So far...

- Symmetric primitives (shared key): encryption, MACs
- Today: first asymmetric (or public-key) primitive: digital signature
- Scribe notes volunteers?
Digital Signature

- Only Signer can sign but everyone can verify
- **Key Generation**: \((sk, pk) \leftarrow \text{Gen}(1^n)\)
- **Sign**: \(\sigma \leftarrow \text{Sign}_{sk}(m)\)
- **Verify**: \(\text{Ver}_{pk}(m, \sigma) : \mathcal{M} \times \mathcal{S} \rightarrow \{0, 1\}\)
- **Correctness**: 
  \[
  \Pr[(sk, pk) \leftarrow \text{Gen}(1^n), \sigma \leftarrow \text{Sign}_{sk}(m) : \text{Ver}_{pk}(m, \sigma) = 1] = 1
  \]
- **Security (UF-CMA)**: 
  \[
  \Pr \left[ \begin{array}{c}
  (sk, pk) \leftarrow \text{Gen}(1^n) \\
  (m, \sigma) \leftarrow \mathcal{A}^{\text{Sign}_{sk}(\cdot)}(1^n, pk)
  \end{array} : \mathcal{A} \text{ did not query } m \land \text{Ver}_{pk}(m, \sigma) = 1 \right] \leq \nu(n)
  \]
- **One-time Signatures**: Adversary is allowed only one query
Security of Digital Signatures (game style)

**Definition**

Security of Digital Signatures A signature scheme \( \{ \text{Gen}, \text{Sign}, \text{Ver} \} \) is said to be secure if for all non-uniform PPT \( A \), there is a negligible function \( \mu \) such that \( \forall n, A \) wins the \text{SigForgingGame}(1^n) \) game with probability at most \( \mu(n) \): the game proceeds between a challenger \( Ch \) and adversary \( A \) in three steps:

1. **Init:** The challenger generates a key pair: \( (vk, sk) \leftarrow \text{Gen}(1^n) \).
2. **Learn:** \( A \) learns many signatures on messages of his choice.
   - \( A \) sends a message \( m_i \in M \) to \( Ch \)
   - \( Ch \) sends back a signature \( \sigma_i \leftarrow \text{Sign}(sk, m_i) \)
   
   Let \( L = \{m_i\} \) be the set of all messages \( A \) sends to \( Ch \).
3. **Guess:** \( A \) outputs a message-signature pair \( (m, \sigma) \)

   \( A \) wins if and only if \( m \notin L \land \text{Ver}(vk, m, \sigma) = 1 \).
Let $f$ be a one-way function
Let $f$ be a one-way function

- $sk := (x_0^0 x_1^0 \ldots x_n^0, x_1^1 x_2^1 \ldots x_n^1)$, where $x_i^b \leftarrow \{0, 1\}^n$ for all $i \in [n]$ and $b \in \{0, 1\}$
Let $f$ be a one-way function

- $sk := (x_0^1 \ x_0^2 \ \cdots \ x_n^0, \ x_1^1 \ x_1^2 \ \cdots \ x_n^1)$, where $x_i^b \leftarrow \{0, 1\}^n$ for all $i \in [n]$ and $b \in \{0, 1\}$
- $pk := (y_0^1 \ y_0^2 \ \cdots \ y_n^0, \ y_1^1 \ y_1^2 \ \cdots \ y_n^1)$, where $y_i^b = f(x_i^b)$ for all $i \in [n]$ and $b \in \{0, 1\}$
Let $f$ be a one-way function

- $sk := \left( x_0^1 \ x_1^1 \ x_2^1 \ \ldots \ x_n^1, \ x_0^0 \ x_1^0 \ x_2^0 \ \ldots \ x_n^0 \right)$, where $x_i^b \xleftarrow{s} \{0, 1\}^n$ for all $i \in [n]$ and $b \in \{0, 1\}$
- $pk := \left( y_0^1 \ y_1^1 \ y_2^1 \ \ldots \ y_n^1, \ y_0^0 \ y_1^0 \ y_2^0 \ \ldots \ y_n^0 \right)$, where $y_i^b = f(x_i^b)$ for all $i \in [n]$ and $b \in \{0, 1\}$
- $\text{Sign}_{sk}(m): \sigma := (x_1^{m_1}, x_2^{m_2}, \ldots, x_n^{m_n})$
Let $f$ be a one-way function

- $sk := (x_1^0 \ x_2^0 \ \ldots \ x_n^0)$, where $x_i^b \xleftarrow{\$} \{0, 1\}^n$ for all $i \in [n]$ and $b \in \{0, 1\}$
- $pk := (y_1^0 \ y_2^0 \ \ldots \ y_n^0)$, where $y_i^b = f(x_i^b)$ for all $i \in [n]$ and $b \in \{0, 1\}$
- $\text{Sign}_{sk}(m): \sigma := (x_1^m, x_2^m, \ldots, x_n^m)$
- $\text{Ver}_{pk}(m, \sigma)$: Accept if $f(\sigma_i) = y_i^m \ \forall i \in [n]$; reject otherwise.
Security of One-Time Signature Scheme

- Suppose that there exists a PPT $A$ who can win the **SigForgingGame** with noticeable probability $\varepsilon$.
- This means, $A$ asks for at most one signature $\sigma$ on some message $m$.
- $A$ outputs a signature $\sigma'$ on a **new** message $m' \neq m$.
- Let $i$ be the first bit-position such that $m_i \neq m'_i$.
- Such an $i$ exists because $m' \neq m$.
- This means $A$ inverts $f$ at position $i$: it sees inverse of either $y_i^0$ or $y_i^1$ but not both. Still it outputs the second one as a forgery.
- Therefore, $A$ inverts $f$ with probability $\varepsilon$ in one of the indices.
- Construct $B$ who gets a challenge $z = f(x)$ for OWF and chooses a random location $(i, b)$ and sets $y_i^b = z$.
- $B$ uses $A$ for forgery. It will invert $y$ with probability at least $\frac{\varepsilon}{2^n}$.
How to sign a long message?
Let $H = \{h_i : \{0, 1\}^* \rightarrow \{0, 1\}^n\}_{i \in I}$ be a CRHF family.

**Idea:** Sign $h_i(m)$ instead of $m$ using Lamport signature

**Think:** Proof?
What about signing multiple messages?
Multi-message Signatures (via chain)

- \((sk_0, pk_0) \leftarrow \text{Gen}(1^n)\)
- **Initialize**: \(\tilde{\sigma}_i = \emptyset, i = 1\)
- To sign \(m_i\):
  - \((sk_i, pk_i) \leftarrow \text{Gen}(1^n)\)
  - \(\tilde{\sigma}_i \leftarrow \text{Sign}_{sk_{i-1}}(m_i \| pk_i)\)
  - Output: \(\sigma_i = (i, \tilde{\sigma}_i, m_i, pk_i, \sigma_{i-1})\)
  - Increment \(i\)

**Think**: Proof?

**Think**: How to reduce signature size?

**Read**: Efficient Signatures from Trapdoor Permutations in the Random Oracle Model
Full-fledged Signature Schemes

- Using Merkle Trees and a lot of other ideas: [Naor-Yung89] show a full fledged scheme from UOWHFs.
- UOWHFs from a standard OWFs [Rompel90] $\implies$ digital signatures from OWFs only!
- Later class: number-theoretic constructions of signatures