CSCI 1510

- Trapdoor Permutations (continued)
- Post-Quantum PKE from LWE Assumption
- Homomorphic Encryption
- Somewhat Homomorphic Encryption over Integers

ANNOUNCEMENT: Mid-semester survey (for extra credit)

Key Exchange: Security

Def A key exchange protocol Π is secure if

$\forall$ PPT $\mathcal{A}$, $\exists$ negligible function $\varepsilon(\cdot)$ s.t. $\Pr[b = b'] \le \frac{1}{2} + \varepsilon(n)$.

$C(1^n)$		$\mathcal{A}(1^n)$
Two parties holding 1^n execute Π. $\Rightarrow$ transcript T containing all the messages & a key k output by each party.		
$b \xleftarrow{\$} \{0,1\}$ If $b=0$, $\hat{k} := k$ If $b=1$, $\hat{k} \xleftarrow{\$} \{0,1\}^n$	$\xrightarrow{(T,\ \hat{k})}$	
		output b'

CPA Security

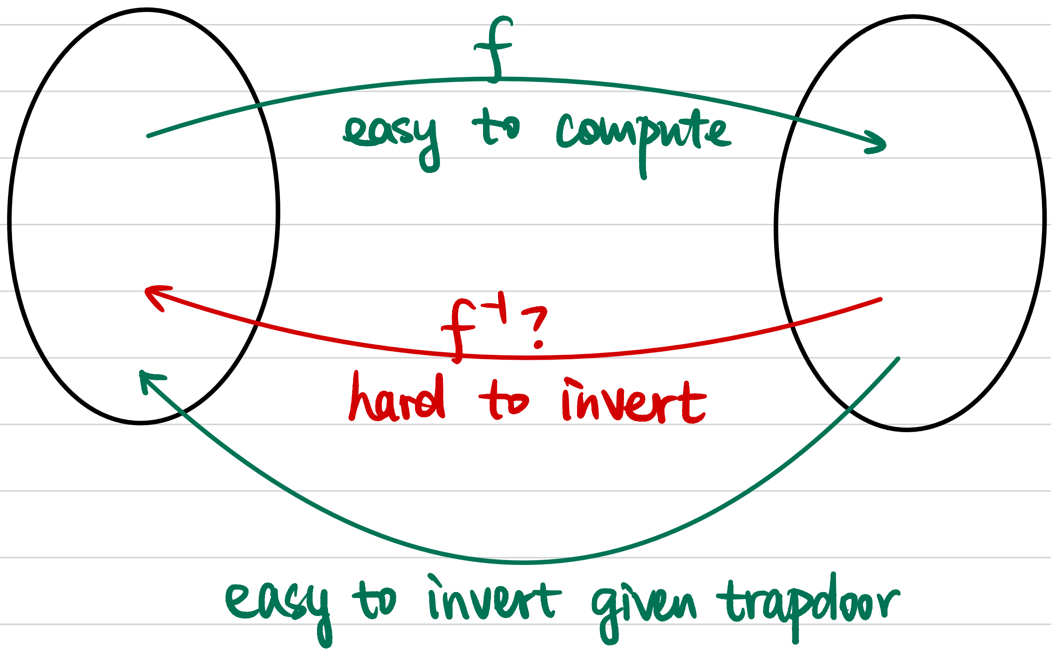
Def A public-key encryption scheme (Gen, Enc, Dec) is CPA-secure if $\forall$ PPT $\mathcal{A}$, $\exists$ negligible function $\varepsilon(\cdot)$ s.t.

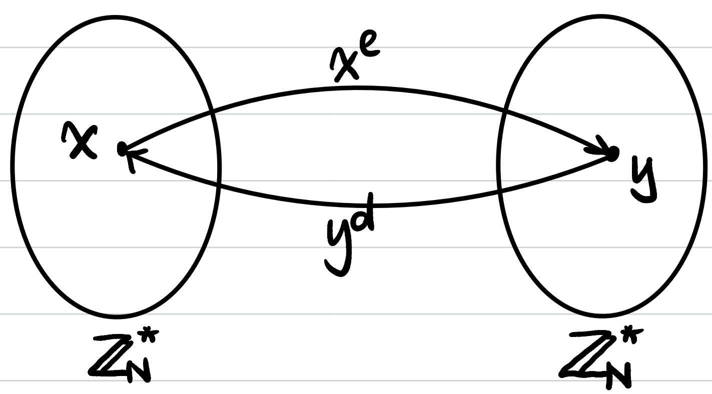
$$\Pr[b=b'] \le \frac{1}{2} + \varepsilon(n)$$

