单向散列函数 – 几个网站

- MD5加密
  - https://www.cmd5.com/hash.aspx

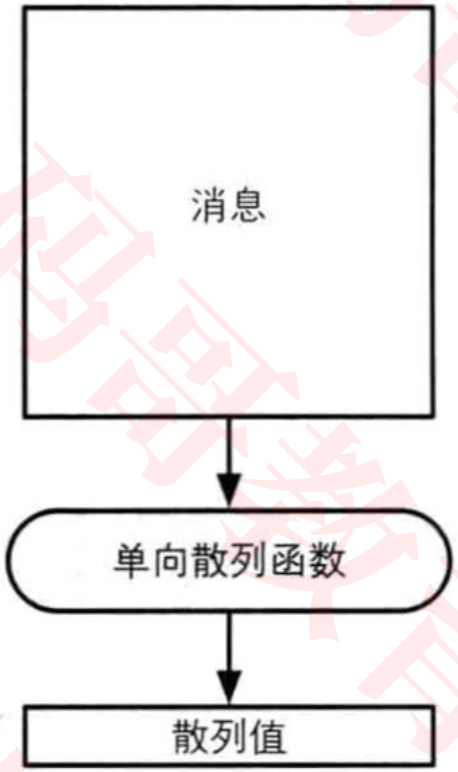
- MD5解密
  - https://www.cmd5.com/

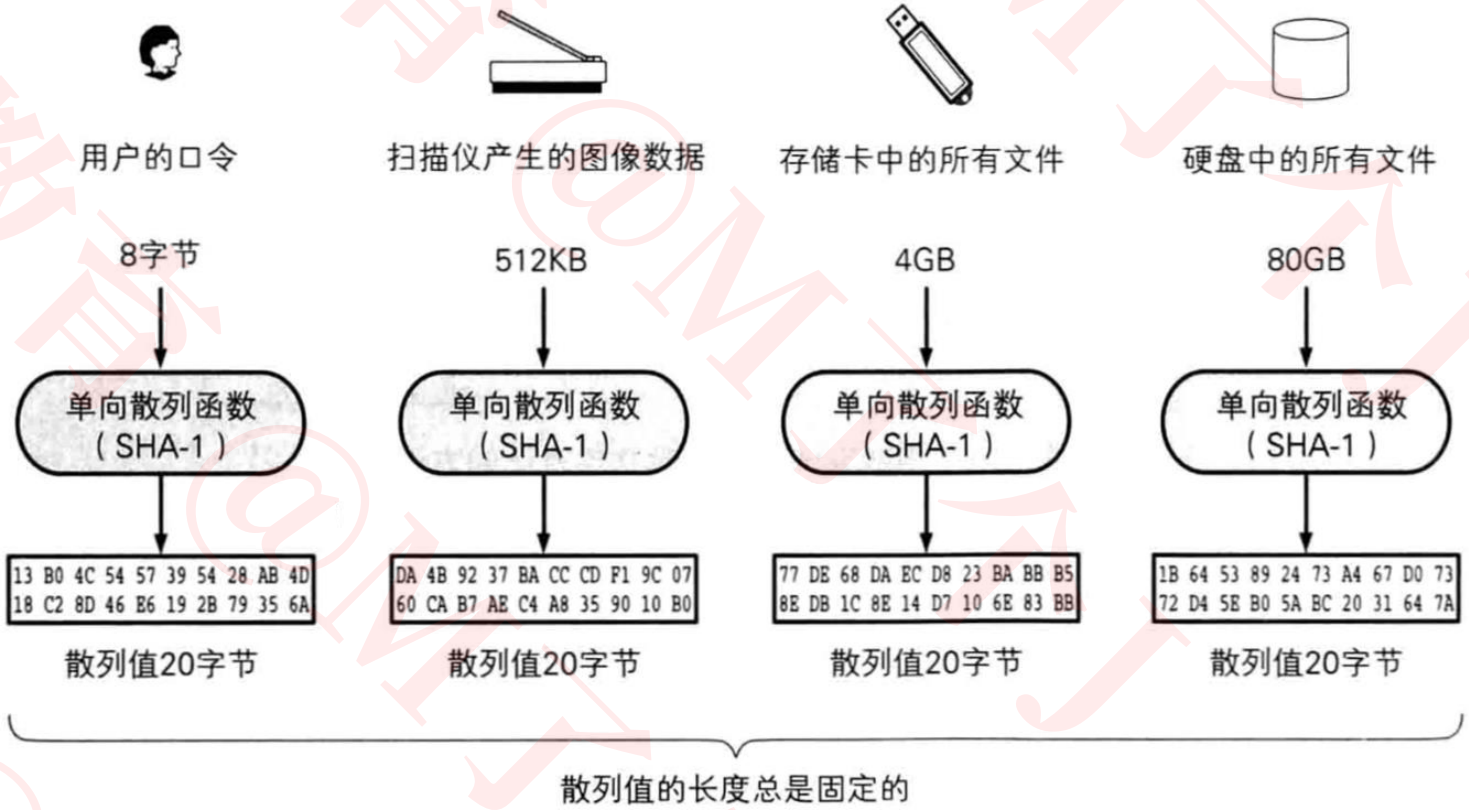
- 其它加密
  - https://www.sojson.com/encrypt_des.html
  - https://tool.chinaz.com/tools/md5.aspx

