么办？

陷门函数



数字签名

- 一个数字签名方案包含以下三个算法：
- KeyGen：生成公私钥对 pk, sk 。其中 sk 表示私钥，用来生成签名， pk 表示公钥，用来验证签名。
- Sign：输入消息 m , 私钥 sk ，输出签名 σ 。
- Verify：验证算法，输入签名 σ ，输出 $true/false$ ，表示签名是否验证通过。

数字签名的安全性

- 正确性 $Verify(PK, m, Sign(sk, m)) = true$

- 不可伪造性

敌手拥有公钥 pk

敌手可以得到指定消息的签名



敌手不可以生成一个新的消息的签名可以通过验证算法

基于陷门函数的数字签名

- $Sign_t(m)$:

$$\sigma = f_t^{-1}(H(m))$$

- $Veify(m, \sigma)$:

$$H(m) = f(\sigma)$$

正确性容易验证

一个陷门函数的实例:RSA

Ron Rivest, Adi Shamir, Leonard Adleman 1977

- 1) 选取两个素数, 计算 $N = p * q$
 - 2) 计算出欧拉函数 $\varphi(N) = (p - 1) * (q - 1)$
 - 3) 选取 $e \in \{1, \dots, \varphi(N)\}$, 并计算出 d 使得 $ed = 1 \bmod \varphi(N)$
- 陷门为 d , 公钥为 e, N 。

$$\begin{aligned} f(x) &= x^e \bmod N \\ f^{-1}(y) &= y^d \bmod N \end{aligned}$$

正确性: $f^{-1}(x^e) = x^{ed} \bmod N = x \bmod N$

注: 对于任意的 α , 有 $\alpha^{\varphi(N)} = 1 \bmod N$

解决借条问题

- 那么Alice可以使用私钥 e ，对内容“Alice借款100元，下月还102元”生成一个数字签名
- Bob收到签名以后，进行签名验证，验证通过后，Bob相信该签名并借款给Alice
- 若Alice事后抵赖，则Bob可以向其它人公开签名，通过验证第三方可以确信该事件。

注：公钥即身份

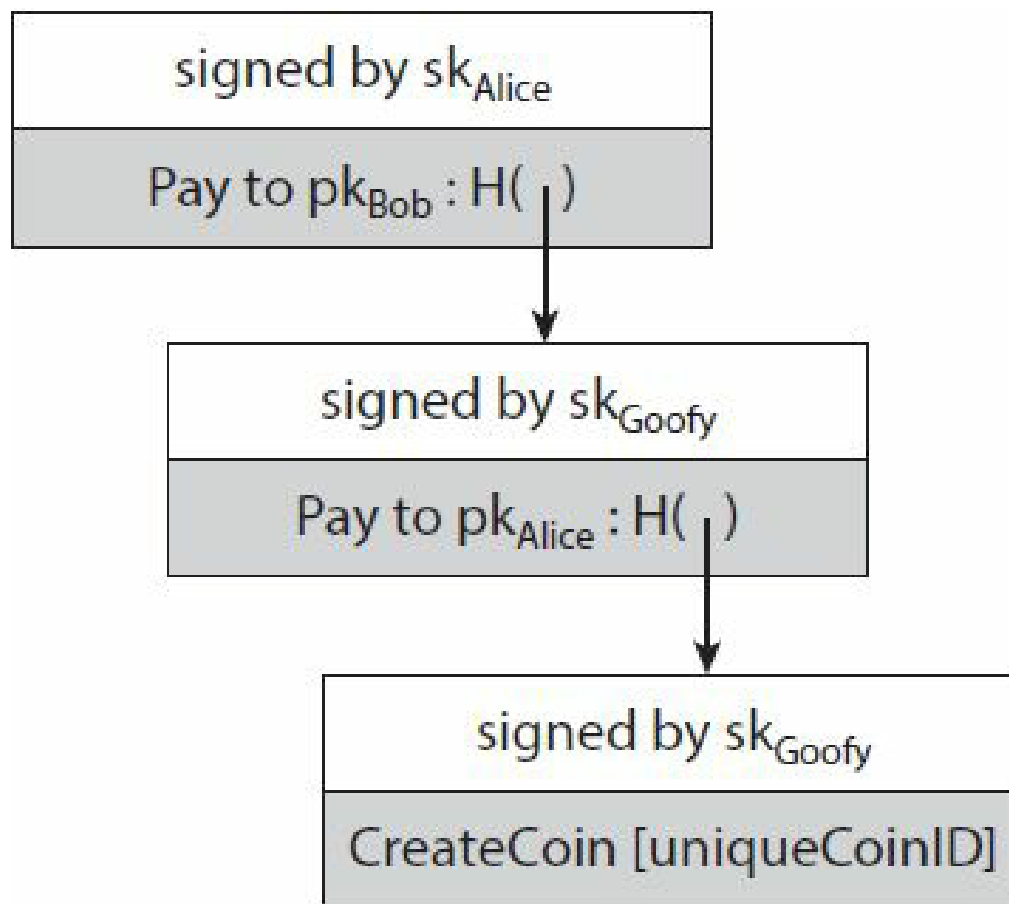
小结： 数字签名

- 相比消息认证码来说可以实现公开验证
- 可以认证消息的来源
- 保证消息的不可篡改性
- 现有的陷门函数只有RSA和Rabin 两类，许多数字签名的构造并不需要陷门函数

