# 计算机密码学理论与应用

## (公钥类)身份认证类协议

身份认证的基本概念：<u>*Stallings*教程</u> 15.1节

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

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

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

# 身份认证协议(1)：基本概念 15.1节

- *Schnorr* 认证协议(1991)

$q$是$k$位素数，$\mathcal{G}$是$q$阶循环群，$g$是$\mathcal{G}$的生成子(因此$\mathcal{G}$的元素是$g^0=e$、$g$、$g^2$、$g^3$、…、$g^{q-1}$)，并且所有这些对象都公开。在$Z_q=\{0,1,2,\ldots,q-1\}$[3]中随机选取一个数$x$，然后计算$y \xleftarrow{\$} g^{-x}$，以$y$和$x$分别作为合法的主体P的公钥和私钥。协议的会话过程如图 10-3。

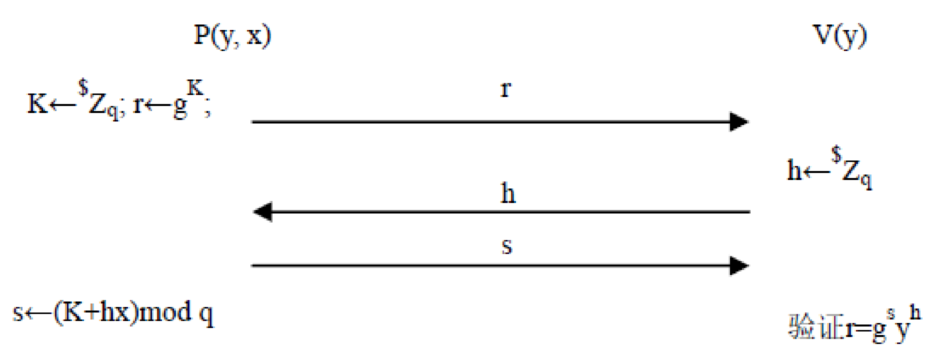



图 10-3　*Schnorr* 身份认证协议

当P需要向V证实自身的身份，即向V证明自己确实持有公钥$y$所对应的私钥$x$，P生成随机数$K$、计算$r \leftarrow g^K$并向V发送$r$；V生成并向P发送随机数$h$；P在接收到$h$后计算出整数$s \leftarrow (K+hx) \bmod q$并向V发送$s$；V在接收到$s$后验证$r=g^s y^h$是否成立，若成立则接受对方确实是P，否则判定对方是冒充者。

# 身份认证协议(2)

- *Feige-Fiat-Shamir*身份认证协议(1987)

p、q是$k$位秘密素数，N=pq，N公开但p、q保密。在{1,2,…,N-1}上随机生成一个数$x \xleftarrow{\$} \{1,2,\ldots,N-1\}$，计算$y \xleftarrow{\$} x^2 \bmod N$，将y和x分别作为合法的主体P的公钥和私钥。协议的会话过程如图 10-4。

| P((y,N), x) | y=$x^2$mod N | V(y,N) |
| --- | --- | --- |
| $r_i \xleftarrow{\$} Z^*_N$; $v_i \leftarrow r_i^2 \bmod N$, i=1,…,k | $\xrightarrow{v_1 \ldots\ldots v_k}$ | |
| | | $h \xleftarrow{\$} \{0,1\}^k$ |
| parse h=$e_1 \ldots\ldots e_k$ | $\xleftarrow{h}$ | |
| | $\xrightarrow{z_1 \ldots\ldots z_k}$ | 验证$z_i^2 = v_i y^{e_i} \bmod N$, i=1,…,k |
| $z_i \leftarrow r_i x^{e_i} \bmod N$, i=1,…,k | | |

