



# 密码学

(第十二讲)

数字签名(2)

张焕国

武汉大学计算机学院

# 目 录

- 1、密码学的基本概念
- 2、古典密码
- 3、数据加密标准（DES）
- 4、高级数据加密标准（AES）
- 5、中国商用密码（SMS4）
- 6、分组密码的应用技术
- 7、序列密码
- 8、习题课：复习对称密码
- 9、公开密钥密码（1）

# 目 录

- 10、公开密钥密码 (2)
- 11、数字签名 (1)
- 12、**数字签名 (2)**
- 13、HASH函数
- 14、认证
- 15、密钥管理
- 16、PKI技术
- 17、习题课：复习公钥密码
- 18、总复习/检查：**综合实验**

## 三、利用ELGamal密码实现数字签名

### 2、利用ELGamal密码实现数字签名：

#### 密钥选择

- 选 $P$ 是一个大素数， $p-1$ 有大素数因子， $a$ 是一个模 $p$ 的本原元，将 $p$ 和 $a$ 公开。
- 用户随机地选择一个整数 $x$ 作为自己的秘密的解密密钥， $1 < x < p-2$ 。
- 计算  $y = a^x \text{ mod } p$ ，取 $y$ 为自己的公开的加密钥。

## 三、利用ELGamal密码实现数字签名

### 产生签名

设明文消息 $m$ 加签名,  $0 < m < p-1$ , 其签名过程如下:

- 用户A随机地选择一个整数  $k$ ,  $1 < k < p-1$ , 且  $(k, p-1) = 1$ ;
- 计算  $r = g^k \bmod p$
- 计算  $s = (m - xr)k^{-1} \bmod p-1$
- 取  $(r, s)$  作为 $m$ 的签名, 并以  $\langle m, r, s \rangle$  的形式发给用户B。

m	r	s
---	---	---

### 三、利用ELGamal密码实现数字签名

#### 验证签名

- 用户B接收： $\langle m, r, s \rangle$
- 用户B用A的公钥 $y$ 验证： $m = y^r r^s \pmod{p}$ ，是否成立，若成立则签名为真，否则签名为假。
- 签名的可验证性可证明如下：

因为 $s = (m - xr) k^{-1} \pmod{p-1}$ ,

所以 $m = xr + ks \pmod{p-1}$ ,

故 $m = xr + ks = (x)^r (k)^s = y^r r^s \pmod{p}$ ，  
故签名可验证。

## 三、利用ELGamal密码实现数字签名

### 验证签名

- 安全性
- 从公开密钥求私钥是离散对数问题。
- $p-1$ 要有大素数因子, 否则易受攻击。
- 为了安全, 随机数 $k$ 应当是一次性的。否则时间一长,  $k$ 将可能泄露。因为,  
$$x = (m - ks)r^{-1} \bmod p-1,$$
如果知道了 $m$ , 便可求出保密的解密密钥。

## 三、利用ELGamal密码实现数字签名

### 验证签名

- 安全性

- 如果 $k$ 重复使用，如用 $k$ 签名 $m_1$ 和 $m_2$ 。于是，

$$m_1 = xr + ks_1 \text{ mod } p-1,$$

$$m_2 = xr + ks_2 \text{ mod } p-1,$$

于是， $(s_1 - s_2)k = (m_1 - m_2) \text{ mod } p-1$

如果知道了 $m_1$ 和 $m_2$ ，便可求出 $k$ ，进而求出保密的解密密钥。

- 由此可知，不要随便给别人签名。
- 不要直接对 $m$ 签名，而是对 $\text{HASH}(m)$ 签名。



## 三、利用ELGamal密码实现数字签名

### 3、 ELGamal密码签名的应用

- 美国数字签名标准 (DSS) 的签名算法 DSA是它的一种变形。
- 安全，方便。
- 缺点：由于取  $(r, s)$  作为  $m$  的签名，所以数字签名的长度是明文的两倍。数据扩张严重。

## 四、利用椭圆曲线密码实现数字签名

- 一个椭圆曲线密码由下面的六元组描述：

$$T = \langle p, a, b, G, n, h \rangle$$

其中， $p$ 为大于3素数， $p$ 确定了有限域 $GF(p)$ ；元素 $a, b \in GF(p)$ ， $a$ 和 $b$ 确定了椭圆曲线； $G$ 为循环子群 $E_1$ 的生成元， $n$ 为素数且为生成元 $G$ 的阶， $G$ 和 $n$ 确定了循环子群 $E_1$ 。

$$y^2 = x^3 + ax + b \pmod{p}$$

## 四、利用椭圆曲线密码实现数字签名

$d$ 为用户的私钥，公开钥为 $Q$ 点， $Q=dG$ 。

### 1、产生签名

- 选择一个随机数 $k$ ， $k \in \{1, 2, \dots, n-1\}$ ；
- 计算点 $R(x_R, y_R) = kG$ ，并记 $r = x_R$ ；
- 利用保密的解密密钥 $d$ 计算：
$$s = (m - dr)k^{-1} \bmod n$$
；
- 以 $\langle r, s \rangle$ 作为消息 $m$ 的签名，并以 $\langle m, r, s \rangle$ 的形式传输或存储。