单向散列函数（One-way hash function）

- 单向散列函数，可以根据根据消息内容计算出散列值

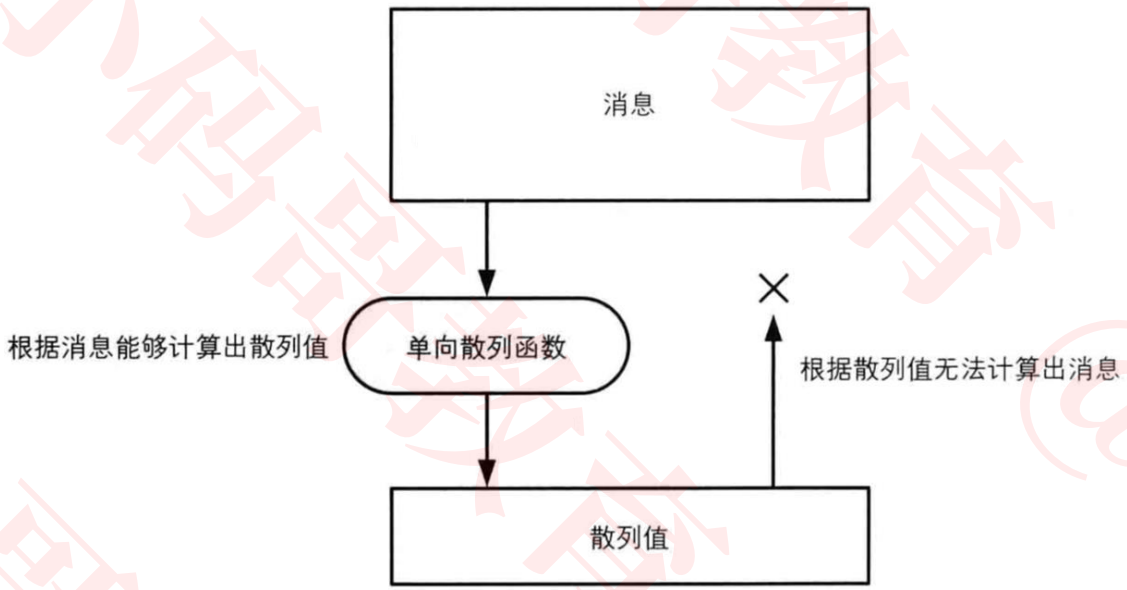
- 散列值的长度和消息的长度无关，无论消息是1bit、10M、100G，单向散列函数都会计算出固定长度的散列值

