



# 关注电子交易的业务安全

单淼

2014年4月

# 调查

- 数字证书、时间戳使用、开发经验?



安全 = 系统安全 + 客户端安全



某银行







某支付机构



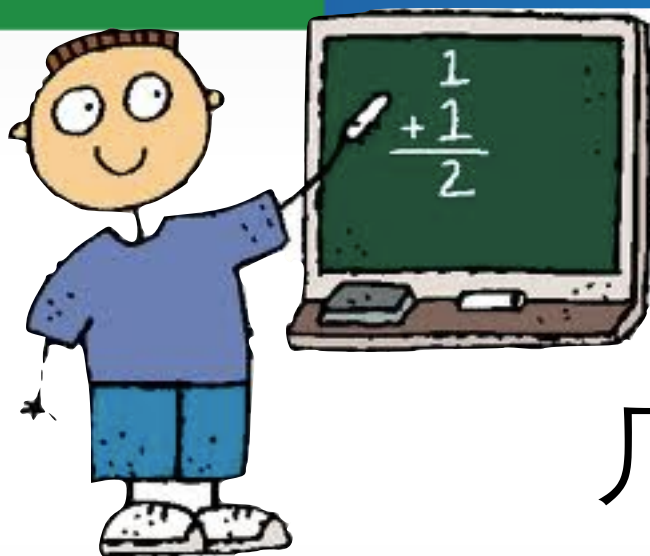
# 被忽略的业务安全





# HowTo

- 几个数学难题
- 几个基础算法
- 一个项目案例



## 几个数学难题

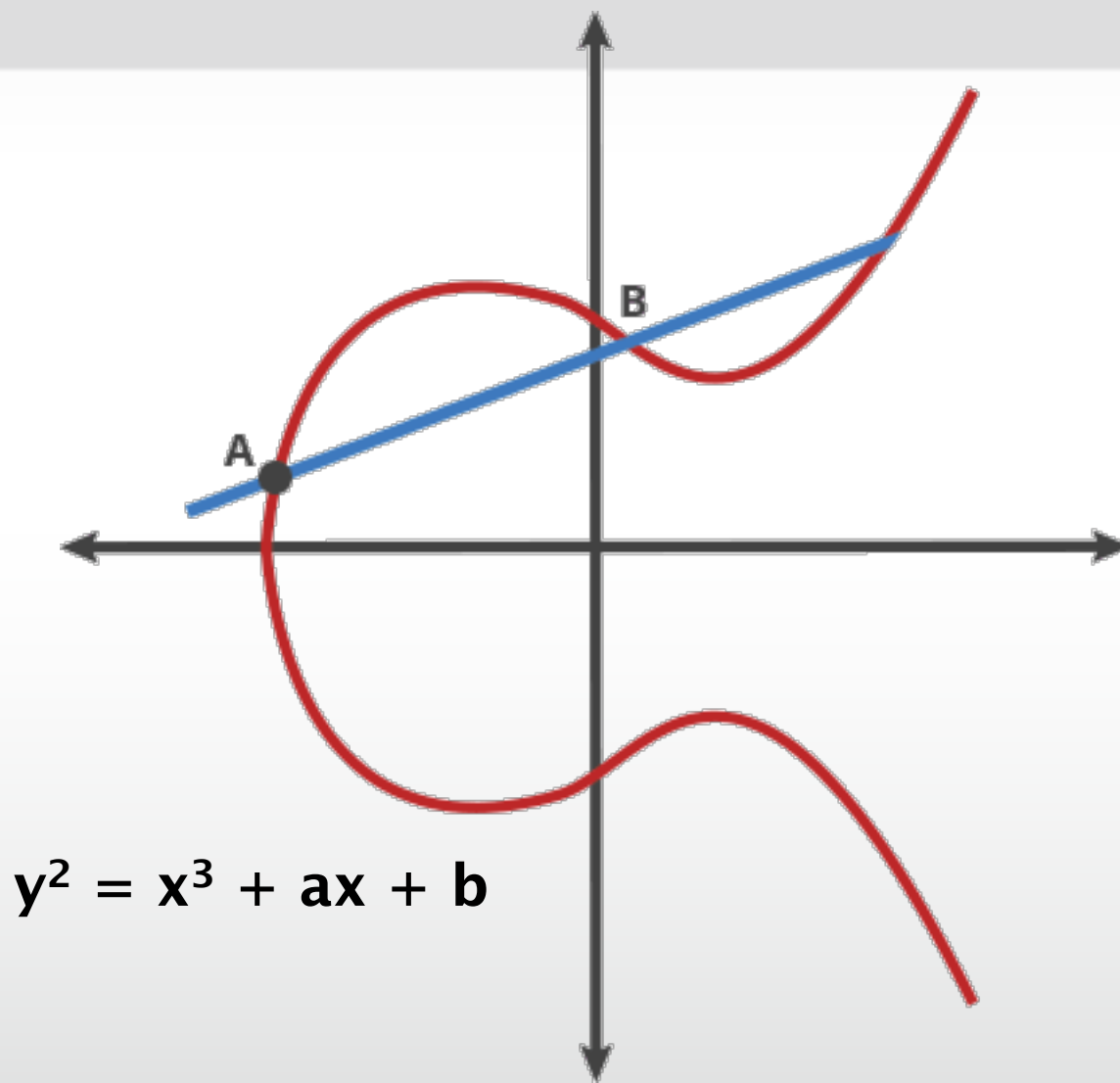
$$2 + 2 = \underline{4}$$



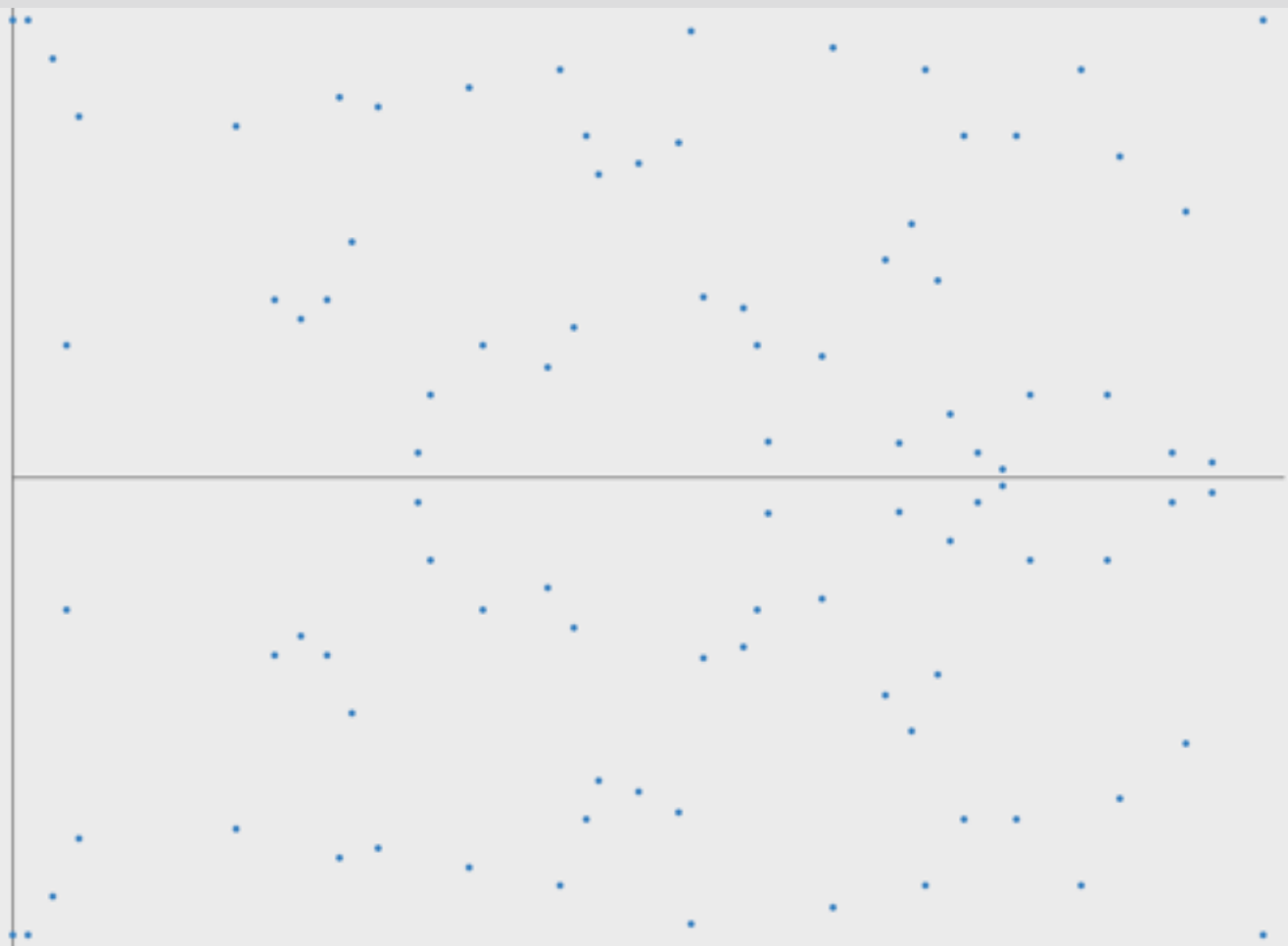
# 大数分解

00a330f8e89464f79c224aced0aff2  
9de10615243d626b6c15639219b771  
540e6a0cbda286b5e60a9f1967f937  
2e55fc0e5e3525c01bc520d3c2597a  
223c114340b561ed7533017d7ea5b9  
7b30d3d7519b7189518ce89ce00ebe  
bf8946b8cf515bf6d4615189748691  
f174d07d56da1e21862968bf747b62  
b850788e448cab30b40ebbc11f3e79  
14ef4f689999de39a9cabba61d61f6  
ca6480208457daff85e035174e51e2  
61d049bbc42964dc3516be2811d818  
459f7401aa76f34dcc7b6911dd1118  
fdeca5511747a6d605c6f6738fa1ae  
64f5d01ccf3319b969eac2e63eee6e  
2462ff44bfce593ef5f87423e70d25  
c3bd457ef7c0f169af4a5cec0cd7d3a5bf

