CSCI 1510

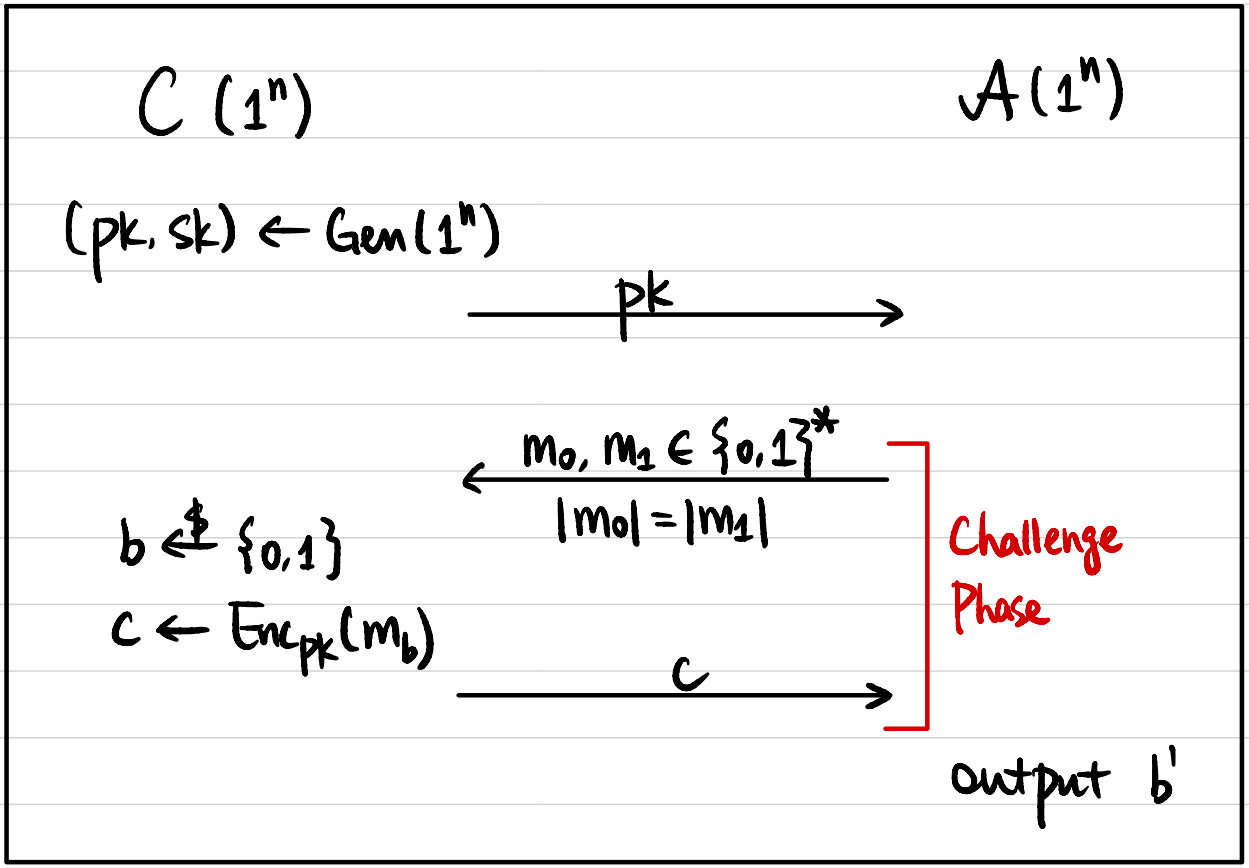
This Lecture:

- PKE from Trapdoor Permutations (continued)
- Post-Quantum PKE from LWE Assumption
- Digital Signatures
- Hash-and-Sign Paradigm
- RSA-based Signatures

