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):

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

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

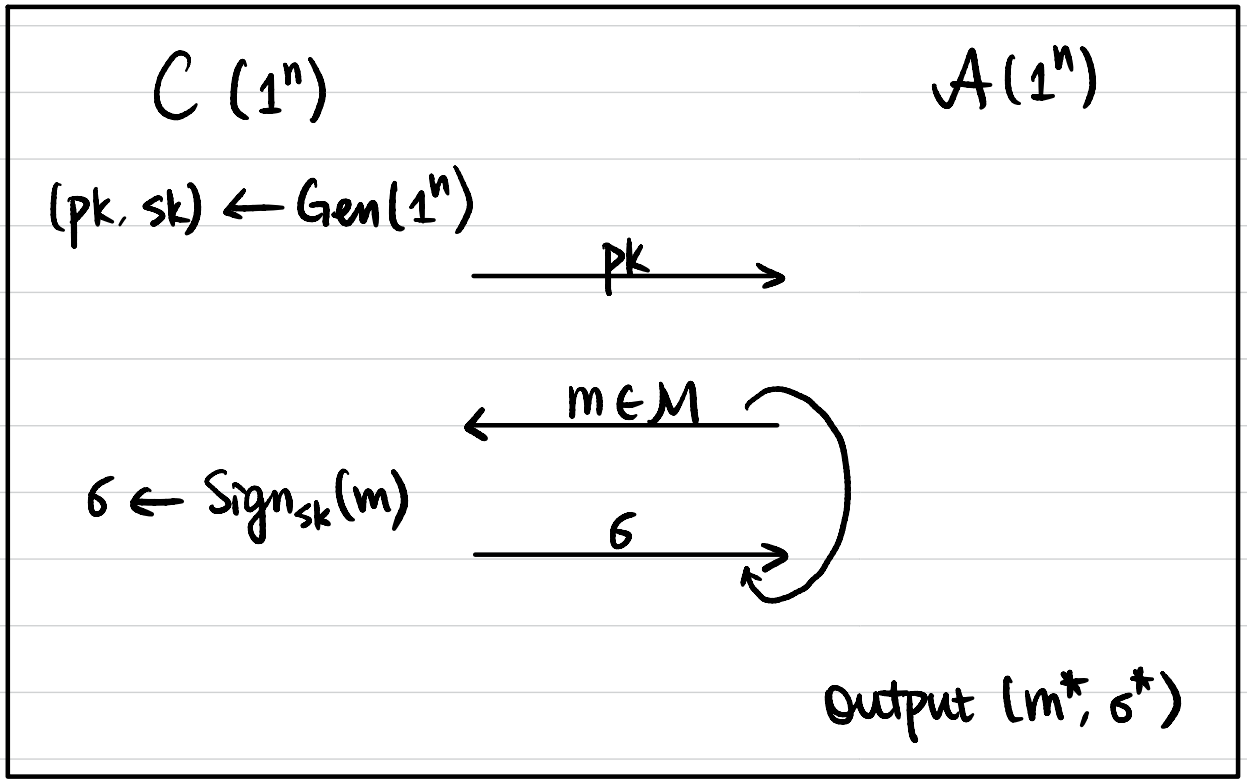
  $0/1 := Vrfy_{pk}(m, \sigma)$

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

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

Digital Signature

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



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

$SigForge_{\mathcal{A},\Pi} = 1$ ($\mathcal{A}$ succeeds) if

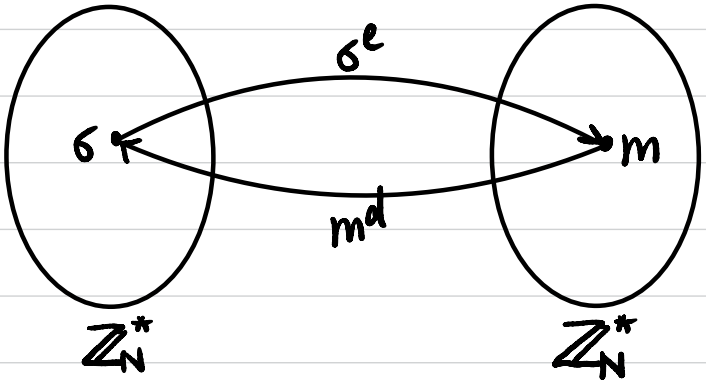
① $m^* \notin Q$, and

② $Vrfy_{pk}(m^*, \sigma^*) = 1$.

RSA-based Signatures

Plain RSA Signature:

- $\text{Gen}(1^n)$:
  $(N, e, d) \leftarrow \text{GenRSA}(1^n)$
  $pk := (N, e)$
  $sk := (N, d)$



- $\text{Sign}_{sk}(m)$: $m \in \mathbb{Z}_N^*$
  $\sigma := m^d \mod N$

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

Is it secure?

