CSCI 1510

This Lecture:

- RSA Signature (Continued)
- Random Oracle Model
- Identification Schemes
- Fiat-Shamir Transform
- Schnorr's Identification / Signature Schemes

Digital Signature

- **Syntax:**
  A digital signature scheme is defined by PPT algorithms (Gen, Sign, Vrfy):

  $(pk, sk) \leftarrow Gen(1^n)$

  $\sigma \leftarrow Sign_{sk}(m) \quad m \in M$

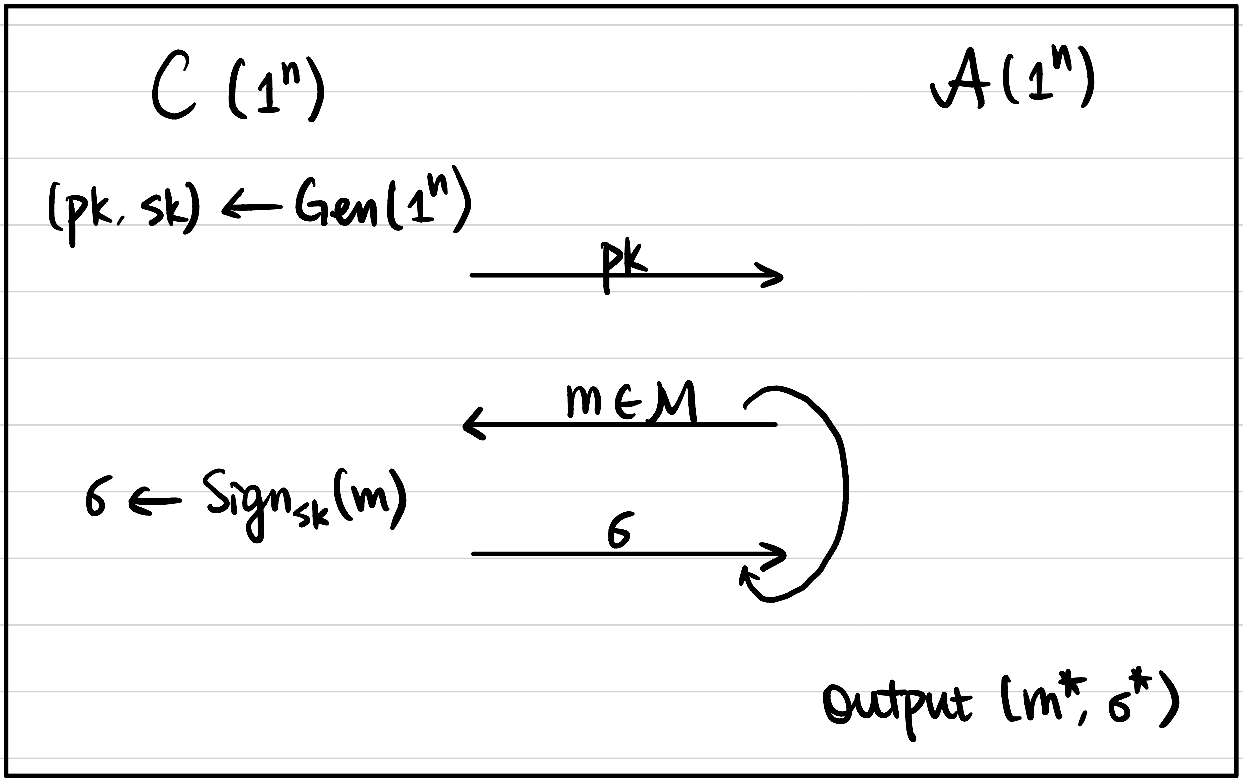
  $0/1 := Vrfy_{pk}(m, \sigma)$

- **Correctness:** $\forall n$, $\forall (pk, sk)$ output by $Gen(1^n)$, $\forall m \in M$

  $Vrfy_{pk}(m, Sign_{sk}(m)) = 1$

Digital Signature

Def A digital signature scheme $\Pi = (\mathrm{Gen}, \mathrm{Sign}, \mathrm{Vrfy})$ is secure if $\forall$ PPT $\mathcal{A}$, $\exists$ negligible function $\varepsilon(\cdot)$ s.t. $\Pr[\mathrm{SigForge}_{\mathcal{A},\Pi} = 1] \leq \varepsilon(n)$.



$Q := \{m \mid m \text{ queried by } \mathcal{A}\}$

$\mathrm{SigForge}_{\mathcal{A},\Pi} = 1$ ($\mathcal{A}$ succeeds) if

① $m^* \notin Q$, and

② $\mathrm{Vrfy}_{pk}(m^*, \sigma^*) = 1$.