# 椭圆曲线离散对数



# 椭圆曲线离散对数

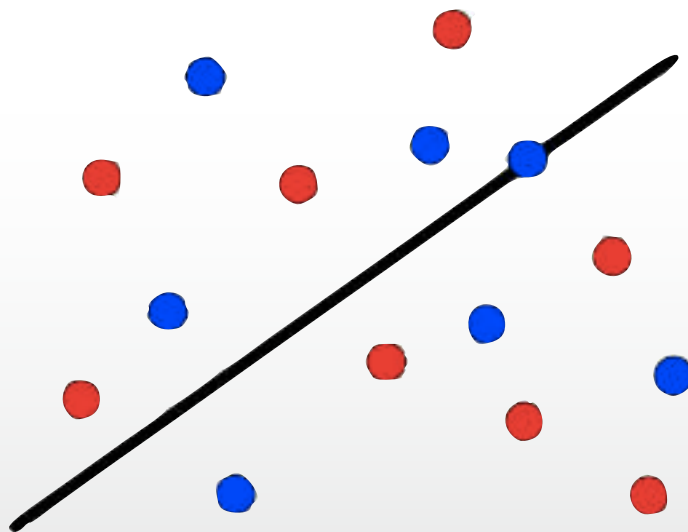


# 哈希函数

- 单向



- 离散





# 几个基础算法



# RSA算法


1. 选择随机质数 $p, q$
2. 计算 $n=p*q$ ,  $n$ 应大于等于2048位
3. 根据欧拉函数计算  $\phi(n)=(p-1)(q-1)$
4. 选择随机数 $e$ ,  $e$ 与 $\phi(n)$ 互质。
5. 使用扩展欧拉函数计算 $d$ , 使 $e*d=1(\text{mod } n)$
6. 公钥是 $(n,e)$ , 私钥是 $(n,d)$

# RSA算法

加密消息  
 $C = m^e \pmod n$

解密消息  
 $m = C^d \pmod n$

# ECC算法


- 
1. 选择一条椭圆曲线和基点 $G$ 。一般由加密标准规定
  2. 随机选择数字 $k$ 作为私钥
  3. 计算 $G$ 的 $k$ 倍点 $P$ ，作为公钥