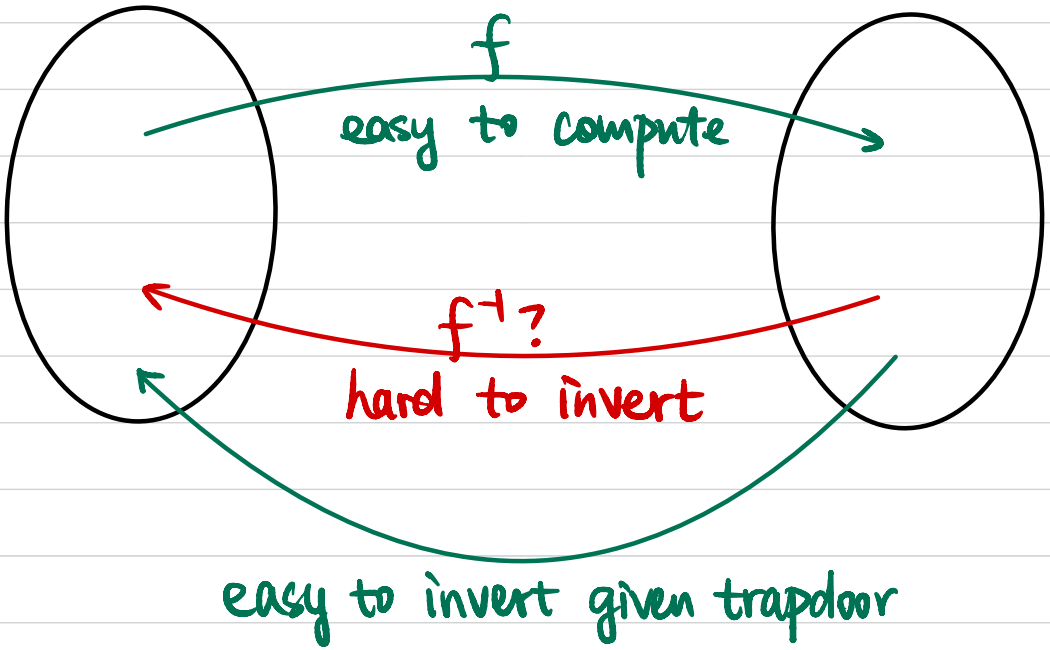
Semantic/CPA Security

Def A public-key encryption scheme (Gen, Enc, Dec) is **semantically secure** (= CPA) if $\forall$ PPT A, $\exists$ negligible function $\varepsilon(\cdot)$ s.t.

$$\Pr[b = b'] \leq \frac{1}{2} + \varepsilon(n)$$



Trapdoor Permutation



Trapdoor Permutation

Def A family $F = \{f_i : D_i \to R_i\}_{i \in I}$ is a **trapdoor permutation** if

① permutation: $\forall i \in I$, f_i is a permutation (bijection) $i = (N, e)$

② easy to sample a function: $(i, t) \leftarrow Gen(1^n)$. $f_i(x) = x^e \bmod N$

③ easy to sample an input: $x \leftarrow Sample(i \in I)$. x uniform in D_i.

④ easy to compute f_i: $f_i(x)$ poly-time computable $\forall i \in I, x \in D_i$.

⑤ hard to invert f_i: $\forall PPT\ A$, $\exists$ negligible function $\varepsilon(\cdot)$ s.t.

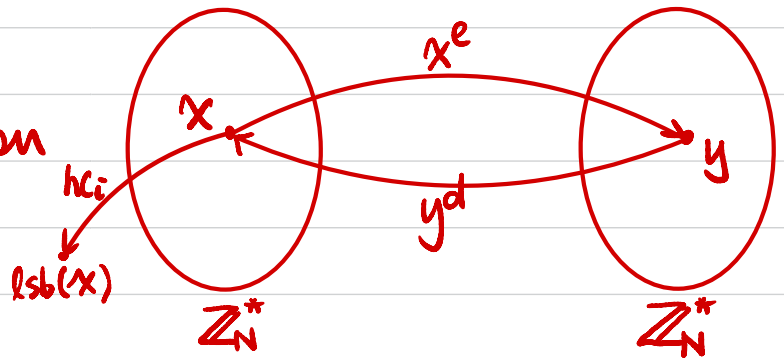
RSA Assumption

$$Pr\left[\begin{array}{l}(i,t) \leftarrow Gen(1^n), \\ x \leftarrow Sample(i) \\ y \leftarrow f_i(x) \\ z \leftarrow A(1^n, i, y)\end{array} : f_i(z) = y\right] \le \varepsilon(n).$$

⑥ easy to invert f_i with trapdoor: $Inv(i, t, f_i(x)) = x$ $(i, t) \leftarrow Gen(1^n)$, $x \in D_i$

(t = d)

Example: RSA trapdoor permutation

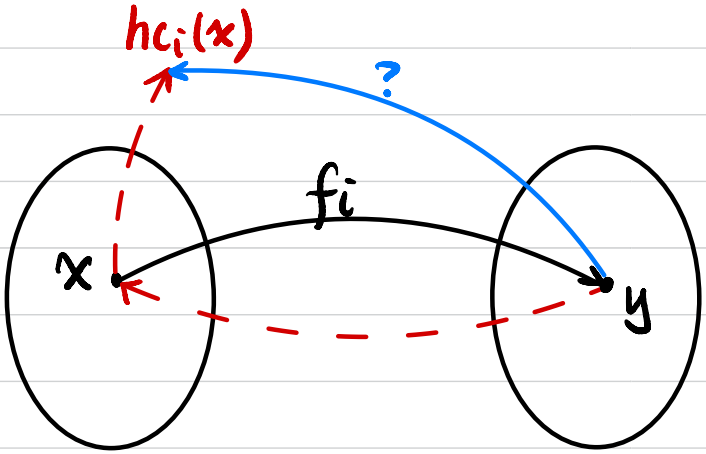


Hard-Core Predicate

Def Let $\Pi = (F, Gen, Inv)$ be a trapdoor permutation,
Let hc be a deterministic poly-time algorithm that, on input i & $x \in D_i$,
Outputs a single bit $hc_i(x)$.

hc is a hard-core predicate of Π if
$\forall$ PPT A, $\exists$ negligible function $\varepsilon(\cdot)$ s.t.

$$\Pr_{\substack{(i,t)\leftarrow Gen(1^n) \\ x \leftarrow D_i}} [A(i, f_i(x)) = hc_i(x)] \leq \frac{1}{2} + \varepsilon(n)$$



Thm Assume trapdoor permutation exists.
Then there exists a trapdoor permutation Π with a hard-core predicate hc of Π.

