Waters digital signature

Let's finish the proof: Recall the reduction to CDH:

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

$$\xleftarrow{pk \; ①} \qquad \xleftarrow{params,\, g_1, g_2} \qquad \text{params}: (\mathbb{G}, \mathbb{G}_T, g, q, \hat{e})$$

$$\xrightarrow{m \; ②} \qquad g_1 = g^a,\ g_2 = g^b$$

$$\xleftarrow{\sigma} \qquad a, b \leftarrow \$ \, \mathbb{Z}_q$$

$$\xrightarrow{(m^*, \sigma^*) \; ③} \qquad \xrightarrow{\sigma_1^* / (\sigma_2^*)^{\gamma(m^*)}}$$

\# of signature queries

① Simulation of public key. Let $l = 2q_s$, sample

$$x_0 \leftarrow \$ \{-k_l, \dots, 0\} ; \; x_{1,\dots,k} \leftarrow \$ \{0, \dots, l\}$$

k : msg size

$$y_{0,\dots,k} \leftarrow \$ \, \mathbb{Z}_q$$

Output $pk = (params, g_1, g_2, u_0, \dots, u_k)$

where $u_i = g_2^{x_i} \cdot g^{y_i} \; \forall i \in [0, k]$

In this way: $\alpha(m) = u_0 \prod u_i^{m[i]} = g_2^{\beta(m)} \cdot g^{\gamma(m)}$

$$\beta(m) = x_0 + \sum_{i=1}^{k} x_i m[i]$$

$$\gamma(m) = y_0 + \sum_{i=1}^{k} y_i m[i]$$

2 Signature queries: $m \in \{0,1\}^k$

If $\beta(m) = 0 \bmod q$, ABORT.

Else $(\sigma_1, \sigma_2) = (g_2^{\beta r} \cdot g^{\gamma r} \cdot g_1^{-\gamma \beta^{-1}}, g^r \cdot g_1^{-\beta^{-1}})$

In last lecture (σ_1, σ_2) distributed as real signatures with $\bar{r} = r - a\beta^{-1}$

3 Forgery (m^*, σ^*)

If $\beta(m^*) \neq 0 \bmod q$, ABORT

Else, output $\sigma_1^* / (\sigma_2^*)^{\gamma(m^*)}$

In last lecture, above value $= g^{ab}$

<u>CLAIM</u>: The reduction aborts with negl. probability.

Proof: When does $\mathcal{B}$ abort? If either

(i) $\beta(m^*) \neq 0$

(ii) $\beta(m^*) = 0 \wedge \beta(m_1) = 0 \vee \beta(m^*) = 0 \wedge \beta(m_2) = 0$

$\dots \vee \beta(m^*) = 0 \wedge \beta(m_{q_s}) = 0$

Let BAD be the event that $\mathcal{B}$ aborts.

By UNION BOUND:

$$\Pr[BAD] \le \Pr[\beta(m^*) \neq 0] + \sum_{i=1}^{k} \Pr[\beta(m^*) = 0 \wedge \beta(m_i) = 0]$$

absolute value

Above, we assume $k.l < q$, so that $|\beta(m)| \le kl < q$ and thus we forget about mod q.

Let's compute $\Pr[\beta(m^*) \neq 0]$.

There is exactly 1 choice of x_0 s.t $\beta(m^*) = 0$.

$$x_0 = -\sum x_i m^*[i]$$

$$\Pr[\beta(m^*) \neq 0] = \frac{kl}{kl+1} \qquad x_0 \leftarrow \$ \{-kl, \ldots, 0\}$$

Similarly, take any $\bar{m}$ part of signature queries.

Since $m^* \neq \bar{m}$, $\exists j \in [k]$ s.t. $m^*[j] \neq \bar{m}[j]$

WLOG, assume $m^*[j] = 1$ and $\bar{m}[j] = 0$.

