CSCI 1510

- SWHE from LWE (Continued)
- Bootstrapping SWHE to FHE
- Digital Signatures
- Hash-and-Sign Paradigm
- RSA-based Signatures

FHE Constructions

Step 1: Somewhat Homomorphic Encryption (SWHE)

- over Integers
- from LWE (GSW)

Step 2: Bootstrapping

Post-Quantum Assumption: Learning With Errors (LWE)

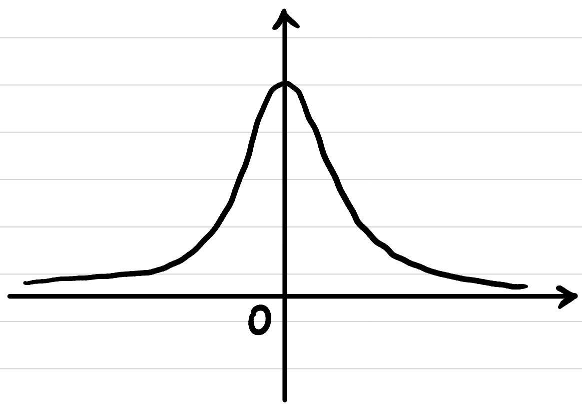
n: security parameter

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

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

χ: distribution over $\mathbb{Z}_q$

(concentrated on "small integers")

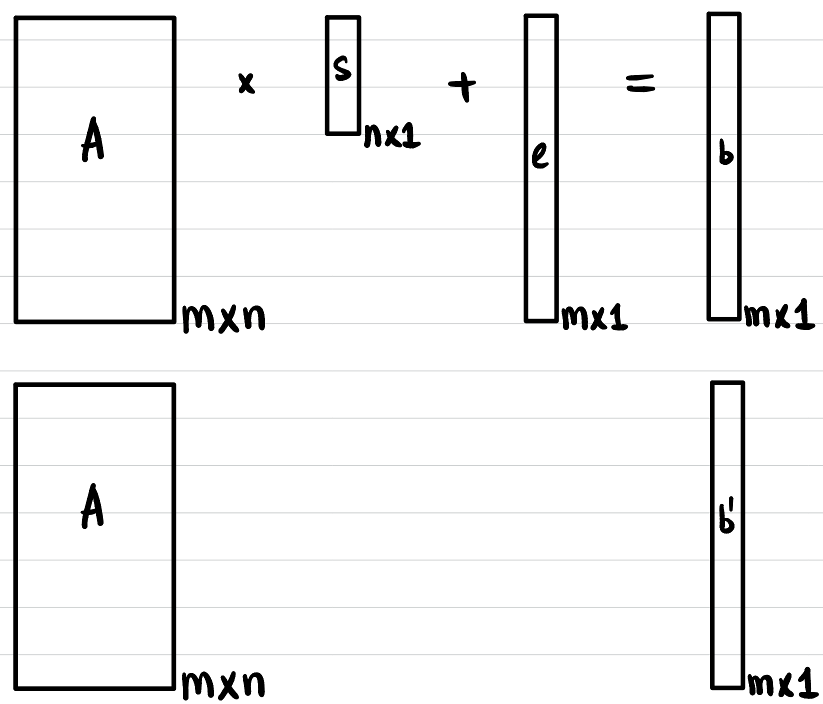


$$\Pr\left[\, |e| > \alpha \cdot q \;\middle|\; e \leftarrow \chi \,\right] \le \mathrm{negl}(n)$$

$\alpha \ll 1$

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

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



SWHE from LWE (GSW)

Attempt 1 (secret-key)

$sk = t_{n\times 1} \qquad \begin{bmatrix} s \\ 1 \end{bmatrix}_{n\times 1}$

$Enc_{sk}(\mu)$: $\mu \in \{0, 1\}$

How?

