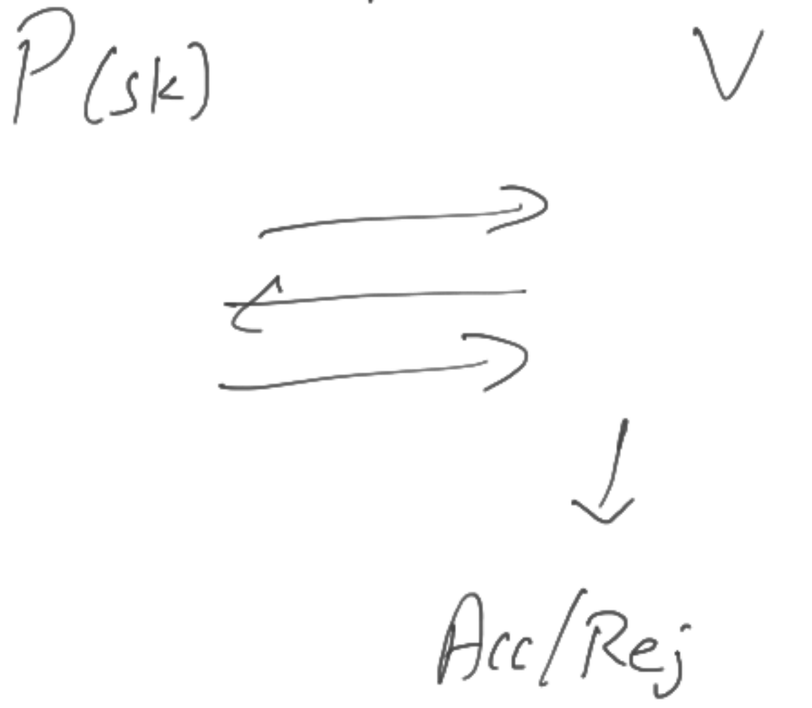
Some Cryptographic Protocols



Completeness: Honest prover with sk always makes verifier accept

Soundness: If V accepts, then P "knows" the sk corresponding to pk

Groups:

Group G is a set with operation $\cdot$.

- Associative: $\forall g_1, g_2, g_3 \; g_1 \cdot (g_2 \cdot g_3) = (g_1 \cdot g_2) \cdot g_3$
- Identity: $\exists \, 1_G : \forall g \in G : 1_G \cdot g = g \cdot 1_G = g$
- Closure: $\forall g_1, g_2 \in G : g_1 \cdot g_2 \in G$
- Inverse: $\forall g \in G \; \exists \, g^{-1} \in G : g \cdot g^{-1} = 1_G = g^{-1} \cdot g$

Cyclic groups: $\exists g \in G : \forall h \in G \; \exists a \in \mathbb{Z} : g^a = h$

Cyclic group of prime order

↓

Size of group

$|G| = q$ ← prime

for some prime p, set of non-zero elements of $\mathbb{Z}_p$ is a group. G is a subgroup of that.

Schnorr Identification Scheme

Discrete Log:

G - cyclic, $|G| = q$ (prime)

- Pick $g, h \leftarrow G$. Find $w \in [0, q-1]$ s.t.

$$h = g^w$$

Assumption: Hard for algorithms running in $\text{poly}\log(q)$ time.

Key Generation: $w \leftarrow [0, q-1]$, $g \leftarrow G$, $h \leftarrow g^w$ | G - cyclic, $|G| = q$

$sk : w$, $pk = (g, h)$

(g, h)

$P(w)$ — V

$\rho \leftarrow [0, q-1]$, $\alpha \leftarrow g^{\rho}$ —α→ $\beta \leftarrow [0, q-1]$

←β—

$r \leftarrow \rho + w \cdot \beta$ —r→ check $\alpha \cdot h^{\beta} = g^{r}$

Completeness: $\alpha \cdot h^{\beta} = g^{\rho} \cdot (g^{\omega})^{\beta} = g^{\rho + \omega\beta} = g^{r}$

Special Soundness: For any $(g, h = g^{\omega})$, given two executions (α, β, r), (α, β', r') s.t. $\beta \neq \beta'$ and both accepting, can recover ω.

$$\Rightarrow \quad r = \rho + \omega \cdot \beta \qquad r' = \rho + \omega \cdot \beta'$$

$$\Rightarrow \quad \omega = \frac{(r - r')}{(\beta - \beta')} \pmod{q}$$

Knowledge Soundness: If $\langle P^*, V \rangle$ accepts with

$pk = (g, h)$ with non-negl. prob., then can "extract"

w s.t. $h = g^w$ in $\text{poly}\log(q)$ time.

