# 第7章 签名方案

苏 明

# 概览

- 7．1 引言
- 7．2 签名方案的安全性需求
- 7．3 ElGamal签名方案
- 7．4 ElGamal签名方案的变形
  - Schnorr签名方案
  - 数字签名算法(DSA)
  - 椭圆曲线DSA

# 7.1 引言

- Digital Signature

**定义** 一个签名方案是一个满足下列条件的 5 元组 $(\mathcal{P}, \mathcal{A}, \mathcal{K}, \mathcal{S}, \mathcal{V})$：

1. $\mathcal{P}$ 是由所有可能的消息组成的一个有限集合。
2. $\mathcal{A}$ 是由所有可能的签名组成的一个有限集合。
3. $\mathcal{K}$ 为密钥空间，它是由所有可能的密钥组成的一个有限集合。
4. 对每一个 $K \in \mathcal{K}$，有一个签名算法 $\mathrm{sig}_K \in \mathcal{S}$ 和一个相应的验证算法 $\mathrm{ver}_K \in \mathcal{V}$。对每一个消息 $x \in \mathcal{P}$ 和每一个签名 $y \in \mathcal{A}$，每个 $\mathrm{sig}_K : \mathcal{P} \to \mathcal{A}$ 和 $\mathrm{ver}_K : \mathcal{P} \times \mathcal{A} \to \{\mathrm{true}, \mathrm{false}\}$ 都是满足下列条件的函数：

$$\mathrm{ver}_K(x, y) = \begin{cases} \mathrm{true} & y = \mathrm{sig}_K(x) \\ \mathrm{false} & y \neq \mathrm{sig}_K(x) \end{cases}$$

由 $x \in \mathcal{P}$ 和 $y \in \mathcal{A}$ 组成的对 $(x, y)$ 称为签名消息。

# 7. 2 签名方案的安全性需求

- 攻击模型
  - **key-only attack**
  - **known message attack**
  - **chosen message attack**

- 攻击目标
  - total break
  - selective forgery
  - existential forgery

# 7.3 ElGamal签名方案

**密码体制** ElGamal 签名方案

设 $p$ 是一个使得在 $\mathbb{Z}_p$ 上的离散对数问题是难处理的素数，设 $\alpha \in \mathbb{Z}_p^*$ 是一个本原元。设 $\mathcal{P} = \mathbb{Z}_p^*, \mathcal{A} = \mathbb{Z}_p^* \times \mathbb{Z}_{p-1}$，定义

$$\mathcal{K} = \{(p, \alpha, a, \beta) : \beta \equiv \alpha^a \pmod p\}$$

值 $p, \alpha, \beta$ 是公钥，$a$ 是私钥。

对 $K = (p, \alpha, a, \beta)$ 和一个(秘密的)随机数 $k \in \mathbb{Z}_{p-1}^*$，定义

$$\underline{\mathrm{sig}_K(x, k) = (\gamma, \delta)}$$

其中

$$\gamma = \alpha^k \bmod p，\quad \delta = (x - a\gamma)k^{-1} \bmod (p-1)$$

对 $x, \gamma \in \mathbb{Z}_p^*$ 和 $\delta \in \mathbb{Z}_{p-1}$，定义

$$\mathrm{ver}_K(x, (\gamma, \delta)) = \mathrm{true} \Leftrightarrow \underline{\beta^\gamma \gamma^\delta \equiv \alpha^x \pmod p}$$

# Security: Elgamal Digital Signature

1. Finite field Discrete Logarithm
2. Hash function
3. Randomness of PRNG
4. Solving a linear equation with two unknowns

# 7.3 ElGamal签名方案安全性

- 假定没有使用Hash(x)
- 存在性伪造： 设法求出满足***签名方程***的参数

- 使用不当：k(***随机值***)泄露→推算出私钥
- 对不同消息签名使用相同k值

# 7.4 变形-Schnorr签名方案

- 缩短签名-支持智能卡的使用
- 签名方程在Zp*的q元子群中构建

---

**密码体制** Schnorr 签名方案

设 $p$ 是使得 $\mathbb{Z}_p^*$ 上离散对数问题难处理的一个素数，$q$ 是能被 $p-1$ 整除的素数。设 $\alpha \in \mathbb{Z}_p^*$ 是 1 模 $p$ 的 $q$ 次根，$\mathcal{P} = \{0,1\}^*$, $\mathcal{A} = \mathbb{Z}_q \times \mathbb{Z}_q$，并定义

$$\mathcal{K} = \{(p, q, \alpha, a, \beta) : \beta \equiv \alpha^a \pmod p\}$$

其中$0 \leqslant a \leqslant q-1$，值 $p$，$q$，$\alpha$ 和 $\beta$ 是公钥，$a$ 为私钥。最后，设$h:\{0,1\}^* \to \mathbb{Z}_q$ 是一个安全 Hash 函数。

