CS-E4340: Cryptography **I-II 2022/2023**

Exercise 7: Introduction to Lattice-based Cryptography

Deadline: 11:30 on November 7, 2022 via MyCourses as a single pdf file

Abstract

This exercise is designed to help students to ...

- understand modular arithmetic,
- understand the short integer solution (SIS) and learning with errors (LWE) assumptions,
- understand the leftover hash lemma in the lattice setting,
- be able to apply the above definitions and lemma to prove security of cryptographic schemes, and
- learn the notion of hiding and binding commitment.

Question 1 (Modular Arithmetic, Dual-Regev Encryption, and Linear Homomorphism)**.**

Answer Part (a) and choose between answering either Part (b) or Part (c).

(a) Consider $\mathbb{Z}_{13}$ (integers with arithmetic modulo 13) represented by $\{-6, \ldots, -1, 0, 1, \ldots, 6\}$. Calculate the following (writing down just the answer): (i) $4+5 \bmod 13$, (ii) $-5 \times 2 \bmod 13$, and (iii) $6^{-1} \bmod 13$, i.e. the element $x \in \mathbb{Z}_{13}$ such that $6x = 1$.

(b) Let $n, m, \log p, \log q \in \mathsf{poly}(\lambda)$ with $p < q$ and χ be the uniform distribution over $\mathbb{Z}_\beta$ for some $\log \beta \in \mathsf{poly}(\lambda)$ with $\beta < q$. In the following, we recall a slight generalisation of the dual-Regev encryption scheme with message space $\mathbb{Z}_p$:

$\mathsf{KGen}(1^\lambda)$	$\mathsf{Enc}(\mathsf{pk}, x \in \mathbb{Z}_p)$	$\mathsf{Dec}(\mathsf{sk}, \mathsf{ctxt})$
$\mathbf{A} \leftarrow\$ \mathbb{Z}_q^{n \times m}$	Parse $(\mathbf{A}, \mathbf{v}) \leftarrow \mathsf{pk}$	Parse $(\mathbf{c}_0, c_1) \leftarrow \mathsf{ctxt}$
$\mathbf{u} \leftarrow\$ \chi^m$	$\mathbf{s} \leftarrow\$ \mathbb{Z}_q^n$	$\mathbf{u} \leftarrow \mathsf{sk}$
$\mathbf{v} := \mathbf{A} \cdot \mathbf{u} \bmod q$	$\mathbf{e}_0 \leftarrow\$ \chi^m$	$\bar{x} := c_1 - \mathbf{c}_0^\mathtt{T} \cdot \mathbf{u} \bmod q$
$\mathsf{pk} := (\mathbf{A}, \mathbf{v})$	$e_1 \leftarrow\$ \chi$	**return** $\left\lceil \frac{p}{q} \cdot \bar{x} \right\rfloor$
$\mathsf{sk} := \mathbf{u}$	$\mathbf{c}_0^\mathtt{T} := \mathbf{s}^\mathtt{T} \cdot \mathbf{A} + \mathbf{e}_0^\mathtt{T} \bmod q$	// rounding to nearest integer
return $(\mathsf{pk}, \mathsf{sk})$	$c_1 := \mathbf{s}^\mathtt{T} \cdot \mathbf{v} + e_1 + \lfloor q/p \rfloor \cdot x \bmod q$	
	$\mathsf{ctxt} := (\mathbf{c}_0, c_1)$	
	return ctxt	

(i) Show that the scheme is correct when $q > m \cdot p \cdot \beta^2$ and $m \cdot \beta^2 \geq 2\beta + 2$. You can use the fact that for any $x, y \in \mathbb{Z}$ we have $|x + y| \leq |x| + |y|$ and $|x \cdot y| \leq |x| \cdot |y|$. Furthermore, you may want to use the fact that $\left| \frac{p}{q} \cdot \left\lfloor \frac{q}{p} \right\rfloor - 1 \right| \leq \frac{1}{q}$. [Hint: Note that decryption is correct when $\left| \frac{p}{q} \cdot \bar{x} - x \right| < \frac{1}{2}$. Read the proof of correctness of the (primal-)Regev encryption scheme in the lecture notes.]

(ii) Let $m \geq n \cdot \log_\beta q + \omega(\log n)$. Prove via a reduction that the scheme is IND-CPA-secure under the $\mathsf{LWE}_{n,m+1,q,\chi}$ assumption. [Hint: Read the proof of IND-CPA-security of the (primal-)Regev encryption scheme in the lecture notes. Follow the level of details of the lecture notes. The level of detail of the answer should be on a similar level as the lecture notes.]