Sample $C_0 \in \mathbb{Z}_q^{n\times n}$ s.t. $C_0 \cdot \vec{t} = \text{small}$

$$\begin{bmatrix} C_0 \end{bmatrix}_{n\times n} \times \begin{bmatrix} t \end{bmatrix}_{n\times 1} = \begin{bmatrix} e \end{bmatrix}_{n\times 1}$$

$$\underbrace{C}_{n\times n} = C_0 + \mu \cdot \underbrace{I}_{\text{identity matrix}}$$

$Dec_{sk}(c)$: $C \cdot \vec{t} = (C_0 + \mu \cdot I) \cdot \vec{t} = \vec{e} + \mu \cdot \vec{t}$

CPA Security ?

SWHE from LWE (GSW)

Attempt 1 (secret-key)

Without Error: $C \cdot \vec{t} = \mu \cdot \vec{t}$

Homomorphism: $C_1 \cdot \vec{t} = \mu_1 \cdot \vec{t}$

$C_2 \cdot \vec{t} = \mu_2 \cdot \vec{t}$

Additive Homomorphism?

$C = C_1 + C_2$

$C \cdot \vec{t} = (C_1 + C_2) \cdot \vec{t} = (\mu_1 + \mu_2) \cdot \vec{t}$

Multiplicative Homomorphism?

$C = C_1 \cdot C_2$

$$\begin{aligned} C \cdot \vec{t} &= (C_1 \cdot C_2) \cdot \vec{t} \\ &= C_1 \cdot (C_2 \cdot \vec{t}) \\ &= C_1 \cdot \mu_2 \cdot \vec{t} \\ &= \mu_2 \cdot (C_1 \cdot \vec{t}) \\ &= \mu_2 \cdot \mu_1 \cdot \vec{t} \end{aligned}$$

With Error: $C \cdot \vec{t} = \mu \cdot \vec{t} + \vec{e}$

Homomorphism: $C_1 \cdot \vec{t} = \mu_1 \cdot \vec{t} + \vec{e}_1$

$C_2 \cdot \vec{t} = \mu_2 \cdot \vec{t} + \vec{e}_2$

Additive Homomorphism?

$C = C_1 + C_2$

$C \cdot \vec{t} = (C_1 + C_2) \cdot \vec{t} = (\mu_1 + \mu_2) \cdot \vec{t} + (\vec{e}_1 + \vec{e}_2)$

Multiplicative Homomorphism?

$C = C_1 \cdot C_2$

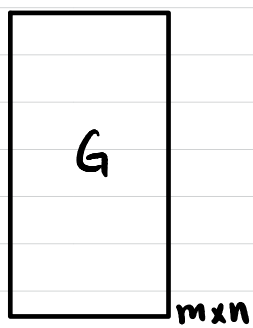
$$\begin{aligned} C \cdot \vec{t} &= (C_1 \cdot C_2) \cdot \vec{t} \\ &= C_1 \cdot (C_2 \cdot \vec{t}) \\ &= C_1 \cdot (\mu_2 \cdot \vec{t} + \vec{e}_2) \\ &= \mu_2 \cdot C_1 \cdot \vec{t} + C_1 \cdot \vec{e}_2 \\ &= \mu_2 \cdot (\mu_1 \cdot \vec{t} + \vec{e}_1) + C_1 \cdot \vec{e}_2 \\ &= \mu_2 \cdot \mu_1 \cdot \vec{t} + \mu_2 \cdot \vec{e}_1 + C_1 \cdot \vec{e}_2 \end{aligned}$$

