

密码学原理与实践 (第三版)

第7章 签名方案



苏 明

[加] Douglas R. Stinson 著

冯登国 等译



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 $\text{sig}_K \in \mathcal{S}$ 和一个相应的验证算法 $\text{ver}_K \in \mathcal{V}$ 。对每一个消息 $x \in \mathcal{P}$ 和每一个签名 $y \in \mathcal{A}$, 每个 $\text{sig}_K : \mathcal{P} \rightarrow \mathcal{A}$ 和 $\text{ver}_K : \mathcal{P} \times \mathcal{A} \rightarrow \{\text{true}, \text{false}\}$ 都是满足下列条件的函数:

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

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, α, β 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

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

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

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



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 \mathbb{Z}_p^* 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 $0 \leq a \leq q-1$, 值 p, q, α 和 β 是公钥, a 为私钥。最后, 设 $h: \{0, 1\}^* \rightarrow \mathbb{Z}_q$ 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 , $1 \leq k \leq q-1$, 定义

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

其中 $\gamma = h(x \parallel \alpha^k \bmod p)$ 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:

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

7.4 变形-DISA

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 $L \equiv 0 \pmod{64}$ 且 $512 \leq L \leq 1024$, 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

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

其中 $0 \leq a \leq q-1$ 。值 p , q , α 和 β 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 , $1 \leq k \leq q-1$, 定义

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

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:

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

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

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

■ NIST

要求 q 为 160 比特素数
建议 p : 1024 bit 素数
改变签名方程的符号



7.4 变形-ECDSA

- DSA VS ECDSA
- \mathbb{Z}_p 上的乘法群 \rightarrow 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 $0 \leq m \leq q-1$ 。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 , $1 \leq k \leq q-1$, 定义

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

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:

$$w = s^{-1} \bmod q$$

$$i = w \text{SHA-1}(x) \bmod q$$

$$j = wr \bmod q$$

$$(u, v) = iA + jB$$

$$\text{ver}_K(x, (r, s)) = \text{true} \Leftrightarrow u \bmod q = r$$