C → A: $PK=(N,e)$

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

A → C: m

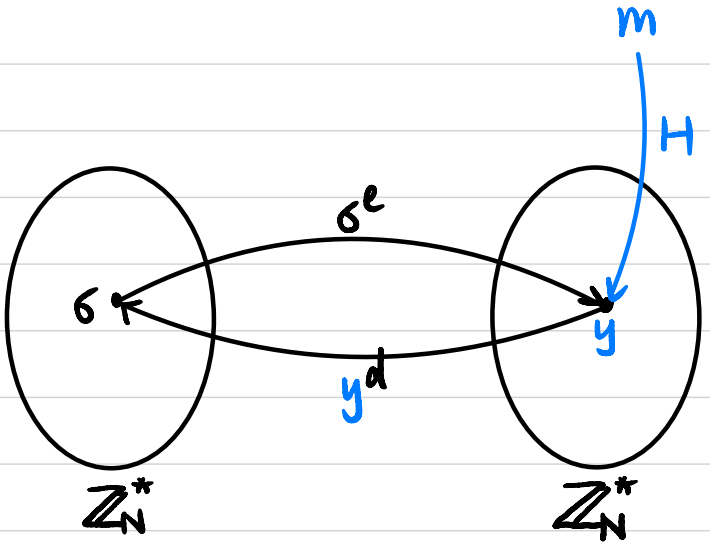
C → A: σ

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

RSA-based Signatures

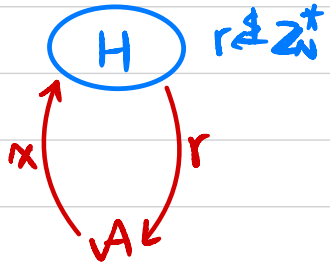
RSA-FDH (Full Domain Hash) Signature:

- $Gen(1^n)$:
  - $(N, e, d) \leftarrow GenRSA(1^n)$
  - $pk := (N, e)$
  - $sk := (N, d)$
  - Specify a hash function $H: \{0,1\}^* \to \mathbb{Z}_N^*$

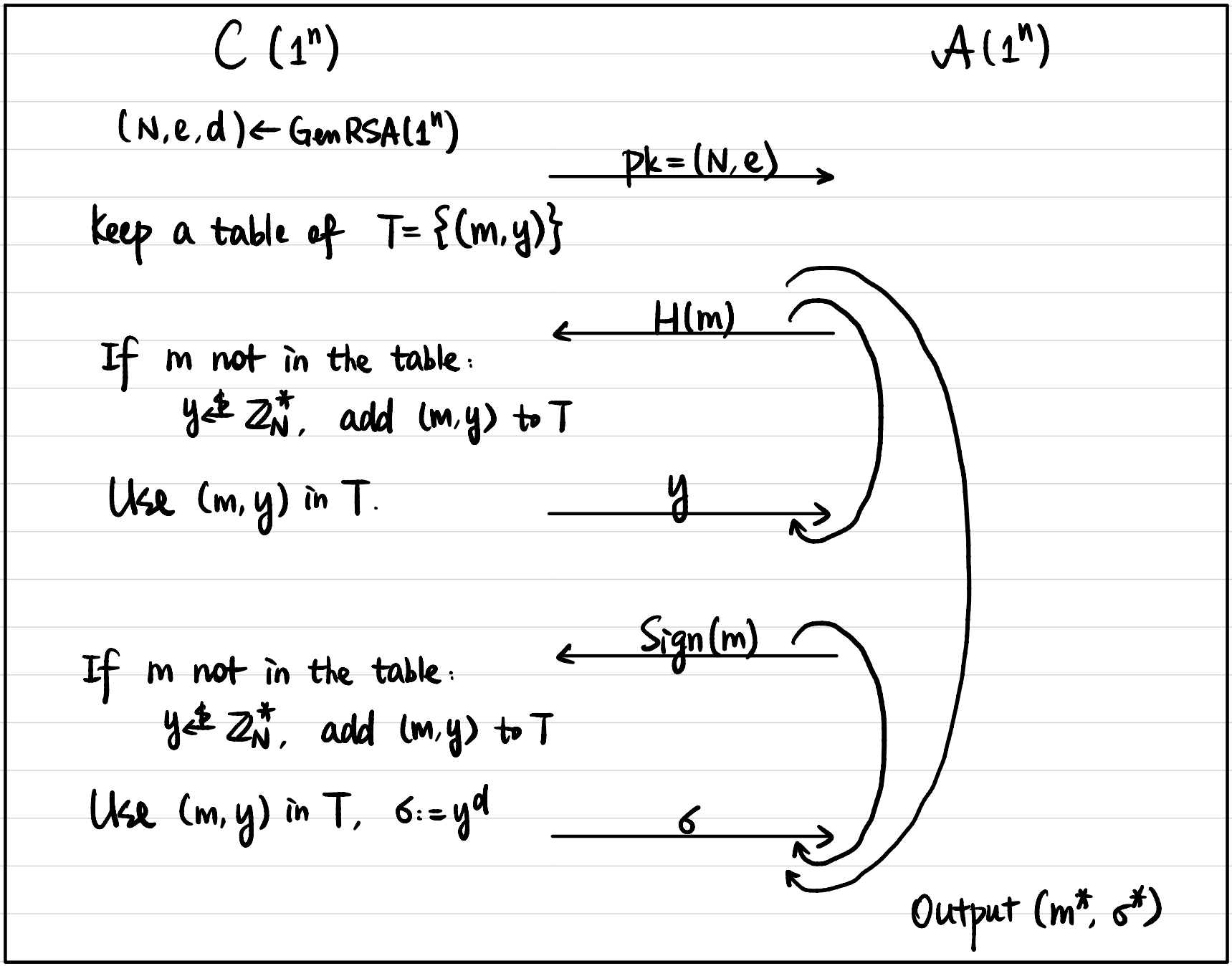


- $Sign_{sk}(m)$: $m \in \{0,1\}^*$
  - $\sigma := H(m)^d \bmod N$
- $Vrfy_{pk}(m, \sigma)$: $H(m) \stackrel{?}{=} \sigma^e \bmod N$

