V. Witness hiding 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.
- Four round variant of Schnorr is not efficient enough.
- Three round protocols can be used to design many variants of digital signatures.

Facts

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

Witness hiding protocols

- witness hiding as alternative to zero-knowledge
- guarantees slightly less, but easier to achive
- witness indistinguishability as important step to prove witness hiding
- Okamoto protocol as example of witness hiding protocol

Witness indistinguishable protocols

Defintion 5.1 Let V/P be a Σ- protocol for relation R. Protocol V/P is called witness indistinguishable if for all $x \in L_R$ and all verifiers V^* the distribution of transcripts between P and V^* does not depend on the witness $w \in W(x)$ that P has as input.

Okamoto identification protocol - security

Okamoto relation

- $x = (p, q, g, h, v), p \in \mathbb{N}$ prime, $g, v \in \mathbb{Z}_p^*, h \in \langle g \rangle, ord(g) = q,$ q prime, $w = (w_1, w_2) \in \mathbb{Z}_q^2$
- $R_{Okamoto}(x, w) = 1 :\Leftrightarrow g^{w_1} h^{w_2} = v \bmod p$

Okamoto identification protocol

P on input (p,q,g,v,w)

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

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

$\xrightarrow{a}$

V on input (p,q,g,v)

$c \leftarrow \{1,\ldots,2^l\}, 2^l < q$

$\xleftarrow{c}$

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

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

$\xrightarrow{r_1, r_2}$

accepts iff

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

Okamoto identification protocol - security

Okamoto relation

- $x = (p, q, g, h, v), p \in \mathbb{N}$ prime, $g, v \in \mathbb{Z}_p^*, h \in \langle g \rangle, ord(g) = q$, q prime, $w = (w_1, w_2) \in \mathbb{Z}_q^2$
- $R_{Okamoto}(x, w) = 1 :\Leftrightarrow g^{w_1} h^{w_2} = v \bmod p$

Theorem 5.2 The Okamoto protocol is a Σ-protocol for the relation $R_{Okamoto}$.

Lemma 5.3 The Okamoto protocol is witness indistinguishable.

Witness hiding protocols – instance generators

Defintion 5.4 An instance generator for relation R is a ppt Gen that an input 1^k outputs a pair $(x,w) \in R$ with $|x| \geq n$.

Witness hiding protocols

Witness hiding game $WH^{\Sigma}_{V^*,Gen}(k)$

1. Run Gen(1^k) to obtain (x,w).
2. V^* gets as input x and can interact with prover P that gets as input (x,w). V^* outputs $w^* \in \{0,1\}^*$.
4. Output of experiment is 1, if and only if $w^* \in W(x)$.

Write $WH^{\Sigma}_{A,Gen}(k) = 1$, if output is 1.

Defintion 5.5 Let V/P be a Σ- protocol and Gen an instance generator for relation R. Protocol V/P is called witness hiding for generator Gen if for all ppts V^* there is a negligible function μ such that

$$\Pr\left[WH^{\Sigma}_{V^*,Gen}(k) = 1\right] = \mu(k).$$

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 5.6 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 5.7 Let Gen be an instance generator for the Okamoto relation. If the SDL problem is hard relative to Gen (ignoring the last element), then the Okamoto protocol is witness hiding for Gen.