Lecture 18: Message Authentication Codes & Digital Signatures
MACs and Signatures

Both are used to assert that a message has indeed been generated by a party.

MAC is the private-key version and Signatures are public-key version.

Note: Message hiding is not part of the (intuitive) security requirements.
Message Authentication Codes

- Defined by (Gen, Tag, Ver) algorithms
- The signer and the verifier meet to generate a secret key 
  \( sk \sim Gen(1^n) \)
- The signer sends a message \( m \in \{0, 1\}^n \) along with a tag 
  \( \tau \sim Tag_{sk}(m) \) (Note that the tag generation algorithm can be randomized)
- The verifier, upon receiving \((\tilde{m}, \tilde{\tau})\) verifies using 
  \( Ver_{sk}(\tilde{m}, \tilde{\tau}) \in \{0, 1\} \)
Correctness and Security

- **Correctness**: For any message $m \in \{0, 1\}^n$,
  $$\Pr[sk \sim \text{Gen}(1^n): \text{Ver}_{sk}(m, \text{Tag}_{sk}(m)) = 1] = 1$$

- **Security**: For any adversary $A$ the following holds
  $$\Pr[sk \sim \text{Gen}(1^n): A^{\text{Tag}_{sk}(\cdot)} = (m', \tau') \land m' \not\in Q \land \text{Ver}_{sk}(m', \tau') = 1] \leq \text{negl}(n),$$
  where $Q$ is the set of all queries made to the tagging oracle $\text{Tag}_{sk}(\cdot)$ by the adversary $A$.

- **Note**: If the security is restricted to $|Q| = k$, then it is called a $k$-time secure MAC.
Computational assumptions are not necessary for MACs

Consider the following construction of 1-time MAC

- \( \text{Gen}(1^n) \) samples \( r^{(b,i)} \leftarrow \{0, 1\}^k \), where \( b \in \{0, 1\} \) and \( i \in [n] \), and outputs:

\[
\text{sk} = \begin{pmatrix}
  r^{(0,1)} & r^{(0,2)} & \ldots & r^{(0,i)} & \ldots & r^{(0,n)} \\
  r^{(1,1)} & r^{(1,2)} & \ldots & r^{(1,i)} & \ldots & r^{(1,n)}
\end{pmatrix}
\]

- \( \text{Tag}_{\text{sk}}(m) \) outputs

\[
\tau = r^{(m_1,1)} r^{(m_2,2)} \ldots r^{(m_n,n)}
\]

- \( \text{Ver}_{\text{sk}}(\tilde{m}, \tilde{\tau}) \) outputs 1 if and only if all the following tests pass:

\[
r^{(\tilde{m}_i,i)} = \tilde{\tau}_i
\]
Proof of Security

- Suppose an adversary $A$ queries the tagging oracle at $m^{(1)}$ and gets outputs $\tau^{(1)}$
- Then it outputs $(m', \tau')$, where $m' \neq m^{(1)}$
- If $m' \neq m^{(1)}$ then there exists $i$ such that $m'_i \neq m_i^{(1)}$
- So, the probability that $(m', \tau')$ is a valid signature is at most the probability of guessing $r(m'_i, i)$, which is at most $2^{-k}$
- So, for $k = \omega(\log n)$ this is a secure 1-time MAC scheme
(poly-time) MAC using One-way Functions

- We will construct it using Pseudo-Random Functions (PRFs) and we already know that PRFs can be constructed from OWFs.
- Suppose \( \{f_1, \ldots, f_k(n)\} \) is a PRF family.
- Consider the following scheme:
  - \( \text{Gen}(1^n) \) samples \( \text{sk} \leftarrow \{1, \ldots, K(n)\} \)
  - \( \text{Tag}_{sk}(m) = f_{sk}(m) \)
  - \( \text{Ver}_{sk}(\tilde{m}, \tilde{\tau}) = 1 \) if and only if \( f_{sk}(\tilde{m}) = \tilde{\tau} \)
- Use the intuition to prove its security:
  - PRF family is computationally indistinguishable from the family of random functions.
  - Given evaluation of a random function at some points \( Q \), it is impossible to predict the output of the function at \( m' \neq Q \).
Digital Signatures