## 四、利用椭圆曲线密码实现数字签名

### 2、验证签名

计算  $s^{-1} \bmod n$  ;

利用公开的加密钥  $Q$  计算

$$U(x_U, y_U) = s^{-1}(mG - rQ);$$

如果  $x_U = r$  , 则  $\langle r, s \rangle$  是用户A对  $m$  的签名。

- 证明：因为  $s = (m - dr) k^{-1} \bmod n$  , 所以
$$s^{-1} = (m - dr)^{-1} k \bmod n ,$$
- 所以  $U(x_U, y_U) = (m - dr)^{-1} k (mG - rQ)$ 
$$= (m - dr)^{-1} (mkG - krdG) = (m - dr)^{-1} (mR - rdR)$$
$$= (m - dr)^{-1} R (m - dr) = R(x_R, y_R) .$$
- 所以  $x_U = x_R = r$  .

## 四、利用椭圆密码实现数字签名

### 3、椭圆曲线密码签名的应用

- 2000年美国已政府已将椭圆曲线密码引入数字签名标准DSS。
- 安全，密钥短、软硬件实现节省资源等特点。

## 五、盲签名

- 在普通数字签名中，签名者总是先知道数据的内容后才实施签名，这是通常的办公事务所需要的。但有时却需要某个人对某数据签名，而又不能让他知道数据的内容。称这种签名为盲签名（Blind Signature）。在无记名投票选举和数字货币系统中往往需要这种盲签名，
- 盲签名在电子商务和电子政务系统中有着广泛的应用前景。

## 五、盲签名

**盲签名与普通签名相比有两个显著的特点：**

**签名者不知道所签署的数据内容；**

**在签名被接收者泄露后，签名者不能追踪签名。即：如果把签名的数据给签名者看，他确信是自己的签名，但他无法知道什么时候对什么样的盲数据施加签名而得到此签名数据。**

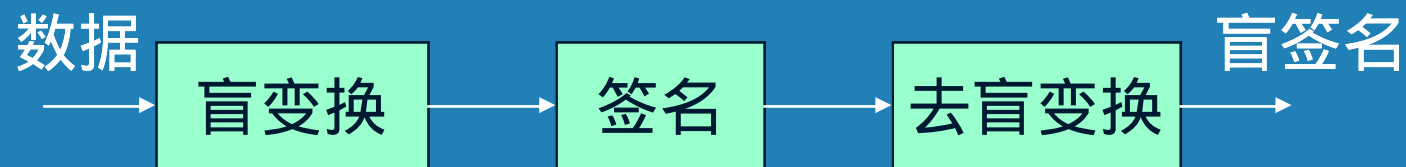
## 五、盲签名

- 接收者首先将待签数据进行盲变换，把变换后的盲数据发给签名者。
- 经签名者签名后再发给接收者。
- 接收者对签名再作去盲变换，得出的便是签名者对原数据的盲签名。
- 这样便满足了条件  $S^{-1}(S(m)) = m$ 。要满足条件  $S^{-1}(S(m)) = m$ ，必须使签名者事后看到盲签名时不能与盲数据联系起来，这通常是依靠某种协议来实现的。