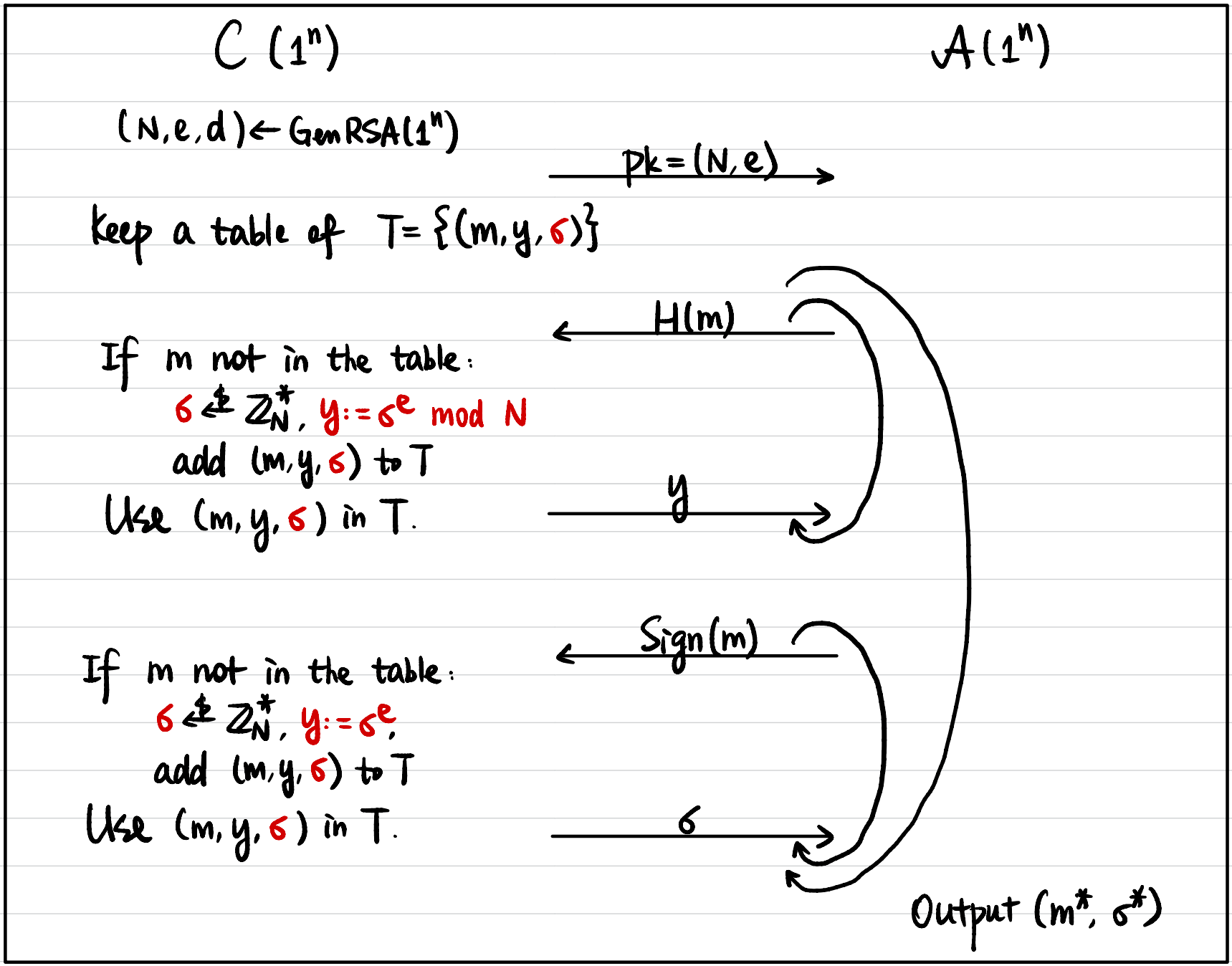
Thm If the RSA problem is hard relative to GenRSA and H is modeled as a random oracle, then this signature scheme is secure.