PKE from TDP

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

  $(i, t) \leftarrow \text{Gen}(1^n)$

  $pk := i$

  $sk := t$

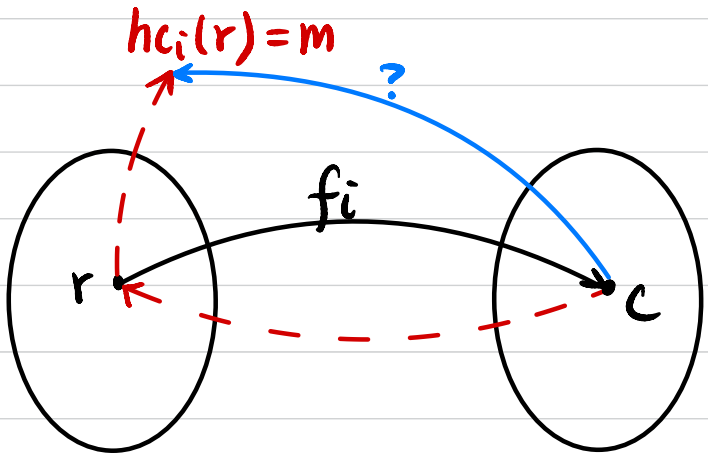
- $\text{Enc}_{pk}(m)$: $m \in \{0,1\}$

  $r \leftarrow D_i$ s.t. $hc_i(r) = m$

  $c := f_i(r)$

- $\text{Dec}_{sk}(c)$:

  $m := hc_i(\text{Inv}(i, t, c))$



Thm If $\Pi = (F, \text{Gen}, \text{Inv})$ be a trapdoor permutation with a hard-core predicate hc, then this encryption scheme is CPA-secure.

PKE from TDP

- $Gen(1^n)$:

  $(i, t) \leftarrow Gen(1^n)$

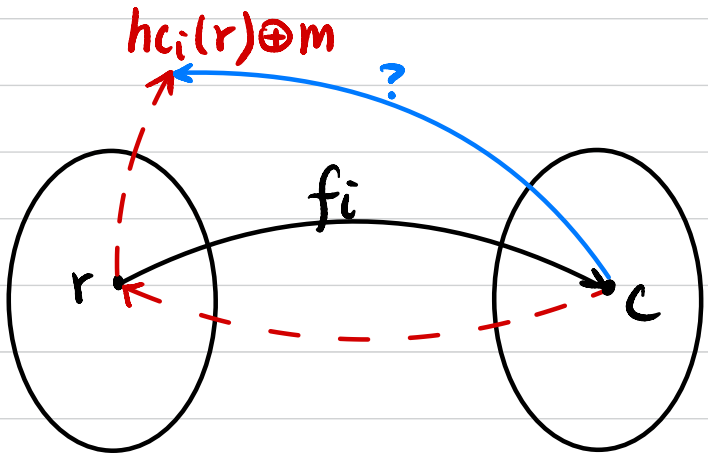
  $pk := i$

  $sk := t$

- $Enc_{pk}(m)$: $m \in \{0,1\}$

  $r \leftarrow D_i$

  $c := \langle f_i(r),\ hc_i(r) \oplus m \rangle$

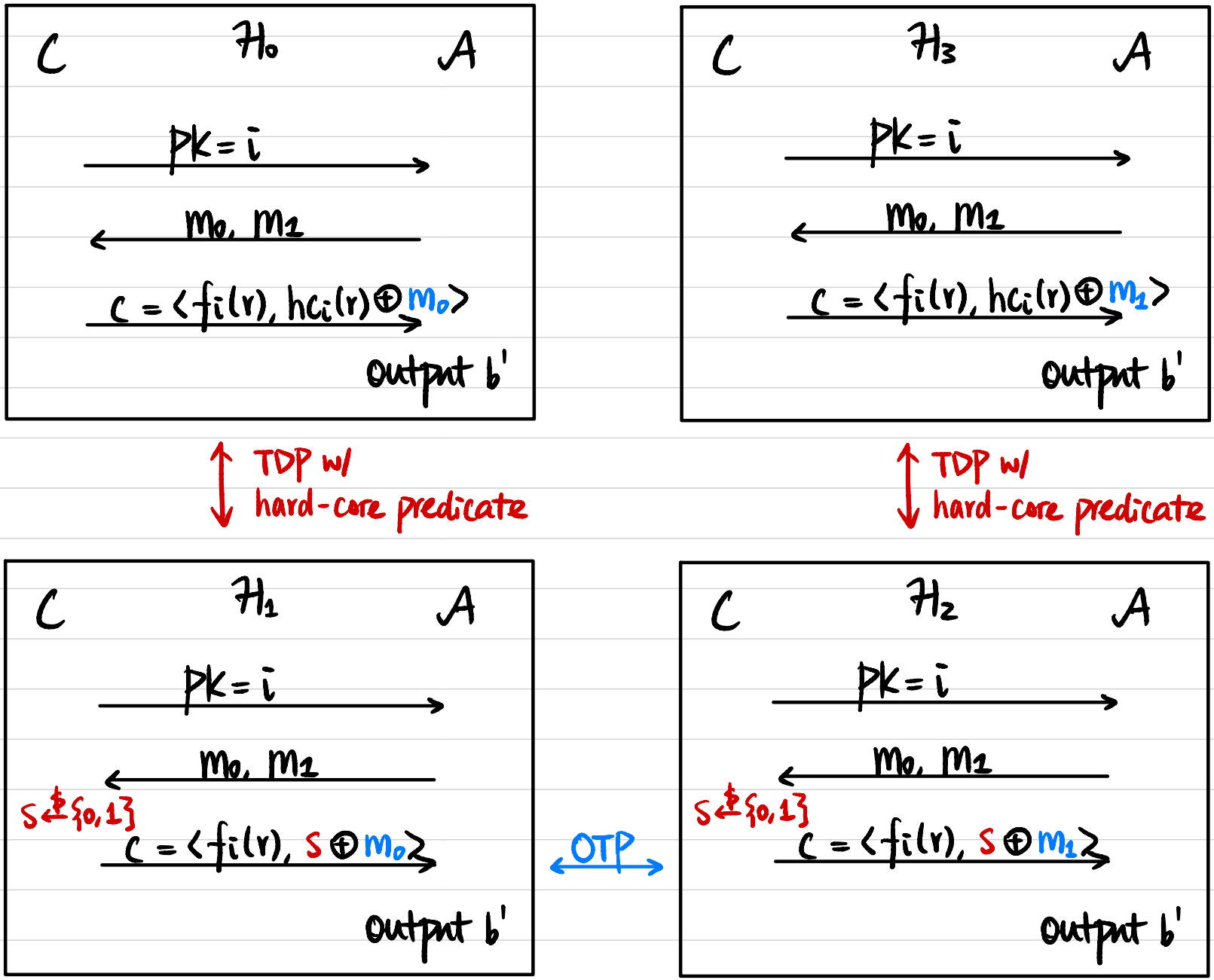


- $Dec_{sk}(c)$: $c = \langle c_1, c_2 \rangle$

  $m := hc_i(Inv(i, t, c_1)) \oplus c_2$

Thm If $\Pi = (F, Gen, Inv)$ be a trapdoor permutation with a hard-core predicate hc, then this encryption scheme is CPA-secure.

Proof Sketch



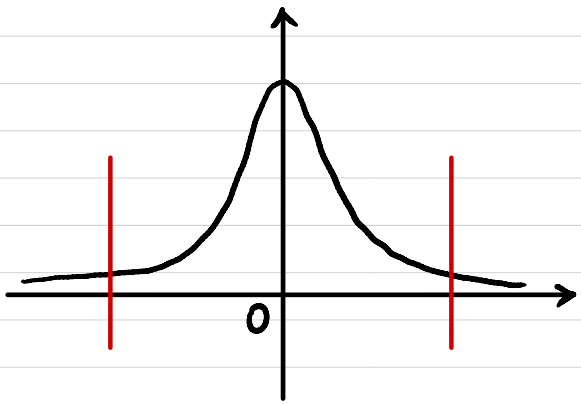
Post-Quantum Assumption: Learning With Errors (LWE)

n: security parameter

$q \sim 2^{n^\epsilon}$

$m = \Omega(n \log q)$

χ: distribution over $\mathbb{Z}_q$
(concentrated on "small integers")

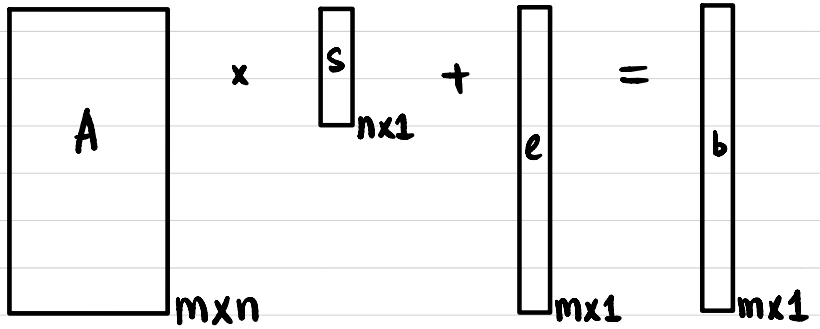


$$\Pr[|e| > \alpha \cdot q \mid e \leftarrow \chi] \leq \text{negl}(n)$$

$\alpha \ll 1$

Def We say the decisional $\text{LWE}_{n,m,q,\chi}$ problem is (quantum) hard if $\forall$ (quantum) PPT $\mathcal{A}$, $\exists$ negligible function $\epsilon(\cdot)$ s.t.