RSA-based Signatures

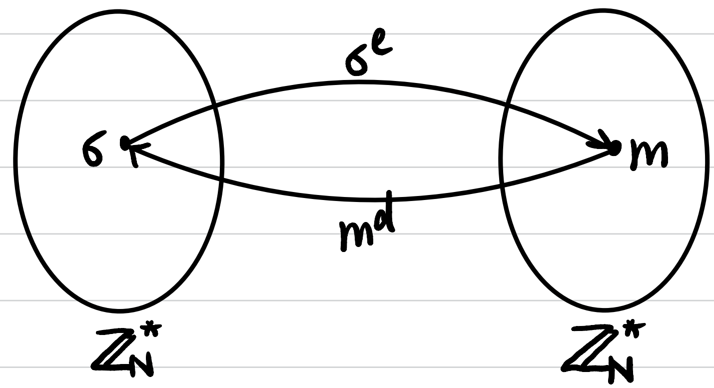
Plain RSA Signature:

- $\mathrm{Gen}(1^n)$:

  $(N, e, d) \leftarrow \mathrm{GenRSA}(1^n)$

  $pk := (N, e)$

  $sk := (N, d)$



- $\mathrm{Sign}_{sk}(m)$: $m \in \mathbb{Z}_N^*$

  $\sigma := m^d \bmod N$

- $\mathrm{Vrfy}_{pk}(m, \sigma)$: $m \stackrel{?}{=} \sigma^e \bmod N$

Is it secure?

C $\qquad\qquad$ A

$\xrightarrow{pk = (N, e)}$

Pick an arbitrary $\sigma^* \in \mathbb{Z}_N^*$, $m^* = (\sigma^*)^e \bmod N$

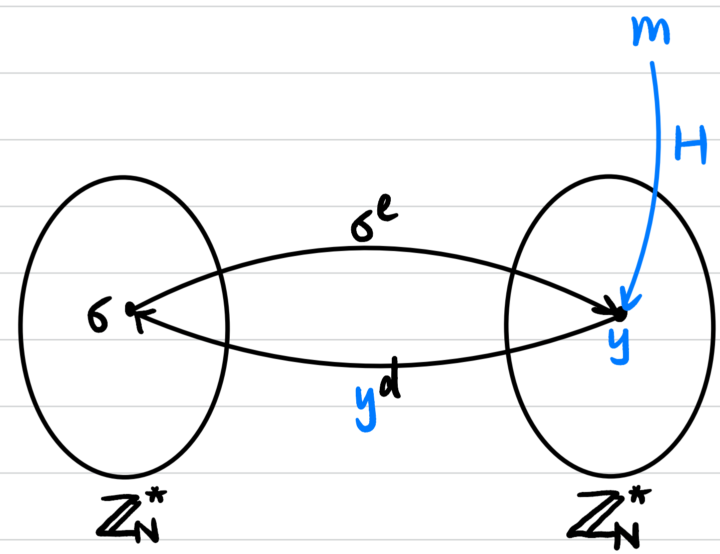
$\xleftarrow{m}$

$\xrightarrow{e}$

$m^* = m^2 \bmod N$, $\sigma^* = \sigma^2 \bmod N$

RSA-based Signatures

RSA-FDH (Full Domain Hash) Signature:



- $Gen(1^n)$:

  $(N,e,d) \leftarrow GenRSA(1^n)$

  $pk := (N,e)$

  $sk := (N,d)$

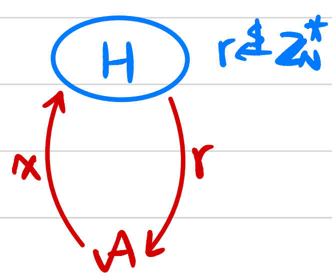
  Specify a hash function $H: \{0,1\}^* \to \mathbb{Z}_N^*$