H₀: RSA-FDH Signature

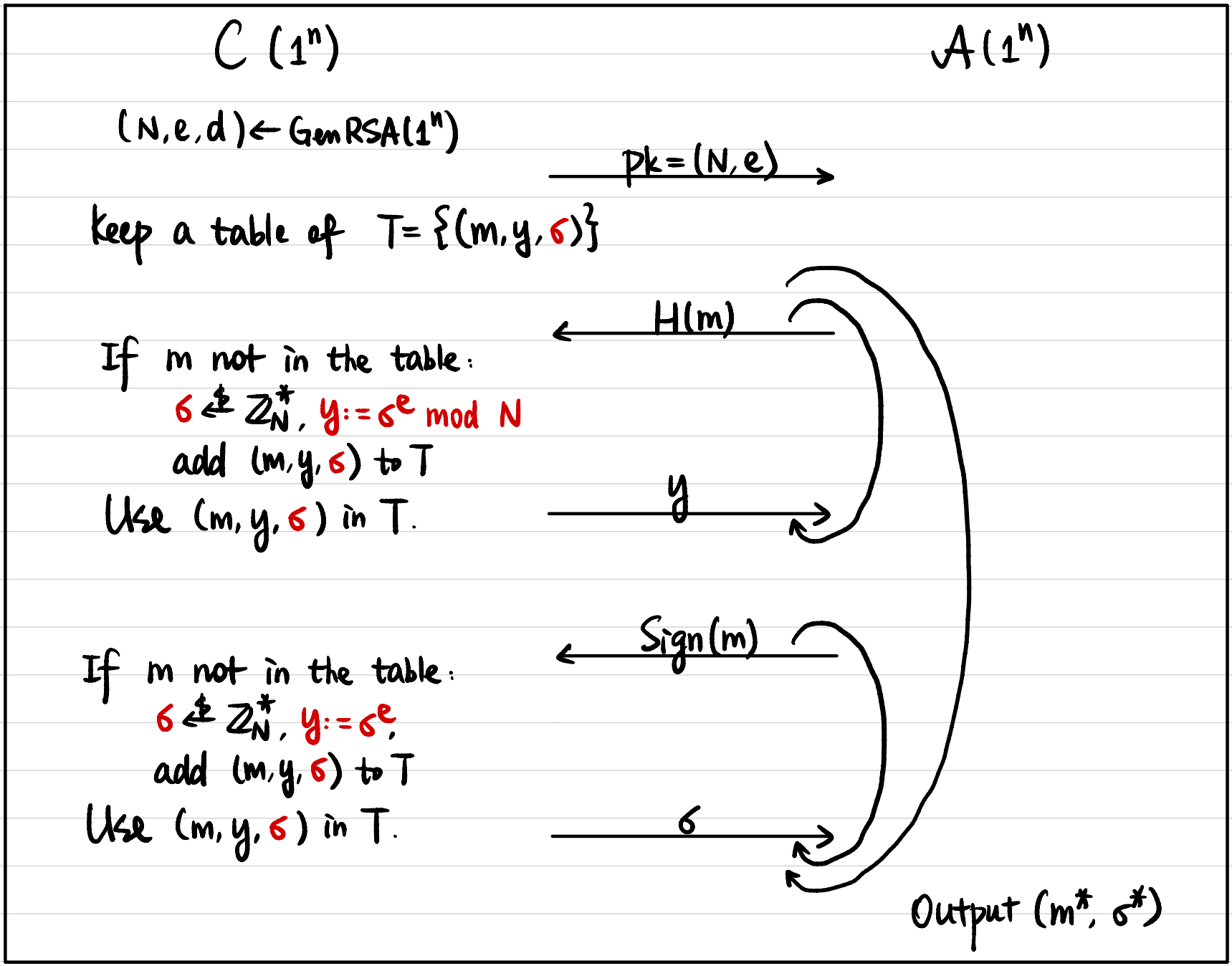


H_1: Sample $\sigma \xleftarrow{\$} \mathbb{Z}_N^*$, set $H(m) := \sigma^e$



H_1 has the same distribution as H_0.

$\mathcal{H}_2$: $m^* \in \{m \mid H(m) \text{ has been queried by } \mathcal{A}\}$



There is a negligible difference in $\mathcal{A}$'s success probability between $\mathcal{H}_1$ & $\mathcal{H}_2$.

$C(1^n)$ RSA $B(1^n)$ H_2 $A(1^n)$

$pk = (N, e, y^*)$ →

$pk = (N, e)$ →

$i \xleftarrow{\$} \{1, 2, \cdots, q\}$

Keep a table of $T = \{(m, y, \sigma)\}$

If i-th $H(\cdot)$ query:
$y := y^*$, add $(m, y^*, ?)$ to T

If m not in the table:
$\sigma \xleftarrow{\$} \mathbb{Z}_N^*$, $y := \sigma^e \bmod N$
add (m, y, σ) to T
Use (m, y, σ) in T.

← $H(m)$

y →

If m not in the table:
$\sigma \xleftarrow{\$} \mathbb{Z}_N^*$, $y := \sigma^e$,
add (m, y, σ) to T
Use (m, y, σ) in T.