图 10-4 *Feige-Fiat-Shamir* 正则身份认证协议

当P需要向V证实自身的身份，即向V证明自己确实持有公钥y所对应的私钥x，P生成一组k个随机数$r_i \xleftarrow{\$} Z_N$, K、计算$v_i \xleftarrow{\$} r_i^2 \bmod N$并向V发送$v_i$, i=1,…,k；V生成并向P发送k位随机数h；P在接收到h后计算出一组k个整数$z_i \leftarrow r_i x^{e_i} \bmod N$，其中$e_i$是h的第i位(因此实际上$z_i=r_i$或$xr_i \bmod N$ ), i=1,…,k 并向V发送$z_1 \ldots\ldots z_k$； V在接收到$z_1 \ldots\ldots z_k$后验证 $z_i^2 = v_i y^{e_i} \bmod N$ 是否对每个i=1,…,k 都成立，若全部成立则接受对方确实是P，否则表明对方是冒充者。

# 身份认证协议(3)

- 身份认证协议和数字签名方案的普遍关系：*Fiat-Shamir*变换

ID=(KG, P, V, C)是一类高效的三消息身份鉴别协议，包括一组 P.P.T.算法 KG 和 P、确定性算法 V 以及复杂性参数 k 的函数 C，KG 是密钥生成算法，以 k 为输入并输出公钥/私钥偶(pk, sk)；P 是身份证实算法，V 是身份验证算法；P 以私钥/公钥偶为初始输入、V 以公钥 pk 为初始输入； C 表示协议第 2 步所生成的随机串的长度。协议的会话过程如图 10-5，所有算法还满足一致性关系：对任意的 k 恒有

$P[(pk,sk)\leftarrow KG(k);\ (Cmt,St)\leftarrow P(pk,sk);\ Ch\leftarrow^{\$}\{0,1\}^{C(k)};\ Rsp\leftarrow P(Ch,St):\ V(pk,\ Cmt\|Ch\|Rsp)=1]=1$。

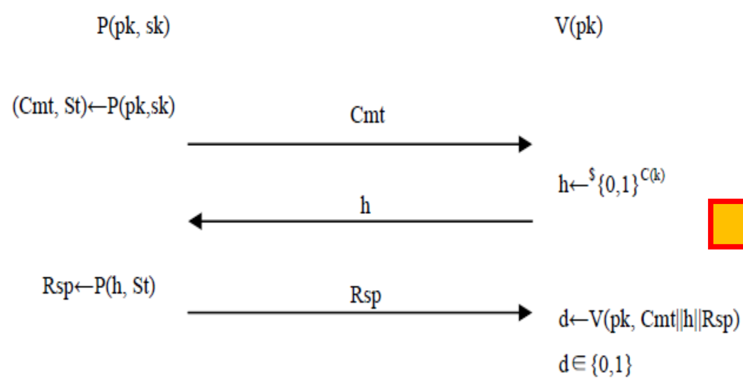



图 10-5 正则身份认证协议

**Abdalla-Pintcheval定理(2002)**

如果正则身份认证协议是抗欺诈的，那么*Fiat-Shamir*变换所生成的数字签名方案具有抗伪造性质；反之亦然。

数字签名方案

设s(k)是值为非负整数的k的函数，$H:\{0,1\}^+\rightarrow\{0,1\}^{C(k)}$ 是一个随机散列函数。正则身份认证协议ID的与s(k)和H相关的*Fiat-Shamir*变换是一个数字签名方案Ξ=(KG, Sig, Vf)，其中公钥/私钥偶的生成算法KG与ID的对应算法KG完全相同，签名算法和验证算法分别定义如下：

签名算法$Sig^H(sk,M)$:

$R\leftarrow\{0,1\}^{s(k)};\ (Cmt,\ St)\leftarrow P(pk,sk);\ h\leftarrow H(R\|Cmt\|M);\ Rsp\leftarrow P(h,St);$

return(R||Cmt||Rsp);

验证算法$Vf^H(pk,M,\sigma)$:

