Lecture 10: Authentication

Intuition

- Intuition: Digital analogue of physical signatures

Intuition

- Intuition: Digital analogue of physical signatures
- Signer signs a message m to produce a signature σ

Intuition

- Intuition: Digital analogue of physical signatures
- Signer signs a message m to produce a signature σ
- A Verifier can verify that σ is indeed generated for a message m

Intuition

- Intuition: Digital analogue of physical signatures
- Signer signs a message m to produce a signature σ
- A Verifier can verify that σ is indeed generated for a message m
- An adversary cannot *forge* a signature

Intuition

- Intuition: Digital analogue of physical signatures
- Signer signs a message m to produce a signature σ
- A Verifier can verify that σ is indeed generated for a message m
- An adversary cannot *forge* a signature
- Two types:

Intuition

- Intuition: Digital analogue of physical signatures
- Signer signs a message m to produce a signature σ
- A Verifier can verify that σ is indeed generated for a message m
- An adversary cannot *forge* a signature
- Two types:
  1. Private Key: Message Authentication Codes

Intuition

- Intuition: Digital analogue of physical signatures
- Signer signs a message m to produce a signature σ
- A Verifier can verify that σ is indeed generated for a message m
- An adversary cannot *forge* a signature
- Two types:
  1. Private Key: Message Authentication Codes
  2. Public Key: Digital Signatures

Message Authentication Codes

- Intuition: Signer and Verifier "share a secret"

Message Authentication Codes

- Intuition: Signer and Verifier "share a secret"
- Key Generation Algorithm: $\mathsf{Gen}(1^n)$ outputs secret key k

Message Authentication Codes

- Intuition: Signer and Verifier "share a secret"
- Key Generation Algorithm: $\text{Gen}(1^n)$ outputs secret key k
- "Signing" Algorithm: $\text{Tag}_k(m)$ outputs the tag σ

Message Authentication Codes

- Intuition: Signer and Verifier "share a secret"
- Key Generation Algorithm: $\mathsf{Gen}(1^n)$ outputs secret key k
- "Signing" Algorithm: $\mathsf{Tag}_k(m)$ outputs the tag σ
- Verification Algorithm: $\mathsf{Ver}_k(m, \sigma)$ is 1 if and only if σ is a valid tag of m under the secret key k

Message Authentication Codes

- Intuition: Signer and Verifier "share a secret"
- Key Generation Algorithm: $\mathsf{Gen}(1^n)$ outputs secret key k
- "Signing" Algorithm: $\mathsf{Tag}_k(m)$ outputs the tag σ
- Verification Algorithm: $\mathsf{Ver}_k(m, \sigma)$ is 1 if and only if σ is a valid tag of m under the secret key k
- Security: An adversary with oracle access to the tag oracle cannot forge the tag of a message

MAC: Algorithms

- $k \xleftarrow{\$} \mathsf{Gen}(1^n)$

MAC: Algorithms

- $k \xleftarrow{\$} \mathsf{Gen}(1^n)$
- $\sigma \xleftarrow{\$} \mathsf{Tag}_k(m)$

MAC: Algorithms

- $k \stackrel{\$}{\leftarrow} \mathsf{Gen}(1^n)$
- $\sigma \stackrel{\$}{\leftarrow} \mathsf{Tag}_k(m)$
- $\mathsf{Ver}_k : \mathcal{M} \times \mathcal{T} \to \{0, 1\}$

MAC: Algorithms

- $k \xleftarrow{\$} \mathsf{Gen}(1^n)$
- $\sigma \xleftarrow{\$} \mathsf{Tag}_k(m)$
- $\mathsf{Ver}_k : \mathcal{M} \times \mathcal{T} \to \{0, 1\}$
- Correctness:
  $\Pr[k \xleftarrow{\$} \mathsf{Gen}(1^n), \sigma \xleftarrow{\$} \mathsf{Tag}_k(m) \colon \mathsf{Ver}_k(m, \sigma) = 1] = 1$