$$\left| \Pr\left[\begin{matrix} A \xleftarrow{\$} \mathbb{Z}_q^{m \times n} \\ s \xleftarrow{\$} \mathbb{Z}_q^n \\ e \leftarrow \chi^m \end{matrix} : \mathcal{A}(A, [As + e \bmod q]) = 1 \right] - \Pr\left[\begin{matrix} A \xleftarrow{\$} \mathbb{Z}_q^{m \times n} \\ b' \xleftarrow{\$} \mathbb{Z}_q^m \end{matrix} : \mathcal{A}(A, b') = 1 \right] \right| \leq \epsilon(n).$$



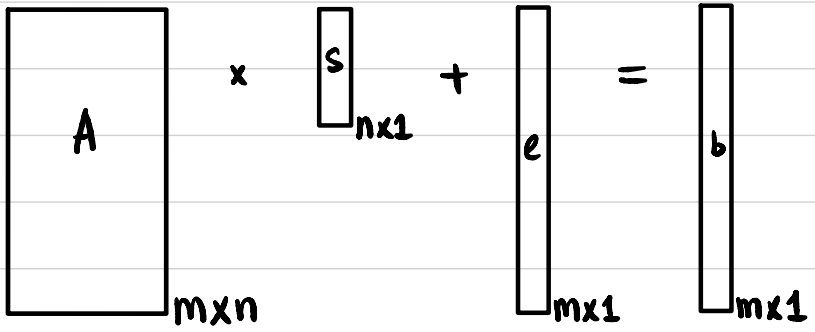
Post-Quantum PKE: Regev Encryption

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

  $A \xleftarrow{\$} \mathbb{Z}_q^{m \times n} \quad s \xleftarrow{\$} \mathbb{Z}_q^n \quad e \leftarrow \chi^m$

  $pk = (A, b = As + e \bmod q)$

  $sk = s$



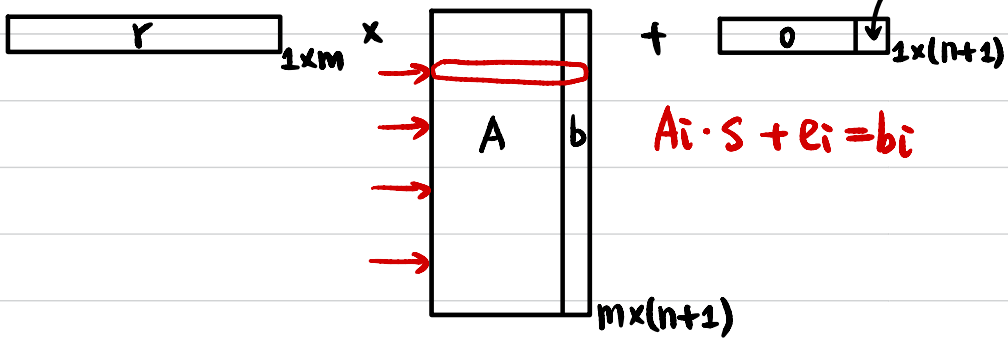
- $\text{Enc}_{pk}(\mu)$: $\mu \in \{0,1\}$

  sample a random $S \subseteq [m]$

  $$c = \left(\sum_{i \in S} A_i \,,\, \left(\sum_{i \in S} b_i \right) + \mu \cdot \lfloor \tfrac{q}{2} \rfloor \right) \bmod q$$

  A_i: i-th row of A

$r \xleftarrow{\$} \{0,1\}^m$



$A_i \cdot s + e_i = b_i$

- $\text{Dec}_{sk}(c)$: $c = [\,c_1 \mid c_2\,]$

  $$c_2 - c_1 \cdot s = \mu \cdot \lfloor \tfrac{q}{2} \rfloor + \sum_{i \in S} e_i$$