$\text{Ext}_{P^*}(g, h)$: 1. Sample random string r_{P^*} for P^*

2. Compute $\alpha \leftarrow P^*(g, h; r_{P^*})$

3. Sample β repeatedly to find $\beta \neq \beta'$

s.t. when $\gamma \leftarrow P^*(\alpha, \beta; r_{P^*})$, $\gamma' \leftarrow P^*(\alpha, \beta'; r_{P^*})$,

both (α, β, γ) and $(\alpha, \beta', \gamma')$ accept.

$$\Pr_{r_{p^*}, \beta} \left[\langle p^*(r_{p^*}), V \rangle \text{ accepts} \right] = \epsilon$$

(1)

for ϵ-fraction of choices of r_{p^*}, β, resulting transcript (α, β, r) is accepting.

$$\Pr_{r_{p^*}} \left[\Pr_{\beta} \left[\langle p^*(r_{p^*}), V \rangle \text{ accepts with this } \beta \right] > \frac{\epsilon}{2} \right] > \frac{\epsilon}{2}$$

Suppose step 3 is run $\left(\frac{1}{\epsilon}\right)^{100}$ times.

w.p. $\frac{\epsilon}{2}$, r_{p^*} is "good"

$$\Rightarrow \Pr_{\beta}\left[\langle P^*(r_{p^*}), V\rangle \text{ accepts}\right] > \frac{\epsilon}{2}$$

$\Rightarrow$ Sample $\beta, \beta' \leftarrow [0, q-1]$

$$\Pr\left[\beta \neq \beta' \wedge (\alpha, \beta, r) \text{ accept} \wedge (\alpha, \beta', r') \text{ accept}\right]$$

$$\geq \left(\frac{\epsilon}{2}\right)^2 - \frac{1}{q}$$

$$\epsilon = \Pr_{r_{p^*}, \beta} \left[\langle p^*(r_{p^*}), V \rangle \text{ with } \beta \text{ acc.} \right]$$

$$= \Pr_{r_{p^*}} \left[r_{p^*} \text{ is "good"} \right] \cdot \Pr_{\beta} \left[\text{acc} \mid r_{p^*} \text{ "good"} \right]$$

$$+ \Pr_{r_{p^*}} \left[r_{p^*} \text{ not "good"} \right] \cdot \Pr_{\beta} \left[\text{acc} \mid r_{p^*} \text{ not good} \right]$$

$$\leq \Pr_{r_{p^*}} \left[r_{p^*} \text{ is "good"} \right] + \frac{\epsilon}{2}$$

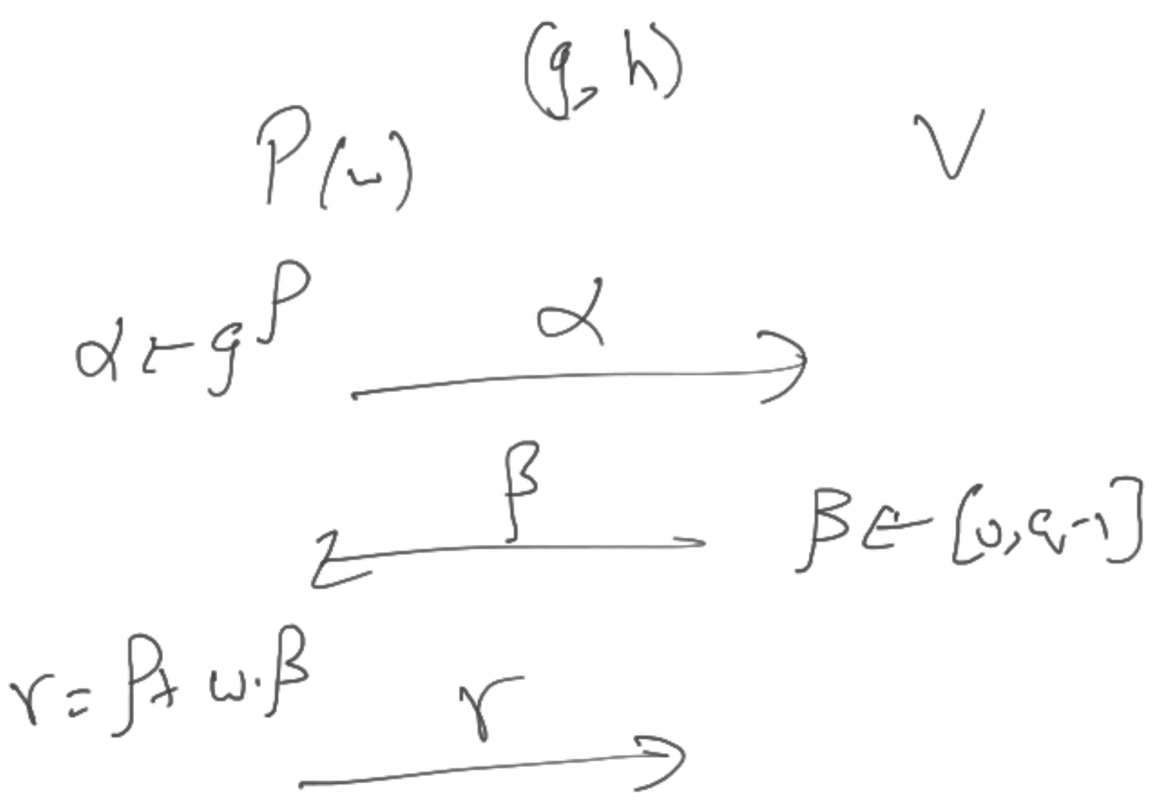
If poly time P^*, given random $pk = (g, h)$, can successfully make V accept with non-negl. prob.