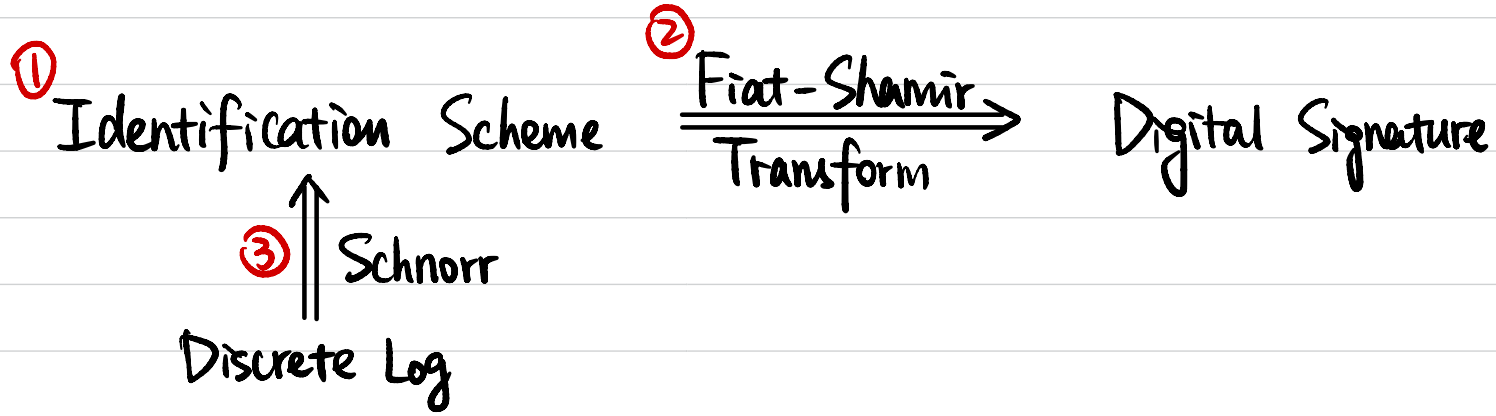
← $Sign(m)$

σ →

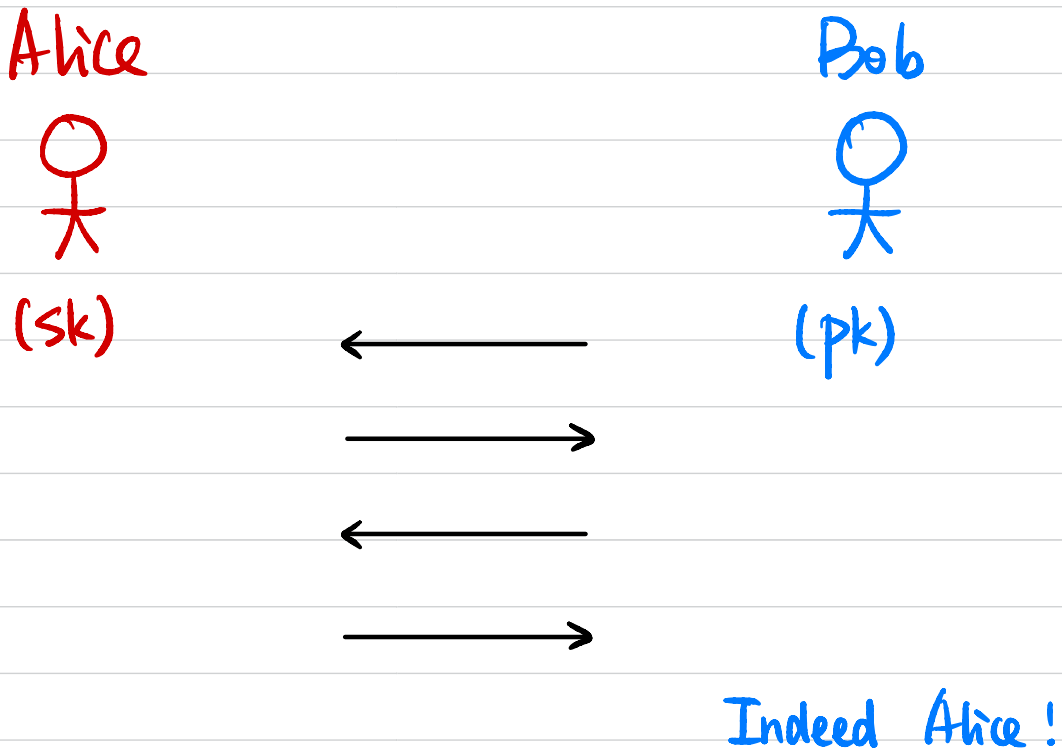
← Output (m^*, σ^*)