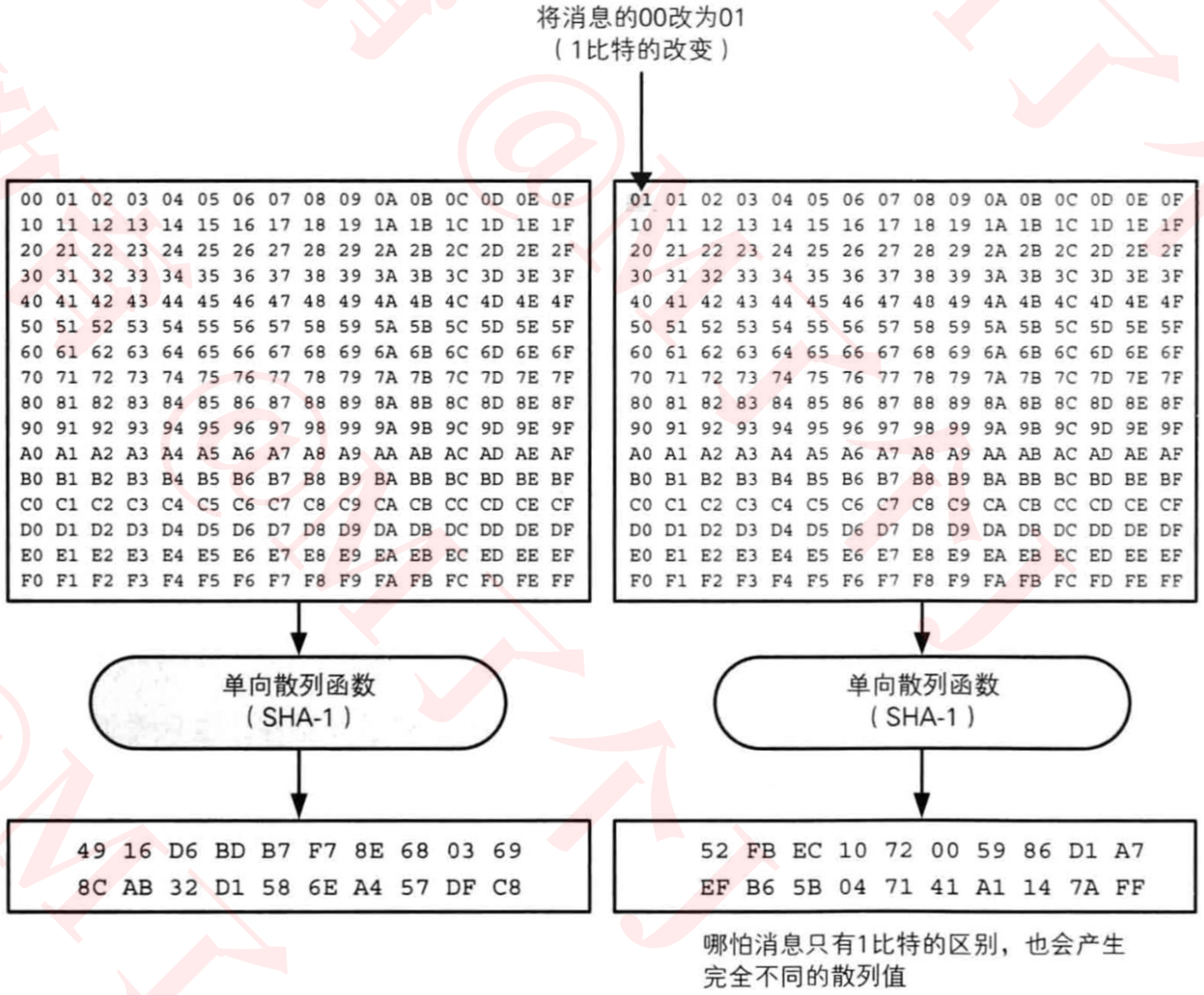




单向散列函数 – 特点

- 根据任意长度的消息，计算出固定长度的散列值
- 计算速度快，能快速计算出散列值
- 消息不同，散列值也不同
- 具备单向性





单向散列函数 – 称呼

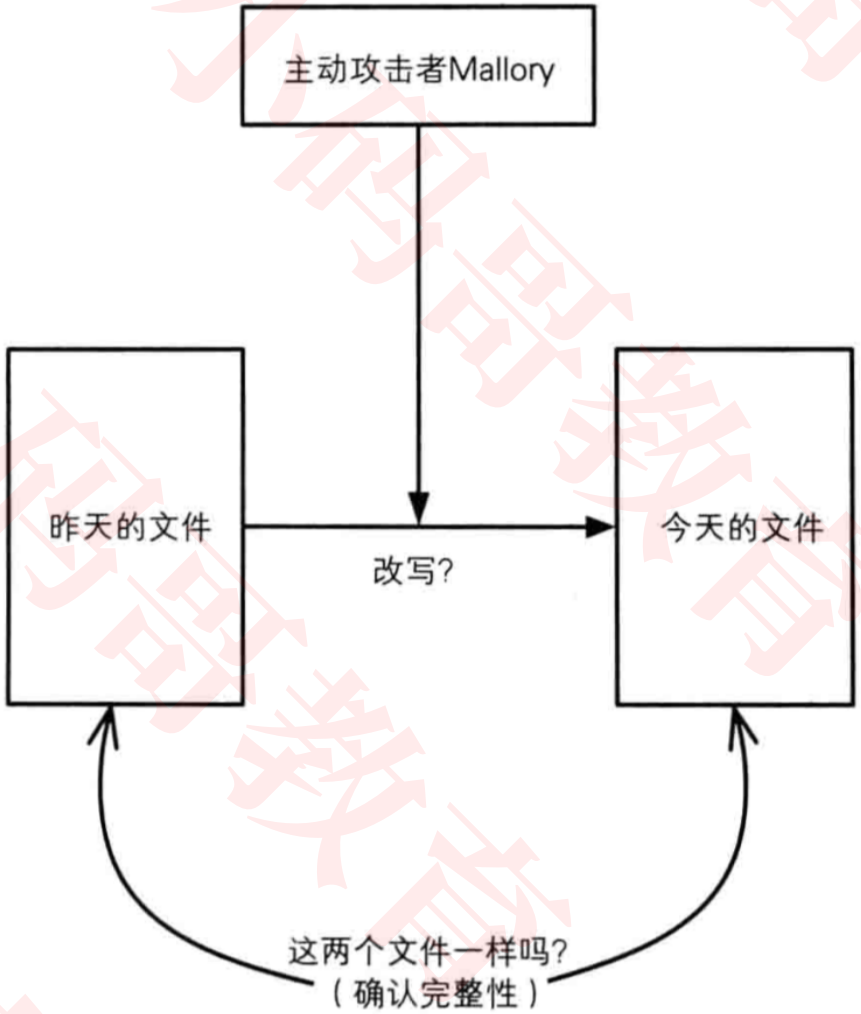