## 五、盲签名

- 盲签名原理图：



## 五、盲签名

### 1、RSA盲签名

A  $\xrightarrow{M}$  B

A对消息M进行盲化处理：他随机选择盲化整数  $k, 1 < k < M$ ，并计算

$$T = M(k)^e \pmod n。$$

**A把T发给B。**

B对T签名：

$$\begin{aligned} T^d &= (Mk^e)^d \pmod n \\ &= (M)^d k \pmod n \end{aligned}$$

## 五、盲签名

### 1、RSA盲签名

**B**把他对T的签名发给A。

**A**通过计算得到B对M的签名。

$$\begin{aligned} S &= T^d / k \pmod n \\ &= M^d \pmod n \end{aligned}$$

- **正确性证明：**

因为  $T^d = (Mk^e)^d = M^d k \pmod n$ ，所以

$T^d / k = M^d \pmod n$ ，而这恰好是B对消息M的签名。

## 五、盲签名

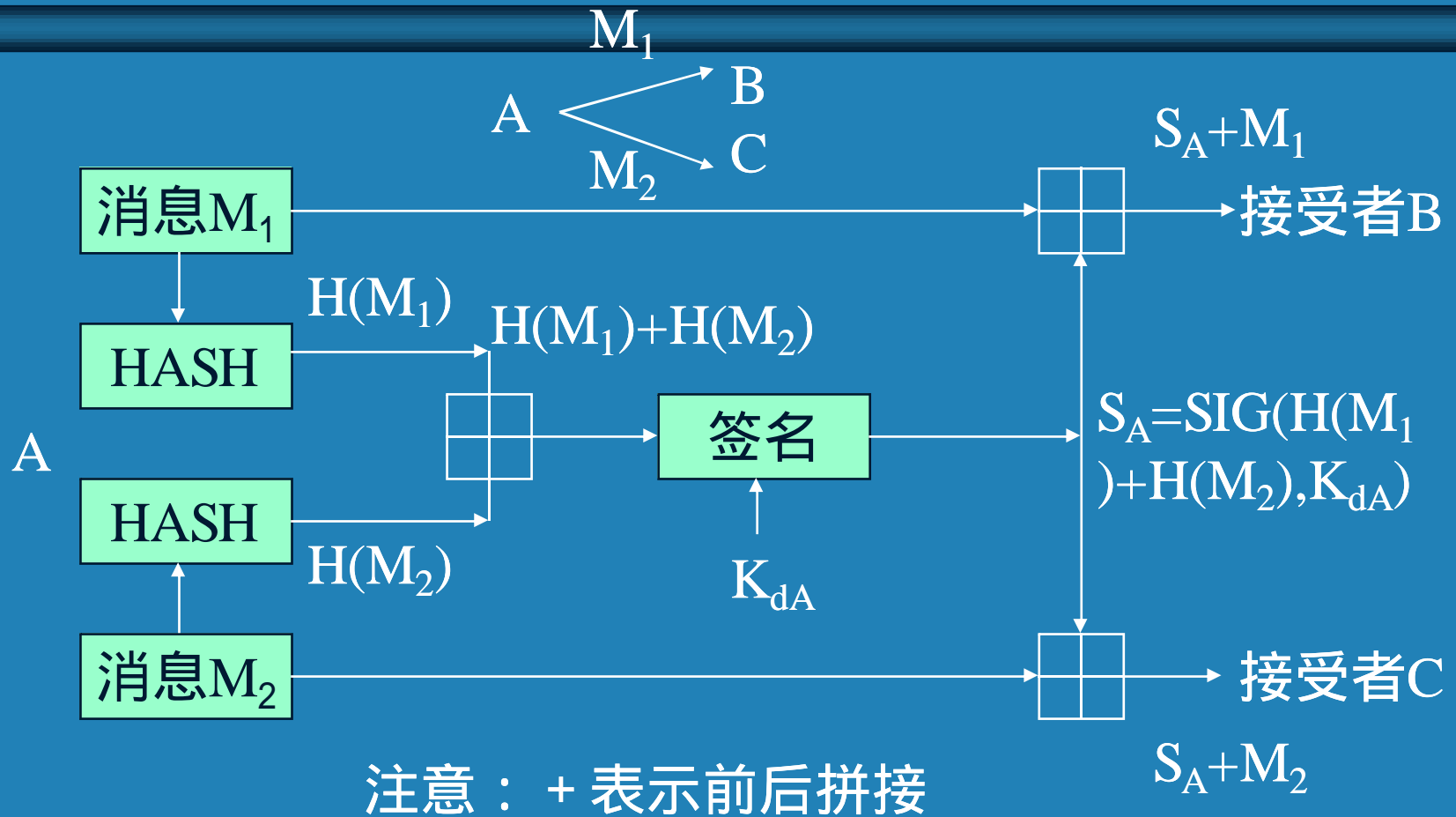
- 盲签名在某种程度上保护了参与者的利益，但不幸的是盲签名的匿名性可能被犯罪份子所滥用。为了阻止这种滥用，人们又引入了公平盲签名的概念。公平盲签名比盲签名增加了一个特性，即建立一个可信中心，通过可信中心的授权，签名者可追踪签名。

## 五、盲签名

### 2、双联签名

- 双联签名是实现盲签名的一种变通方法。它利用协议和密码将消息与人关联起来而并不需要知道消息的内容。从而实现盲签名。
- 双联签名采用单向HASH函数和数字签名技术相结合，实现盲签名的两个特性。

# 五、盲签名



## 五、盲签名

- 接收者B和C都可用发信者A的公开钥验证双联签名 $S_{A_0}$ ，获得 $H(M_1)$ 和 $H(M_2)$ 。
- B只能阅读 $M_1$ ，计算 $H(M_1)$ ，通过 $H(M_1)$ 验证 $M_1$ 是否正确。而对消息 $M_2$ 却一无所知，但通过验证签名 $S_A$ 可以相信消息 $M_2$ 的存在。
- 同样，C也只能阅读 $M_2$ ，计算 $H(M_2)$ ，通过 $H(M_2)$ 验证 $M_2$ 是否正确。而对消息 $M_1$ 却一无所知，但通过验证签名 $S_A$ 可以相信消息 $M_1$ 的存在。

## 五、盲签名

- 优点：发信者对两个消息 $M_1$  和 $M_2$ 只需要计算一个签名。
- 在电子商务系统中，许多支付系统都采用这一方案。这是因为在一次支付过程中，显然有两个关联数据，一个是关于财务数据，另一个是关于所购的物品数据。



# 习题

说明在ELGamal密码签名中，参数 $k$ 为什么必须是一次性的。

说明在椭圆曲线密码签名中，参数 $k$ 有无一次性的要求。



谢谢！