对于 $K = (p, q, \alpha, a, \beta)$ 和一个(秘密的)随机数$k$，$1 \leqslant k \leqslant q-1$，定义

$$\mathrm{sig}_K(x, k) = (\gamma, \delta)$$

其中 $\gamma = h(x \| \alpha^k \bmod p)$ 且 $\delta = k + a\gamma \bmod q$。

对于 $x \in \{0,1\}^*$ 和 $\gamma, \delta \in \mathbb{Z}_q$，验证是通过下面的计算完成的：

$$\mathrm{ver}_K(x, (\gamma, \delta)) = \mathrm{true} \Leftrightarrow h(x \| \alpha^\delta \beta^{-\gamma} \bmod p) = \gamma$$

---

# 7.4 变形-DSA

**密码体制 7.4** 数字签名算法(DSA)

设 $p$ 是长为 $L$ 比特的素数，在 $\mathbb{Z}_p$ 上其离散对数问题是难处理的，其中 $L \equiv 0 (\bmod 64)$ 且 $512 \leqslant L \leqslant 1024$， $q$ 是能被 $p-1$ 整除的 160 比特的素数。设 $\alpha \in \mathbb{Z}_p^*$ 是 1 模 $p$ 的 $q$ 次根。设 $\mathcal{P} = \{0,1\}^*, \mathcal{A} = \mathbb{Z}_q^* \times \mathbb{Z}_q^*$，并定义

$$\mathcal{K} = \{(p,q,\alpha,a,\beta) : \beta \equiv \alpha^a (\bmod p)\}$$

其中 $0 \leqslant a \leqslant q-1$。值 $p$， $q$， $\alpha$ 和 $\beta$ 是公钥， $a$ 为私钥。

对于 $K = (p,q,\alpha,a,\beta)$ 和一个(秘密的)随机数 $k$， $1 \leqslant k \leqslant q-1$，定义

$$\mathrm{sig}_K(x,k) = (\gamma,\delta)$$

其中

$$\gamma = (\alpha^k \bmod p) \bmod q$$

$$\delta = (\text{SHA-1}(x) + a\gamma)k^{-1} \bmod q$$

(如果 $\gamma = 0$ 或 $\delta = 0$，应该为 $k$ 另选一个随机数)。

对于 $x \in \{0,1\}^*$ 和 $\gamma, \delta \in \mathbb{Z}_q^*$，验证是通过下面的计算完成的：

$$e_1 = \text{SHA-1}(x)\delta^{-1} \bmod q$$

$$e_2 = \gamma\delta^{-1} \bmod q$$

$$\mathrm{ver}_K(x,(\gamma,\delta)) = \mathrm{true} \Leftrightarrow (\alpha^{e_1}\beta^{e_2} \bmod p) \bmod q = \gamma$$

- **NIST**

要求q为160比特素数
建议p:1024bit 素数
改变签名方程的符号

# 7.4 变形-ECDSA

- DSA VS ECDSA

- Zp上的乘法群→ECC加法群
- ECDSA的第一个分量取 ***kA的x坐标*** 模q

# 7.4 变形-ECDSA

**密码体制** 椭圆曲线数字签名算法

设 $p$ 是一个大素数，$E$ 是定义在 $\mathbb{F}_p$ 上的椭圆曲线。设 $A$ 是 $E$ 上阶为 $q$（$q$ 是素数）的一个点，使得在 $\langle A\rangle$ 上的离散对数问题是难处理的。设 $\mathcal{P}=\{0,1\}^*, \mathcal{A}=\mathbb{Z}_q^*\times\mathbb{Z}_q^*$，定义

$$\mathcal{K}=\{(p,q,E,A,m,B): B=mA\}$$

其中 $0\leqslant m\leqslant q-1$。值 $p$，$q$，$E$，$A$ 和 $B$ 是公钥，$m$ 是私钥。

对于 $K=(p,q,E,A,m,B)$ 和一个（秘密的）随机数 $k$，$1\leqslant k\leqslant q-1$，定义

$$\mathrm{sig}_K(x,k)=(r,s)$$

其中

$$kA=(u,v)$$
$$r=u \bmod q$$

以及

$$s=k^{-1}(\text{SHA-1}(x)+mr) \bmod q$$

（如果 $r=0$ 或 $s=0$，应该为 $k$ 另选一个随机数）。

对于 $x\in\{0,1\}^*$ 和 $r,s\in\mathbb{Z}_q^*$，验证是通过下面的计算完成的：

$$w=s^{-1} \bmod q$$
$$i=w\text{SHA-1}(x) \bmod q$$
$$j=wr \bmod q$$
$$(u,v)=iA+jB$$
$$\mathrm{ver}_K(x,(r,s))=\mathrm{true}\Leftrightarrow u \bmod q=r$$