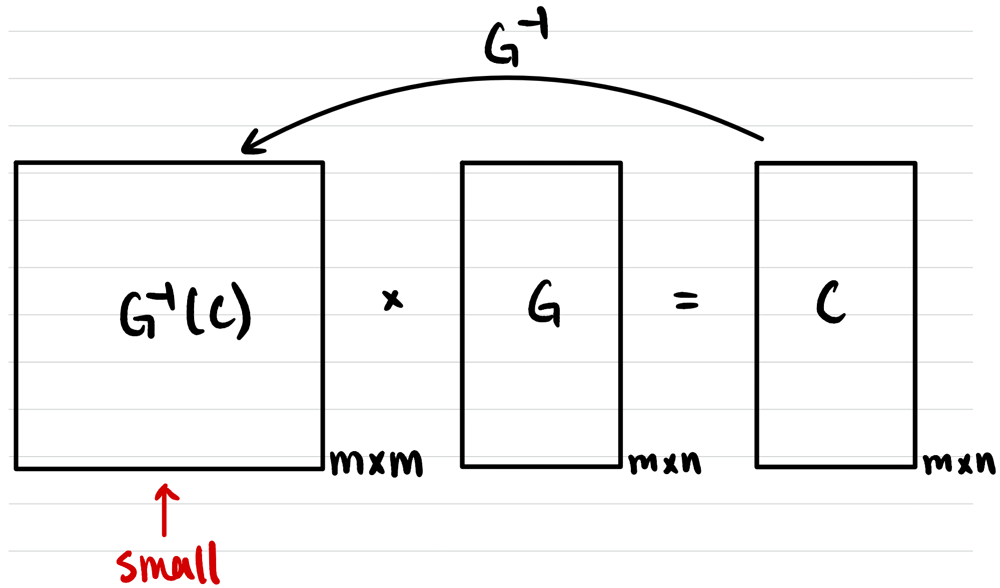
SWHE from LWE (GSW)

Attempt 2 (secret-key)

Flattening Gadget:

Gadget matrix $G \in \mathbb{Z}_q^{m \times n}$



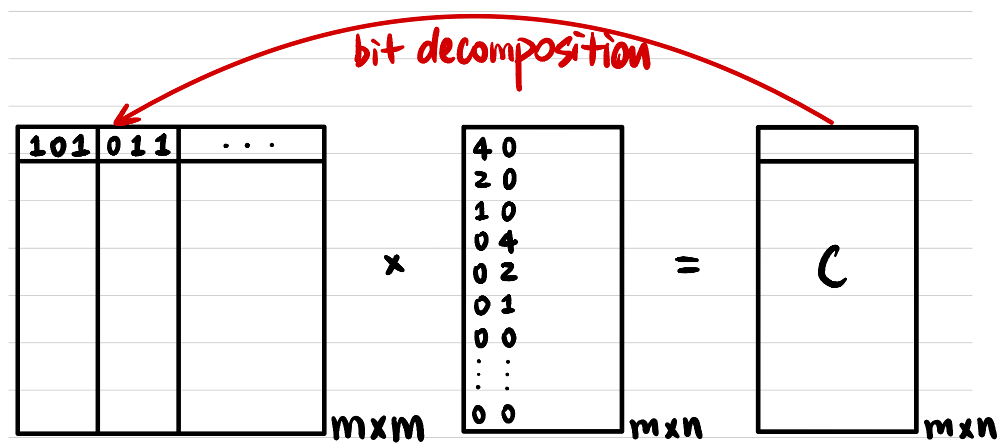


Inverse transformation

$$G^{-1}: \mathbb{Z}_q^{m \times n} \to \mathbb{Z}_q^{m \times m}$$

$\forall C \in \mathbb{Z}_q^{m \times n}$, $G^{-1}(C) = \text{small}$

$$G^{-1}(C) \cdot G = C$$



$m = ?$

SWHE from LWE (GSW)

Attempt 2 (secret-key)

$$sk = t_{n\times1} = \begin{bmatrix} s \\ 1 \end{bmatrix}_{n\times1}$$

$Enc_{sk}(\mu)$: $\mu \in \{0,1\}$

Sample $C_0 \in \mathbb{Z}_q^{m\times n}$ s.t. $C_0 \cdot \vec{t} = \text{small}$

$$\begin{bmatrix} C_0 \end{bmatrix}_{m\times n} \times \begin{bmatrix} t \end{bmatrix}_{n\times1} = \begin{bmatrix} e \end{bmatrix}_{m\times1}$$

$$C = C_0 + \mu \cdot \underbrace{G}_{\text{gadget matrix}}$$

$Dec_{sk}(c)$:

$$C \cdot \vec{t} = (C_0 + \mu \cdot G) \cdot \vec{t}$$
$$= \vec{e} + \mu \cdot (G \cdot \vec{t})$$

CPA Security?