$C(1^n)$		$\mathcal{A}(1^n)$
$(pk, sk) \leftarrow Gen(1^n)$		
	$\xrightarrow{\quad pk \quad}$	
	$\xleftarrow[\lvert m_0\rvert = \lvert m_1\rvert]{m_0, m_1 \in \{0,1\}^*}$	
$b \xleftarrow{\$} \{0,1\}$		
$c \leftarrow Enc_{pk}(m_b)$		
	$\xrightarrow{\quad c \quad}$	
		output b'

CPA-Secure PKE $\Rightarrow$ Key Exchange

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)

② easy to sample a function: $(i, t) \leftarrow Gen(1^n)$.

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 $\mathcal{A}$, $\exists$ negligible function $\varepsilon(\cdot)$ s.t.

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

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

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 $\mathcal{A}$, $\exists$ negligible function $\varepsilon(\cdot)$ s.t.

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

Thm Assume trapdoor permutation exists.

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

PKE from TDP

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

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

  $pk := i$

  $sk := t$

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

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

  $c := f_i(r)$

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

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

Post-Quantum Assumption: Learning With Errors (LWE)

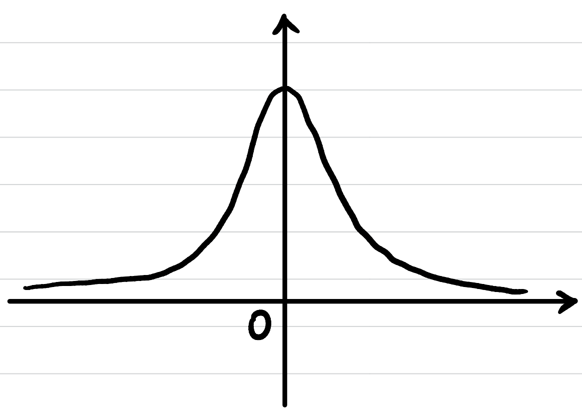
n: security parameter

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

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

χ: distribution over $\mathbb{Z}_q$

(concentrated on "small integers")

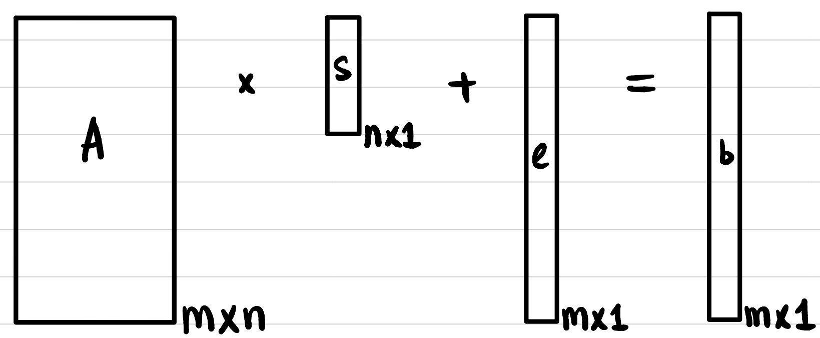


$$\Pr\left[\, |e| > \alpha \cdot q \;\middle|\; e \leftarrow \chi \,\right] \leq \text{negl}(n)$$