# ECC算法

计算公共秘密  
 $k_a * P_b = k_a * k_b * G$   
 $k_b * P_a = k_b * k_a * G$

多种算法  
ECDH  
ECDSA

# 非对称算法特性




用公钥加密的消息，  
能且只能使用私钥解密

反之亦然



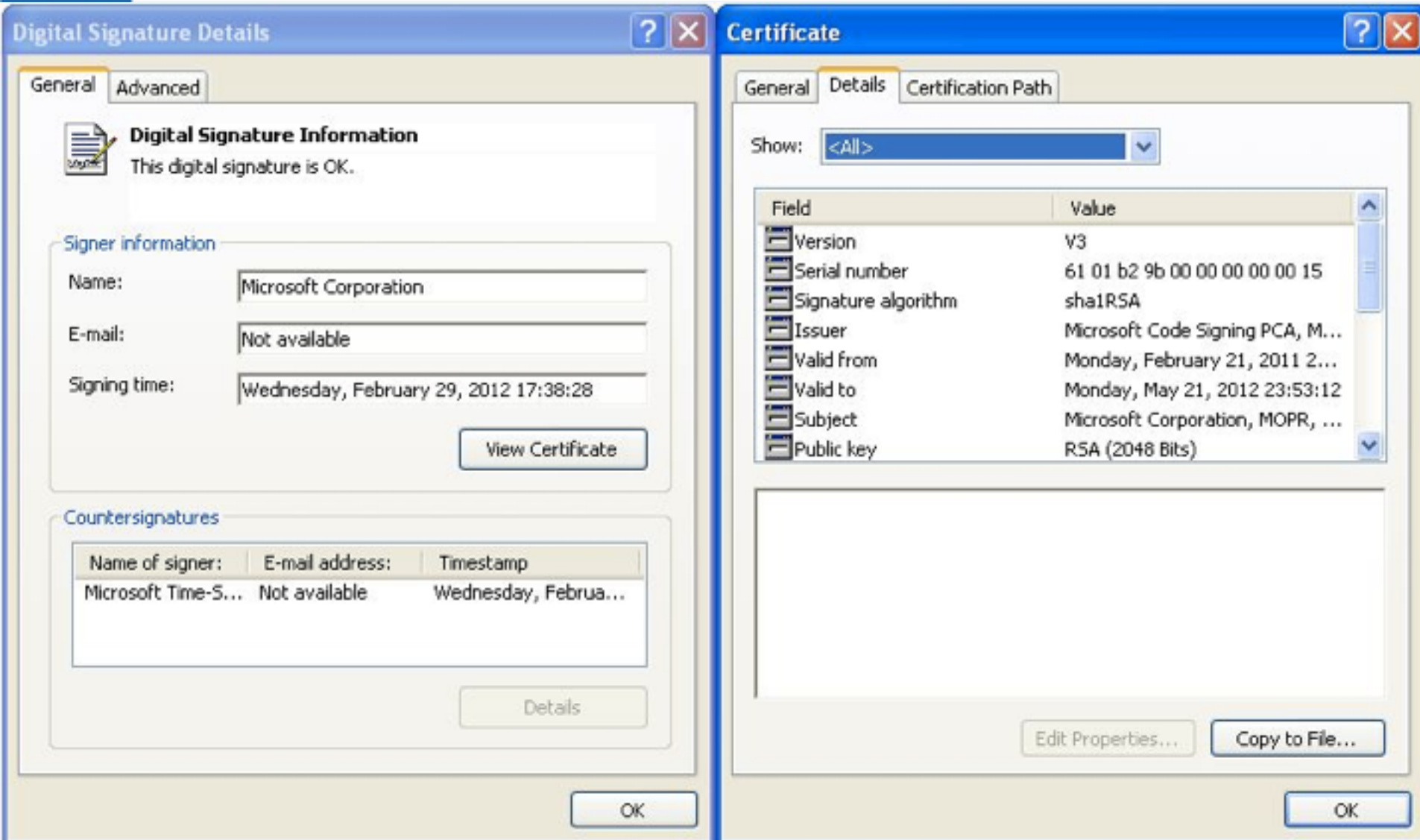
# 非对称加/解密


$$E = \text{enc}(m, \text{pubkey})$$

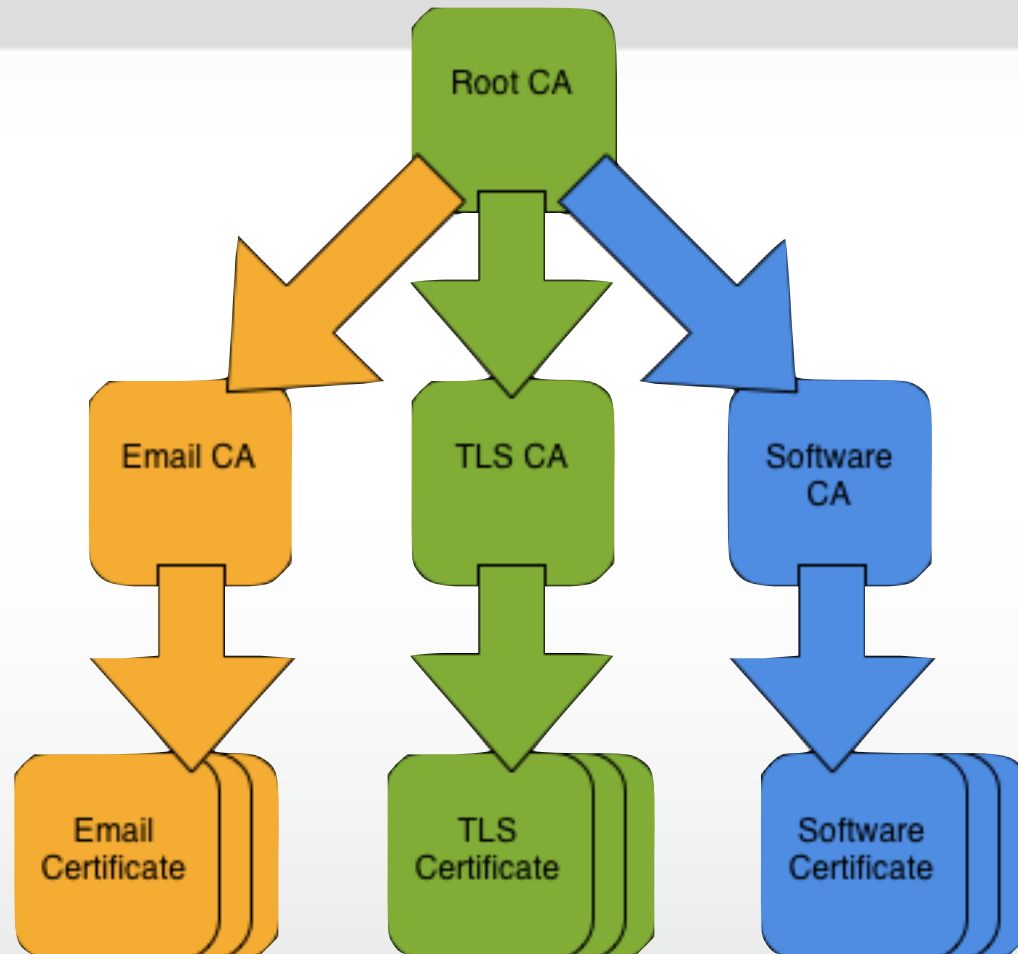
