ID Schemes

Last lecture we proved that passively secure ID Schemes imply UF-CMA signatures using Fiat-Shamir transform. (ROM)

We want to construct a passively secure scheme.

We'll see 2 criteria for ID Schemes.

1) Honest verifyer - Zero Knowledge HVZK

Def: We say an ID scheme Π is HVZK if

$\exists$ PPT algo Sim s.t.

$$\left\{ (pk,sk) \leftarrow\$ Gen(1^\lambda) : sk, pk, Sim(pk) \right\} \approx_c$$

$$\approx_c \left\{ (pk,sk) \leftarrow\$ Gen(1^\lambda) : sk, pk, Trans(pk,sk) \right\}$$

This shows that the Gen algo reveals nothing about sk (zero knowledge)

2) Special Soundness

$GAME^{ss}_{\Pi,A}(\lambda)$

$A(1^\lambda)$ $\qquad\qquad\qquad\qquad$ $C(1^\lambda)$

$$\xleftarrow{\quad pk \quad} \quad (pk,sk) \leftarrow\$ Gen(1^\lambda)$$

$$\xrightarrow{\quad \alpha, \beta, \beta', \gamma, \gamma' \quad} \quad \text{OUTPUT } 1 \text{ iff}$$

(α, β, γ)

$(\alpha', \beta', \gamma')$ are VALID

$\wedge\ \beta \neq \beta'$

DEF: An ID scheme Π has special soundness $\forall$ PPT $\mathcal{A}$: f

$$\Pr[\text{GAME}^{ss}_{\Pi,\mathcal{A}}(\lambda) = 1] \leq \text{negl}(\lambda)$$

In this way 1) + 2) $\Rightarrow$ Passive Security

<u>THM</u>: Let Π be an ID scheme with SS and HVZK s.t. $|\mathcal{B}_{\lambda,pk}| = \omega(\log \lambda)$. Then Π is passively secure.

<u>Proof</u>: We start with $\text{GAME}^{id}_{\Pi,\mathcal{A}}(\lambda)$

$\mathcal{A}(1^\lambda)$ $\qquad\qquad\qquad$ $\mathcal{C}(1^\lambda)$

$\xleftarrow{\quad pk \quad}$ $\quad pk, sk \leftarrow\$ \text{Gen}(1^\lambda)$

\# poly

$\xrightarrow{\quad \text{"EMPTY"} \quad}$

$\xleftarrow{\quad \tau_i \quad}$ $\quad \tau_i \leftarrow\$ \text{Trans}(pk, sk)$

$\tau_i = (\alpha_i, \beta_i, \gamma_i)$

$\xrightarrow{\quad \alpha \quad}$

$\xleftarrow{\quad \beta \quad}$ $\quad \beta \leftarrow\$ \mathcal{B}_{\lambda,pk}$

$\xrightarrow{\quad \gamma \quad}$

And $\text{HYB}^{id}_{\Pi,\mathcal{A}}(\lambda)$

$\mathcal{A}(1^\lambda)$ $\qquad\qquad\qquad$ $\mathcal{C}(1^\lambda)$

$\xleftarrow{\quad pk \quad}$ $\quad pk, sk \leftarrow\$ \text{Gen}(1^\lambda)$

\# poly

$\xrightarrow{\quad \text{"EMPTY"} \quad}$

$\xleftarrow{\tau_i}$ $\quad \tau_i \leftarrow_\$ \mathrm{Sim}(pk)$

$\quad \tau_i = (\alpha_i, \beta_i, \gamma_i)$

$\xrightarrow{\alpha}$

$\xleftarrow{\beta}$ $\quad \beta \leftarrow_\$ B_{\lambda, pk}$

$\xrightarrow{\gamma}$

<u>LEMMA</u>: $\mathrm{GAME}^{id}_{\Pi,\mathcal{A}} \approx_c \mathrm{HYB}^{id}_{\Pi,\mathcal{A}}$

Proof: Assume $\exists$ PPT distinguisher D that can distinguish GAME from HYB.

