Identication Scheme.

Prover. (pk, sk) Verifier. (pk).

$(I, st) \leftarrow P_1(sk)$. $\xrightarrow{I}$

$\xleftarrow{r}$ $r \leftarrow\$ \Omega_{pk}$.

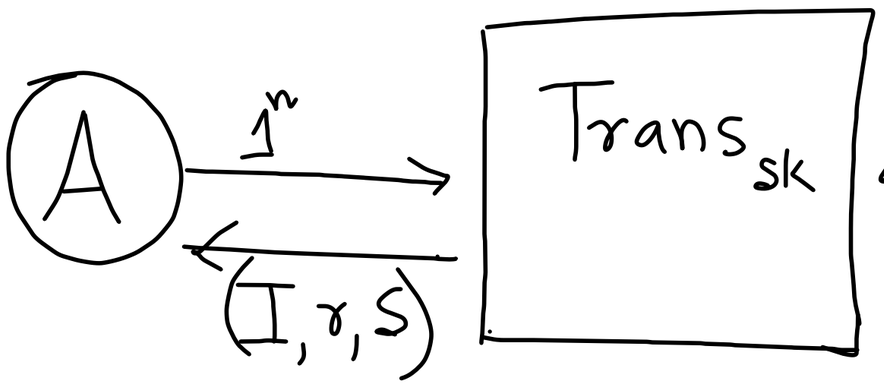
$s \leftarrow P_2((I, st), r, sk)$ $\xrightarrow{s}$ $V(pk, s, r) \stackrel{?}{=} I$.

$\downarrow$

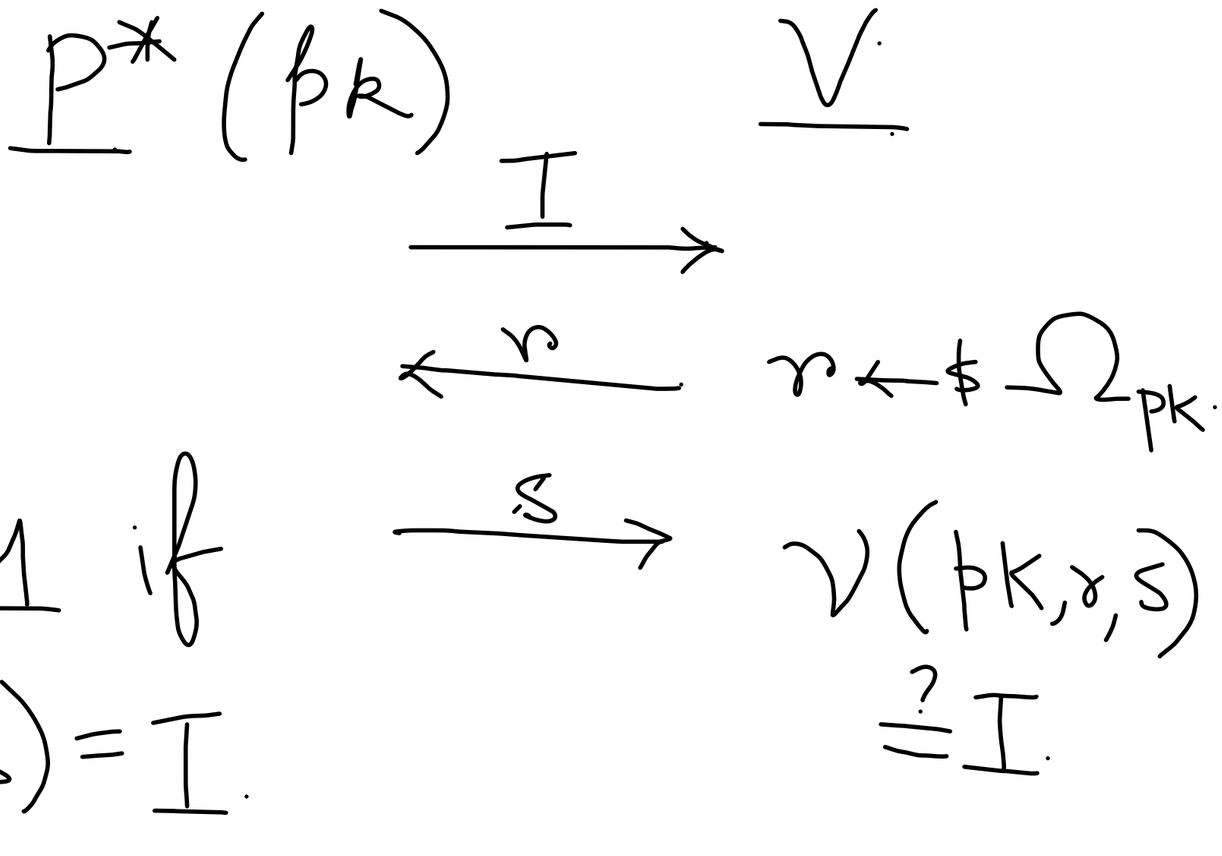
0/1.

(I, r, s) is called the transcript of the interaction.

