ZK Proofs

Thursday, September 7, 2017 12:31 PM

$ZKPoK\{(x): g^x = X\}$

witness

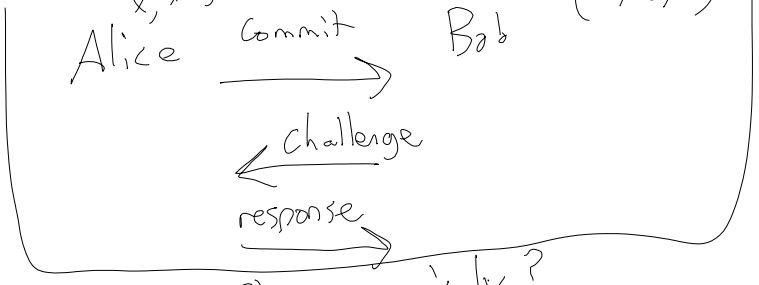
predicate

sometimes "statement"

Camenisch-Stadler notation

Desired Security:
- Bob should not learn X.
- Alice actually has to use x to convince Bob

Schnorr Identification protocol / Sigma (Σ) protocol



- How to define precisely?

Alice — first 128 bits of X → Bob

- Random protocol
- Prove security by simulation (as good as ideal world)

Interactive protocols

$P(x) \rightleftarrows V(X)$

Interactive Polynomial-Time Probabilistic Turing Machines

— probabilistic ⇒ able to make coin flips.

$b \leftarrow M(1^\lambda, \ldots)$

λ: security parameter

b: output; M: machine; inputs

probability distribution over outputs

— polynomial time ⇒ produce output in poly($|\lambda|$) steps

same polynomial

1^λ: λ-length string of ones

M is polynomial in λ and in input length

— Turing machines ⇒ "universal" ⇒ strong-church-turing thesis

Simulates any other machine

Distributions:

D is a distribution, probability

$D: S \rightarrow \mathbb{R}$, $\sum_{s \in S} D(s) = 1$

S: sample space

Notation:

$X \leftarrow D$ means X samples from D

$X \xleftarrow{\$} S$ means X samples uniformly from S.

Example: $Pr\left[\begin{matrix} b \xleftarrow{\$} \{0,1\} \\ b' \leftarrow M(1^\lambda) \end{matrix} : b = b'\right] = \frac{1}{2}$

Negligible functions:

$negl(\lambda)$ a "vanishingly small" function

Defn: for any polynomial $p(n)$,
$\exists n$ s.t. $\forall n' > n$, $f(n') < p(n')$

DLOG Assumption:

Let $\{G_\lambda\}_\lambda$ be a family of groups,
$|G_\lambda| = 2^{poly(\lambda)}$

Define $Adv_A^{DLOG}(\lambda) = Pr\left[x \xleftarrow{\$} \mathbb{Z}_{|G|},\ x' \leftarrow A(1^\lambda, g^x) : x = x' \right] = negl(\lambda)$
advantage

DLOG is hard for $\{G_\lambda\}$ iff
$\forall A,\ Adv_A^{DLOG}(\lambda) = negl(\lambda)$

Thought to hold for:
- Schnorr subgroups
- Some elliptic curves
...

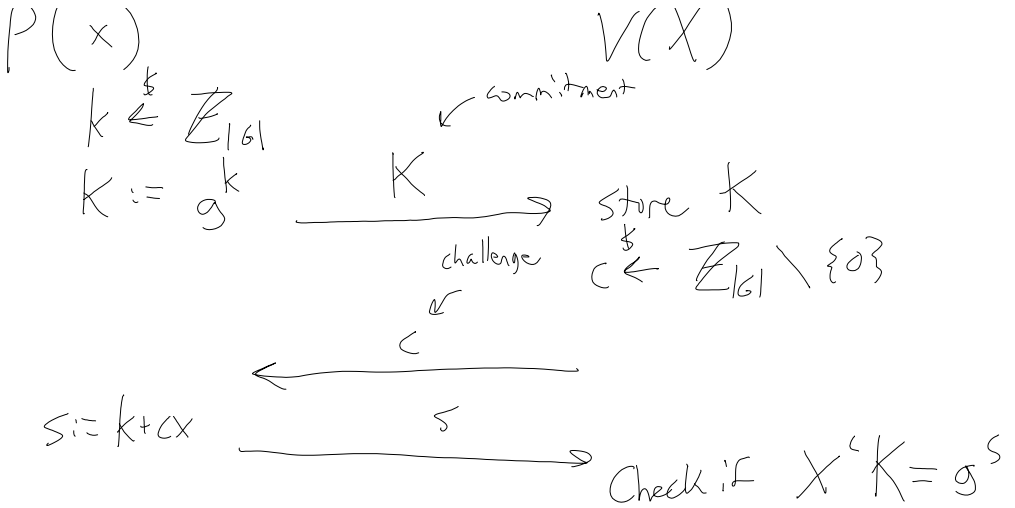
Computational Indistinguishability:

$\{D_\lambda\}_\lambda \approx_c \{E_\lambda\}_\lambda$ ← Distribution ensemble

iff

$\forall A,\ \left| Pr\left[x \leftarrow D_\lambda; A(1^\lambda, x) = 1 \right] - Pr\left[x \leftarrow E_\lambda; A(1^\lambda, x) = 1 \right] \right|$
$\leq negl(\lambda)$

Schnorr ID Protocol
Start with $(G, g, \cdot)$, $X = g^x$



Sanity Check (correctness):

$X^c K = g^s$

$(g^x)^c (g^k) = g^{k+cx}$ ✓

Why is it safe for P to send s. ?

Simulation:

Exists a simulator S for view of V.

$\{ View_V[P(x) \leftrightarrow V(g^x)] \} \approx \{ S(g^x) \}$

View of V is (K, c, s)

- all interactions with P, all coins flipped.

$S(x)$ is:

$s \xleftarrow{\$} \mathbb{Z}_{|G|}$

$c \xleftarrow{\$} \mathbb{Z}_{|G|} \setminus \{0\}$

$K := g^s / X^c$

Proof: The distributions are identical, even given X.

$$D(K,S,C) = \begin{cases} \frac{1}{|G|\cdot(|G|-1)} & \text{iff } K = g^S / X^C \\ 0 & \text{otherwise.} \end{cases}$$

Given K and C, there is a bijection between S and X

$$f_{K,C}(x) = K + Cx$$

$$f^{-1}_{K,C}(S) = (S-K)/C$$

We have not covered division in $\mathbb{Z}_p$, but notice, if $C \neq 0$, then C is a generator of $\mathbb{Z}_p$ (by Lagrange thm)

So, $(S-K)$ can be written as $X \cdot C$ for some $X \in \mathbb{Z}_p$.