# 数字签名


$$S = \text{sign}(m, \text{privkey})$$

# PKI



# PKI



# PKI

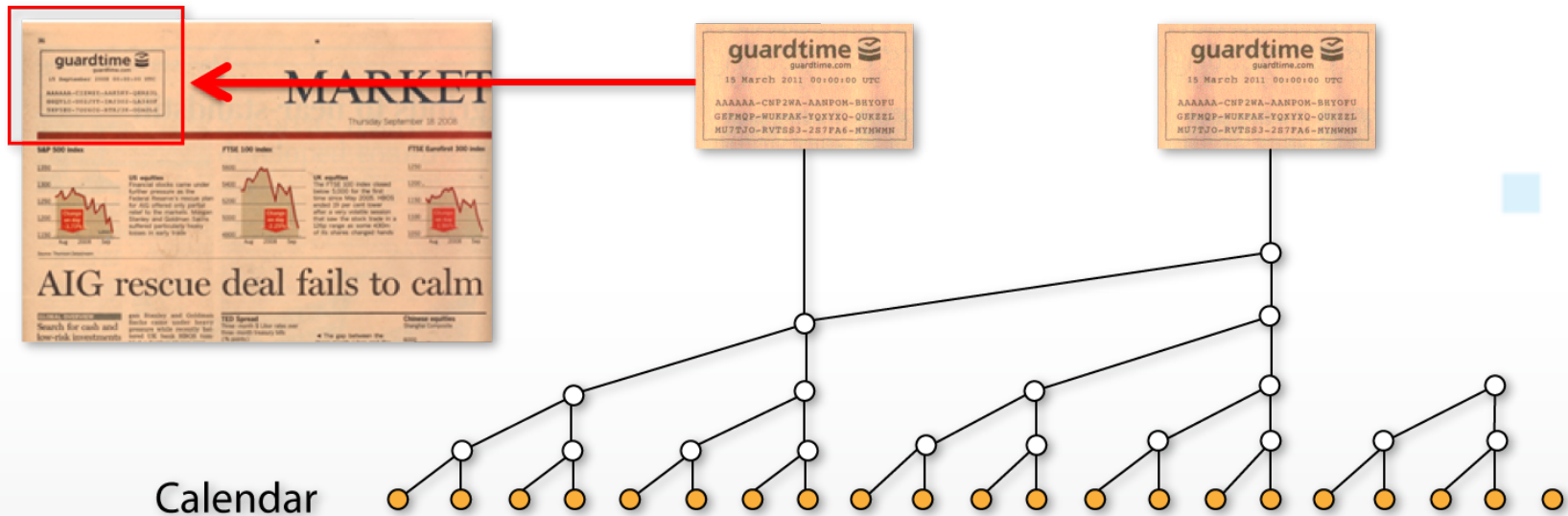
- 密钥管理简化
- 强身份
- 防篡改
- 抗抵赖

# 新技术KSI

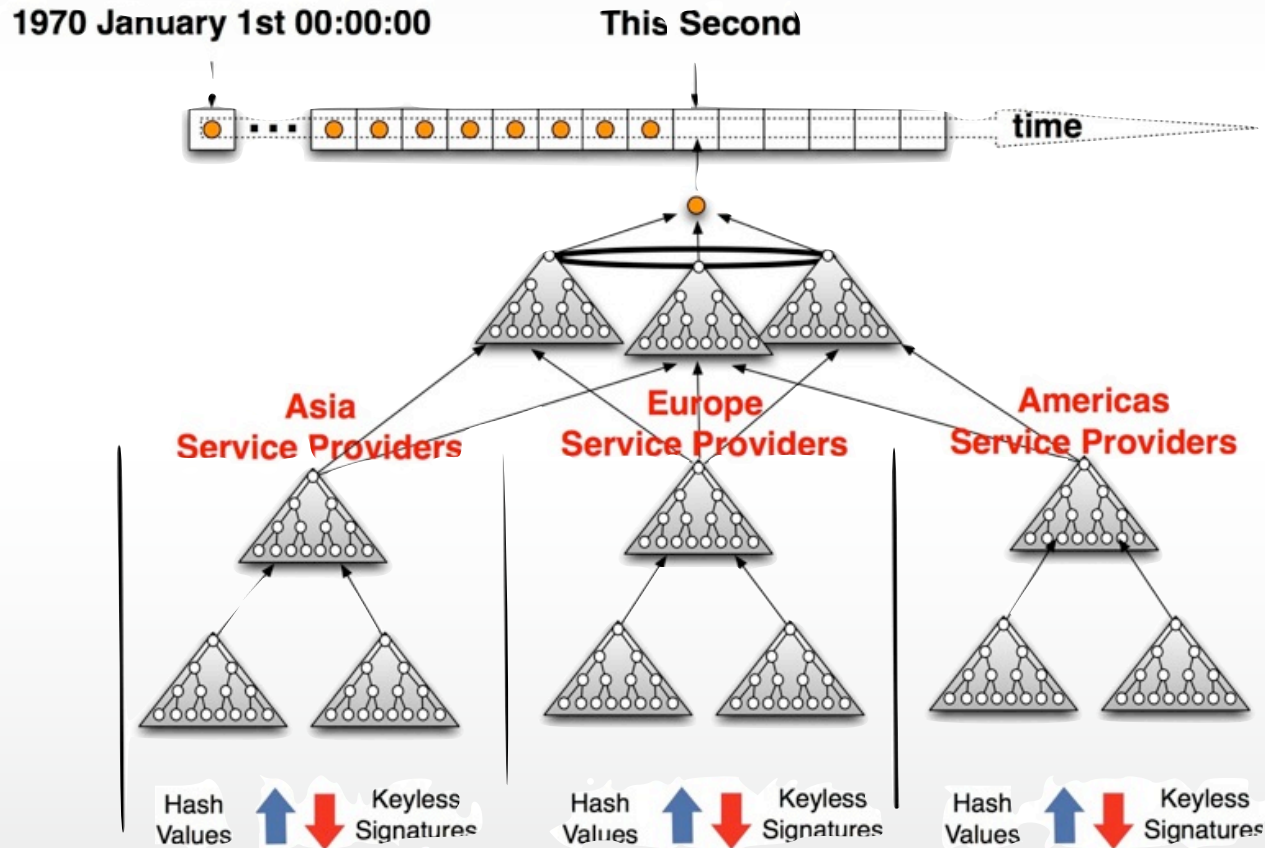
- 无钥签名
- 以Hash技术为基础
  - 单向性
  - 难以伪造特定哈希值的原文
  - 效率极高
  - 以SHA-1/SHA-2为代表



