Digital signatures

Myrto Arapinis
School of Informatics
University of Edinburgh

October 16, 2017
Goal

Data integrity and origin authenticity in the public-key setting

key generation algorithm: $G : \to \mathcal{K} \times \mathcal{K}$

signing algorithm $S : \mathcal{K} \times \mathcal{M} \to S$

verification algorithm $V : \mathcal{K} \times \mathcal{M} \times S \to \{\top, \bot\}$

s.t. $\forall (sk, vk) \in G$, and $\forall m \in \mathcal{M}$, $V(vk, m, S(sk, m)) = \top$
Advantages of digital signatures over MACs

MACs

- are not publicly verifiable (and so not transferable)
  No one else, except Bob, can verify $t$.

- do not provide non-repudiation
  $t$ is not bound to Alice’s identity only. Alice could later claim she didn’t compute $t$ herself. It could very well have been Bob since he also knows the key $k$. 
Advantages of digital signatures over MACs

Digital signatures

- are publicly verifiable - anyone can verify a signature
- are transferable - due to public verifiability
- provide non-repudiation - if Alice signs a document with her secret key, she cannot deny it later
A good digital signature schemes should satisfy existential unforgeability.

**Existential unforgeability**

- Given \((m_1, S(sk, m_1)), \ldots, (m_n, S(sk, m_n))\) (where \(m_1, \ldots, m_n\) chosen by the adversary)
- It should be hard to compute a valid pair \((m, S(sk, m))\) without knowing \(sk\) for any \(m \not\in \{m_1, \ldots, m_n\}\)
Textbook RSA signatures

\[
G_{RSA}() = (pk, sk) \quad \text{where } pk = (N, e) \text{ and } sk = (N, d) \\
\text{and } N = p \cdot q \text{ with } p, q \text{ random primes} \\
\text{and } e, d \in \mathbb{Z} \text{ st. } e \cdot d \equiv 1 \pmod{\phi(N)}
\]
Textbook RSA signatures

\[ G_{RSA}() = (pk, sk) \]
where \( pk = (N, e) \) and \( sk = (N, d) \)
and \( N = p \cdot q \) with \( p, q \) random primes
and \( e, d \in \mathbb{Z} \) st. \( e \cdot d \equiv 1 \) (mod \( \phi(N) \))

\[ M = C = \mathbb{Z}_N \]
Textbook RSA signatures

- $G_{RSA}() = (pk, sk)$ where $pk = (N, e)$ and $sk = (N, d)$ and $N = p \cdot q$ with $p, q$ random primes and $e, d \in \mathbb{Z}$ st. $e \cdot d \equiv 1$ (mod $\phi(N)$)

- $M = C = \mathbb{Z}_N$

- Signing: $S_{RSA}(sk, x) = (x, x^d \pmod{N})$ where $pk = (N, e)$
Textbook RSA signatures

\[ G_{RSA}() = (pk, sk) \]
where \( pk = (N, e) \) and \( sk = (N, d) \)
and \( N = p \cdot q \) with \( p, q \) random primes
and \( e, d \in \mathbb{Z} \) st. \( e \cdot d \equiv 1 \pmod{\phi(N)} \)

\[ M = C = \mathbb{Z}_N \]

\[ M = C = \mathbb{Z}_N \]

\[ S_{RSA}(sk, x) = (x, x^d \pmod{N}) \]
where \( pk = (N, e) \)

\[ V_{RSA}(pk, m, x) = \begin{cases} 1 & \text{if } m = x^e \pmod{N} \\ \bot & \text{otherwise} \end{cases} \]
where \( sk = (N, d) \)
Textbook RSA signatures

- \( G_{RSA}(\cdot) = (pk, sk) \) where \( pk = (N, e) \) and \( sk = (N, d) \)
  and \( N = p \cdot q \) with \( p, q \) random primes
  and \( e, d \in \mathbb{Z} \) st. \( e \cdot d \equiv 1 \pmod{\phi(N)} \)

- \( M = C = \mathbb{Z}_N \)

- Signing: \( S_{RSA}(sk, x) = (x, x^d \pmod{N}) \) where \( pk = (N, e) \)

- Verifying: \( V_{RSA}(pk, m, x) = \begin{cases} 
\top & \text{if } m = x^e \pmod{N} \\
\bot & \text{otherwise}
\end{cases} 
\)
  where \( sk = (N, d) \)

- st \( \forall(pk, sk) = G_{RSA}(), \forall x, V_{RSA}(pk, x, S_{RSA}(sk, x)) = \top \)
Textbook RSA signatures

\[
\text{G}_{RSA}() = (pk, sk) \quad \text{where } pk = (N, e) \text{ and } sk = (N, d) \\
\text{and } N = p \cdot q \text{ with } p, q \text{ random primes} \\
\text{and } e, d \in \mathbb{Z} \text{ st. } e \cdot d \equiv 1 \pmod{\phi(N)}
\]

\[
\mathcal{M} = \mathcal{C} = \mathbb{Z}_N
\]

\[
\text{Signing: } S_{RSA}(sk, x) = (x, x^d \pmod{N}) \quad \text{where } pk = (N, e)
\]

\[
\text{Verifying: } V_{RSA}(pk, m, x) = \begin{cases} 
\top & \text{if } m = x^e \pmod{N} \\
\bot & \text{otherwise}
\end{cases}
\]

where \( sk = (N, d) \)

\[
\forall (pk, sk) = \text{G}_{RSA}(), \forall x, V_{RSA}(pk, x, S_{RSA}(sk, x)) = \top
\]

Proof: exactly as proof of consistency of RSA encryption/decryption
Problems with “textbook RSA signatures”

Textbook RSA signatures are not secure

The “textbook RSA signature” scheme does not provide existential unforgeability

- Suppose Eve has two valid signatures \( \sigma_1 = M_1^d \mod n \) and \( \sigma_2 = M_2^d \mod n \) from Bob, on messages \( M_1 \) and \( M_2 \).
- Then Eve can exploit the homomorphic properties of RSA and produce a new signature
Problems with “textbook RSA signatures”

Textbook RSA signatures are not secure

The “textbook RSA signature” scheme does not provide existential unforgeability

- Suppose Eve has two valid signatures $\sigma_1 = M_1^d \mod n$ and $\sigma_2 = M_2^d \mod n$ from Bob, on messages $M_1$ and $M_2$.
- Then Eve can exploit the homomorphic properties of RSA and produce a new signature

$$\sigma = \sigma_1 \cdot \sigma_2 \mod n = M_1^d \cdot M_2^d \mod n = (M_1 \cdot M_2)^d \mod n$$

which is a valid signature from Bob on message $M_1 \cdot M_2$. 
How to use RSA for signatures

Solution

Before computing the RSA function, apply a hash function $H$.

- Signing: $S_{RSA}(sk, x) = (x, H(x)^d \pmod N)$
How to use RSA for signatures

Solution

Before computing the RSA function, apply a hash function $H$.

- Signing: $S_{RSA}(sk, x) = (x, H(x)^d \pmod{N})$

- Verifying: $V_{RSA}(pk, m, x) = \begin{cases} \top & \text{if } H(m) = x^e \pmod{N} \\ \bot & \text{otherwise} \end{cases}$