Fix arbitrary choice of $x_1, \ldots, x_{j-1}, x_{j+1}, \ldots, x_k \in [0, l]$

Then, $\beta(m^*) = 0$ and $\beta(\bar{m}) = 0$ only if

$$x_0 + x_j = -\sum_{i \neq j} x_i m^*[i] \; ; \; x_0 = -\sum_{i \neq j} x_i \bar{m}[i]$$

$$\Rightarrow \Pr[\beta(m^*) = 0 \wedge \beta(m_i) = 0] \le \frac{1}{kl+1} \cdot \frac{1}{l+1}$$

$$\Pr[BAD] \le \frac{kl}{kl+1} + q_s \cdot \frac{1}{kl+1} \cdot \frac{1}{l+1}$$

$$\Pr[\text{GOOD}] = 1 - \Pr[\text{BAD}] \geq 1 - \frac{kl}{kl+1} - q_s \cdot \frac{1}{kl+1} \cdot \frac{1}{l+1}$$

$$= \frac{1}{kl+1}\left(kl+1-kl-\frac{q_s}{l+1}\right)$$

$$= \frac{1}{kl+1} \cdot \left(1 - \frac{q_s}{l+1}\right)$$ Recall: $l = 2q_s$

$$= \frac{1}{kl+1} \cdot \left(1 - \frac{l/2}{l+1}\right)$$ Since $l/(l+1) < 1$

$$> \frac{1}{kl+1}\left(1-\frac{1}{2}\right) = \frac{1}{2} \cdot \frac{1}{kl+1} = \frac{1}{4kq_s+2} = 1/\text{poly}(\lambda)$$

$$\Rightarrow \Pr[B \text{ wins}] \geq \Pr[\text{GOOD}] \cdot 1/\text{poly} \geq 1/\text{poly}$$

QUANTUM COMPUTER: Algo by SHOR can solve factoring and discrete log in PPT.

What about POST-QUANTUM CRYPTO?

IDENTIFICATION SCHEMES

$\Pi = (\text{Gen}, \mathcal{P}, \mathcal{V})$

Alice (PROVER $\mathcal{P}$)		Bob (VERIFIER $\mathcal{V}$)
$pk, sk \leftarrow\$ \text{Gen}(1^\lambda)$	$\xrightarrow{\hspace{3em}}$ $\xleftarrow[\dots]{\hspace{3em}}$	pk

$\longrightarrow$

$\longleftarrow$ at the end Bob outputs $d \in \{0,1\}$

INTERACTIVE PROTOCOL

Notation:

$$\text{Transcript } \tau \leftarrow\$ \big(\mathcal{P}(pk, sk) \rightleftarrows \mathcal{V}(pk)\big) = \text{Trans}(pk, sk)$$

$$\text{Output } \quad d = \text{Output}\big(\mathcal{P}(pk, sk) \rightleftarrows \mathcal{V}(pk)\big)$$

Properties:

<u>CORRECTNESS</u>: $\forall \lambda \in \mathbb{N}, \forall (pk, sk) \leftarrow\$ \text{Gen}(1^\lambda)$

$$\Pr\big[\text{Output}\big(\mathcal{P}(pk, sk) \rightleftarrows \mathcal{V}(pk)\big) = 1\big] = 1$$

<u>PASSIVE SECURITY</u>: An adversary observing honest executions cannot impersonate Alice

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

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

\# poly

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

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

$\vdots$

$\xrightarrow{\mathcal{A} \text{ impersonates Alice}}$ Output of GAME is the decision of Bob

<u>DEF</u>: ID scheme Π is passively secure if $\forall$ PPT $\mathcal{A}$

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

THE FIAT-SHAMIR TRANSFORM

A recipe for obtaining UF-CMA signatures from a class of ID schemes called CANONICAL.