- $Sign_{sk}(m)$: $m \in \{0,1\}^*$

  $\sigma := H(m)^d \bmod N$

- $Vrfy_{pk}(m,\sigma)$: $H(m) \stackrel{?}{=} \sigma^e \bmod N$

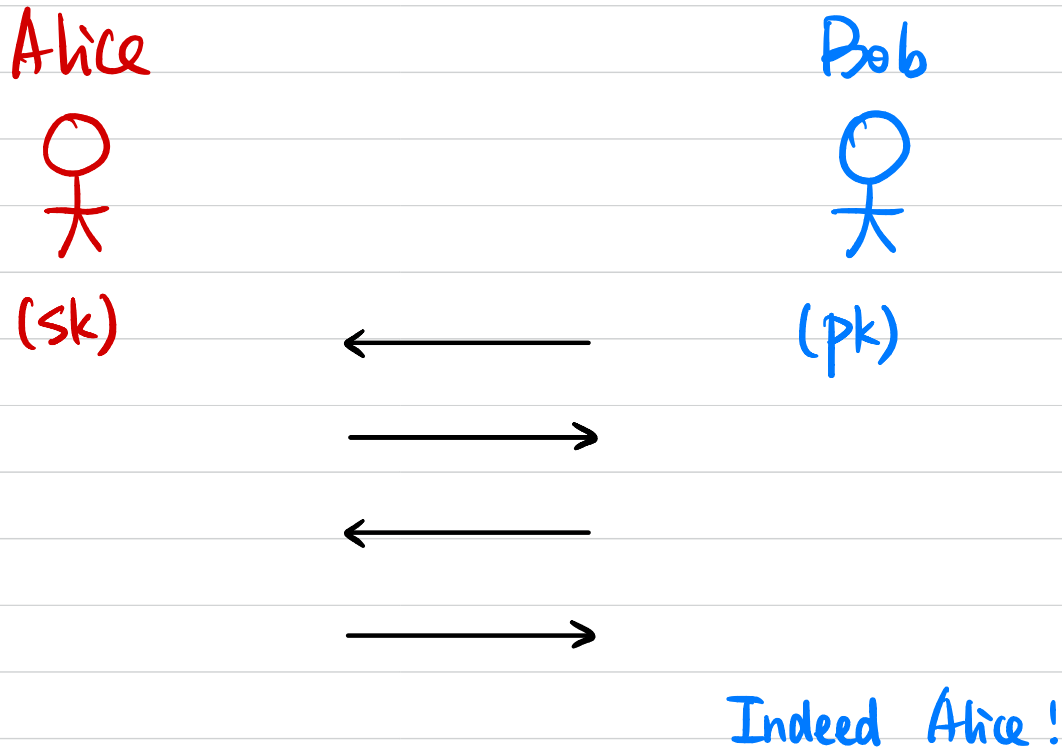
<u>Thm</u> If the RSA problem is hard relative to GenRSA and H is modeled as a random oracle, then this signature scheme is secure.



Signatures from DLOG

$$\begin{tikzcd} \text{1 Identification Scheme} \arrow[r, Rightarrow, "\text{2 Fiat-Shamir}", "\text{Transform}"'] & \text{Digital Signature} \\ \text{Discrete Log} \arrow[u, Rightarrow, "3", "\text{Schnorr}"'] & \end{tikzcd}$$

Identification Scheme



Special 3-Round Identification Scheme

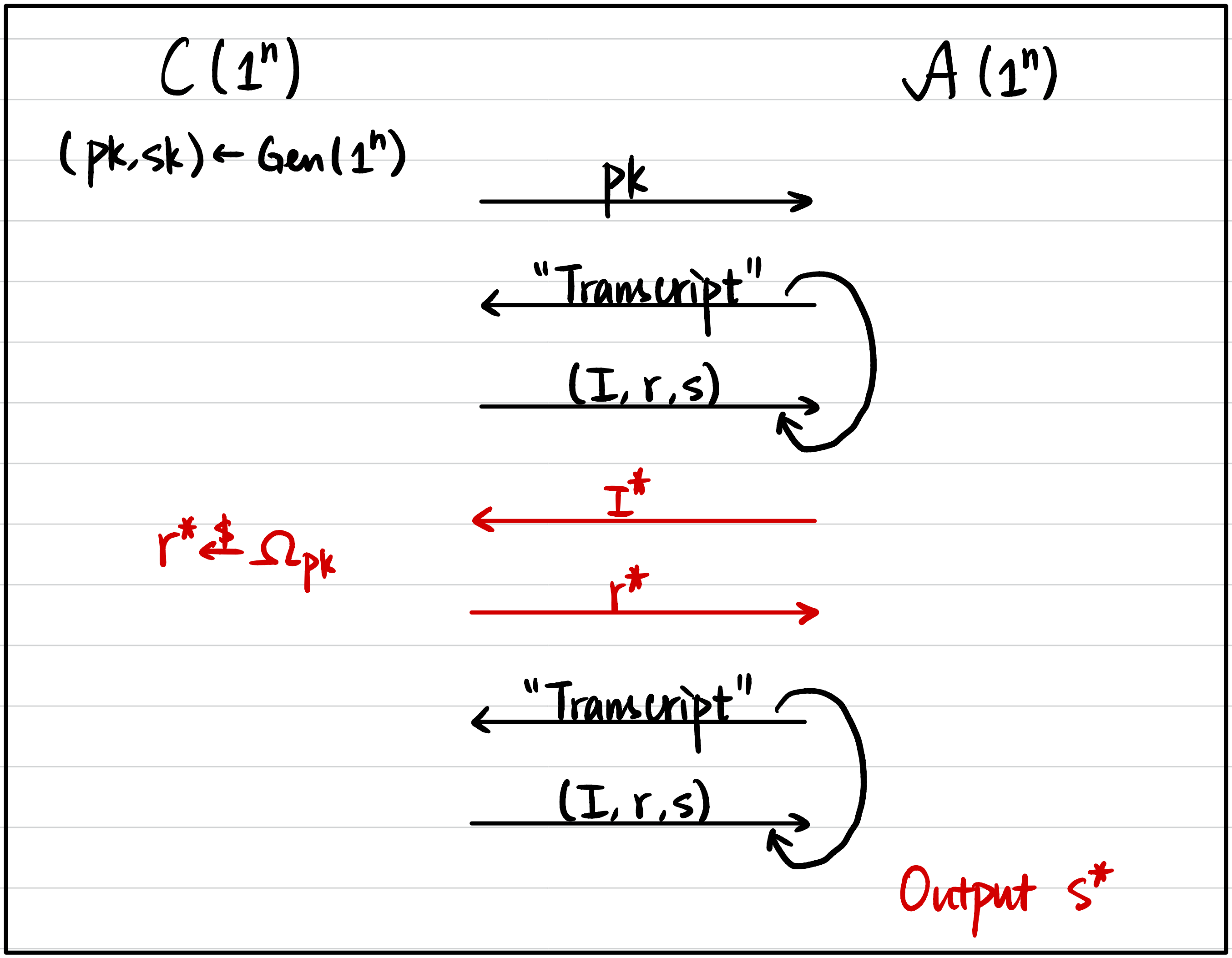
$$(pk, sk) \leftarrow \mathrm{Gen}(1^n)$$