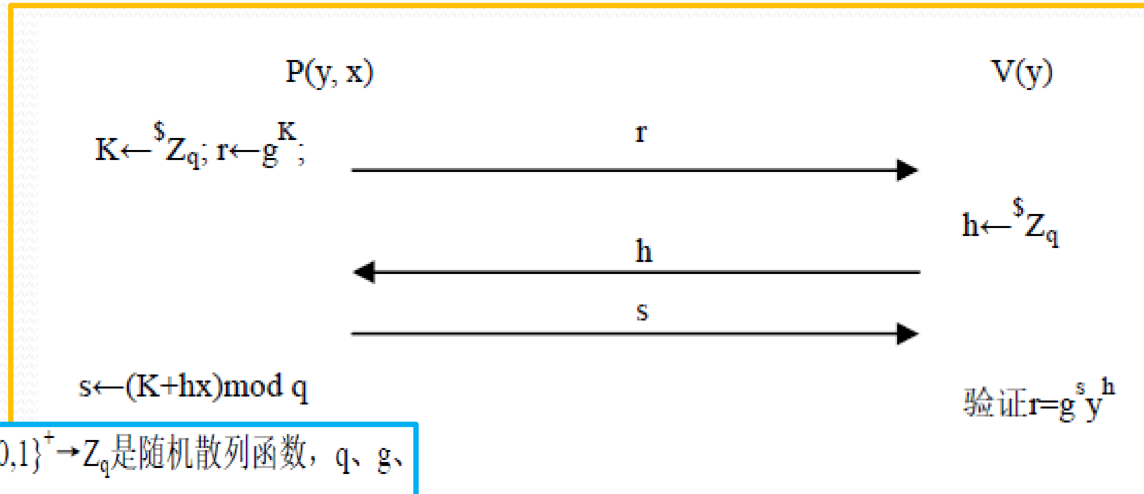
parse σ as R||Cmt||M; h←H(R||Cmt||M);

return(V(pk, Cmt||h||Rsp));

读者不难验证从协议 ID 的一致性关系能直接导出数字签名方案 Ξ 的一致性关系。

# 身份认证协议(4)

- *Fiat-Shamir*变换的例子之一：*Schnorr*签字方案




10-3 *Schnorr* 身份认证协议

例 10-1 $\mathcal{G}$是q阶循环群，q是k位素数，g是$\mathcal{G}$的生成子；$H:\{0,1\}^+\rightarrow Z_q$是随机散列函数，q、g、$\mathcal{G}$和*H*公开。*Schnorr*协议(图 10-3)的*Fiat-Shamir*变换所导出的数字签名方案的组成算法如下：

公钥/私钥生成算法 KG(k, $\mathcal{G}$, g, q):

$x\xleftarrow{\$}Z_q$; $y\xleftarrow{\$}g^{-x}$; vk←y; sk←x; return(vk,sk);

签名算法$Sig^H$(sk, M)，其中sk=x:

$K\xleftarrow{\$}Z_q$; $r\leftarrow g^K$; $h\leftarrow H(M\|r)$; $s\leftarrow(K+xh) \bmod q$; return(r,h,s);

验证算法$Vf^H$(vk, M, (r,h,s))，其中vk=y:

return($h=H(M,r) \wedge r=g^s y^h$)

# 身份认证协议(5)

- *Fiat-Shamir*变换的例子之二：*Feige-Fiat*签字方案

p、q是$k$位秘密素数，N=pq，N公开但p、q保密。在{1,2,…,N-1}上随机生成一个数$x \xleftarrow{\$} \{1,2,\ldots,N-1\}$，计算$y \xleftarrow{\$} x^2 \bmod N$，将y和x分别作为合法的主体P的公钥和私钥。协议的会话过程如图 10-4。

| P((y,N), x) | $y=x^2 \bmod N$ | V(y,N) |
|---|---|---|
| $r_i \xleftarrow{\$} Z^*_N;\ v_i \leftarrow r_i^2 \bmod N,\ i=1,\ldots,k$ | $v_1 \ldots v_k$ → | |
| | ← h | $h \xleftarrow{\$} \{0,1\}^k$ |
| parse $h=e_1 \ldots e_k$ | | |
| $z_i \leftarrow r_i x^{e_i} \bmod N, i=1,\ldots,k$ | $z_1 \ldots z_k$ → | 验证$z_i^2 = v_i y^{e_i} \bmod N, i=1,\ldots,k$ |

图 10-4 *Feige-Fiat-Shamir* 正则身份认证协议

**例 10-2** p、q是k位秘密素数，N=pq，$H:\{0,1\}^* \to \{0,1\}^k$是随机散列函数，N、$H$公开。*Feige-Fiat-Shamir*协议(图 10-4)的*Fiat-Shamir*变换所导出的数字签名方案的组成算法如下：

