

第13章 数字签名与认证协议

1 ElGamal签名方案

该方案是特别为签名的目的而设计的。**1985**年提出，很大程度上为**Diffe-Hellman**密钥交换算法的推广和变形。这个方案的改进已被美国**NIST**（国家标准和技术研究所）采纳作为数字签名标准。

方案： p 为素数， F_p 中的离散对数问题是难处理的。取本原元 $\alpha \in F_p^*$ ，消息集合 $M=F_p^*$ ，签名集合 $A=F_p^* \times Z_{p-1}$ ，定义 $K=\{ (p, \alpha, a, \beta) \mid \beta = \alpha^a \pmod{p} \}$ ，值 p, α 和 β 是公开的， a 是保密的。对 $K=(p, \alpha, a, \beta)$ 和一个（秘密）随机数 $k \in Z_{p-1}^*$ ，我们做

对消息 $x \in M$ 进行签名: $\text{Sig}_k(x, k) = (\gamma, \delta)$,

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

对 x , $\gamma \in F_p^*$ 和 $\delta \in Z_{p-1}$, 验证签名定义为

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

对 **ElGamal** 签名方案安全性的讨论:

若 **Oscar** 在不知道 a 的情况下企图伪造一个给定消息 x 的签名: $\text{Sig}_{\text{Oscar}}(x, k) = (\gamma, \delta)$

(1) **Oscar** 先选定一个 δ , 然后企图找 γ , 这样, 他就必须解一个关于未知数 γ 的方程:

$$\beta^\gamma \gamma^\delta \equiv \alpha^x \pmod{p}$$

这个方程是一个已知无可行解法的难处理问题!

(2)**Oscar**先选定一个 γ ，使其满足： $\beta^\gamma \gamma^\delta \equiv \alpha^x \pmod{p}$ ，
于是 $\gamma^\delta \equiv \beta^{-\gamma} \alpha^x \pmod{p}$ ，这样，他就必须计算离散对数 $\log_\gamma(\beta^{-\gamma} \alpha^x) = ?$ ，这自然是难处理的问题！

(3)若两者 γ, δ 都被 **Oscar**首先选定,然后企图解出一个随机消息 x ,使得 $\beta^\gamma \gamma^\delta \equiv \alpha^x \pmod{p}$ ，也相当于求对数问题,所以**Oscar**利用这种方式也不能伪造随机消息的签名。

(4) **Oscar**同时选择 γ, δ 和 x 来伪造签名问题:

假设 i 和 j 是整数, $0 \leq i \leq p-2, 0 \leq j \leq p-2$,且 $(j, p-1)=1$,先完成下列计算:

$$\gamma = \alpha^i \beta^j \pmod{p}$$

$$\delta = -\gamma j^{-1} \pmod{p-1}$$

$$x = -\gamma i j^{-1} \pmod{p-1}$$

(其中 j^{-1} 是用模 $p-1$ 来计算的)

可以证实 (γ, δ) 是一个消息 x 的有效签名:

$$\beta^\gamma \gamma^\delta \equiv \beta^{\alpha^i \beta^j} (\alpha^i \beta^j)^{-\alpha^i \beta^j j^{-1}} \pmod{p}$$

$$\equiv \beta^{\alpha^i \beta^j} \alpha^{-ij^{-1} \alpha^i \beta^j} \beta^{-\alpha^i \beta^j} \pmod{p}$$

$$\equiv \alpha^{-ij^{-1} \alpha^i \beta^j} \pmod{p}$$

$$\equiv \alpha^{-ij^{-1} \gamma} \pmod{p}$$

$$\equiv \alpha^x \pmod{p}$$

例子:假设 $p=467$, $\alpha=2$ 和 $\beta=132$, 它们为**Bob**公开的签名方案中的参数。**Oscar**利用这些参数伪造对一随机信息 x 的签名:

选择 $i=99$ 和 $j=179$, 那么 $j^{-1} \pmod{p-1}=151$, 计算出下列的 x, γ, δ :

$$\gamma = \alpha^i \beta^j = 2^{99} \cdot 132^{179} \pmod{467} = 117$$

$$\delta = -117 \times 151 \pmod{466} = 41$$

$$x = 99 \times 41 \pmod{466} = 331$$

那么 **(117, 41)** 是消息**331**的一个有效签名。验证：

$$132^{117} \cdot 117^{41} \equiv 303 \pmod{467}$$

$$2^x = 2^{331} \equiv 303 \pmod{467}$$

因此，这个伪造的签名有效！

(5) 其他类型的伪造签名：

Oscar依据**Bob**已签名的消息来做伪签名。假设 (γ, δ) 是一个消息**x**的有效签名，那么**Oscar**可以用此来伪签其它消息：

设**h,i,j**为整数, $0 \leq h,i,j \leq p-2$ 且 $(h\gamma - j\delta, p-1) = 1$,计算

$$\lambda = \gamma^h \alpha^i \beta^j \pmod{p}$$

$$\mu = \delta \lambda (h\gamma - j\delta)^{-1} \pmod{p-1}$$

$$x' = \lambda (hx + i\delta)(h\gamma - j\delta)^{-1} \pmod{p-1}$$

(其中 $(h\gamma - j\delta)^{-1}$ 是模**p-1**算出)

然后可验证出

$$\beta^\lambda \lambda^\mu \equiv \alpha^{x'} \pmod{p}$$

因此， (λ, μ) 为假消息 x' 的一个有效签名

讨论两个问题：

(1) 用**ElGamal**方案计算一个签名时，使用的随机数**k**为什么不能泄露？

(2) 若**Bob**用相同的**k**值来签名不同的两份消息，**Oscar**能否攻破这个体制？

2 数字签名标准

公布于1994年5月19日的联邦记录上，并于1994年12月1日采纳为标准DSS。DSS为ElGamal签名方案的改进。

DSS: p 为512bit的素数， q 为160比特的素数，且 $q|p-1$ ， $\alpha \in F_p^*$ ，且 α 为模 p 的 q 次单位根。消息集合 $P=F_p^*$ ，签名集合 $A=F_q \times F_q$ ，定义 $K=\{ (p, \alpha, a, \beta) | \beta = \alpha^a \pmod{p} \}$ ，值 p, q, α 和 β 是公开的， a 是保密的。

取 $x \in P$ ，对 $K=(p, q, \alpha, a, \beta)$ 和一个（秘密）随机数 k ($1 \leq k \leq q-1$)，定义

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

其中， $\gamma = (\alpha^k \pmod{p}) \pmod{q}$ ， $\delta = (x + a \gamma) k^{-1} \pmod{q}$

对 $x \in F_p^*$ 和 $\gamma, \delta \in F_q$ 来说，按下述计算来验证签名的真伪：

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

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

$$V_{erK}(x, \gamma, \delta) = \text{真} \Leftrightarrow (\alpha^{e_1}\beta^{e_2}(\bmod p))(\bmod q) = \gamma$$

$$\text{事实上, } \alpha^{e_1}\beta^{e_2} \equiv \alpha^{x\delta^{-1} + a\gamma\delta^{-1}(\bmod q)}(\bmod p)$$

$$\equiv \alpha^{\delta^{-1}(x+a\gamma)} \equiv \alpha^k \equiv \gamma(\bmod q)(\bmod p)$$

注：1*.DSS的使用涉及到Smart卡的使用,要求短的签名。DSS以一个巧妙的方法修改了ElGamal方案，使得签名160bits消息产生一个320bit的签名，但是计算使用了512比特的模p.

2*.要求 $\delta \neq 0(\bmod p)$ 在整个签名算法中，如果计算了一个值 $\delta \equiv 0(\bmod p)$ ，程序自动拒绝，并且产生一个新的随机值k计算新的签名，事实上， $\delta \equiv 0(\bmod p)$ 的发生概率大约为 2^{-160} .

