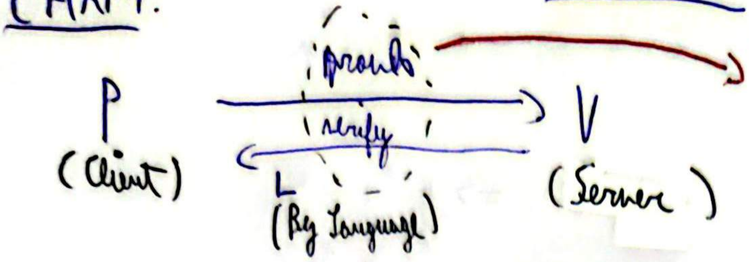
PRIVACY :

CHAP1:



→ This is an interactive proof

→ Complete : A Negligible proba to prove wrong when legitimate.

→ Sound : Negligible proba to prove right when not legitimate.

Protect° for prover : Verifier needs only to know that $l \in L$.

BPT PPT = Probabilistic Polynomial Time | TRANS = Transcript of interaction → NO ORDER → INDISTINGABLE*

* { A real transcript comes from interaction with the prover (who knows the secret).

L→ Authenticate someone (PRACTICE) NO CMP/DISTINGUISH

A simulated transcript is generated without the prover or the secret.

L→ Prove privacy (THEORY) → Verifier gains no information about prover's secret.

L→ It shows verifier learns nothing secret L→ only that statement is true.

L→ It proves trans cannot be reused to impersonate the prover.

L→ A proof tool not used in real systems.

Zero Knowledge Proofs (ZK) : (S.9)

→ Security : Cannot learn the prover's secret.

→ Privacy : Any transcript could have been simulated without the prover.

→ Authenticity : Only a prover who knows the secret can produce a valid transcript.

ZK proof for Discrete Log (DL) :

1) Group $G \mid |G| = q \in \mathbb{N} \wedge g \in G$

2) $x \in \mathbb{Z}_q = \{0, 1, \dots, q-1\}$, $h = g^x$

3) Give $A = (G, g, h)$ → Discrete log

4) A wins if $x = \log_g(h)$ ⇒ But very NP-HARD to compute

$Z_p^* = \{1, 2, \dots, p-1\}$ 1.1

$a, b \in Z_p^* \Rightarrow a \times b = (a . b) \% p = c \in Z_p^*$

$a \in Z_p^* \Rightarrow a \times a^{-1} = 1 = (a . a^{-1}) \% p \Rightarrow a^{-1} \in Z_p^*$

NOTE ($a^{-1} \neq 1/a$)

p is prime $\Rightarrow$ a b has an inverse a^{-1} in Z_p^*

Group : $p, q, g, Z_p \Rightarrow G$

SCHNORR

Prover		Verifier
$x \in Z_p$		$h = g^x \% p \in Z_p$
$r = rand(Z_q)$ $a = g^r \% p$	$\xrightarrow{a}$	$e = rand(Z_{2^n})$
	$\xleftarrow{e}$	
$f = (r + e . x) \% q$	$\xrightarrow{f}$	Check : $(g^f \% p) = (a . h^e \% p)$ $\Leftrightarrow g^{r+ex} = (g^r).(g^x)^e \quad (\% p)$

Completeness: If x is well associated to h, equation holds.

Soundness: Small proba for malicious to pass.

$\Rightarrow$ we need to run multiple challenges, at least P must respond correct to two challenges e and e'.

If P passes both $(a, e, f) \wedge (a, e', f')$ then

with same r and diff e, e', a remains the same.

$g^f = \underbrace{\textcircled{a}}_{\text{common}} h^e \ (\% p) \wedge g^{f'} = \textcircled{a} h^{e'} (\% p)$ holds

Then

$$\begin{cases} a = g^f . (h^e = g^{xe})^{-1} = g^{f'} . (h^{e'} = g^{xe'})^{-1} & (\% p) \\ x = \dfrac{f - f'}{e - e'} = \dfrac{\cancel{r} + ex - (\cancel{r} + e'x)}{e - e'} = \dfrac{x\cancel{(e - e')}}{\cancel{(e - e')}} \end{cases}$$