(c) In this question, we study the linearly homomorphic property of the dual-Regev encryption scheme, which is useful for understanding Lecture 9. You may assume that $m \cdot \beta^2 \geq 2\beta + 2$. [Hint: Read hint of Question 1 (b) (i)]

(i) Let $(\mathsf{pk}, \mathsf{sk}) \in \mathsf{KGen}(1^\lambda)$, $x, x' \in \mathbb{Z}_p$, $\mathsf{ctxt} := (\mathbf{c}_0, c_1) \in \mathsf{Enc}(\mathsf{pk}, x)$, and $\mathsf{ctxt}' := (\mathbf{c}'_0, c'_1) \in \mathsf{Enc}(\mathsf{pk}, x')$. Consider $\mathsf{ctxt}'' := (\mathbf{c}_0 + \mathbf{c}'_0 \bmod q, c_1 + c'_1 \bmod q)$. Derive a lower bound $\underline{q}(m, p, \beta)$ of q so that $\mathsf{Dec}(\mathsf{sk}, \mathsf{ctxt}'') = x + x'$ whenever $x + x' \in \mathbb{Z}_p$ and $q > \underline{q}(m, p, \beta)$.

(ii) Generalising, let $\ell \in \mathbb{N}$, $(\mathsf{pk}, \mathsf{sk}) \in \mathsf{KGen}(1^\lambda)$, $\mathbf{a} \in \mathbb{Z}_p^\ell$, $\mathbf{x} \in \mathbb{Z}_p^\ell$, and $\mathsf{ctxt}_i \in \mathsf{Enc}(\mathsf{pk}, x_i)$ for all $i \in [\ell]$. Consider $\mathsf{ctxt} := \sum_{i=1}^{\ell} a_i \cdot \mathsf{ctxt}_i \bmod q$. Derive a lower bound $\underline{q}'(\ell, m, p, \beta)$ of q so that $\mathsf{Dec}(\mathsf{sk}, \mathsf{ctxt}'') = \langle \mathbf{a}, \mathbf{x} \rangle$ whenever $\langle \mathbf{a}, \mathbf{x} \rangle \in \mathbb{Z}_p$ and $q > \underline{q}'(\ell, m, p, \beta)$.

Fact 1. For several questions, we will use the following fact.

(i) $a \in \mathbb{Z}_\beta \;\rightarrow\; |a| \leq \frac{\beta}{2}$

(ii) $\mathbf{a} \in \mathbb{Z}_\beta^m \;\rightarrow\; |\mathbf{a}| \leq m \cdot \frac{\beta}{2}$

(iii) $\mathbf{a}, \mathbf{a}' \in \mathbb{Z}_\beta^m \;\rightarrow\; |\mathbf{a} \cdot \mathbf{a}'| \leq m\frac{\beta^2}{4}$

(i) and (ii) follow directly from the representation of $\mathbb{Z}_\beta$ as $\{-\left\lfloor \frac{\beta}{2} \right\rfloor, .., 0, .., \left\lfloor \frac{\beta}{2} \right\rfloor\}$, and for (iii), we observe that after component-wise multiplication of $\mathbf{a}$ and $\mathbf{a}'$, each component has norm at most $\frac{\beta^2}{4}$, and there are m entries, so their sum is upper bounded by $m\frac{\beta^2}{4}$.

We now turn to the answers of Question 1, (a)-(c).

(a) **(i)** 4+5 mod 13 = 4+5-13 mod 13= -4 mod 13,

(ii) -5×2 mod 13 = -10 mod 13 = -10+13 mod 13 = 3 mod 13, and

(iii) -2 mod 13, because 6 × (-2) mod 13 = -12 mod 13 = -12 + 13 mod 13 = 1 mod 13

(b) (i) Fix any public key $(\mathbf{A}, \mathbf{v}) \in \mathbb{Z}_q^{n \times m} \times \mathbb{Z}_q^n$, message $x \in \mathbb{Z}_p$, and ciphertext $(\mathbf{c}_0, c_1) \in \mathbb{Z}_q^m \times \mathbb{Z}_q$ with encryption randomness $(\mathbf{s}, \mathbf{e}_0, e_1) \in \mathbb{Z}_q^n \times \mathbb{Z}_\beta^m \times \mathbb{Z}_\beta$. The decryption algorithm rounds $\frac{p}{q} \cdot (c_1 - \mathbf{c}_0^{\mathsf{T}} \cdot \mathbf{u})$ to the nearest integer. For correctness to hold, the closest integer should be x and hence, correctness holds when $\left|\frac{p}{q}\cdot(c_1 - \mathbf{c}_0^\intercal\cdot\mathbf{u}) - x\right| < \frac{1}{2}$. Observe that

