Zero-knowledge protocols

Observations

- Fiat-Shamir protocol is perfect zero-knowledge, but due to its sequential round structure not efficient.
- The Schnorr protocol is not known to be perfect zero-knowledge, but very efficient.

Facts

- Zero-knowledge is preserved under sequential composition.
- Zero-knowledge is not preserved under parallel composition.

Okamoto protocol

- efficient, zero-knowledge, not perfect zero-knowledge,
- but almost as good, i.e. witness hiding.

Okamoto identification – setup

TA on input 1^k chooses primes p,q such that $q \mid p-1$ and $q > 2^k$, chooses generator z of $\mathbb{Z}_p^*$ and sets $g := z^{(p-1)/q}$, chooses $e \leftarrow \mathbb{Z}_q^*$, sets $h := g^e$

A chooses $w_1, w_2 \leftarrow \mathbb{Z}_q$, sets $v := g^{w_1} \cdot h^{w_2} \bmod p$.

TA sets $cert(A) := \left(id(A), v, Sign_{TA}\left(id(A), v\right)\right)$

Remark g,h have order q.

Okamoto identification protocol

A

$k_1, k_2 \leftarrow \mathbb{Z}_q$,

$z := g^{k_1} \cdot h^{k_2} \bmod p$

$\xrightarrow{\text{cert(A),z}}$

B

verifies cert(A)

$c \leftarrow \mathbb{Z}_q$

$\xleftarrow{c}$

$r_1 := k_1 - w_1 \cdot c \bmod q$

$r_2 := k_2 - w_2 \cdot c \bmod q$

$\xrightarrow{r_1, r_2}$

accepts iff

$z = g^{r_1} \cdot h^{r_2} \cdot v^c \bmod p$

Okamoto identification protocol - security

- security against cheating prover as in Schnorr protocol
- security against cheating verifier in 2 steps
  - show that Okamoto is witness indistinguishable (un-conditionally)
  - under assumption that discrete logarithm is hard show that witness indistinguishability implies witness hiding, i.e. cheating B cannot learn A's secret.

Witnesses and discrete logarithms

Definition 4.20 Given p,q,g,h and $v \in \langle g \rangle$ as before, the elements of $W(p,q,g,h,v) = W(v) := \left\{ (b_1, b_2) \middle| v = g^{-b_1} \cdot h^{-b_2} \bmod p \right\}$ are called witnesses for v.

Observation $\forall p,q,g,h,v : |W(v)| = q$

Witnesses and witness indistinguishability

Definition 4.20 Given p,q,g,h and $v \in \langle g \rangle$ as before, the elements of $W(p,q,g,h,v) = W(v) := \left\{ (b_1, b_2) \middle| v = g^{-b_1} \cdot h^{-b_2} \bmod p \right\}$ are called witnesses for v.

Lemma 4.21 Given p,q,g,h and $v \in \langle g \rangle$ as before, then for all $(b_1, b_2) \in W(v)$ and all possible transcripts (z, c, r_1, r_2) of the Okamoto protocol there is a unique $(l_1, l_2) \in \mathbb{Z}_q^2$ chosen by A with

- on input v the transcript is (z, c, r_1, r_2),
- B accepts,

i.e. the Okamoto protocol is witness indistinguishable.

The subgroup discrete logarithm problem

Let Gen be a ppt that on input 1^k

- choose primes p,q such that $q \mid p-1$ and $q \geq 2^k$
- chooses a generator z for $\mathbb{Z}_p^*$ and sets $g := z^{(p-1)/q}$.

Let A be a ppt.

Subgroup DL game $SDL_{A,Gen}(k)$

1. Run Gen(1^k) to obtain (p,q,g).
2. $e \leftarrow \mathbb{Z}_q, h := g^e \bmod p$.
3. A is given (p,q,g) and h. A outputs $e' \in \mathbb{Z}_q$.
4. Output of experiment is 1, if and only if $g^{e'} = h \bmod p$.

Write $SDL_{A,Gen}(k) = 1$, if output is 1.

The subgroup discrete logarithm problem

Subgroup DL game $\mathrm{SDL}_{A,\mathrm{Gen}}(k)$

1. Run $\mathrm{Gen}(1^k)$ to obtain (p,q,g).
2. $e \leftarrow \mathbb{Z}_q, h := g^e \bmod p$.
3. A is given (p,q,g) and h. A outputs $e' \in \mathbb{Z}_q$.
4. Output of experiment is 1, if and only if $g^{e'} = h \bmod p$.

Write $\mathrm{SDL}_{A,\mathrm{Gen}}(k) = 1$, if output is 1.

Definition 4.22 The SDL problem is hard relative to the generation algorithm Gen if for every ppt adversary A there is a negligible function $\mu : \mathbb{N} \to \mathbb{R}^+$ such that

$$\Pr\left[\mathrm{SDL}_{A,\mathrm{Gen}}(k) = 1\right] \leq \mu(k).$$

Okamoto protocol and witness hiding

Theorem 4.23 Assuming that the SDL problem is hard relative to the generation algorithm used in the setup of the Okamoto protocol (ignoring the last element), no ppt B, even after given the transcripts of polynomially many runs of the Okamoto protocol on input v, can compute a pair $(b_1, b_2) \in W(v)$, except with negligible probability. I.e. the Okamoto protocol is witness hiding.