- 单向散列函数，也被称为
  - 消息摘要函数（message digest function）
  - 哈希函数（hash function）

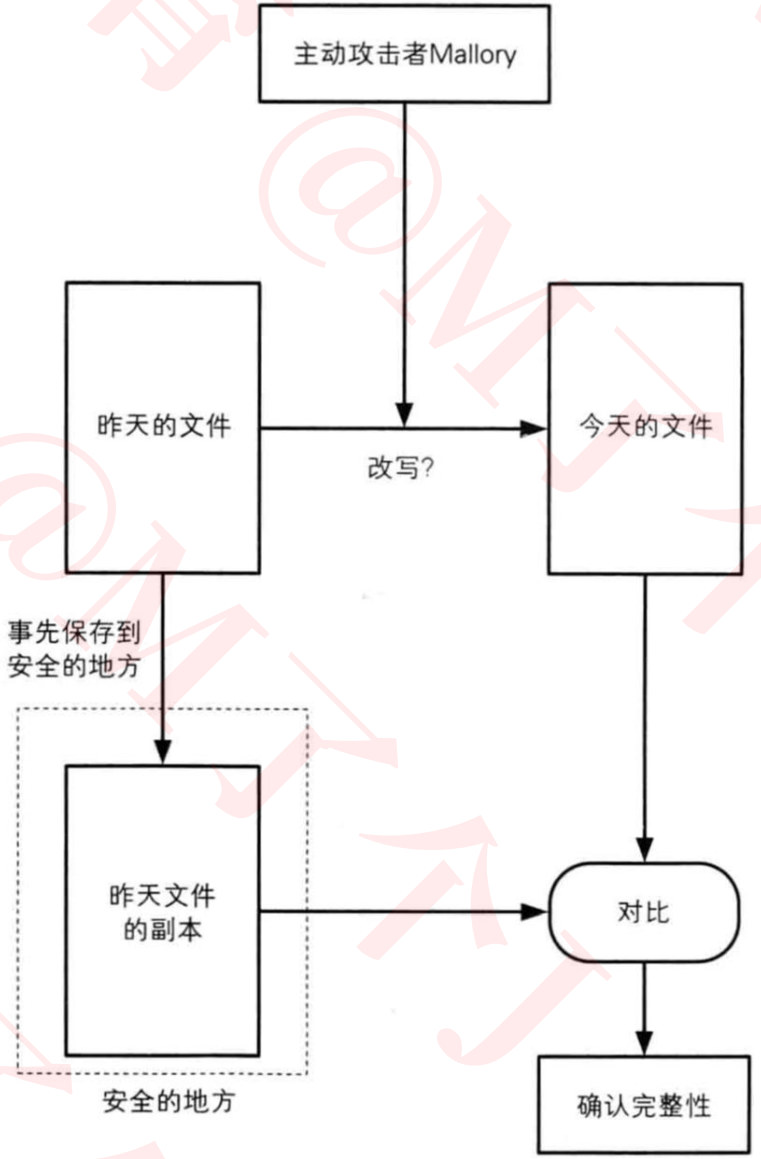
- 输出的散列值，也被称为
  - 消息摘要（message digest）
  - 指纹（fingerprint）