$$\begin{array}{lcl}
\mathcal{P}(pk, sk) & & \mathcal{V}(pk) \\
(s, \alpha) \leftarrow \mathcal{P}_1(pk, sk) & \xrightarrow{\alpha} & \\
& \xleftarrow{\beta} & \beta \leftarrow \$ \mathcal{B}_{pk,\lambda} \\
\gamma \leftarrow \$ \mathcal{P}_2(s, \beta) & \xrightarrow{\gamma} &
\end{array}$$

commitment

challenge space

state

challenge

response

NON DEGENERACY: For any sk and fixed $\hat{\alpha}$,

$$\Pr[\alpha = \hat{\alpha} : (\alpha, s) \leftarrow \$ \mathcal{P}_1(pk, sk)] \leq \text{negl}(\lambda)$$

α has high min-entropy (hard to guess α)

RUNNING EXAMPLE: The Schnorr ID scheme.

$$\text{params} = (\mathbb{G}, g, q) \leftarrow \$ \text{GroupGen}(1^\lambda)$$

$$x \leftarrow \$ \mathbb{Z}_q, \; y = g^x$$

$$pk = (\text{params}, y), \; sk = x \; ; \; \mathcal{B}_{pk,x} = \mathbb{Z}_q$$

$$\begin{array}{lcl}
\mathcal{P}(pk, sk) & & \mathcal{V}(pk) \\
& \xrightarrow{\alpha} & \\
\mathcal{P}_1 : \alpha = g^a ; \; a \leftarrow \$ \mathbb{Z}_q & \xleftarrow{\beta} & \beta \leftarrow \$ \mathbb{Z}_q
\end{array}$$

(COINS)

STATE : $s = (pk, sk, a)$ $\xrightarrow{\gamma}$ Check: $g^{\gamma} \cdot y^{-\beta} = \alpha$

x è la secret key

$P_2 : \gamma = \beta x + a$

CORRECTNESS: $g^{\gamma} = g^{\beta x + a} = (g^x)^{\beta} \cdot g^a = y^{\beta} \cdot \alpha$

NON-DEGENERACY:

è negl

$$\Pr[\alpha = \hat{\alpha}] = \Pr[\alpha = \hat{\alpha} ; \alpha \leftarrow \$ \mathbb{G}] = 1/|\mathbb{G}| \leq 1/\text{negl}(\lambda)$$

PASSIVE SECURITY: Next lecture ¯_(ツ)_/¯

With Fiat-Shamir we can make Π non interactive.

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

Alice | Bob

$(s, \alpha) \leftarrow \$ P_1(pk, sk)$ $\xrightarrow{m, \sigma = (\alpha, \gamma)}$

↳ sign. on $m \in \{0,1\}^*$

$\beta = H(\alpha || m)$

$\gamma = \$ P_2(s, \beta)$

m

$Vrfy(pk, m, \sigma)$:

Let $\beta = H(\alpha || m)$

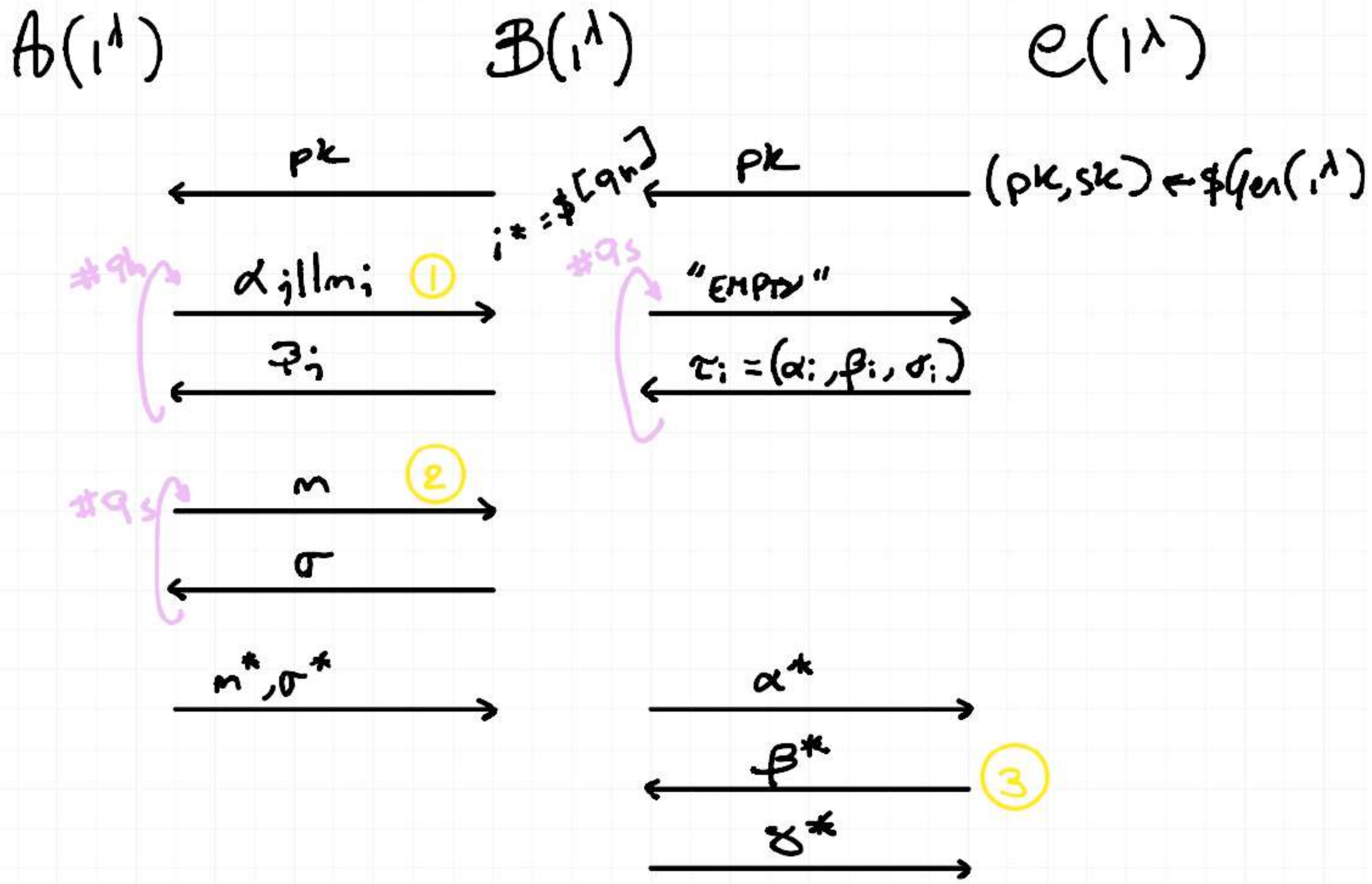
check $\tau = (\alpha, \beta, \gamma)$ is valid

THM: The above Signature is UF-CMA in the ROM assuming Π is passively secure and canonical.

Proof: Reduction to passive security of Π. Assume

∃ PPT A that forges in the UF-CMA game w.p. $1/poly$. Notice that A can make both Sign. and RO queries. A few simplifying assumptions

1) A never repeats RO queries
2) After obtaining a signature $\sigma = (\alpha, \gamma)$ on m, the attacker A does not query the RO on $\alpha || m$.
3) If A forges on m^* with $\sigma^* = (\alpha^*, \gamma^*)$ it already asked $\alpha^* || m^*$ to RO.



① Simulation of RO queries (α_j, m_j)

If $j = i^*$, start impersonation by sending α_{i^*}.

after receiving β^* ⇒ Output β^*

Else, $\beta_j \leftarrow_\$ \mathcal{B}_{\lambda, pk}$

② Simulation of signature on m_i

Take $\tau_i = (\alpha_i, \beta_i, \gamma_i)$ and let $\sigma_i = (\alpha_i, \gamma_i)$

Program the RO s.t. $H(m_i || \alpha_i) = \beta_i$

Caveat: what if $m_i || \alpha_i$ was already queried to RO? ABORT

③ If $m^*, \sigma^* = (\alpha^*, \gamma^*)$ is s.t. $m^* || \alpha^* = m_i^* || \alpha_i^*$ (guessed j correctly), OUTPUT γ^*, else ABORT.