Homomorphism:

$$C_1 \cdot \vec{t} = \mu_1 \cdot (G \cdot \vec{t}) + \vec{e_1}$$
$$C_2 \cdot \vec{t} = \mu_2 \cdot (G \cdot \vec{t}) + \vec{e_2}$$

Additive Homomorphism?

$$C = C_1 + C_2 \Rightarrow C \cdot \vec{t} = (\mu_1 + \mu_2) \cdot (G \cdot \vec{t}) + (\vec{e_1} + \vec{e_2})$$

Multiplicative Homomorphism?

$$C = G^{-1}(C_1) \cdot C_2$$

$$\begin{aligned}
C \cdot \vec{t} &= G^{-1}(C_1) \cdot C_2 \cdot \vec{t} \\
&= G^{-1}(C_1) \cdot (\mu_2 \cdot (G \cdot \vec{t}) + \vec{e_2}) \\
&= \mu_2 \cdot G^{-1}(C_1) \cdot G \cdot \vec{t} + G^{-1}(C_1) \cdot \vec{e_2} \\
&= \mu_2 \cdot C_1 \cdot \vec{t} + G^{-1}(C_1) \cdot \vec{e_2} \\
&= \mu_2 \cdot (\mu_1 \cdot (G \cdot \vec{t}) + \vec{e_1}) + G^{-1}(C_1) \cdot \vec{e_2} \\
&= \mu_2 \cdot \mu_1 \cdot (G \cdot \vec{t}) + \mu_2 \cdot \vec{e_1} + G^{-1}(C_1) \cdot \vec{e_2}
\end{aligned}$$

How homomorphic is it?

#MULT ?

FHE Constructions

Step 1: Somewhat Homomorphic Encryption (SWHE)

- over Integers
- from LWE (GSW)

Step 2: Bootstrapping

Step 2: Bootstrapping

$$\begin{array}{c} ct_1 \quad ct_2 \quad \cdots \quad ct_n \\ \Big\downarrow f \\ ct_f \leftarrow \text{too much noise!} \\ \Big\downarrow \text{Dec} \\ y \\ \Big\downarrow \text{Enc} \\ ct_y \leftarrow \text{fresh noise!} \end{array}$$

Leveled FHE

(pk_1, sk_1) $\qquad ct_1 \quad ct_2 \quad \cdots \quad ct_n$

$$\Big\downarrow f$$

ct_f ← too much noise! $\qquad sk_1$

$$ct_f = \underbrace{1001011\cdots0}_{\ell} \qquad sk_1 = \underbrace{01101\cdots1}_{k}$$

(pk_2, sk_2) $\qquad \xrightarrow{Enc_{pk_2}}$ $\qquad \xrightarrow{Enc_{pk_2}}$

$$ct_1^{(2)} \quad ct_2^{(2)} \quad \cdots \quad ct_\ell^{(2)} \qquad \tilde{ct}_1^{(2)} \quad \cdots \quad \tilde{ct}_k^{(2)}$$