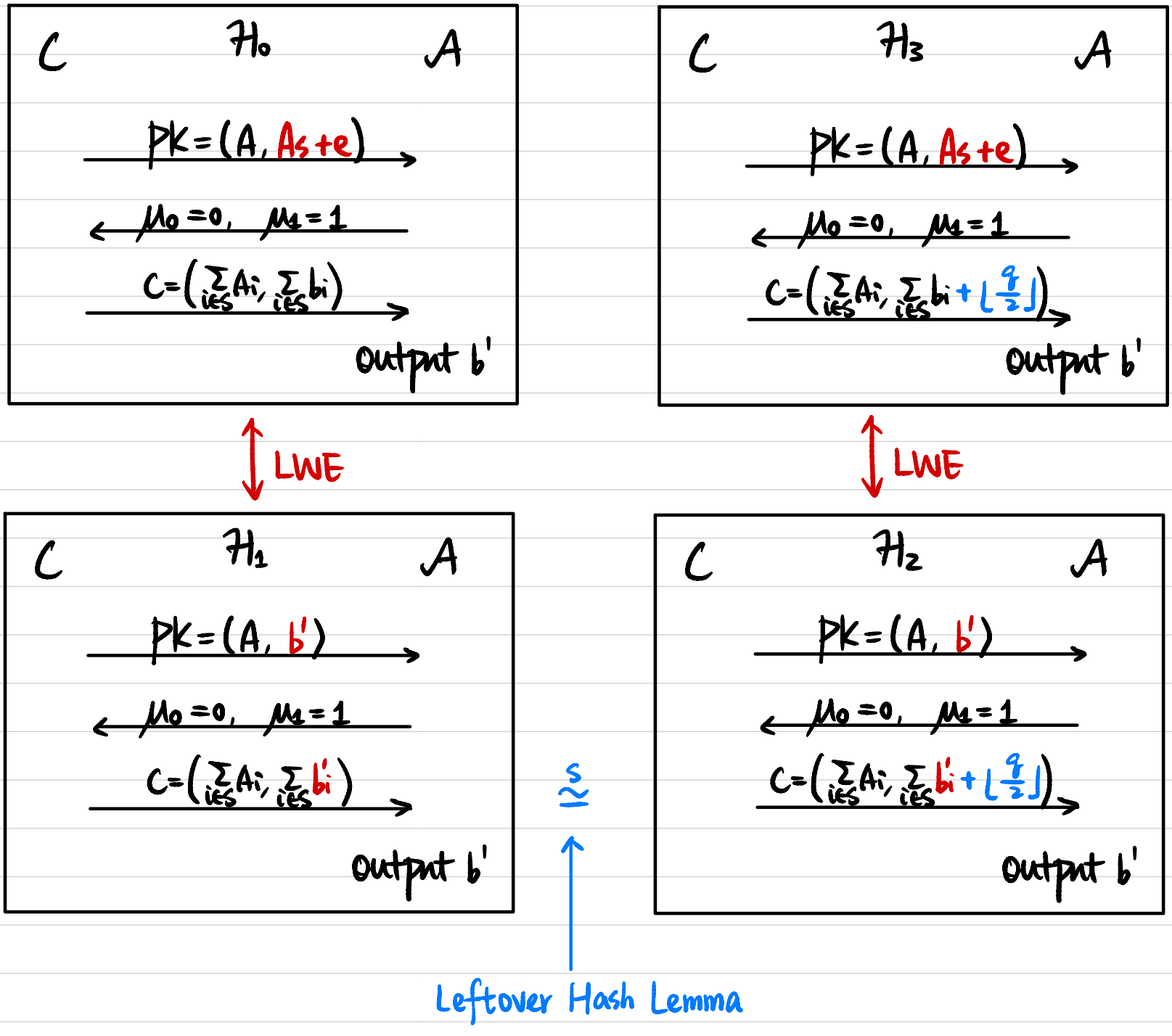
  small noise

$$c_1 \cdot s = \sum_{i \in S} b_i - \sum_{i \in S} e_i$$

$$c_2 = \sum_{i \in S} b_i + \mu \cdot \lfloor \tfrac{q}{2} \rfloor$$

Thm If $\text{LWE}_{n,m,q,\chi}$ is (quantum) hard, then Regev encryption is (post-quantum) CPA-secure.

Proof Sketch



Homomorphic Properties of Encryption Schemes

Multiplicatively Homomorphic

$Enc(m_1) \rightarrow$
$Enc(m_2) \rightarrow$ $Enc(m_1 \cdot m_2)$

Additively Homomorphic

$Enc(m_1) \rightarrow$
$Enc(m_2) \rightarrow$ $Enc(m_1 + m_2)$

ElGamal:

$C_1 = (g^{r_1},\ h^{r_1} \cdot m_1)$
$C_2 = (g^{r_2},\ h^{r_2} \cdot m_2)$
$\rightarrow (g^{r_1+r_2},\ h^{r_1+r_2} \cdot (m_1 \cdot m_2))$

Exponential ElGamal:

$Enc(m) = (g^r,\ h^r \cdot g^m)$

$C_1 = (g^{r_1},\ h^{r_1} \cdot g^{m_1})$
$C_2 = (g^{r_2},\ h^{r_2} \cdot g^{m_2})$
$\rightarrow (g^{r_1+r_2},\ h^{r_1+r_2} \cdot g^{m_1+m_2})$