$\alpha \ll 1$

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

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



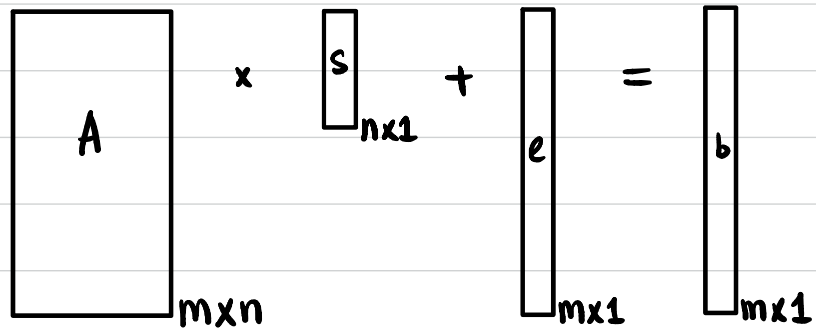
Post-Quantum PKE: Regev Encryption

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

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

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

  $sk = s$

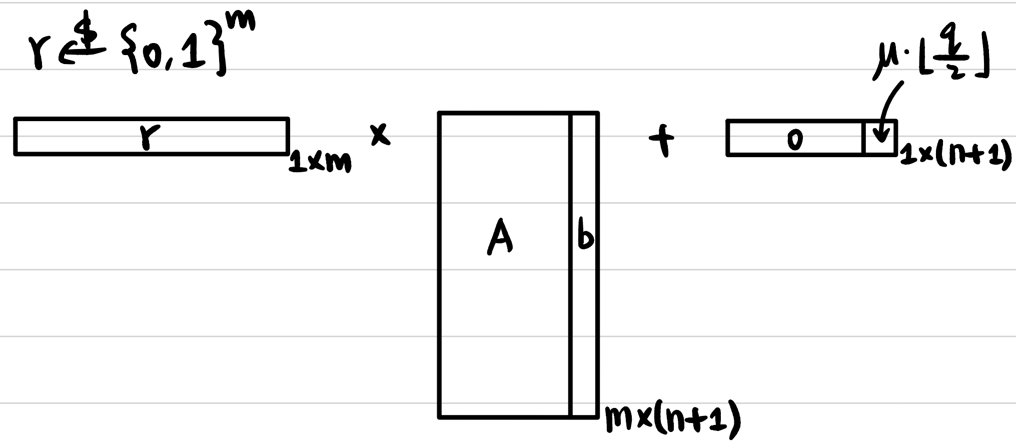


- $\mathrm{Enc}_{pk}(\mu)$: $\quad \mu \in \{0,1\}$

  sample a random $S \subseteq [m]$

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

  i-th row of A



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

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

Homomorphic Encryption

So far, encryption schemes:

$$ct \leftarrow \mathrm{Enc}(x)$$

$$x \leftarrow \mathrm{Dec}_{sk}(ct)$$

All-or-Nothing:

w/ sk $\rightarrow$ x

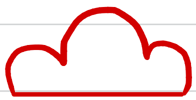
w/o sk $\rightarrow$ Nothing

Homomorphic Evaluation:

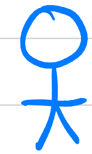
$$\begin{tikzcd}
\mathrm{Enc}(x) \arrow[dr] & & \\
 & \boxed{\mathrm{Eval}} \arrow[r] & \mathrm{Enc}(f(x)) \\
f \arrow[ur] & &
\end{tikzcd}$$

Application: Outsourcing Storage & Computation

Server



Client



Data x

Key sk

$ct \leftarrow \mathrm{Enc}(x)$

$\xleftarrow{\quad ct \quad}$

$\xleftarrow{\quad f \quad}$

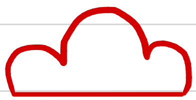
$ct' \leftarrow \mathrm{Eval}(f, ct)$

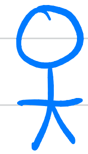
$\xrightarrow{\quad ct' \quad}$

$f(x) \leftarrow \mathrm{Dec}_{sk}(ct')$

Application: Privacy-Preserving Query

Server | **Client**





Input x

key sk

$ct \leftarrow Enc(x)$

$\xleftarrow{\quad ct \quad}$

ML/GPT/...

$\downarrow$

$ct' \leftarrow Eval(f, ct)$

$\xrightarrow{\quad ct' \quad}$

$f(x) \leftarrow Dec_{sk}(ct')$

Homomorphic Properties of Encryption Schemes

Multiplicatively Homomorphic

$$\left.\begin{array}{l} Enc(m_1) \\ Enc(m_2) \end{array}\right\} \rightarrow Enc(m_1 \cdot m_2)$$

Additively Homomorphic

$$\left.\begin{array}{l} Enc(m_1) \\ Enc(m_2) \end{array}\right\} \rightarrow Enc(m_1 + m_2)$$

El Gamal:

$$c_1 = (g^{r_1},\ h^{r_1} \cdot m_1)$$

$$c_2 = (g^{r_2},\ h^{r_2} \cdot m_2)$$

Exponential El Gamal:

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

$$c_1 = (g^{r_1},\ h^{r_1} \cdot g^{m_1})$$

$$c_2 = (g^{r_2},\ h^{r_2} \cdot g^{m_2})$$

Regev:

$$c_1 = (r_1^T \cdot A,\ r_1^T \cdot b + \mu_1 \cdot \lfloor \tfrac{q}{2} \rfloor)$$

$$c_2 = (r_2^T \cdot A,\ r_2^T \cdot b + \mu_2 \cdot \lfloor \tfrac{q}{2} \rfloor)$$

Fully Homomorphic: Additively & Multiplicatively Homomorphic

Is it possible?