Trans_{sk}

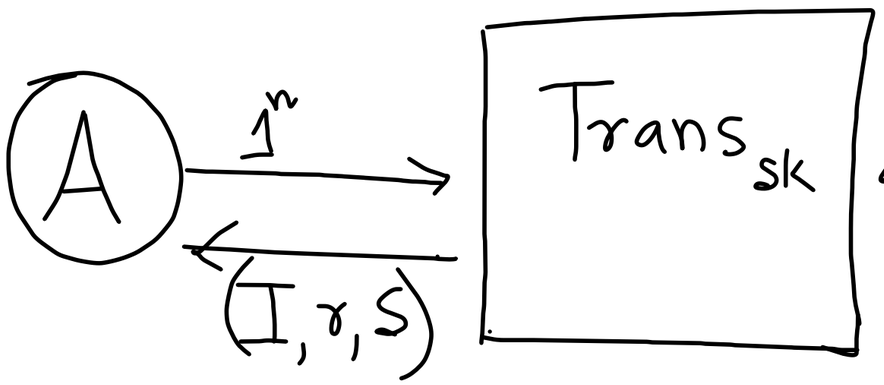


Security Game $\text{Ident}_{A,\Pi}^{(n)}$.

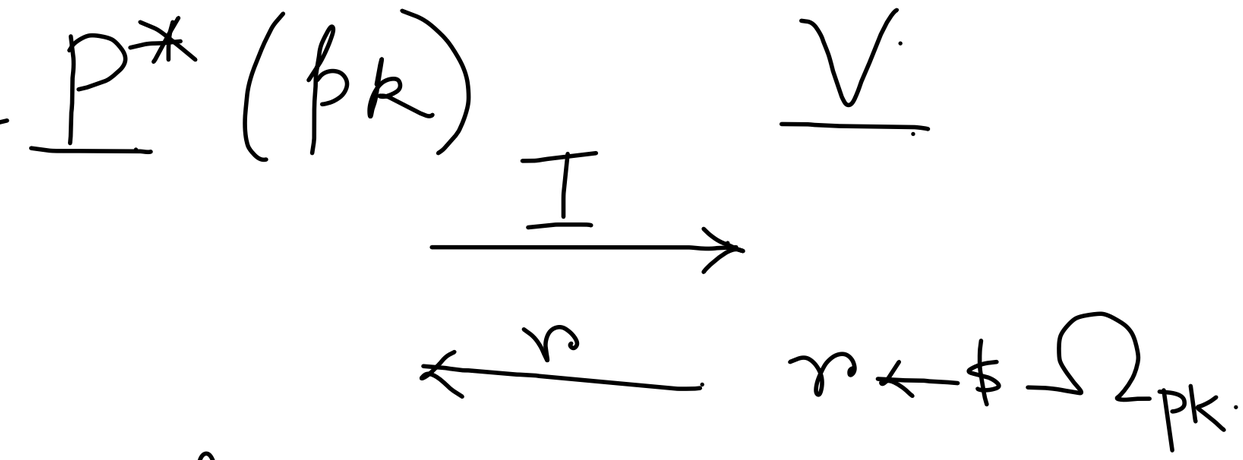


The experiment outputs 1 if and only if $V(pk, r, s) = I$.

Trans_{sk}



Security Game $\text{Ident}_{A,\Pi}^{(n)}$.



The experiment outputs 1 if and only if $V(pk, r, S) = I$.

Defn: An identification scheme $\Pi = (Gen, P_1, P_2, V)$ is secure against passive attack if for all PPT algorithms A, $\exists$ a negligible fn $negl(\cdot)$ such that

$$Pr[Ident_{A,\Pi}(n) = 1] \leq negl(n)$$

Schnorr Identification Scheme

KeyGen: on i/p 1^n, it samples a prime number q of n bits and generates a cyclic group G of order q. such that 'g' is the generator of G.
Then it randomly samples $x \leftarrow\$ \mathbb{Z}_q$. and computes

$y = g^x$. $\langle pk = (G, q, g, y), sk = x \rangle$

P_1 algorithm:

It will randomly sample $k \leftarrow\$ Z_q$ and compute $I = g^k$ and send it to the verifier.

If will output $(I, st) = (g^k, k)$.

P_2 algorithm:

i/p is $(g^k, k), r, x)$ o/p $s = (rx + k) \bmod q$.

P_1 algorithm:

It will randomly sample $k \leftarrow\$ Z_q$ and compute $I = g^k$ and send it to the verifier.

If will output $(I, st) = (g^k, k)$.

P_2 algorithm:

i/p is $(g^k, k), r, x)$ o/p $s = (rx + k) \bmod q$.

Verification algorithm:

$I/p : \left(pk = \langle G, q, g, y = g^x \rangle, r, s = (rx + k) \bmod q\right)$

Verification algorithm:

$I/p: (pk = \langle G, q, g, y = g^x \rangle,\ r,\ s = (rx + k) \bmod q)$

$V(pk, r, s) = g^k$

$V(pk, r, s) = y^{-r} \cdot g^s$

$g^s y^{-r} = I \Rightarrow g^s = I \cdot y^r \Rightarrow s = \log_g (I \cdot y^r)$

$P\ (y = g^x, x)$		$V\ (y = g^x)$
$I = g^k$	→	
	←	$r \leftarrow \$\ \mathbb{Z}_q$
$s = (rx + k) \bmod q$	→	

$V(pk, r, s) =$

$g^s \cdot y^{-r} \stackrel{?}{=} I$

An identification scheme is called non-degenerate if no I has higher prob. over others.