MAC: Algorithms

- $k \xleftarrow{\$} \mathsf{Gen}(1^n)$
- $\sigma \xleftarrow{\$} \mathsf{Tag}_k(m)$
- $\mathsf{Ver}_k \colon \mathcal{M} \times \mathcal{T} \to \{0,1\}$
- Correctness:
  $\Pr[k \xleftarrow{\$} \mathsf{Gen}(1^n), \sigma \xleftarrow{\$} \mathsf{Tag}_k(m) \colon \mathsf{Ver}_k(m,\sigma) = 1] = 1$
- Security: For all n.u. PPT adversary $\mathcal{A}$ there exists a negligible $\nu(\cdot)$ such that:

$$\Pr\left[\begin{array}{c} k \xleftarrow{\$} \mathsf{Gen}(1^n) \\ (m,\sigma) \xleftarrow{\$} \mathcal{A}^{\mathsf{Tag}_k(\cdot)}(1^n) \end{array} : \begin{array}{c} \mathcal{A} \text{ did not query } m \wedge \\ \mathsf{Ver}_k(m,\sigma)=1 \end{array} \right] \leqslant \nu(n)$$

MAC: Construction

- PRF $\implies$ MAC

MAC: Construction

- PRF $\implies$ MAC
- Gen(1^n): Output $k \xleftarrow{\$} \{0,1\}^n$

MAC: Construction

- PRF $\implies$ MAC
- $\mathsf{Gen}(1^n)$: Output $k \xleftarrow{\$} \{0,1\}^n$
- $\mathsf{Tag}_k(m)$: Output $f_k(m)$

MAC: Construction

- PRF $\implies$ MAC
- $\text{Gen}(1^n)$: Output $k \xleftarrow{\$} \{0,1\}^n$
- $\text{Tag}_k(m)$: Output $f_k(m)$
- $\text{Ver}_k(m,\sigma)$: Output $f_k(m) \stackrel{?}{=} \sigma$

MAC: Construction

- PRF $\implies$ MAC
- Gen(1^n): Output $k \xleftarrow{\$} \{0,1\}^n$
- Tag$_k(m)$: Output $f_k(m)$
- Ver$_k(m,\sigma)$: Output $f_k(m) \stackrel{?}{=} \sigma$
- Think: Proof?

One-time MAC

- (Only modification) Security: Adversary is allowed only one query

One-time MAC

- (Only modification) Security: Adversary is allowed only one query
- Unconditionally-secure construction exists

One-time MAC

- (Only modification) Security: Adversary is allowed only one query
- Unconditionally-secure construction exists
- Think & Read

Digital Signature

- Intuition: Only Signer can sign and everyone can verify

Digital Signature

- Intuition: Only Signer can sign and everyone can verify
- Key Generation Algorithm: $(sk, pk) \xleftarrow{\$} \mathrm{Gen}(1^n)$

Digital Signature

- Intuition: Only Signer can sign and everyone can verify
- Key Generation Algorithm: $(sk, pk) \xleftarrow{\$} \mathsf{Gen}(1^n)$
- Signing Algorithm: $\sigma \xleftarrow{\$} \mathsf{Sign}_{sk}(m)$

Digital Signature

- Intuition: Only Signer can sign and everyone can verify
- Key Generation Algorithm: $(sk, pk) \stackrel{\$}{\leftarrow} \mathrm{Gen}(1^n)$
- Signing Algorithm: $\sigma \stackrel{\$}{\leftarrow} \mathrm{Sign}_{sk}(m)$
- Verify Algorithm: $\mathrm{Ver}_{pk}(m, \sigma) \colon \mathcal{M} \times \mathcal{S} \to \{0, 1\}$