$$\begin{aligned}
&\left|\frac{p}{q}\cdot(c_1 - \mathbf{c}_0^\intercal\cdot\mathbf{u}) - x\right| \\
=&\left|\frac{p}{q}\cdot(\mathbf{s}^\intercal\cdot\mathbf{v} + e_1 + \lfloor q/p\rfloor\cdot x - (\mathbf{s}^\intercal\cdot\mathbf{A} + \mathbf{e}_0^\intercal)\cdot\mathbf{u}) - x\right| && \text{(plug-in } c_1 \text{ and } \mathbf{c}_0^\intercal) \\
=&\left|\frac{p}{q}\cdot(\mathbf{s}^\intercal\cdot\mathbf{A}\cdot\mathbf{u} + e_1 + \lfloor q/p\rfloor\cdot x - (\mathbf{s}^\intercal\cdot\mathbf{A} + \mathbf{e}_0^\intercal)\cdot\mathbf{u}) - x\right| && \text{(plug-in } \mathbf{v}) \\
=&\left|\frac{p}{q}\cdot(e_1 - \mathbf{e}_0^\intercal\cdot\mathbf{u} + \lfloor q/p\rfloor\cdot x) - x\right| && \text{(re-order and cancel } \mathbf{s}^\intercal\cdot\mathbf{A}\cdot\mathbf{u}) \\
\leq&\frac{p}{q}\cdot|e_1| + \frac{p}{q}\cdot\left|\mathbf{e}_0^\intercal\cdot\mathbf{u}\right| + \left|\frac{p}{q}\cdot\left\lfloor\frac{q}{p}\right\rfloor - 1\right|\cdot|x| && \text{(triangle inequality)} \\
\leq&\frac{p}{q}\cdot\frac{\beta}{2} + \frac{p}{q}\cdot m\cdot\frac{\beta^2}{4} + \frac{1}{q}\cdot\frac{p}{2} && (\textit{Fact } 1) \\
=&\frac{p}{q}\cdot\left(\frac{\beta}{2} + \frac{m\beta^2}{4} + \frac{1}{2}\right) \\
\leq&\frac{p}{q}\cdot\frac{m\beta^2}{2} && (m\cdot\beta^2 \geq 2\beta + 2) \\
<&\frac{p}{m\cdot p\cdot\beta^2}\cdot\frac{m\beta^2}{2} && (q > m\cdot p\cdot\beta^2) \\
=&\frac{1}{2}.
\end{aligned}$$

(ii) Let Π denote the dual-Regev public-key encryption scheme and let $\mathcal{A}$ be any PPT adversary. The proof proceeds via *game-hopping*, also called *hybrid argument*. That means, we define a sequence of hybrid security experiments where the first is identical to $\text{IND-CPA}^0_{\Pi,\mathcal{A}}$ and the last is identical to $\text{IND-CPA}^1_{\Pi,\mathcal{A}}$, and show that any two consecutive experiments are computationally or statistically indistinguishable from each other. Consequently, we have that $\text{IND-CPA}^0_{\Pi,\mathcal{A}}$ and $\text{IND-CPA}^1_{\Pi,\mathcal{A}}$ are computationally indistinguishable from each other, as desired.

The sequence of hybrids are as follows.

- Hyb_0: This experiment is identical to $\text{IND-CPA}^0_{\Pi,\mathcal{A}}$.
- Hyb_1: This experiment is almost identical to Hyb_0, except that for the public key $\mathsf{pk} = (\mathbf{A}, \mathbf{v})$, the vector $\mathbf{v}$ is now sampled uniformly from $\mathbb{Z}_q^n$ and not computed as $\mathbf{v} := \mathbf{A}\cdot\mathbf{u} \bmod q$ anymore.
- Hyb_2: This experiment is almost identical to Hyb_1, except that in the challenge ciphertext, the term $\mathbf{s}^\intercal\cdot\mathbf{A} + \mathbf{e}_0^\intercal \bmod q$ is replaced by a uniform sample from $\mathbb{Z}_q^m$ and the term $\mathbf{s}^\intercal\cdot\mathbf{v} + e_1 \bmod q$ is replaced by a uniform sample from $\mathbb{Z}_q$.
- Hyb_3: This experiment is almost identical to Hyb_2, except that the message being encrypted is changed from x_0 to x_1.
- Hyb_4: This experiment is almost identical to Hyb_3, except that the challenge ciphertext is computed as in $\mathsf{Enc}(\mathsf{pk}, x_1)$.
- Hyb_5: This experiment is almost identical to Hyb_4, except that the public key $\mathsf{pk} = (\mathbf{A}, \mathbf{v})$ is sampled as in $\mathsf{KGen}(1^\lambda)$. This experiment is identical to $\text{IND-CPA}^1_{\Pi,\mathcal{A}}$.