Discrete log hard $\Rightarrow$ Schnorr Identification Scheme is secure.

A' be the adversary breaking DLOG.

What is the i/p of $A' = ? \langle G, q, g, y = g^x \rangle$.

A $\xrightarrow{I}$ A'

$\xleftarrow{r}$

$\xrightarrow{s}$

(r, s)

$\longrightarrow$ (r', s').

$x = (r_1 - r_2)^{-1}(s_1 - s_2)$.

$g^{s_1 - r_1} \cdot y = I = g^{s_2 - r_2} \cdot y$.

$\Rightarrow g^{(s_1 - s_2)} = y^{r_1 - r_2}$.

$\Rightarrow g^{(s_1 - s_2)} = g^{x(r_1 - r_2)}$.

Algorithm A'

$I/p: \langle G, q, g, y \rangle$

1. Run $A(pk)$, answering all its queries to $Trans_{SK}$ oracle using the idea of simulation.

2. When A outputs $I \in \mathbb{Z}_q$, Choose $r \leftarrow \$ \mathbb{Z}_q$, send it to A, who responds with s_1

3. Run $A(pk)$ second time from the beginning using the same randomness as before except for uniform and

independent $r_2 \leftarrow\$ \mathbb{Z}_q$. send it to $\mathcal{A}$, who responds with s_2

4. If $g^{s_1} y^{-r_1} = I = g^{s_2} y^{-r_2}$, and $r_1 \neq r_2$, then

$\text{rel}\overline{\text{wrn}}\,(r_1 - r_2)^{-1} \cdot (s_1 - s_2) \bmod q$.

independent $r_2 \leftarrow\$ \mathbb{Z}_q$. send it to $\mathcal{A}$, who responds with s_2

4. If $g^{s_1} y^{-r_1} = \underline{I} = g^{s_2} y^{-r_2}$, and $r_1 \neq r_2$, then

$\text{rel}\overline{\text{wrn}}\,(r_1 - r_2)^{-1} \cdot (s_1 - s_2) \bmod q$.

independent $r_2 \leftarrow\$ \mathbb{Z}_q$. send it to $\mathcal{A}$, who responds with s_2

4. If $g^{s_1} y^{-r_1} = I = g^{s_2} y^{-r_2}$, and $r_1 \neq r_2$, then

$\text{rel}\overline{\text{wrn}}\,(r_1 - r_2)^{-1} \cdot (s_1 - s_2) \bmod q$.

Analysis:

Consider a single run of the experiment with randomness w.

Randomness comprised of:

- (i) used by keyGen to generate G, private key x
- (ii) Randomness used by A itself.
- (iii) Randomness used by A' when answering queries of A to the oracle $Trans_{sk}$.

$V(w,r) = 1$ if and only if A correctly responds to challenge r, when the randomness used is w.

$$\delta_w := Pr_r\left[V(w, r) = 1\right].$$

(w: fixed element)

$$Pr\left[Ident_{A,\Pi}(n) = 1\right] = Pr\left[V(w, r) = 1\right].$$

$$= \sum_w Pr\left[V(w, r) = 1 \wedge w = w\right].$$

$$\Pr[\mathrm{Ident}_{A,\pi}(n)=1]$$

$$= \sum_{w} \delta_w \cdot \Pr[\omega = w].$$

$$\Pr[\mathrm{DLOG}_{A,G}(n)=1] = \Pr[V(\omega, r_1)=1 \wedge V(\omega, r_2)=1 \wedge r_1 \neq r_2]$$

$$\geq \Pr[V(\omega, r_1)=1 \wedge V(\omega, r_2)=1] - \Pr[r_1 = r_2]$$

$$P_\delta[DLOG_{A,G_2}(n)=1] \geq P_\delta[V(w,r_1)=1 \wedge V(w,r_2)=1] - \frac{1}{q}.$$

$$P_\delta[V(w,r_1)=1 \wedge V(w,r_2)=1]$$

$$\sum_w P_\delta[V(w,r_1)=1 \wedge V(w,r_2)=1] \cdot P_\delta[w=\omega]$$

Jensen inequality

$$= \sum_w (\delta_\omega)^2 \cdot P_\delta[\omega=w] \geq \sum_w \left(\delta_\omega \cdot P_\delta[\omega=w]\right)^2$$

$$\Pr[DLOG_{A,G}(n) = 1] \geq \left(\Pr[Ident_{A,\pi}(n) = 1]\right)^2 - \frac{1}{q}$$

$$\Rightarrow \left(\Pr[Ident_{A,\pi}(n) = 1]\right)^2 \leq \Pr[DLOG_{A,G}(n) = 1] + \frac{1}{q}$$