Output σ^*

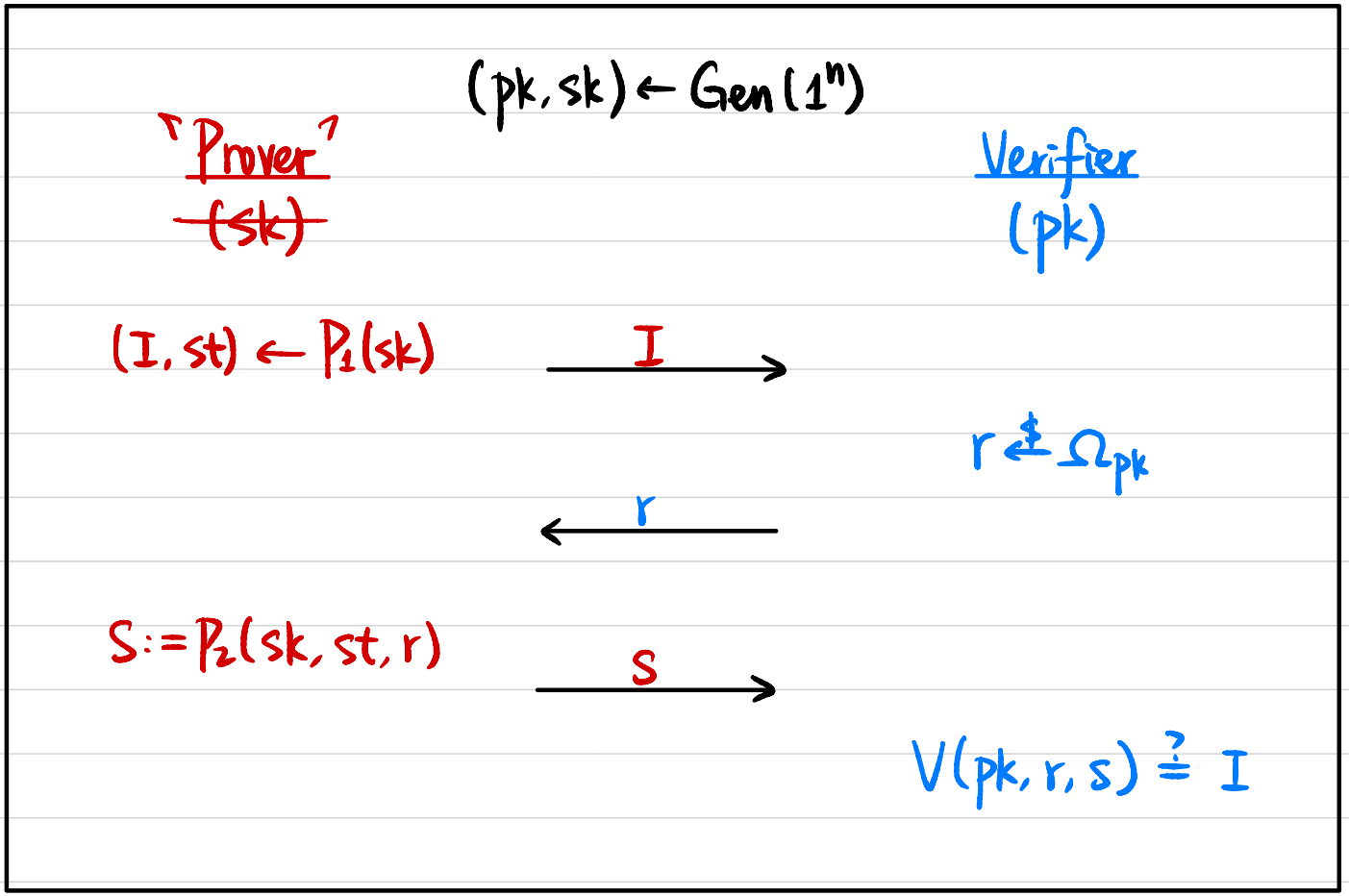
Signatures from DLOG



Identification Scheme



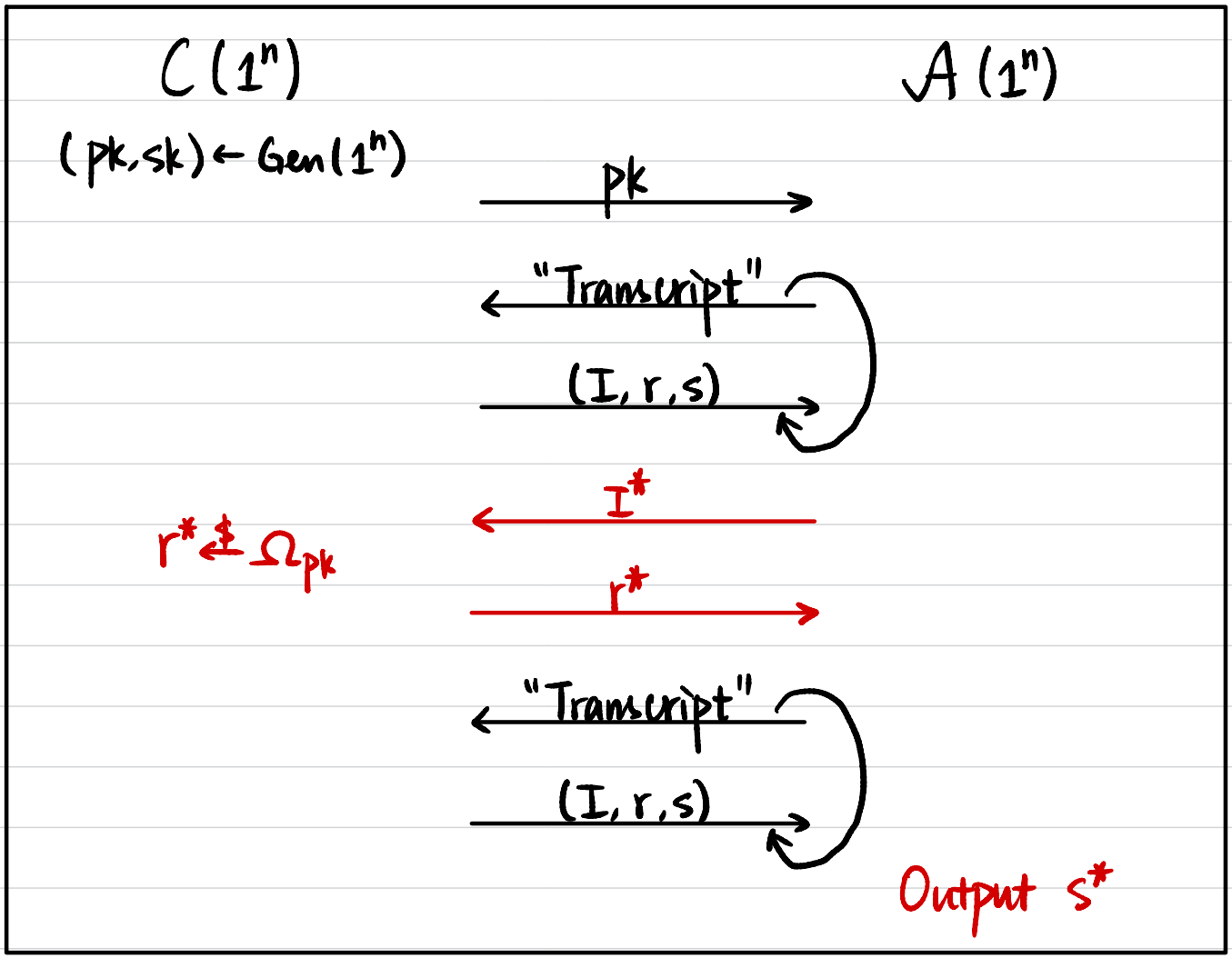
Special 3-Round Identification Scheme



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 $\Pi = (Gen, P_1, P_2, V)$ is **secure** if $\forall$ PPT A, $\exists$ negligible function $\varepsilon(\cdot)$ s.t. $\Pr[V(pk, r^*, s^*) = I^*] \leq \varepsilon(n)$.



Fiat-Shamir Transform

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