then, Discrete Log can be solved in poly $\log(q)$ time.

Honest Verifier Security:

- $pk = (g, h)$ is sampled
- P^* is given (g, h), and several accepting honest transcripts (α_i, β_i, r_i)
- P^* then interacts with V
- Then, V should accept with negl. prob.

Honest Verifier P2K:



$(g^\rho, \beta, \rho + w \cdot \beta)$

$\rho = r - w\beta$

Sim (g, h):

- $\beta, r \leftarrow [0, q-1]$
- $\alpha = g^{r - w\beta}$

$= g^r \cdot (g^w)^{-\beta}$

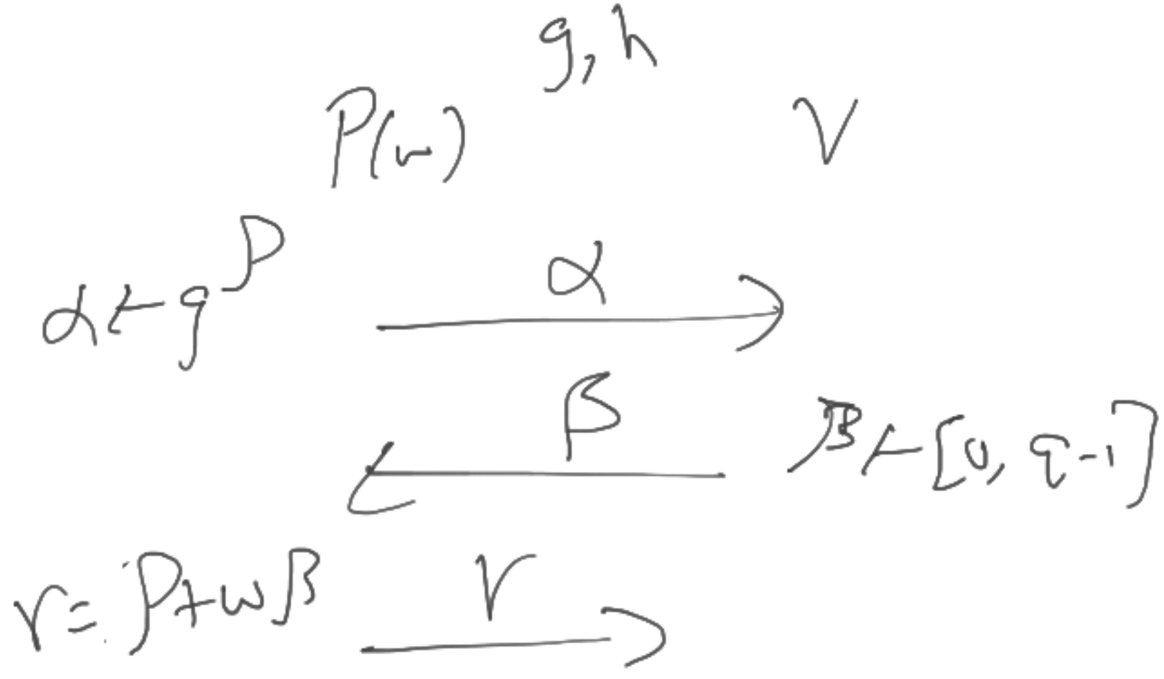
$= \underline{g^r \cdot (h^\beta)^{-1}}$

seiret signing key sk, public verification key pk

$m \longrightarrow \sigma$

message signature

- $Sign(m, sk) \to \sigma$: $Verify(m, \sigma, pk)$ accept
- $A(pk) \to m, \sigma$: $Verify(m, \sigma, pk)$ rejects



$sk = w$, $pk = g, h$

$Sign^{H}(m, w)$:

$\alpha \leftarrow g^{\rho}$

$\beta \leftarrow H(\alpha, m)$

$r \leftarrow \rho + w \cdot \beta$

$\sigma = (\alpha, \beta, r)$

$Versfy^{H}(g, h, m, \sigma)$:

$\beta \leftarrow H(\alpha, m)$

$V(\alpha, \beta, r)$