3*. **DSS**是一个产生签名比验证签名快得多的方案，验证签名太慢！

4*. **Smart**卡的应用！！**Smart**卡有有限的处理能力，但是能与计算机进行通信。人们企图设计一种让**Smart**卡仅作小量运算的签名方案。该方案必须完成签名、验证签名两部分，而且方便安全。

用**DSS**签名的例子：

假设取 $q=101$ ， $p=78q+1=7879$ ，3为 F_{7879} 的一个本原元，所以能取 $\alpha=3^{78} \pmod{7879}=170$ 为模 p 的 q 次单位根。假设 $a=75$ ，那么 $\beta=\alpha^a \pmod{7879}=4567$ 。现在，假设Bob想签名一个消息 $x=1234$ ，且他选择了随机值 $k=50$ ，可算得 $k^{-1} \pmod{101}=99$ ，签名算出：

$$\gamma=(170^{50} \pmod{7879}) \pmod{101}=2518 \pmod{101}=94$$

$$\delta = (1234 + 75 * 94) 99 \pmod{101} = 97$$

签名为 (1234, 94, 97) 。

验证：

$$\delta^{-1} = 97^{-1} \pmod{101} = 25 ,$$

$$e_1 = 1234 * 25 \pmod{101} = 45, e_2 = 94 * 25 \pmod{101} = 27$$

$$(170^{45} * 4567^{27} \pmod{7879}) \pmod{101} = 2518 \pmod{101} = 94$$

因此，该签名是有效的。

3 一次签名

任何单向函数都可用来构造一次签名方案。该签名对一个消息来说，唯一对应着一个确定的签名。这样的签名可验证任意多次。

Lamport方案：

设 k 为一个正整数， $P=\{0,1\}^k$ ，设 $f:Y \rightarrow Z$ 是一个单向函数，签名集合 $A=Y^k$ ，对于 $1 \leq i \leq k, j=0,1$ 来说， $y_{ij} \in Y$ 可随机地选择。选后，可算得

$$Z_{ij}=f(y_{ij}) \quad 1 \leq i \leq k, j=0,1$$

密钥 K 由 $2k$ 个 y 值和 $2k$ 个 Z 值组成， y 值保密而 Z 值公开。消息 $x=x_1, x_2, \dots, x_k$ （kbit串）。

对于 $K= (y_{ij}, Z_{ij} | 1 \leq i \leq k, j=0,1)$

定义

$$Sig_K(x_1, x_2, \dots, x_k) = (y_{1x1}, y_{2x2}, \dots, y_{kxk})$$

其中, $y_{ixi} = a_i, f(a_i) = Z_{ixi}$

验证:

$$V_{erK}(x_1, x_2, \dots, x_k; a_1, a_2, \dots, a_k) = \text{真} \Leftrightarrow$$

$$f(a_i) = Z_{ixi} \quad 1 \leq i \leq K$$

注: 1*. 待签名的消息为一个二进制元组, 每一个都单独签名. 这个特征决定了“一次签名”

2*. 验证是简单的检查: 签名结果的每一个元素是相应公开钥元素的原象.

例子: 取单向函数 $f(x) = \alpha^x \pmod{p}$, 设 $p = 7879$ (素数), 3 为 F_{7879} 的本原元, 定义 $f(x) = 3^x \pmod{7879}$

假设 Bob 想签名 3 比特消息, 他选择了 6 个 (秘密的) 随机数:

$$y_{10}=5831, y_{11}=735, y_{20}=803, y_{21}=2467, y_{30}=4285, y_{31}=6449$$

在f的作用下计算y的像:

$$z_{10}=2009, z_{11}=3810, z_{20}=4672, z_{21}=4721, z_{30}=268, z_{31}=5732$$

将这些Z值公开。现在Bob打算签名消息 $x=(1,1,0)$,那么对的签名为 $(y_{11}, y_{21}, y_{30})=(735, 2467, 4285)$.

验证签名:

$$3^{735}(\text{mod } 7879)=3810$$

$$3^{2467}(\text{mod } 7879)=4721$$

$$3^{4285}(\text{mod } 7879)=268$$

因此,该签名有效。

注: 该方案, 仅能用于签一个消息! 一次, 无法伪造。

4 不可否认的签名

(Chaum 和Van Antwerprn 1989年提出)

该签名的特征是：验证签名者必须与签名者合作。

验证签名是通过询问—应答协议来完成。这个协议可防止签名者**Bob**否认他以前做的签名。一个不可否认的签名方案有三个部分组成：签名算法、验证协议、否认协议

Bob: 设 $p=2q+1$ 是一个素数，它满足 q 为素数，且 F_p 中的对数问题是难解的； $\alpha \in F_p^*$ ，且阶为 q ，取 $1 \leq a \leq q-1$ ，定义 $\beta = \alpha^a \pmod{p}$ ， G 表示阶为 q 的 F_p^* 的子群。易见 $G = \langle \alpha \rangle$ ，（事实上 G 由模 p 的二次剩余组成）。

