密码学理论与应用

数据完整性保护

消息认证、数字签名（续）

$$ed = 1 \bmod \varphi(N)$$

$$Y = M^e \bmod N$$

$$M = Y^d \bmod N$$

数字签名方案(

- *Schnorr*方案(1991)： 基本算

安全性：

(因为F_p^*上的判定性*Diffie-Hellman*问题难解)，Schnorr方案具有CMF-抗伪造性。

其他实现：

Schnorr签名方案也可以在椭圆曲线上实现，并具有相同的抗伪造性。

- 公开的参数：G是q阶循环群，g是 $\boldsymbol{H}$:{0,1}$^+$→F_q是一个抗冲突的散列函
- 公钥/私钥生成算法KG(k, G, g, q):
- $x \leftarrow^{\$} F_q^*$; $y \leftarrow g^{-x}$; $\boldsymbol{pk} \leftarrow y$; $\boldsymbol{sk} \leftarrow x$;
- 签名算法$Sig^H(sk, M)$, 其中sk=x:
- $K \leftarrow^{\$} F_q$; $r \leftarrow g^K$; $h \leftarrow H(\mathrm{M}\|\mathrm{r})$; $\boldsymbol{s} \leftarrow (K+xh) \bmod q$;
- 签名$\sigma \leftarrow (r,h,s)$。
- 验证算法Vf^H(pk, M, (r,h,s)), 其中pk=y:
- $h=\boldsymbol{H}(\mathrm{M}\|\mathrm{r}) \wedge r=g^s y^h$;

一致性：

$g^s y^h = g^s\, g^{-xh} = g^{s-hx} = g^{(s-hx) \bmod q}$ (思考题：为什么？) $= g^K = r$。

数字签名方案(6)

- *Schnorr*方案(1991)： 更多的细节

注意签名算法$Sig^H(sk, M)$每次必须独立地随机生成K，K不能够取常数或使多个消息共享同一个K，否则达不到安全目的：假如Sig^H对两个不同的消息M_1、M_2使用同一个K，显然r在两个签名中也有相同的值，由此所输出的数字签名分别为(r,h_1,s_1)和(r,h_2,s_2)，并且因为消息$M_1 \neq M_2$故$h_1 \neq h_2 \bmod q$ (这一点源于*H*的抗冲突性质，在实践中应用MD5 或SHA这类散列函数时就会具有这类性质)。攻击者(一个P.P.T.算法)A从所观测到的(r,h_1,s_1)、(r,h_2,s_2)、M_1、M_2(但这里不需要消息M_1和M_2)和公钥信息q解以下方程组，其中K和x作为未知量：

$$s_1=(K+xh_1) \bmod q$$

$$s_2=(K+xh_2) \bmod q$$

因为$h_1 \neq h_2 \bmod q$，即$(h_1-h_2, q)=1$(为什么?)，所以能完全解出私钥$x=(h_1-h_2)^{-1}(s_1-s_2) \bmod q$(请

公钥/私钥生成算法KG(*k*, *G*, g, q):

$x \leftarrow^{\$} F_q^*$; $y \leftarrow g^{-x}$; $\boldsymbol{pk} \leftarrow y$; $\boldsymbol{sk} \leftarrow x$;

签名算法$Sig^H(sk, M)$, 其中sk=x:

$K \leftarrow^{\$} F_q$; $r \leftarrow g^K$; $h \leftarrow H(M\|r)$; $\boldsymbol{s} \leftarrow (K+xh) \bmod q$;

签名$\sigma \leftarrow (r,h,s)$。

数字签名方案(7)

- *Fegei-Fiar-Shamir*签字方案(1986)

8-20 (*Fegei-Fiat-Shamir*数字签名方案) p、q是k位秘密素数，N=pq，H:$\{0,1\}^+ \rightarrow \{0,1\}^k$是抗冲突的散列函数，N、$H$公开, p、q保密。方案的组成算法如下：

公钥/私钥生成算法 KG(k, $\mathcal{G}$, g, q):

$x \xleftarrow{\$} \{1,2,\ldots,N\text{-}1\}$; $y \xleftarrow{\$} x^2 \bmod N$; vk←y; sk←x; return(vk,sk);

公钥和私钥分别为 vk 和 sk。

签名算法Sig^H(sk, M)，其中sk=x:

$r_i \xleftarrow{\$} Z_N$, $v_i \leftarrow r_i^2 \bmod N$, i=1,…,k;

$h \leftarrow H(M, v_1,\ldots,v_k)$;

$z_i \leftarrow r_i x^{e_i} \bmod N$, e_i是h的第i位, i=1,…,k;

$\sigma_1 \leftarrow v_1 \ldots v_k$; $\sigma_2 \leftarrow z_1 \ldots z_k$;

return(σ_1,h,σ_2); /*对M的数字签名*/

验证算法Vf^H(vk, M, (σ_1,h,σ_2))，其中vk=y:

parse σ_1 as $v_1 \ldots v_k$;

parse σ_2 as $z_1 \ldots z_k$; parse h as $e_1 \ldots e_k$;

$$\text{return}(h = H(M, \sigma_1) \bigwedge_{i=1,\ldots,k} z_i^2 = v_i y^{e_i} \bmod N);$$

验证该方案满足一致性条件，并解释为什么算法Sig^H(sk, M)必须随机独立地生成各个r_i。

数字签名方案(8)

- 数字签名方案【习题】

8-21 S=(KG, Sig, Vf)是一个抗伪造的数字签名方案，KG, Sig, Vf分别是签字私钥/公钥生成算法、签字算法和验证算法。*H*是一个散列算法，将任意的字符串M映射到S的消息域。做以下签名方案S^H，其私钥/公钥生成算法就是以上的KG，签字算法Sig^H(sk, M)= Sig(sk, H(M))。注意S^H比S的优越之处在于计算效率：H(M)通常比M短得多而且长度固定，例如取H为MD5或SHA，则无论M多长H(M)总是固定的 128 位或 160 位，所以计算效率更高。

(1) 请给出方案S^H的验证算法Vf^H(vk, M, σ)并证明你的算法满足一致性条件；

(2) 如果存在一个有效算法A可以算出*H*的一个冲突，即A能有效计算出一对不同的消息$M_1 \neq M_2$使$H(M_1)=H(M_2)$，则A可以用来伪造签名方案S^H的数字签名，即S^H不能抵抗伪造攻击(虽然S抗伪造攻击)，为什么？这表明要使S^H抗伪造攻击，*H*必须抗冲突。

1