$$\boxed{\boxed{y}_{pk_1} \quad sk_1}_{pk_2}$$

$$\Big\downarrow f^{(2)} = Dec_{sk_1}(ct_f)$$

$$ct_{f^{(2)}} = Enc_{pk_2}(y)$$

$$\Big\downarrow$$

One more operation ADD & MULT

Step 2: Bootstrapping

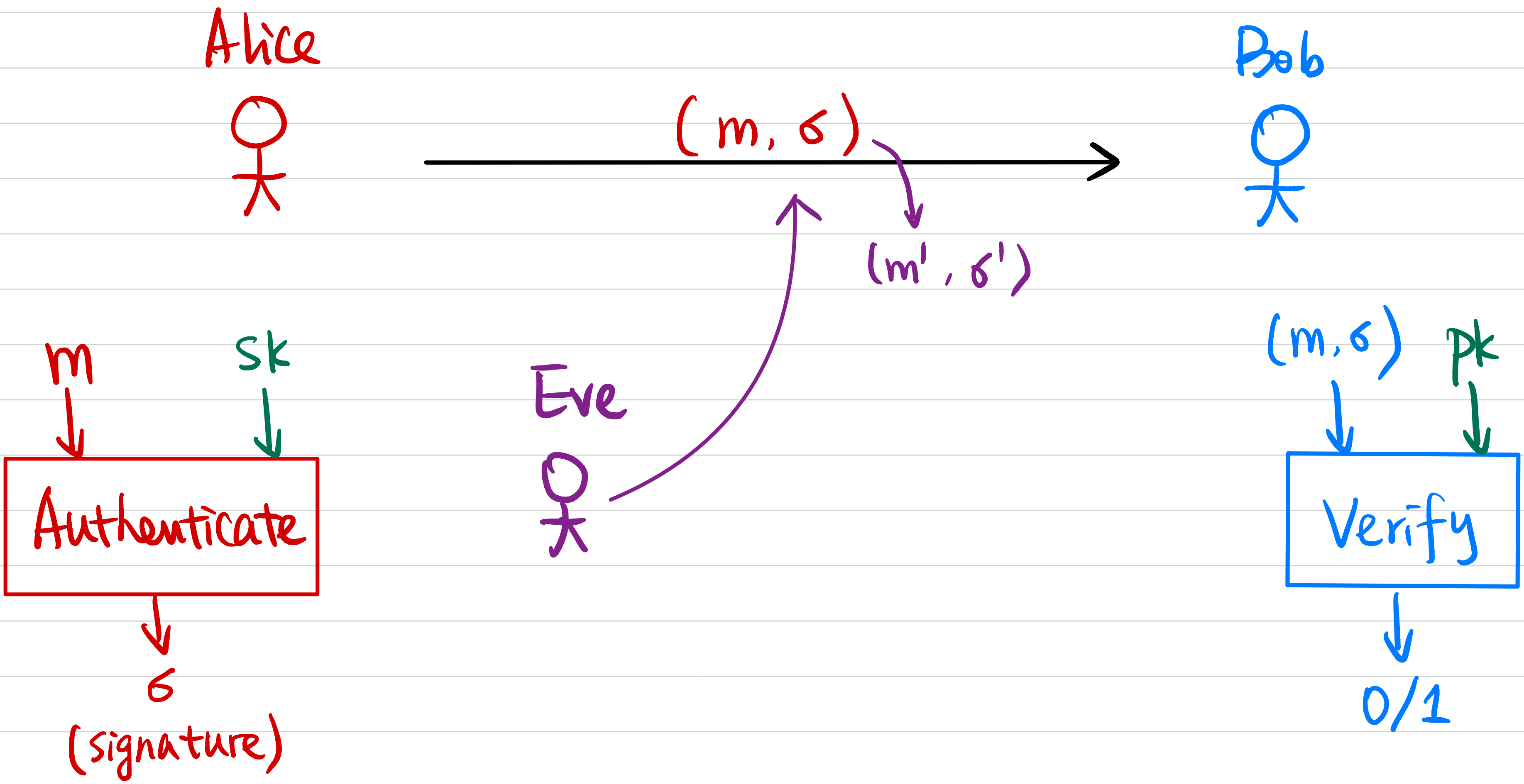
Leveled FHE: pk_1, pk_2, pk_3, ..., pk_n