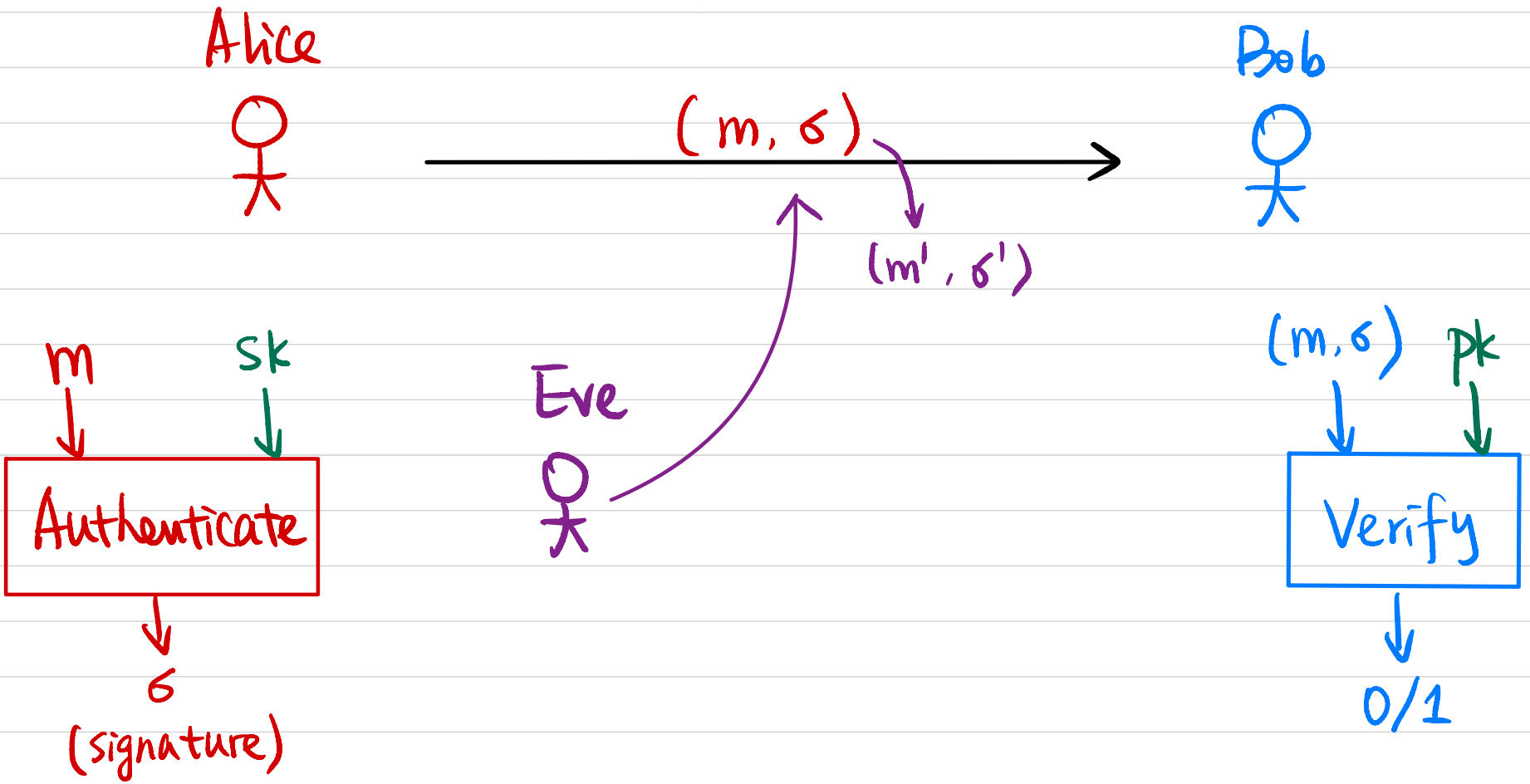
Regev:

$C_1 = (r_1^T \cdot A,\ r_1^T \cdot b + \mu_1 \cdot \lfloor \frac{q}{2} \rfloor)$
$C_2 = (r_2^T \cdot A,\ r_2^T \cdot b + \mu_2 \cdot \lfloor \frac{q}{2} \rfloor)$

$\Downarrow$

$((r_1+r_2)^T \cdot A,\ (r_1+r_2)^T \cdot b + (\mu_1+\mu_2) \cdot \lfloor \frac{q}{2} \rfloor)$