- Question was asked back in 1978
- Big breakthough in 2009 (Gentry)
  - Complicated construction
  - Non-standard assumptions
- By now: much simpler constructions from standard assumptions.

Fully Homomorphic Encryption (FHE)

- **Syntax:** A (public-key) homomorphic encryption scheme $\Pi = (\text{Gen}, \text{Enc}, \text{Dec}, \text{Eval})$ w.r.t. function family $\mathcal{F}$:
  - $(pk, sk) \leftarrow \text{Gen}(1^n)$
  - $ct \leftarrow \text{Enc}_{pk}(m) \quad m \in \{0,1\}$
  - $m \leftarrow \text{Dec}_{sk}(ct)$
  - $ct_f \leftarrow \text{Eval}(f, ct_1, \cdots, ct_k) \qquad f: \{0,1\}^k \rightarrow \{0,1\}$

- **Correctness:** $\forall f \in \mathcal{F}, \quad \forall m_1, m_2, \cdots, m_k \in \{0,1\}$

  $\Pr[\text{Dec}_{sk}(ct_f) = f(m_1, \cdots, m_k)] \geq 1 - \text{negl}(n)$

  where $(pk, sk) \leftarrow \text{Gen}(1^n)$, $ct_i \leftarrow \text{Enc}_{pk}(m_i) \ \forall i \in [k]$,

  $ct_f \leftarrow \text{Eval}(f, ct_1, \cdots, ct_k)$.

- **CPA/CCA Security ?**

Missing Requirement ?

Fully Homomorphic Encryption (FHE)

- **Syntax:** A (public-key) homomorphic encryption scheme $\Pi = (\mathrm{Gen}, \mathrm{Enc}, \mathrm{Dec}, \mathrm{Eval})$ w.r.t. function family $\mathcal{F}$:
  - $(pk, sk) \leftarrow \mathrm{Gen}(1^n)$
  - $ct \leftarrow \mathrm{Enc}_{pk}(m) \quad m \in \{0,1\}$
  - $m \leftarrow \mathrm{Dec}_{sk}(ct)$
  - $ct_f \leftarrow \mathrm{Eval}(f, ct_1, \cdots, ct_k) \qquad f: \{0,1\}^k \to \{0,1\}$

- If $\mathcal{F}$ is the set of all poly-sized Boolean circuits, then Π is fully homomorphic.

FHE Constructions

Step 1: Somewhat Homomorphic Encryption (SWHE)

- over Integers
- from LWE (GSW)

Step 2: Bootstrapping

SWHE over Integers

Attempt 1 (Secret-key)

- secret key: odd number p Why odd?
- $\mathrm{Enc}(m)$: $m \in \{0,1\}$
  Sample a random q.
  Output $ct = p \cdot q + m$
  Encryption of 0 is a multiple of p.
- $\mathrm{Dec}(ct)$: $ct \bmod p$
- Eval ADD: $ct \leftarrow ct_1 + ct_2$
  Eval MULT: $ct \leftarrow ct_1 \cdot ct_2$

CPA Security?

SWHE over Integers

Attempt 2 (secret-key)

- secret key: odd number p
- Enc(m): $m \in \{0,1\}$

  Sample a random q. Sample a random $e \ll p$

  Output $ct = p \cdot q + m + 2e$

  Encryption of 0 is small and even modulo p.
- Dec(ct): $[ct \bmod p] \bmod 2$
- Eval ADD: $ct \leftarrow ct_1 + ct_2$

  Eval MULT: $ct \leftarrow ct_1 \cdot ct_2$

- Approximate GCD Problem:

  Given poly-many $\{x_i = p \cdot q_i + s_i\}$, output p.

Example parameters: $p \sim 2^{O(n^2)}$, $q_i \sim 2^{O(n^5)}$, $s_i \sim 2^{O(n)}$

Best known attacks require 2^n time.

SWHE over Integers

Attempt 3 (public-key)

- secret key: odd number p

  public key: "encryptions of 0"

  $\{x_i = p \cdot q_i + 2e_i\}_{i \in [n]}$

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

  Sample a random $e \ll p$

  Output $ct = (\text{random subset sum of } x_i\text{'s}) + m + 2e$

  Encryption of 0 is small and even modulo p.

- Dec(ct): $[ct \bmod p] \bmod 2$

- Eval ADD: $ct \leftarrow ct_1 + ct_2$

  Eval MULT: $ct \leftarrow ct_1 \cdot ct_2$

How homomorphic is it?