Digital Signature

- Intuition: Only Signer can sign and everyone can verify
- Key Generation Algorithm: $(sk, pk) \xleftarrow{\$} \mathsf{Gen}(1^n)$
- Signing Algorithm: $\sigma \xleftarrow{\$} \mathsf{Sign}_{sk}(m)$
- Verify Algorithm: $\mathsf{Ver}_{pk}(m, \sigma) \colon \mathcal{M} \times \mathcal{S} \to \{0, 1\}$
- Correctness:
  $\Pr[(sk, pk) \xleftarrow{\$} \mathsf{Gen}(1^n), \sigma \xleftarrow{\$} \mathsf{Sign}_{sk}(m) \colon \mathsf{Ver}_{pk}(m, \sigma) = 1] = 1$

Digital Signature

- Intuition: Only Signer can sign and everyone can verify
- Key Generation Algorithm: $(sk, pk) \xleftarrow{\$} \mathsf{Gen}(1^n)$
- Signing Algorithm: $\sigma \xleftarrow{\$} \mathsf{Sign}_{sk}(m)$
- Verify Algorithm: $\mathsf{Ver}_{pk}(m, \sigma) \colon \mathcal{M} \times \mathcal{S} \to \{0, 1\}$
- Correctness:
  $\Pr[(sk, pk) \xleftarrow{\$} \mathsf{Gen}(1^n), \sigma \xleftarrow{\$} \mathsf{Sign}_{sk}(m) \colon \mathsf{Ver}_{pk}(m, \sigma) = 1] = 1$
- Security:

$$\Pr\left[\begin{matrix} (sk,pk) \xleftarrow{\$} \mathsf{Gen}(1^n) \\ (m,\sigma) \xleftarrow{\$} \mathcal{A}^{\mathsf{Sign}_{sk}(\cdot)}(1^n, pk) \end{matrix} : \begin{matrix} \mathcal{A} \text{ did not query } m \wedge \\ \mathsf{Ver}_{pk}(m,\sigma)=1 \end{matrix} \right] \leqslant \nu(n)$$

Digital Signature

- Intuition: Only Signer can sign and everyone can verify
- Key Generation Algorithm: $(sk, pk) \stackrel{\$}{\leftarrow} \mathsf{Gen}(1^n)$
- Signing Algorithm: $\sigma \stackrel{\$}{\leftarrow} \mathsf{Sign}_{sk}(m)$
- Verify Algorithm: $\mathsf{Ver}_{pk}(m, \sigma) \colon \mathcal{M} \times \mathcal{S} \to \{0, 1\}$
- Correctness:
  $\Pr[(sk, pk) \stackrel{\$}{\leftarrow} \mathsf{Gen}(1^n), \sigma \stackrel{\$}{\leftarrow} \mathsf{Sign}_{sk}(m) \colon \mathsf{Ver}_{pk}(m, \sigma) = 1] = 1$
- Security:

$$\Pr\left[\substack{(sk,pk) \stackrel{\$}{\leftarrow} \mathsf{Gen}(1^n) \\ (m,\sigma) \stackrel{\$}{\leftarrow} \mathcal{A}^{\mathsf{Sign}_{sk}(\cdot)}(1^n, pk)} \colon \substack{\mathcal{A} \text{ did not query } m \wedge \\ \mathsf{Ver}_{pk}(m,\sigma)=1}\right] \leqslant \nu(n)$$

- One-time Digital Signatures: Adversary is allowed only one query

One-time Digital Signature: Construction (Lamport's Signature)

- $sk := \begin{pmatrix} x_0^{(1)} & x_0^{(2)} & \dots & x_0^{(n)} \\ x_1^{(1)} & x_1^{(2)} & \dots & x_1^{(n)} \end{pmatrix}$, where $x_b^{(i)} \xleftarrow{\$} \{0,1\}^n$ for all $i \in [n]$ and $b \in \{0,1\}$

One-time Digital Signature: Construction (Lamport's Signature)