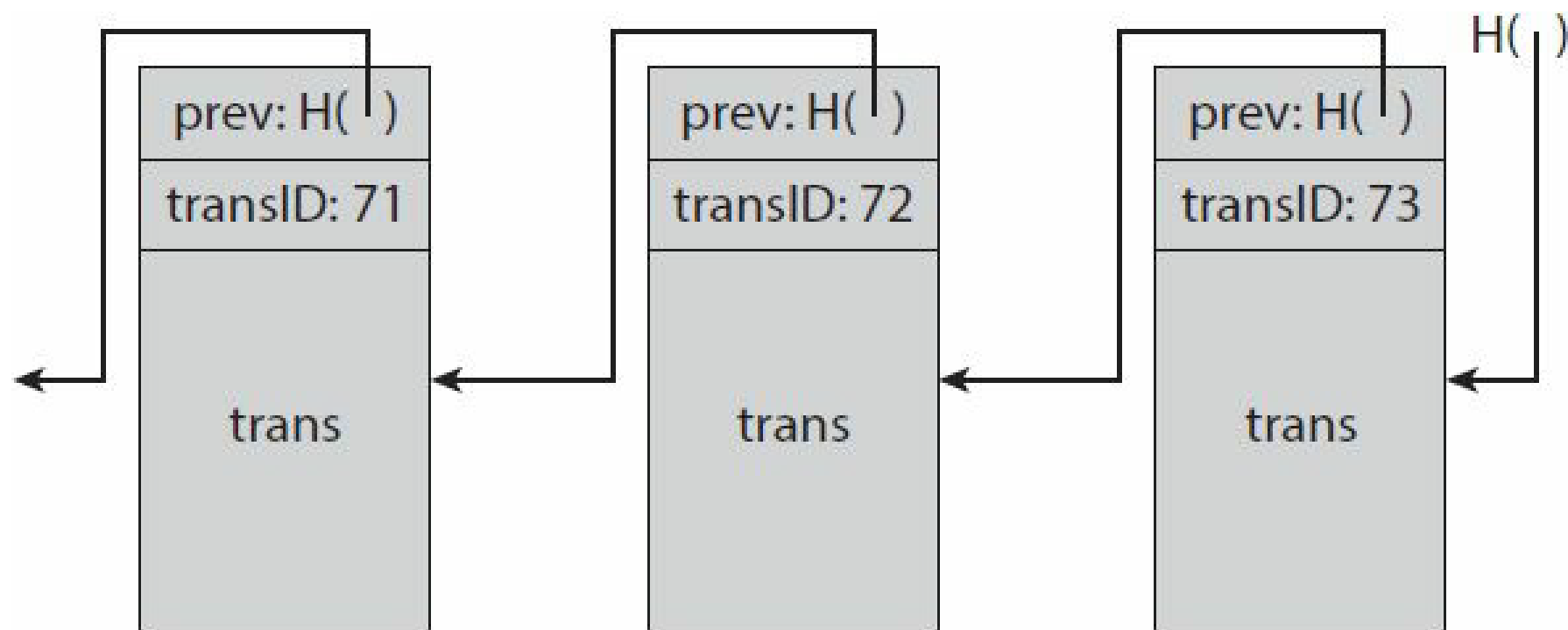
问题三：数字货币

- 移动支付：纸币的数字化表示。其本质仍然依赖银行的信用。银行/移动支付公司是所有交易的中间人
- 如何构造一种数字货币以代替纸币？
- 一串数字就能代表一个货币，如何防止双花？

一种简单的数字货币



数字货币——解决双花问题



数字货币——去中心化

- 中心化 V.S. 去中心化

- 1) 互联网是一个巨大的去中心化系统

- 2) 几乎所有的系统都是混合模式 (hybrid)

区块链与加密货币 (Cryptocurrency)

1. 谁维护交易账本?
2. 谁决定哪些交易是合法的?
3. 谁生成比特币?
4. 谁决定系统规则?

区块示例: <https://www.blockchain.com/btc/blocks?page=1>

金融科技

支付

支付处理、转账、外汇、信用卡

保险

风险管理工具、理赔

数据分析

大数据解决方案、数据可视化

区块链

数字货币、智能合约、资产身份管理

安全

数字身份、欺诈管理、数据隐私

总结

- 密码学是理论计算机科学的一个分支，它在信息安全，金融科技领域扮演着重要的角色。
- 现代密码学的核心在于可证明安全
- 现实世界的金融业务的实现通常需要借助密码学，结合其它技术完成

阅读推荐

- Arvind Narayanan, Joseph Bonneau, Edward Felten, Andrew Miller, and Steven Goldfeder. Bitcoin and cryptocurrency technologies: a comprehensive introduction. Princeton University Press, 2016.
- Jonathan Katz, and Yehuda Lindell. *Introduction to modern cryptography*. CRC press, 2014.