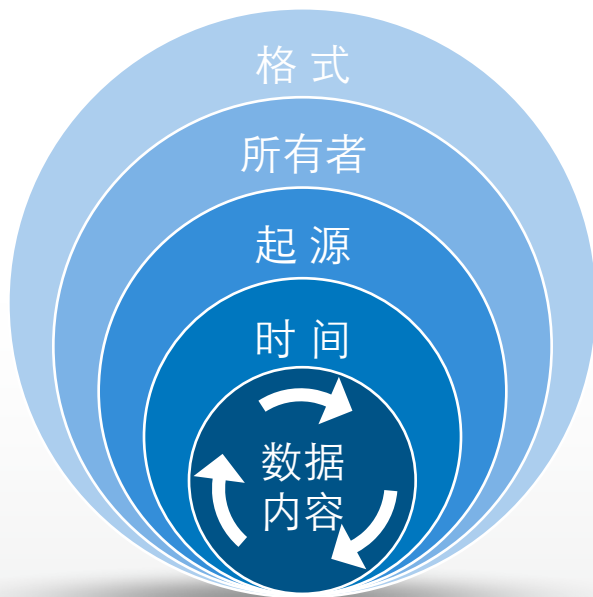
# KSI: GuardTime



# KSI: GuardTime



# KSI: GuardTime



# 国产算法

- 非对称加解密算法 SM-2
- 哈希算法 SM-3
- 对称加解密 SM-1/SM-4

# 项目案例



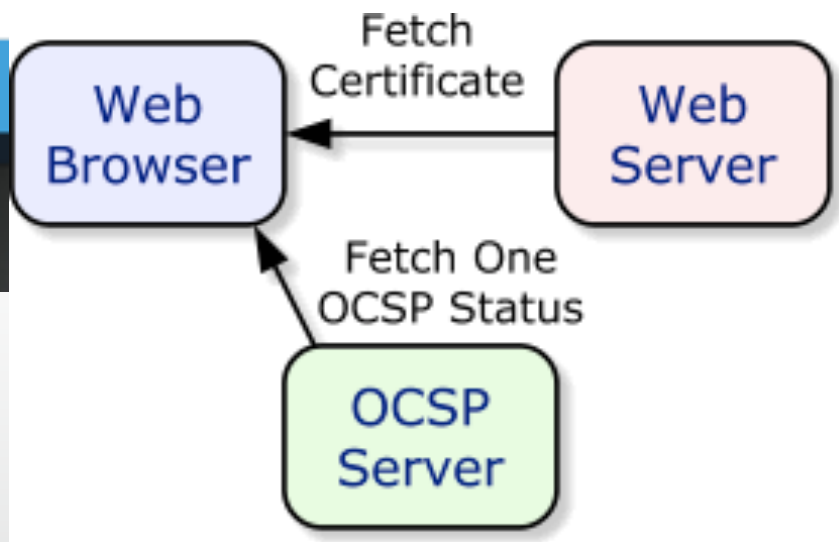
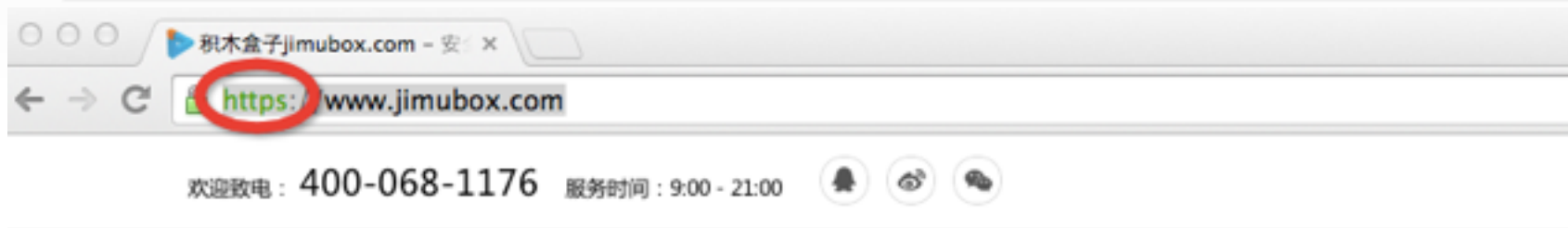