Digital Signature



Digital Signature

- **Syntax:**

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

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

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

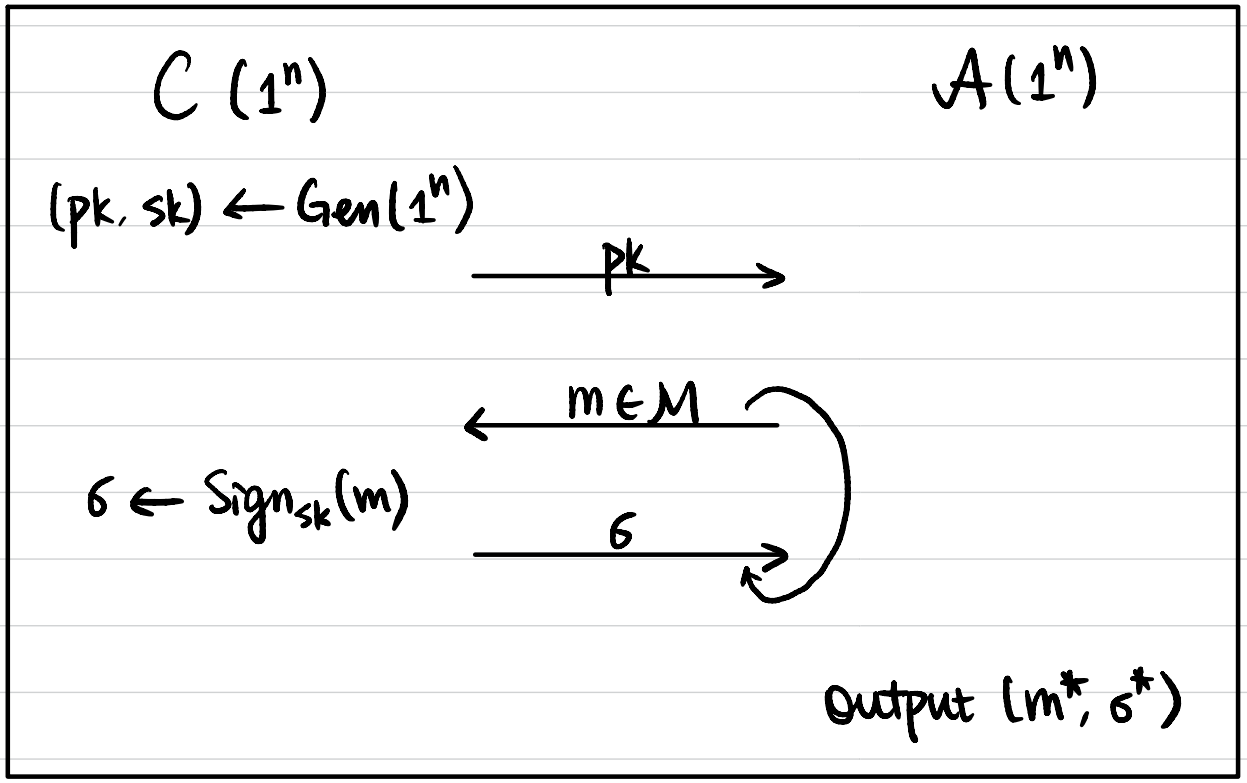
  $0/1 := Vrfy_{pk}(m, \sigma)$

- **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 $Vrfy_{pk}(m^*, \sigma^*) = 1$.

Hash-and-Sign Paradigm

Recall: Hash-and-MAC

Secure MAC for fixed-length messages
+
CRHF for arbitrary-length inputs
$\Rightarrow$ Secure MAC for arbitrary-length messages

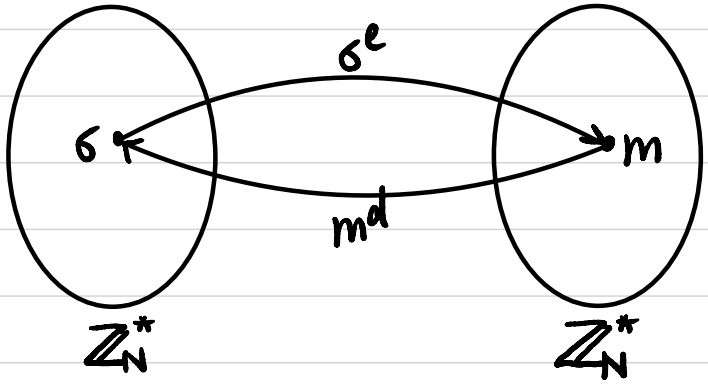
Hash-and-Sign

Secure Signature for fixed-length messages
+
CRHF for arbitrary-length inputs
$\Rightarrow$ Secure Signature for arbitrary-length messages

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 $\xrightarrow{PK=(N,e)}$ A

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

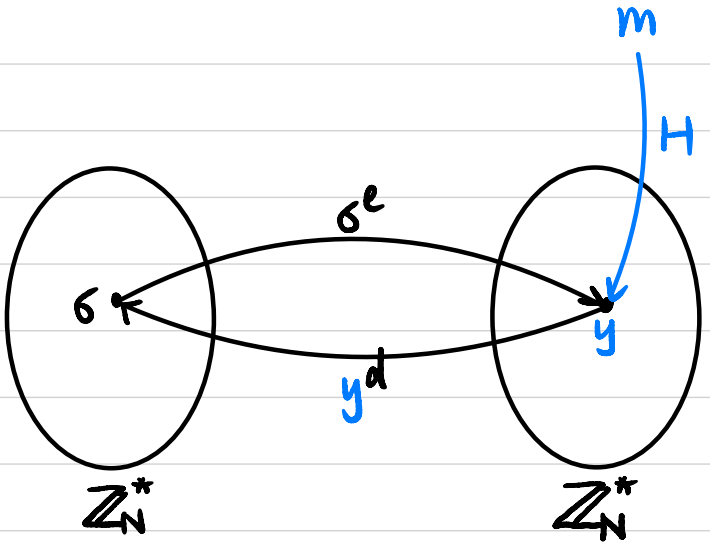
$\xleftarrow{m}$
$\xrightarrow{e}$

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

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.