

一段话总结

数字签名作为公钥密码学中实现消息完整性与认证的核心技术，与消息认证码相比，其优势在于支持公开验证、可传递性及不可否认性，能让签名者用私钥签名、验证者用公钥核实。文档介绍了基于RSA和离散对数问题的签名方案，如存在安全缺陷的Plain RSA、借助随机预言机模型保障安全的RSA-FDH，以及基于 identification scheme 转换的Schnorr签名，还阐述了数字证书与公钥基础设施（PKI）在公钥安全分发中的作用，最后以TLS协议为例展示了数字签名在实际网络安全中的综合应用。

思维导图



详细总结

一、数字签名与消息认证码（MAC）的对比

特性	数字签名	MAC
密钥类型	公私钥对（公钥公开）	共享私钥
验证方式	任何人可用公钥验证	仅共享密钥方验证
不可否认性	支持（签名者无法否认）	不支持（双方均可生成）
密钥管理	公钥可公开分发，私钥需保密	每对通信方需独立密钥
应用场景	开放系统、第三方验证	封闭系统、双方通信

## 二、安全模型：Existential Unforgeability

定义：攻击者无法在适应性选择消息攻击下，伪造未被签名过的消息的有效签名。 - 实验描述：攻击者获公钥和签名预言机访问，若能输出未签名消息的有效签名则成功，安全方案要求此概率可忽略。

## 三、具体签名方案

### 1. RSA-based方案

#### - Plain RSA

- 流程：签名为( $\sigma = m^d \pmod N$ )，验证( $m = \sigma^e \pmod N$ )。

- 攻击： - 无消息攻击：选随机( $\sigma$ )，算( $m = \sigma^e \pmod N$ )伪造签名。 - 乘积攻击：若有( $m_1, m_2$ )的签名，可伪造( $m = m_1 \cdot m_2$ )的签名。

#### - RSA-FDH

- 流程：先哈希消息( $H(m)$ )，签名为( $\sigma = H(m)^d \pmod N$ )，验证( $H(m) = \sigma^e \pmod N$ )。

- 安全：在随机预言机模型下，基于RSA问题困难性。

### 2. 离散对数-based方案

#### - Schnorr签名

- 流程： 1. 选( $k$ )算( $l = g^k$ )，哈希得( $r = H(l, m)$ )。 2. 签名( $s = rx + k \pmod q$ )，验证( $g^s \cdot y^{-r} = l$ )。 - 安全：基于离散对数问题，通过Fiat-Shamir转换从identification scheme而来。

#### - DSA/ECDSA

- 注意事项：随机数( $k$ )必须严格随机，重复使用( $k$ )可泄露私钥，如Sony PS3因( $k$ )重复被攻击。

## 四、证书与公钥基础设施 (PKI)

- 证书结构：CA用私钥签名的“实体身份-公钥”绑定，如( $\text{cert} = \text{Sign}\{sk\{CA\}}("Bob's key is pk\_B")$ )。 - PKI模型 - 单CA：所有人信任唯一CA，需安全获取CA公钥。 - 证书链：根CA签中间CA，中间CA签用户公钥，如( $\text{cert}\{\text{根} \rightarrow \text{中间}\}, \text{cert}\{\text{中间} \rightarrow \text{用户}\}$ )。 - 证书管理 - 过期：证书含失效日期，如1年后过期。 - 撤销：CA发布证书撤销列表 (CRL)，含失效证书序列号。

## 五、实际应用：TLS协议 - 握手阶段

1. 客户端与服务器进行Diffie-Hellman密钥交换，服务器发送公钥及CA签名的证书。

2. 客户端验证证书有效性，用服务器公钥验证握手消息签名，防止中间人攻击。 - 安全性：结合数字签名认证服务器身份，确保密钥交换安全，提供forward secrecy (Diffie-Hellman临时密钥删除后，旧会话密钥不被泄露)。

### 关键问题

#### 1. 问题：数字签名与MAC在实现不可否认性上的本质区别是什么？

答案：数字签名基于公钥密码学，签名由私钥生成，公钥验证，签名者无法否认；MAC依赖共享私钥，通信双方均可生成标签，无法区分签名者身份，故无法提供不可否认性。

#### 2. 问题：RSA-FDH为何比Plain RSA更安全？

答案：Plain RSA直接对消息签名，易受代数攻击；RSA-FDH通过随机预言机将消息哈希为固定长度值再签名，在随机预言机模型下，若RSA问题困难，则无法伪造签名，且哈希的抗碰撞性防止消息篡改。

### 3. 问题：TLS中如何利用数字签名保障通信安全？

答案：TLS中服务器发送含CA签名的公钥证书，客户端验证证书确认服务器身份；服务器用私钥签名握手消息，客户端用公钥验证，确保消息未被篡改，结合Diffie-Hellman交换密钥，实现身份认证与密钥安全协商。