- $sk := \begin{pmatrix} x_0^{(1)} & x_0^{(2)} & \dots & x_0^{(n)} \\ x_1^{(1)} & x_1^{(2)} & \dots & x_1^{(n)} \end{pmatrix}$, where $x_b^{(i)} \xleftarrow{\$} \{0,1\}^n$ for all $i \in [n]$ and $b \in \{0,1\}$
- $pk := \begin{pmatrix} y_0^{(1)} & y_0^{(2)} & \dots & y_0^{(n)} \\ y_1^{(1)} & y_1^{(2)} & \dots & y_1^{(n)} \end{pmatrix}$, where $y_b^{(i)} = f(x_b^{(i)})$ for all $i \in [n]$ and $b \in \{0,1\}$

One-time Digital Signature: Construction (Lamport's Signature)

- $sk := \begin{pmatrix} x_0^{(1)} & x_0^{(2)} & \cdots & x_0^{(n)} \\ x_1^{(1)} & x_1^{(2)} & \cdots & x_1^{(n)} \end{pmatrix}$, where $x_b^{(i)} \xleftarrow{\$} \{0,1\}^n$ for all $i \in [n]$ and $b \in \{0,1\}$
- $pk := \begin{pmatrix} y_0^{(1)} & y_0^{(2)} & \cdots & y_0^{(n)} \\ y_1^{(1)} & y_1^{(2)} & \cdots & y_1^{(n)} \end{pmatrix}$, where $y_b^{(i)} = f(x_b^{(i)})$ for all $i \in [n]$ and $b \in \{0,1\}$
- $\mathrm{Sign}_{sk}(m)$: $\sigma := \left(x_{m_1}^{(1)}, x_{m_2}^{(2)}, \ldots, x_{m_n}^{(n)}\right)$

One-time Digital Signature: Construction (Lamport's Signature)

- $sk := \begin{pmatrix} x_0^{(1)} & x_0^{(2)} & \dots & x_0^{(n)} \\ x_1^{(1)} & x_1^{(2)} & \dots & x_1^{(n)} \end{pmatrix}$, where $x_b^{(i)} \xleftarrow{\$} \{0,1\}^n$ for all $i \in [n]$ and $b \in \{0,1\}$
- $pk := \begin{pmatrix} y_0^{(1)} & y_0^{(2)} & \dots & y_0^{(n)} \\ y_1^{(1)} & y_1^{(2)} & \dots & y_1^{(n)} \end{pmatrix}$, where $y_b^{(i)} = f(x_b^{(i)})$ for all $i \in [n]$ and $b \in \{0,1\}$
- $\text{Sign}_{sk}(m)$: $\sigma := \left(x_{m_1}^{(1)}, x_{m_2}^{(2)}, \dots, x_{m_n}^{(n)}\right)$
- $\text{Ver}_{pk}(\sigma)$: $\bigwedge_{i\in[n]} f(\sigma_i) \stackrel{?}{=} y_{m_i}^{(i)}$

One-time Digital Signature: Construction (Lamport's Signature)

- $sk := \begin{pmatrix} x_0^{(1)} & x_0^{(2)} & \dots & x_0^{(n)} \\ x_1^{(1)} & x_1^{(2)} & \dots & x_1^{(n)} \end{pmatrix}$, where $x_b^{(i)} \stackrel{\$}{\leftarrow} \{0,1\}^n$ for all $i \in [n]$ and $b \in \{0,1\}$
- $pk := \begin{pmatrix} y_0^{(1)} & y_0^{(2)} & \dots & y_0^{(n)} \\ y_1^{(1)} & y_1^{(2)} & \dots & y_1^{(n)} \end{pmatrix}$, where $y_b^{(i)} = f(x_b^{(i)})$ for all $i \in [n]$ and $b \in \{0,1\}$
- $\mathrm{Sign}_{sk}(m)$: $\sigma := \left(x_{m_1}^{(1)}, x_{m_2}^{(2)}, \dots, x_{m_n}^{(n)}\right)$
- $\mathrm{Ver}_{pk}(\sigma)$: $\wedge_{i\in[n]} f(\sigma_i) \stackrel{?}{=} y_{m_i}^{(i)}$
- Proof?