# 积木盒子

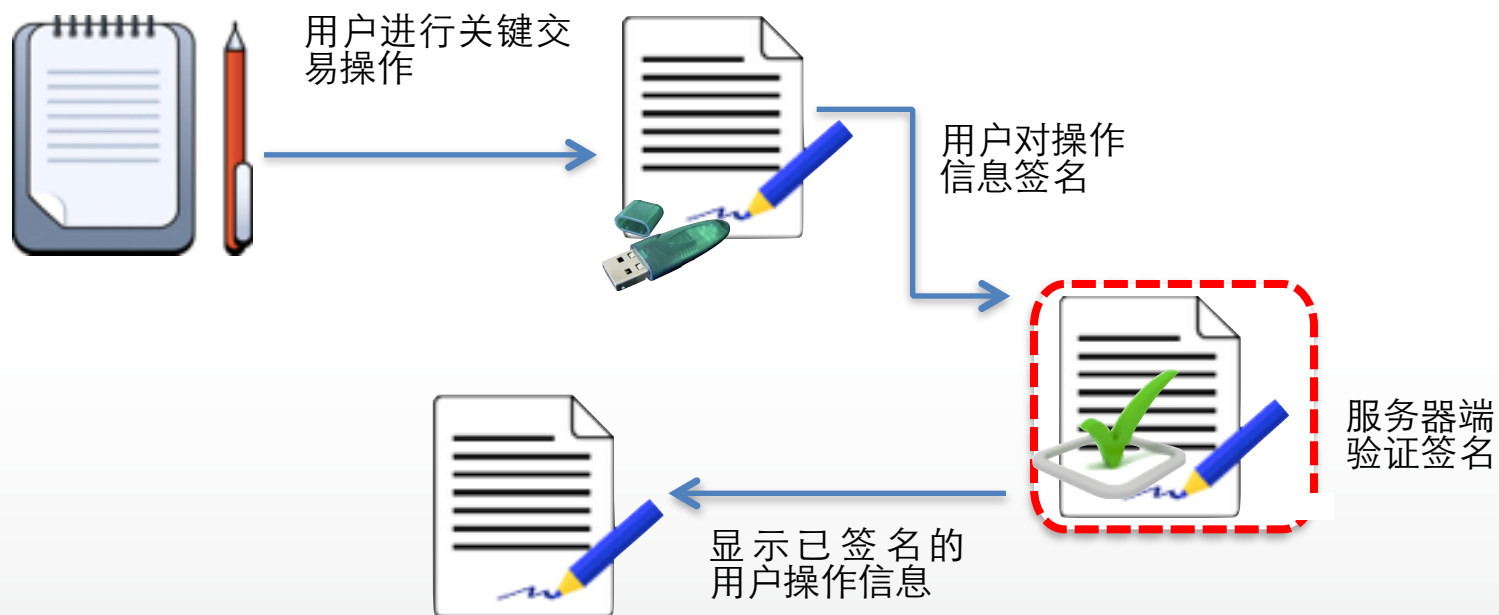




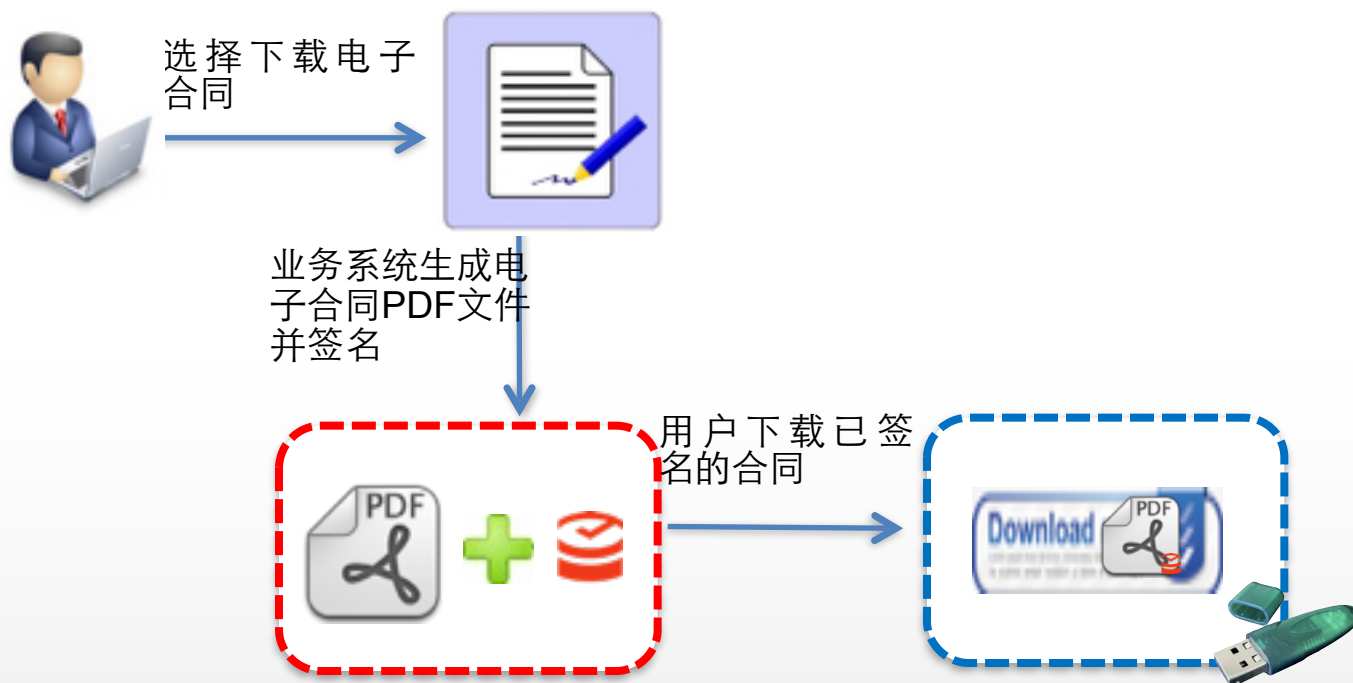
# SSL通信



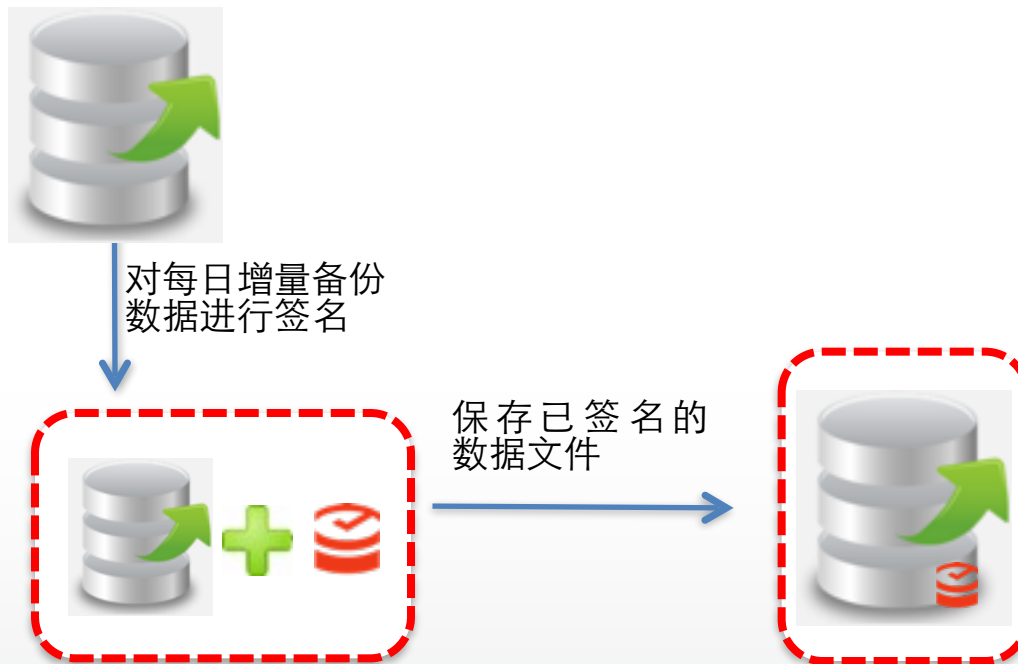
# 交易签名



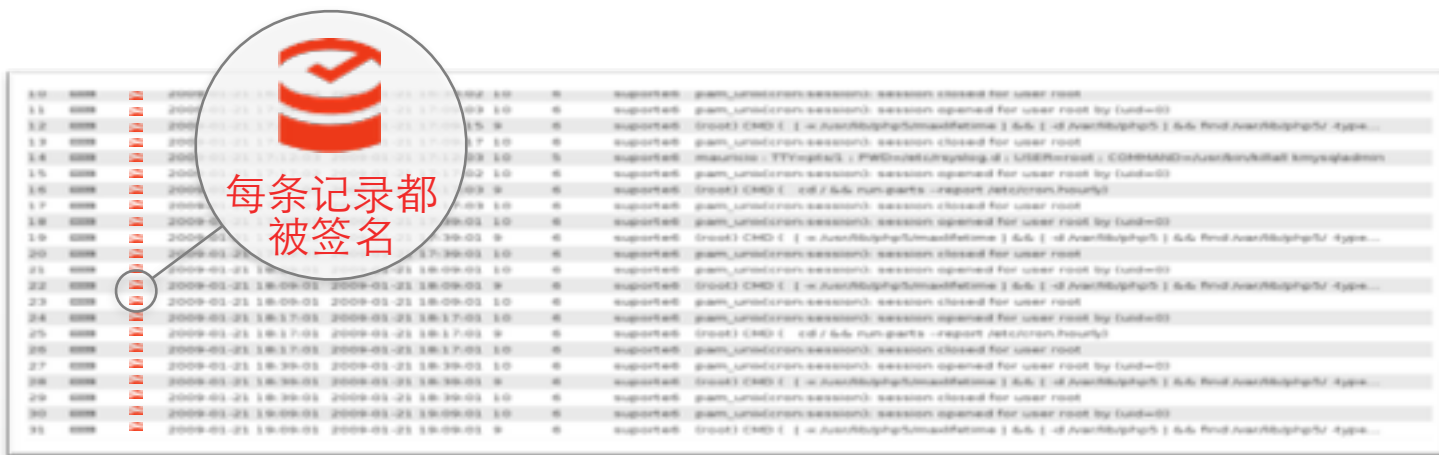
# 电子文件签名



# 数据备份签名



# 后台日志签名



# 项目效果

- 服务器身份证明
- 通信加密
- 电子交易签名
- 运行期数据签名

# 回顾

- 几个数学难题
- 几个基础算法
- 一个项目案例

# 单淼



- @善良三水



- @samuelshan



- 18601156318



- [shm.shan@gmail.com](mailto:shm.shan@gmail.com)





# Q&A



Brought by **InfoQ**



# 感谢聆听

Brought by **InfoQ**