设 $P=A=G$ ，且定义 $K = \{ (p, \alpha, a, \beta) \mid \beta = \alpha^a \pmod{p} \}$ ，值 p, α 和 β 是公开的， a 是保密的。

对 $K = (p, \alpha, a, \beta)$ 和消息 $x \in G$, Bob 签名
 $y = \text{Sig}_K(x) = x^a \pmod{p}$

易见 $y \in G$ 。按如下协议完成验证：

- (1) **Alice** 随机选择 $e_1, e_2 \in F_q^*$ 。
- (2) **Alice** 计算 $C = y^{e_1} \beta^{e_2} \pmod{p}$ ，且将 **C** 送给 **Bob**。
- (3) **Bob** 计算 $d = C^{a^{-1} \pmod{q}} \pmod{p}$ ，且 **d** 将送给 **Alice**。
- (4) **Alice** 接受 **y** 作为一个有效签名, 当且仅当

$$d \equiv x^{e_1} \alpha^{e_2} \pmod{p}$$

对上述这个签名方案，要证明以下两点：

- 1) **Alice** 将会接受按如上方案的有效签名
- 2) **Bob** 几乎不可否认经 **Alice** 验证过的自己的签名。

证明(1): (**alice** 接受 **Bob** 的签名)。下面计算的所有指数都已做到模 **q** 约简：

$$d \equiv C^{a^{-1}} \pmod{p} \equiv y^{e_1 a^{-1}} \beta^{e_2 a^{-1}} \pmod{p}$$

知 $y = x^a \pmod{p}, \beta = \alpha^a \pmod{p}$

代入上式得 $d \equiv x^{e_1} \alpha^{e_2} \pmod{p}$

刚好与协议 (4) 相符, 故**Alice**接受**Bob**的签名。

对于(2) **Bob**几乎不可否认经**Alice**验证过的自己的签名。

相当于证明下述定理。

定理1: 若 $y \neq x^a \pmod{p}$, 那么**Alice**以概率 $1/(q-1)$ 接受**y**作为**x**的有效签名。

证明: **Bob**对**x**做了签名**y(=x^a)**给**Alice**后。**Bob**接受了**Alice**的一个询问 $C = y^{e_1} \beta^{e_2} \pmod{p}$, 这个询问对应于**q-1**个有序对**(e₁, e₂)**。(原因是 $y, \beta \in G$, **C** 一旦固定, 有**e₂=f(e₁)**) 然而, **Bob**不知**Alice**选择了哪一对**(e₁, e₂)**来构造出**C**。

如果 $y \neq x^a \pmod{p}$, 那么Bob能做的任何可能回答 $d (= C^{a^{-1} \pmod{q}} \pmod{p}) \in G$, 刚好与 $q-1$ 个可能的有序对 (e_1, e_2) 中的一个相对应。

由 $G = \langle \alpha \rangle$, 所以对 c, d, x, y 来说, 可设 $c = \alpha^i, d = \alpha^j, x = \alpha^k, y = \alpha^l$, 这里 $i, j, k, l \in F_q^*$,

考虑同余式:

$$C \equiv y^{e_1} \beta^{e_2} \pmod{p}, d \equiv (y^{e_1} \beta^{e_2})^{a^{-1} \pmod{q}} \pmod{p} \Rightarrow$$

$$d \equiv x^{e_1} \alpha^{e_2} \pmod{p}$$

写出关于 α 的指数表示:

$$\begin{cases} \alpha^i \equiv \alpha^{le_1} \cdot \alpha^{ae_2} \pmod{p} \\ \alpha^j \equiv \alpha^{ke_1} \cdot \alpha^{e_2} \pmod{p} \end{cases}$$

等价于下述方程组:

$$\begin{cases} i = le_1 + ae_2 \pmod{q} \\ j = ke_1 + e_2 \pmod{q} \end{cases}$$