$Enc_{pk_2}(sk_1)$ $Enc_{pk_3}(sk_2)$ $Enc_{pk_n}(sk_{n-1})$

FHE: pk, $Enc_{pk}(sk)$

"circular secure" assumption

Digital Signature



Digital Signature

- **Syntax:**

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

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

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

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

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

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

- **Security?**

Digital Signature

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

$C(1^n)$		$\mathcal{A}(1^n)$
$(pk, sk) \leftarrow \text{Gen}(1^n)$		
	$\xrightarrow{pk}$	
	$\xleftarrow{m \in \mathcal{M}}$	
$\sigma \leftarrow \text{Sign}_{sk}(m)$	$\xrightarrow{\sigma}$	
		Output (m^*, σ^*)

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

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

① $m^* \notin Q$, and

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

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

$$\boxed{\quad\quad\quad m \quad\quad\quad} \xrightarrow{H^s} \boxed{\ h\ } \xrightarrow{\mathrm{Mac}} \boxed{\ t\ }$$

Hash-and-Sign

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

$$\boxed{\quad\quad\quad m \quad\quad\quad} \xrightarrow{H^s} \boxed{\ h\ } \xrightarrow{\mathrm{Sign}} \boxed{\ \sigma\ }$$

RSA-based Signatures

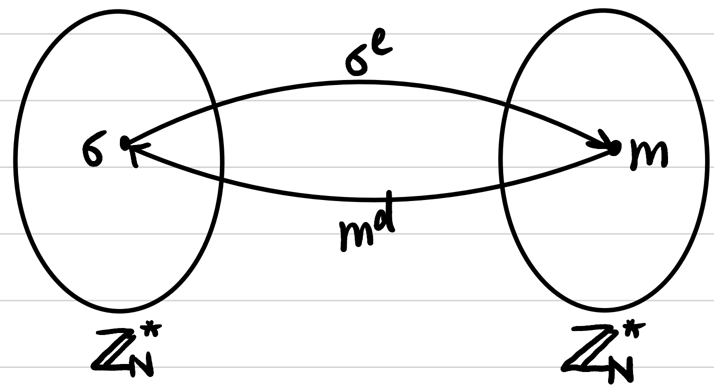
Plain RSA Signature:

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

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

  $pk := (N,e)$

  $sk := (N,d)$



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

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

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

Is it secure?

RSA-based Signatures

RSA-FDH (Full Domain Hash) Signature:

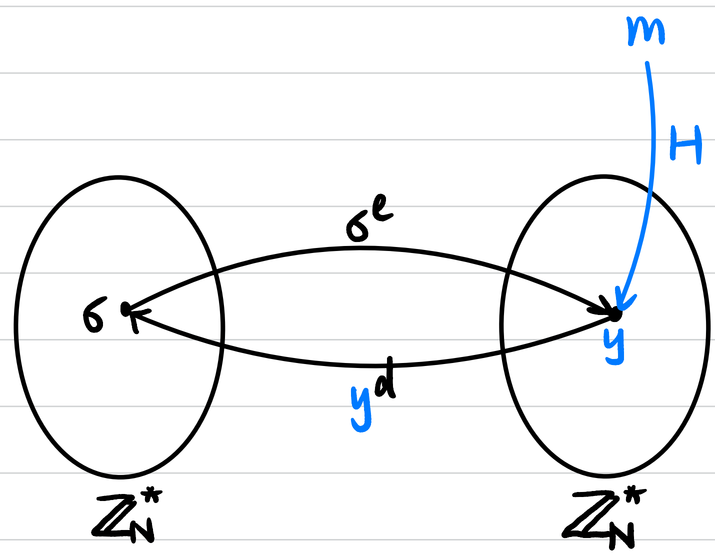
- $\mathrm{Gen}(1^n)$:

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

  $pk := (N,e)$

  $sk := (N,d)$

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



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

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

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

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