- Defined by \((\text{Gen}, \text{Sign}, \text{Ver})\) algorithms

- Correctness:

\[
\Pr[(sk, pk) \sim \text{Gen}(1^n) : \text{Ver}_{pk}(m, \text{Sign}_{sk}(m)) = 1] = 1
\]

- Security:

\[
\Pr \left[(sk, pk) \sim \text{Gen}(1^n) : \mathcal{A}_{\text{Sign}_{sk}(.)(pk)} = (m', \sigma') \land m' \notin Q \land \text{Ver}_{pk}(m', \sigma') = 1 \right] \leq \text{negl}(n)
\]
1-time Digital Signatures using OWF: Lamport Scheme

- Let $f : \{0, 1\}^n \to \{0, 1\}^n$ be a OWF
- $\text{Gen}(1^n)$ samples $r^{(b, i)} \leftarrow \{0, 1\}^n$, for $b \in \{0, 1\}$ and $i \in \{1, \ldots, n\}$ and computes $y^{(b, i)} = f(r^{(b, i)})$. Output $\text{sk} = (r^{(0, 1)} \ldots r^{(0, i)} \ldots r^{(0, n)})$
  $$\begin{pmatrix} r^{(0, 1)} & \ldots & r^{(0, i)} & \ldots & r^{(0, n)} \\ r^{(1, 1)} & \ldots & r^{(1, i)} & \ldots & r^{(1, n)} \end{pmatrix}$$
- $\text{pk} = (y^{(0, 1)} \ldots y^{(0, i)} \ldots y^{(0, n)})$
  $$\begin{pmatrix} y^{(0, 1)} & \ldots & y^{(0, i)} & \ldots & y^{(0, n)} \\ y^{(1, 1)} & \ldots & y^{(1, i)} & \ldots & y^{(1, n)} \end{pmatrix}$$
- $\text{Enc}_{\text{sk}}(m)$ outputs $\sigma = r^{(m_1, 1)} \ldots r^{(m_n, n)}$
- $\text{Ver}_{\text{pk}}(\tilde{m}, \tilde{\sigma})$ outputs 1 if and only if all the following tests pass

$$y^{(\tilde{m}_i, i)} = f(\tilde{\sigma}_i), \text{ where}$$
Suppose $A^*$ breaks the Lamport Scheme with probability $\varepsilon$

Following is the code of $\tilde{A}$ on input $y$:

1. Prepare sk and pk of Lamport Scheme
2. Pick random $i^* \leftarrow [n]$ and $b^* \leftarrow \{0, 1\}$
3. Replace $y(i^*, b^*)$ by $y$ in the public-key pk
4. Send pk to $A^*$
5. Receive $m$ from $A^*$
6. If $b^* = m_{i^*}$, then stop executing $A^*$ and return 0 to the external honest challenger of OWF experiment (this corresponds to the case where we need to know an inverse of $y$ to prepare the signature of $m$)
7. Otherwise, generate the signature $\sigma$ on $m$ using the secret key sk
8. Obtain $(m', \sigma')$ from $A^*$
9. If $(m', \sigma')$ is not a valid message and signature pair, then return 0 to the external honest challenger of OWF experiment (this corresponds to the case that the adversary $A^*$ failed to produce a forgery)
10. Otherwise, if $b^* = m'_{i^*}$, i.e. $A^*$ has helped us invert $y$ (think why this is the case), then return $\sigma'_{i^*}$ (This is the inverse of $y$)
Note that we succeed if we satisfy the following conditions:

- $b^* = m'_i$ but $b^* \neq m_i$
- $\mathcal{A}^*$ successfully breaks the signature scheme.

Conditioned on $\mathcal{A}^*$ successfully breaking the signature scheme, the probability that random $(i^*, b^*)$ satisfy the first condition is $1/2n$. So, overall probability of successfully inverting the OWF $f$ is $\varepsilon/2n$. 

Lecture 18: Message Authentication Codes & Digital Signatures
Think & Read about the following:

- Signing Arbitrary length messages: Use CRHF family that hash arbitrary length messages (Merkle-Damgård Construction) and the “Hash-then-sign” Paradigm
- Signatures where an adversary can ask for arbitrary-polynomial number of signatures of messages of its choice