单向散列函数 – 常见的几种单向散列函数

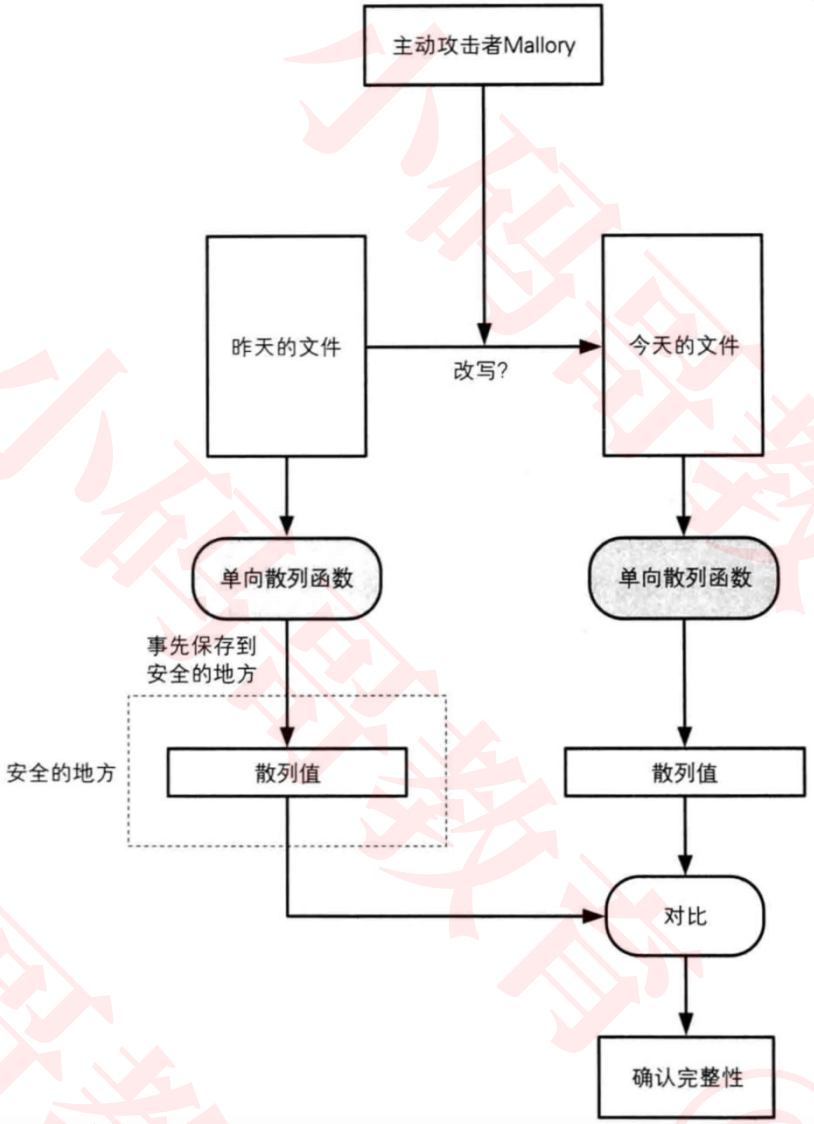
- MD4、MD5
  - 产生128bit的散列值，MD就是Message Digest的缩写
- SHA-1
  - 产生160bit的散列值
- SHA-2
  - SHA-256、SHA-384、SHA-512，散列值长度分别是256bit、384bit、512bit
- SHA-3
  - 全新标准