$D(1^\lambda)$ $\quad\quad D'(1^\lambda)$ $\quad\quad \mathcal{C}(1^\lambda)$

$D \xleftarrow{pk} D'$ $\quad D' \xleftarrow{pk} \mathcal{C}$ $\quad pk, sk \leftarrow \mathrm{Gen}(1^\lambda)$

#poly

$D \xrightarrow{\text{"EMPTY"}} D'$

$D \xleftarrow{\tau} D'$

$\tau \to \$\mathrm{Trans}$

$\tau \to \$\mathrm{Sim}$

Solve through Hybrid argument.

<u>LEMMA</u>: $\Pr[\mathrm{HYB}(\lambda) = 1] \leq \mathrm{negl}(\lambda)$

Proof: Reduction to SS.

$\mathcal{A}(1^\lambda)$ $\quad\quad B(1^\lambda)$ $\quad\quad \mathcal{C}(1^\lambda)$

$\mathcal{A} \xleftarrow{pk} B$ $\quad B \xleftarrow{pk} \mathcal{C}$ $\quad (pk, sk) \leftarrow_\$ \mathrm{Gen}(1^\lambda)$

#poly

$\mathcal{A} \xrightarrow{\text{"EMPTY"}} B$

$\mathcal{A} \xleftarrow{\mathrm{Sim}(pk)} B$

$\mathcal{A} \xrightarrow{\alpha} B$

$$\xleftarrow{\qquad \beta \qquad} \quad \beta \leftarrow\$ B_{\lambda,pk}$$

$$\xrightarrow{\qquad \gamma \qquad}$$

$$\xleftarrow{\qquad \beta' \qquad}$$

$$\xrightarrow{\qquad \gamma' \qquad} \qquad \xrightarrow{\quad \alpha, \beta, \beta', \gamma, \gamma' \quad}$$

The analysis is a bit tricky.
Let z be the state of A after sending α.
(z is a random variable).

Let $\varepsilon(\lambda) = \Pr[H_1(\lambda) = 1]$ and
$\delta_z = \Pr[H_1(\lambda) = 1 \mid z]$

$$\Rightarrow \varepsilon(\lambda) = \sum_z p_z \cdot \delta_z$$
$$= E[\delta_z]$$

ε is just the average of each δ_z.

Let GOOD be the event $\beta \neq \beta'$.

$$\Pr[B \text{ wins}] \geq \Pr[H_1(\lambda) = 1 \wedge \text{GOOD}]$$
$$\geq \Pr[B \text{ wins} \wedge \text{GOOD}]$$
$$\geq \Pr[B \text{ wins} \mid \text{GOOD}] - |B_{\lambda,pk}|^{-1}$$
$$= \sum_z p_z \delta_z^2 - |B_{\lambda,pk}|^{-1}$$
$$= E[\delta_z^2] - |B_{\lambda,pk}|^{-1}$$
$$= \varepsilon^2(\lambda) - \text{negl}(\lambda)$$

$\geq 1/\text{poly} - \text{negl}(\lambda)$

SCHNORR

$(\mathbb{G}, g, q) \leftarrow \$ \text{groupgen}(1^\lambda),\ y = g^x,\ x \leftarrow \$ \mathbb{Z}_q$

$P(x,y)$ $\qquad\qquad\qquad\qquad$ $V(y)$

$\alpha = g^a \quad \xrightarrow{\quad \alpha \quad}$

$a \leftarrow \$ \mathbb{Z}_q \quad \xleftarrow{\quad \beta \quad} \quad \beta \leftarrow \mathbb{Z}_q$

$\gamma = \beta x + a \bmod q \quad \xrightarrow{\quad \gamma \quad} \quad$ Check

$$g^\gamma = \alpha y^\beta$$

Let's now prove passive security (from last lecture).

1) HVZK. Consider following Sim(y)

$\gamma, \beta \leftarrow \mathbb{Z}_q,\ \alpha = g^\gamma \cdot y^{-\beta}$

OUTPUT (α, β, γ)

2) SS

Assume $\exists$ PPT $A(y)$
outputs $\alpha, \beta, \beta', \gamma, \gamma'$ s.t.

i) $(\alpha, \beta, \gamma) = (\alpha, \beta', \gamma')$
ii) $\beta \neq \beta'$