Prover (sk)		**Verifier** (pk)
$(I, st) \leftarrow P_1(sk)$	$\xrightarrow{\quad I \quad}$	
		$r \overset{\$}{\leftarrow} \Omega_{pk}$
	$\xleftarrow{\quad r \quad}$	
$s := P_2(sk, st, r)$	$\xrightarrow{\quad s \quad}$	
		$V(pk, r, s) \overset{?}{=} I$

Correctness: If both parties follow the protocol description, then the verifier accepts with probability 1.

Special 3-Round Identification Scheme

Def A 3-round identification scheme $\Pi = (\mathrm{Gen}, P_1, P_2, V)$ is secure if $\forall$ PPT $\mathcal{A}$, $\exists$ negligible function $\varepsilon(\cdot)$ s.t. $\Pr[V(pk, r^*, s^*) = I^*] \le \varepsilon(n)$.



Fiat-Shamir Transform

Let $\Pi = (\mathrm{Gen}_{ID}, P_1, P_2, V)$ be a secure identification scheme.

Construct a signature scheme $\Pi' = (\mathrm{Gen}, \mathrm{Sign}, \mathrm{Vrfy})$:

- $\mathrm{Gen}(1^n)$:

  $(pk, sk) \leftarrow \mathrm{Gen}_{ID}(1^n)$

  Specify a hash function $H: \{0,1\}^* \to \Omega_{pk}$

- $\mathrm{Sign}_{sk}(m)$: $m \in \{0,1\}^*$

  $(I, st) \leftarrow P_1(sk)$

  $r := H(I \| m)$

  $s := P_2(sk, st, r)$

  Output $\sigma = (I, r, s)$

- $\mathrm{Vrfy}_{pk}(m, \sigma)$:

  $I := V(pk, r, s)$

  Output 1 iff $H(I \| m) = r$.

<u>Thm</u> If Π is secure and H is modeled as a random oracle, then Π' is secure.

Schnorr's Identification Scheme

$$(\mathbb{G}, q, g) \leftarrow \mathcal{G}(1^n)$$

$$x \xleftarrow{\$} \mathbb{Z}_q$$

$$h := g^x$$

Prover (x)		Verifier $(\mathbb{G}, q, g, h)$
$y \xleftarrow{\$} \mathbb{Z}_q$		
$I := g^y$	$\xrightarrow{\quad I \quad}$	
		$r \xleftarrow{\$} \mathbb{Z}_q$
	$\xleftarrow{\quad r \quad}$	
$s := (x \cdot r + y) \bmod q$	$\xrightarrow{\quad s \quad}$	
		$g^s / h^r \stackrel{?}{=} I$

Thm If DLOG is hard relative to $\mathcal{G}$, then this is a secure identification scheme.