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

- $Gen(1^n)$:

  $(pk, sk) \leftarrow Gen_{ID}(1^n)$

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

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

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

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

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

  Output $\sigma = (r, s)$

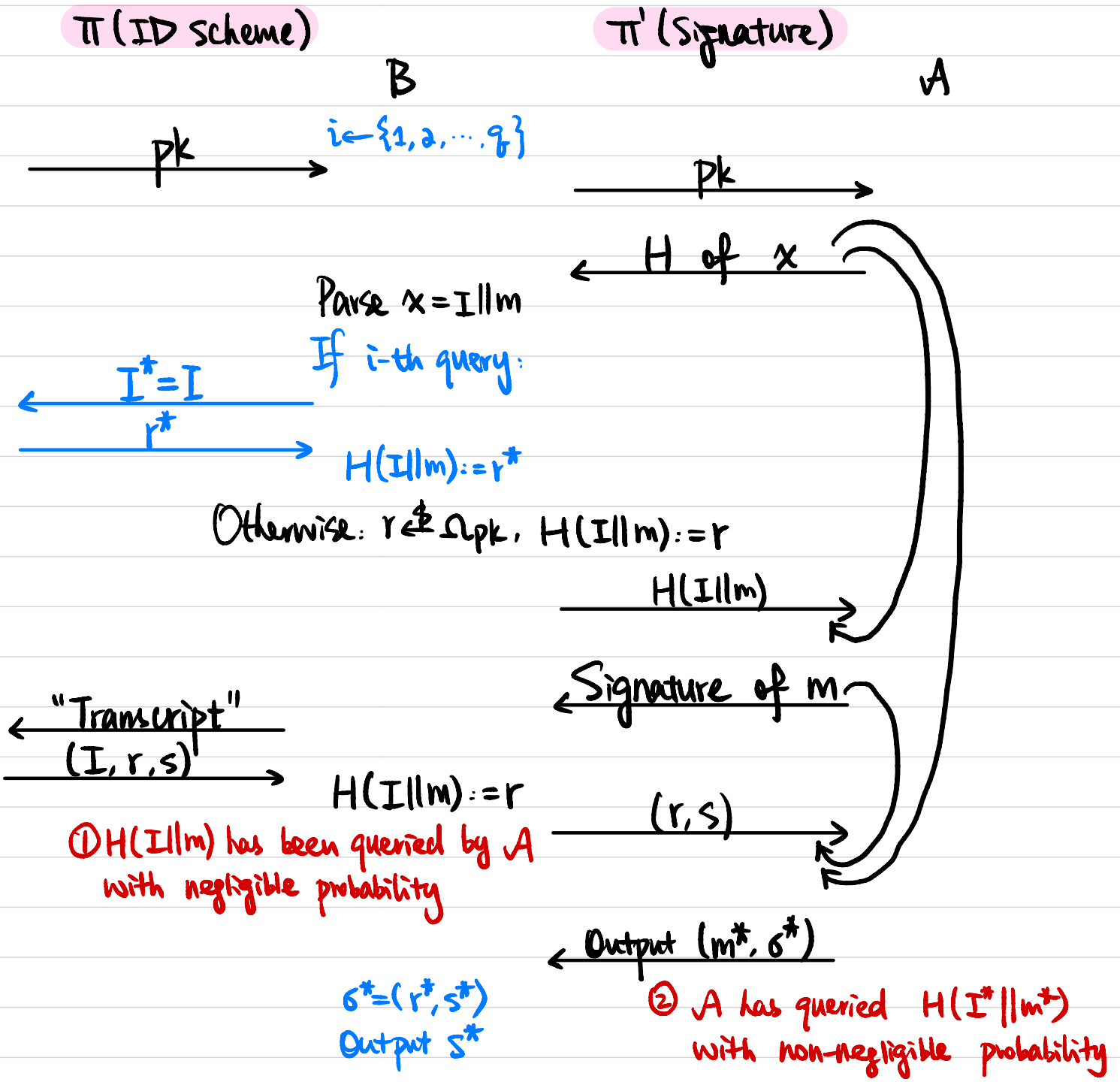
- $Vrfy_{pk}(m, \sigma)$:

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

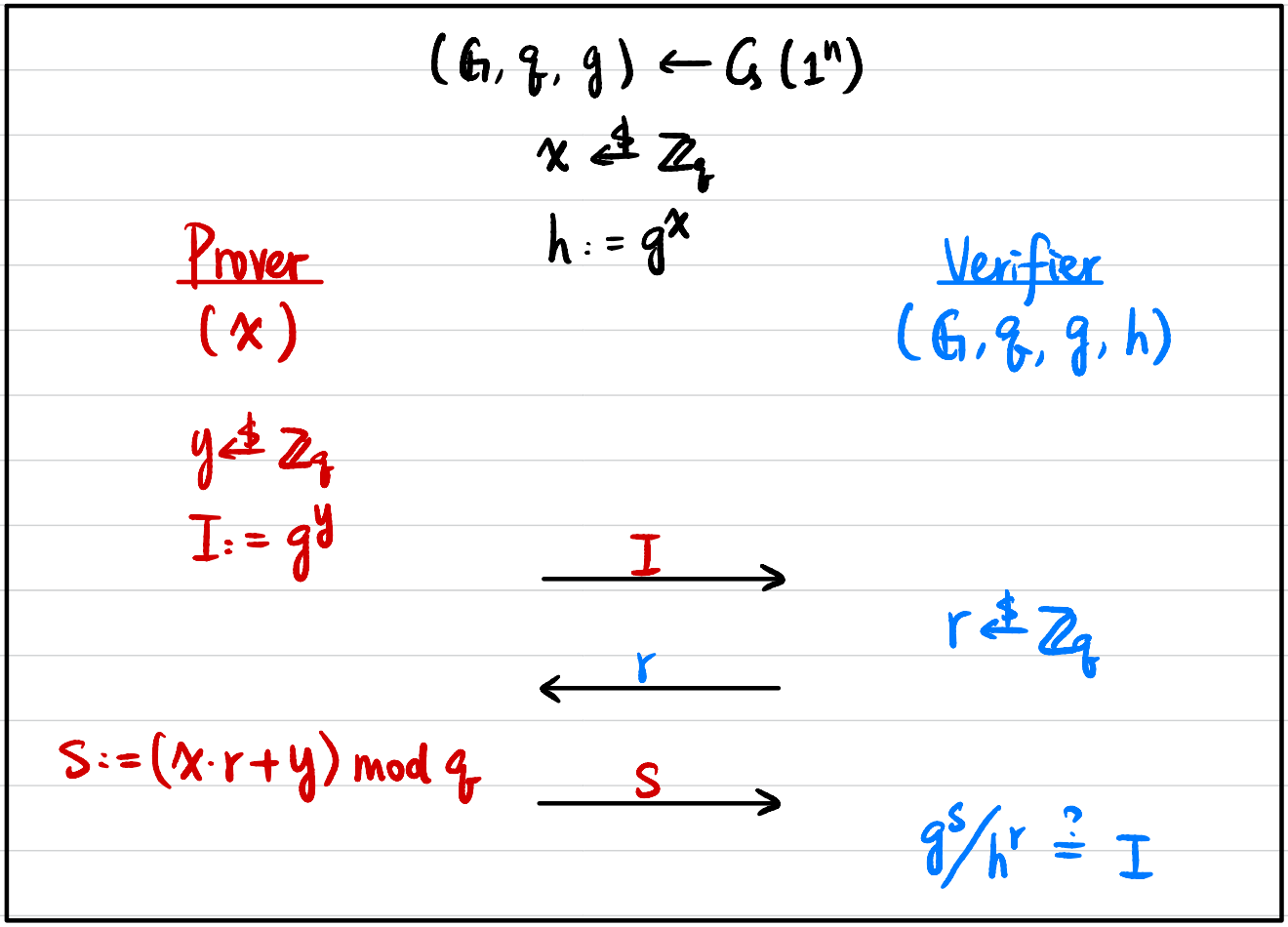
  Output 1 iff $H(I \| m) = r$.

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

Proof Sketch



Schnorr's Identification Scheme



Thm If DLOG is hard relative to G, then this is a secure identification scheme.