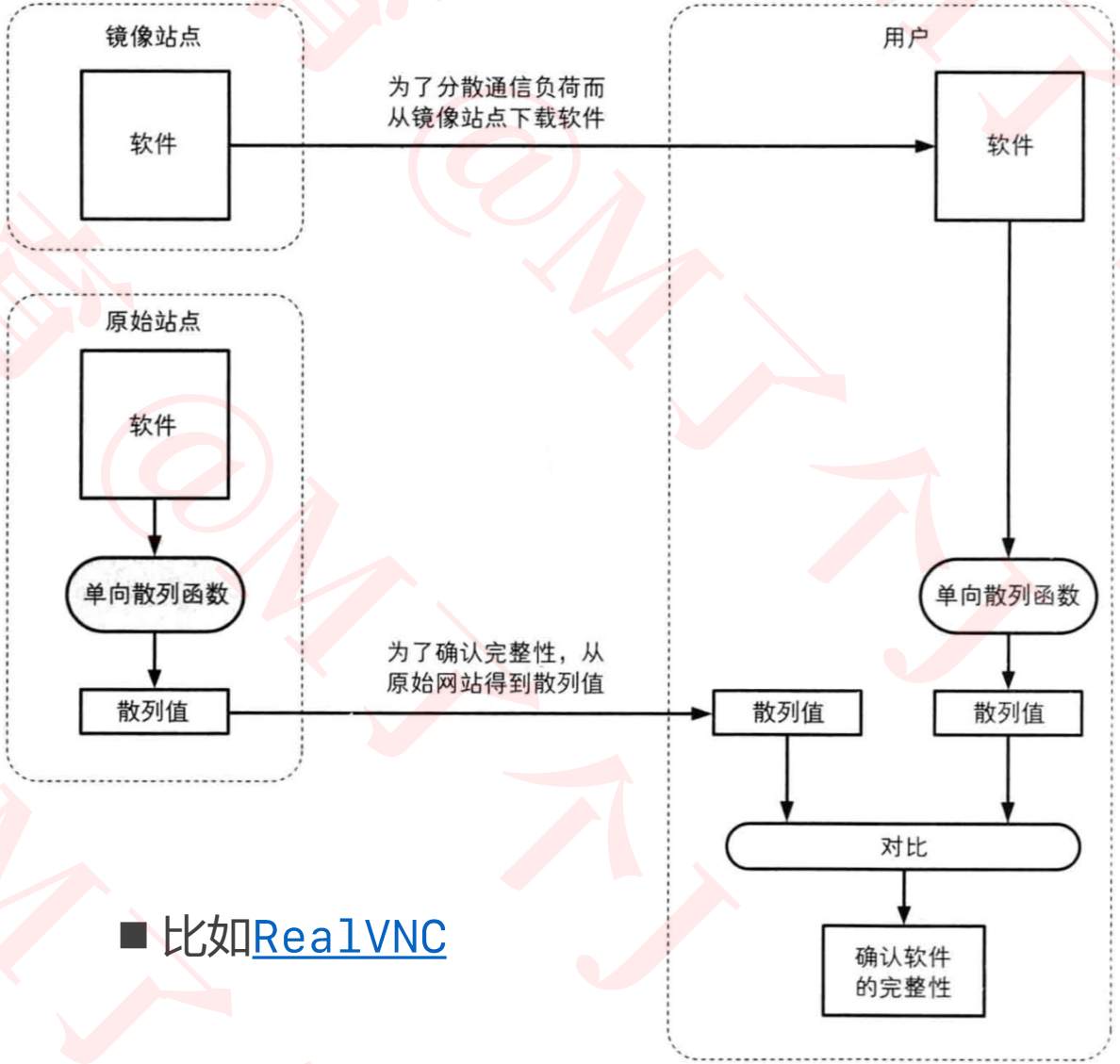
单向散列函数 – 如何防止数据被篡改





单向散列函数 – 应用：防止数据被篡改





- 比如RealVNC

单向散列函数 – 应用：密码加密