Last week

A request for Bob's public key

Alice → Bob

Eve

A gives Bob a certificate

Digital Signature

Non-repudiation

DL-based signature scheme

$D = \mathbb{Z}_p^*$

${g_0, g_1, \ldots, g_7}$

$x \in \mathbb{Z}_q^*$

$y = g^x \mod p$

$k \in \mathbb{Z}_q^*$

$y' = g^k \mod p$

$c = H(m_1 r)$

$s = (k + c \cdot x) \mod q$

$m_1, c, s$

$r^x = g^s \cdot y' \mod q$

$C = H(m_1 r^x)$
Theorem: Schnorr is CMA secure in Random Oracle Model.

Proof:

\[ g^y = g^{sx} \]

A: computes
\[ r = g^{sy} \]

It then simulates the random oracle by sending \((m_i, r)\).

Whatever response it receives, it computes \(g^r\) with \(r\).

If \(c = c\), A wins.

Run A once \(\rightarrow (m, s, c)\) \(\rightarrow E\)

Run it again \(\rightarrow (m, s', c')\) \(\rightarrow\) with \(\text{Adv} \lt 0\) \(\frac{E}{2^n}\)

\[
\begin{align*}
g^s &= y^c \\
g^s' &= y^{c'} \\
g^{s+s'} &= y^{c-c'} \mod P \\
g^{s-s'} &= g^{x(c-c')} \mod P \\
s-s' &= x(c-c') \mod q \\
x &= (s-s')(c-c')^{-1} \mod q
\end{align*}
\]
Signatures in a Multi-user setting

Security Notion (CMA-muli)

Theorem: If any signature scheme is CMA in a single user, then it is also secure in the multi-user case.

Proof: \[\text{If } \exists \text{ an adversary } A \text{ which breaks } \text{CMA-muli}, \text{then } \exists \text{B which breaks single user CMA}.\]
The probability $A$ winning with $(m, s, k = 1)$ is $\frac{1}{n}$. That is, $B$ breaks CMA security with prob $P$ 
\[
\frac{1}{n} = P \Rightarrow \frac{1}{n} = np
\]
If for the single user case, if no adversary which can win with a prob $\geq P$, then for multi-user case $f$, no adversary with a prob $\geq np$.

---

**Optimal Asymmetric Encryption Padding (OAEP)**

$f: \{0, 1\}^k \rightarrow \{0, 1\}^k$, $f$ is one-way function.

$k$: parameter of the one-way function

$k_0 + k_1 < k$

$n = k - (k_0 + k_1)$

Given $G: \{0, 1\}^{k_0} \rightarrow \{0, 1\}^k$

$H: \{0, 1\}^{k_1} \rightarrow \{0, 1\}^{k_0}$

$G, H$: Random Oracle

**Encryption** $r \in \{0, 1\}^k$

$s = G(r) \oplus (x \| 0_{k_1}^k)$, $x$: length $n$

$t = H(s) \oplus r$: length $k_0$

$w = r \| t$: length $n$

$y = f(w)$

$y$ is encryption of $x$

**Decryption** $\hat{y} = f^{-1}(y) \Rightarrow (\hat{s}, \hat{t})$

$\hat{x} = t \oplus H(\hat{s})$

\[\hat{z} = (\hat{x})^0 \oplus \hat{s}\]

Last $k_1(\hat{x}) = 0^k$, then $\hat{y}$ is a valid cyphertext and output $\text{First}_k(\hat{x})$
Theorem:

\[ f \text{-OW} \Rightarrow \text{OAEP is IND-CCA1 in ROM} \]

Proof:

\[ \neg \text{OAEP IND-CCA1} \Rightarrow \neg f \text{-OW} \]

If there exists \( A \) which can break OAEP IND-CCA1, then \( \exists B \) which can break OW under \( A \).

\[ \begin{array}{c}
A \xrightarrow{x_0, x_1} y^* \\
\text{Encryption Oracle} \\
\text{Encryption Oracle} \\
\text{Decryption Oracle} \\
\text{Decryption Oracle} \\
\end{array} \]

B adversarially has to simulate Decryption oracle under \( A \).

\[ \begin{array}{c|c}
\text{r} & \text{G(r)} \\
\hline
\text{r} & \text{H(r)} \\
\end{array} \]

\[ \begin{array}{c}
\text{r} \\
\hline
\text{H(r)} \\
\end{array} \]

\[ A \xrightarrow{y} x \]

\[ \begin{array}{c}
( t', s') \\
\text{t'} = H(s') \oplus w' \\
w' = s' \| t' \\
y' = f(w') \\
\text{if } y = y', x' \| H = s' \oplus G(y') \end{array} \]