公钥/私钥生成算法 KG(k, $\mathcal{G}$, g, q):

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

$\mathrm{Sig}^H(sk, M)$，其中sk=x:

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

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

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

$\sigma_1 \leftarrow v_1 \ldots v_k$;

$\sigma_2 \leftarrow z_1 \ldots z_k$;

return($\sigma_1$,h,$\sigma_2$);

$\mathrm{Vf}^H(vk, M, (\sigma_1,h,\sigma_2))$，其中vk=y:

parse $\sigma_1$ as $v_1 \ldots v_k$;

parse $\sigma_2$ as $z_1 \ldots z_k$;

parse h as $e_1 \ldots e_k$;

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

# 身份认证协议(6)

- 零知识证明：实例
- 以*Schnorr*协议为例，***P***向***V***证明自己持有公钥***y***对应的私钥***x***、
- 同时不向***V***泄露***x***。

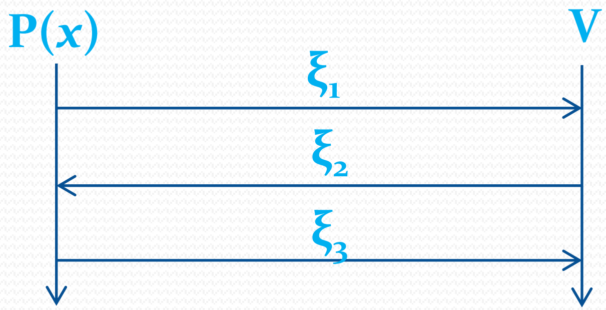
q是$k$位素数，$\mathcal{G}$是q阶循环群，g是$\mathcal{G}$的生成子(因此$\mathcal{G}$的元素是$g^0=e$、$g$、$g^2$、$g^3$、…、$g^{q-1}$)，并且所有这些对象都公开。在$Z_q=\{0,1,2,\ldots,q-1\}^3$中随机选取一个数x，然后计算$y \xleftarrow{\$} g^{-x}$，以y和x分别作为合法的主体P的公钥和私钥。协议的会话过程如图 10-3。

| P(y, x) | | V(y) |
|---|---|---|
| $K \xleftarrow{\$} Z_q$; $r \leftarrow g^K$; | $\xrightarrow{\quad r \quad}$ | |
| | $\xleftarrow{\quad h \quad}$ | $h \xleftarrow{\$} Z_q$ |
| | $\xrightarrow{\quad s \quad}$ | |
| $s \leftarrow (K+hx) \bmod q$ | | 验证$r=g^s y^h$ |

# 身份认证协议(7)

- 零知识证明：普遍机制

- $R(x,Y)$是一个二元关系，其中$Y$是公开的参数，$x$是秘密参数。
- 例如：$Y$=$(g,p,y)$, $g$是素数$p$的原根，$R$：$y = g^x \bmod p$。
- 零知识证明协议是这样一种过程，使$P$向$V$证明自己知道与$Y$对应的秘密$x$、
- 但不向$V$泄露$x$。




- (1) 一致性 $Pr[Vf(Y, \xi_1,\xi_2,\xi_3)=1 | R(x,Y)=1 \wedge_i \xi_i=P(x,Y, \xi_{i-1})] = 1$。
- $k$是协议的安全参数，$A$是任何P.P.T算法，协议安全性指以下两条性质
- (2) 抗欺诈 $Pr[Vf(Y, \xi_1,\xi_2,\xi_3)=1 | \wedge_i \xi_i=A(Y, \xi_{i-1})] = O(2^{-k})$
- (3) 零知识泄露 $Pr[A(Y, \xi_1,\xi_2,\xi_3)=x | R(x,Y)=1 \wedge_i \xi_i=P(x,Y, \xi_{i-1})] = O(2^{-k})$

# 作　业

## 阅读*Stallings*教程15.4节

通过阅读本节，理解公钥类身份认证协议的其他实例

（建议阅读原文教材）