既然假设 $y \neq x^a \pmod{p}$ 而 $y = \alpha^l$,

$x^a = (\alpha^k)^a = \alpha^{ak}$, 所以 $l \neq ak$,

相当于说上述方程的系数行列式:

$$\begin{vmatrix} l & a \\ k & 1 \end{vmatrix} = l - ak \not\equiv 0 \pmod{q}$$

知该方程组仅有唯一一组解。

即对每一个 $d \in G$, 对于 $q-1$ 个可能的有序对中 (e_1, e_2) , 刚好有一个是正确的回答, **Bob** 给 **Alice** 的一个回答 d , 将被验证的概率刚好为

$1/(q-1)$ 。定理得证!

下面讨论否认协议：

目的：(1) Bob能使Alice相信一个无效的签名是伪造的。

(2) Bob签名有效，而导致Alice判决错误的概率为小概率事件。

否认协议：(y?=x^a)暂视为对的签名

- 1) Alice 随机选取 $e_1, e_2 \in F_q^*$
- 2) Alice 计算 $C = y^{e_1} \beta^{e_2} \pmod p$ 且将送给Bob,
- 3) Bob 计算 $d = C^{a^{-1} \pmod q} \pmod p$, 且将他回送Alice
- 4) Alice 验证 $d \neq x^{e_1} \alpha^{e_2} \pmod p$
- 5) Alice 再随机选取 $f_1, f_2 \in F_q^*$
- 6) Alice 计算 $C = y^{f_1} \beta^{f_2} \pmod p$, 且将他送给Bob
- 7) Bob 计算 $D = C^{a^{-1} \pmod q} \pmod p$, 且将他回送给Alice
- 8) Alice 验证 $D \neq x^{f_1} \alpha^{f_2} \pmod p$

9) Alice 推出 y 是伪造的

$$\Leftrightarrow (d \alpha^{-e_2})^{f_1} \equiv (D \alpha^{-f_2})^{e_1} \pmod{p}$$

定理2: 如果 $y \neq x^a \pmod{p}$, 且 Alice 和 Bob 都遵守否认协议, 那么 $(d \alpha^{-e_2})^{f_1} \equiv (D \alpha^{-f_2})^{e_1} \pmod{p}$

证明: 注意, $d \equiv C^{a^{-1}} \pmod{p}$, 而 $C \equiv y^{e_1} \beta^{e_2} \pmod{p}$

又 $\beta = \alpha^a \pmod{p}$, 从而有

$$(d \alpha^{-e_2})^{f_1} \equiv ((y^{e_1} \beta^{e_2})^{a^{-1}} \alpha^{-e_2})^{f_1} \pmod{p}$$

进一步有

$$(d \alpha^{-e_2})^{f_1} \equiv y^{e_1 a^{-1} f_1} \beta^{e_2 a^{-1} f_1} \alpha^{-e_2 f_1} \pmod{p}$$

$$\equiv y^{e_1 a^{-1} f_1} \alpha^{a e_2 a^{-1} f_1} \alpha^{-e_2 f_1} \pmod{p}$$

$$\equiv y^{e_1 a^{-1} f_1} \alpha^{e_2 f_1} \alpha^{-e_2 f_1} \pmod{p}$$

$$\equiv y^{e_1 a^{-1} f_1} \pmod{p}$$

类似地，按如上方式推出

$$(D\alpha^{-f_2})^{e_1} \equiv y^{e_1 a^{-1} f_1} \pmod{p}$$

证毕。

注：我们不能假设遵守了否认协议，他可以想方设法构造 \mathbf{d}, \mathbf{D} ,来达到否认自己签过名的目的。然而，只要**Alice**严格遵守协议，**Bob**是无法否认的。我们给出：

定理3，假设 $y \equiv x^a \pmod{p}$ 且Alice遵守否认协议，如果

$$d \neq x^{e_1} \alpha^{e_2} \pmod{p}$$

$$D \neq x^{f_1} \alpha^{f_2} \pmod{p}$$

那么 $(d\alpha^{-e_2})^{f_1} \neq (D\alpha^{-f_2})^{e_1} \pmod{p}$

成立的概率为 $1-1/(q-1)$ 。（证明，略）。