By the leftover hash lemma (Lecture 8, Lemma 8.8), we have

$$\left|\Pr\left[\mathsf{Hyb}_0(1^\lambda) = 1\right] - \Pr\left[\mathsf{Hyb}_1(1^\lambda) = 1\right]\right| \le \mathsf{negl}(\lambda)$$

and

$$\left|\Pr\left[\mathsf{Hyb}_4(1^\lambda) = 1\right] - \Pr\left[\mathsf{Hyb}_5(1^\lambda) = 1\right]\right| \le \mathsf{negl}(\lambda).$$

For the following two game-hops, we can build a reduction to the Decision-$\mathsf{LWE}_{n,m+1,q,\chi}$ assumption, by ovserving that $\mathbf{A}' := \mathbf{A}||\mathbf{v}$ is a uniformly random matrix. We then obtain that

$$\left|\Pr\left[\mathsf{Hyb}_1(1^\lambda) = 1\right] - \Pr\left[\mathsf{Hyb}_2(1^\lambda) = 1\right]\right| \le \mathsf{negl}(\lambda)$$

and

$$\left|\Pr\left[\mathsf{Hyb}_3(1^\lambda) = 1\right] - \Pr\left[\mathsf{Hyb}_4(1^\lambda) = 1\right]\right| \le \mathsf{negl}(\lambda).$$

Finally, we realise that statistically, $\Pr\left[\mathsf{Hyb}_2(1^\lambda) = 1\right] = \Pr\left[\mathsf{Hyb}_3(1^\lambda) = 1\right]$. Using triangle inequality, we thus obtain that

$$\begin{aligned}
&\left|\Pr\left[\text{IND-CPA}^0_{\Pi,\mathcal{A}}(1^\lambda) = 1\right] - \Pr\left[\text{IND-CPA}^1_{\Pi,\mathcal{A}}(1^\lambda) = 1\right]\right| \\
=&\left|\Pr\left[\mathsf{Hyb}_0(1^\lambda) = 1\right] - \Pr\left[\mathsf{Hyb}_1(1^\lambda) = 1\right]\right| \\
\le&\ \mathsf{negl}(\lambda) + \mathsf{negl}(\lambda) + \mathsf{negl}(\lambda) + \mathsf{negl}(\lambda) + \mathsf{negl}(\lambda),
\end{aligned}$$

and the sum of 4 negligible functions is negligible.

(c) (i) Let $\underline{q}(m, p, \beta) = 2 \cdot m \cdot p \cdot \beta^2$.
Fix any public key $(\mathbf{A}, \mathbf{v}) \in \mathbb{Z}_q^{n\times m} \times \mathbb{Z}_q^n$, message $x, x' \in \mathbb{Z}_p$, and ciphertexts $(\mathbf{c}_0, c_1), (\mathbf{c}'_0, c'_1) \in \mathbb{Z}_q^m \times \mathbb{Z}_q$ with encryption randomness $(\mathbf{s}, \mathbf{e}_0, e_1), (\mathbf{s}', \mathbf{e}'_0, e'_1) \in \mathbb{Z}_q^n \times \mathbb{Z}_\beta^m \times \mathbb{Z}_\beta$. For correctness to hold, we want $\left|\frac{p}{q} \cdot (\mathbf{c}_1 + \mathbf{c}'_1 - (\mathbf{c}_0 - \mathbf{c}'_0)^\mathtt{T} \cdot \mathbf{u}) - (x + x')\right| < \frac{1}{2}$. Observe that

$$\begin{aligned}
&\left|\frac{p}{q} \cdot (\mathbf{c}_1 + \mathbf{c}'_1 - (\mathbf{c}_0^\mathtt{T} - (\mathbf{c}'_0)^\mathtt{T}) \cdot \mathbf{u}) - (x + x')\right| \\
=&\left|\frac{p}{q} \cdot (e_1 + e'_1 - (\mathbf{e}_0 + \mathbf{e}'_0)^\mathtt{T} \cdot \mathbf{u} + \lfloor q/p \rfloor \cdot (x + x')) - (x + x')\right| \\
\le&\frac{p}{q} \cdot |e_1 + e'_1| + \frac{p}{q} \cdot \left|(\mathbf{e}_0 + \mathbf{e}'_0)^\mathtt{T} \cdot \mathbf{u}\right| + \left|\frac{p}{q} \cdot \left\lfloor \frac{q}{p} \right\rfloor - 1\right| \cdot |x + x'| && \text{(triangle inequality)} \\
\le&\frac{p}{q} \cdot \beta + \frac{p}{q} \cdot m \cdot \frac{\beta^2}{2} + \frac{1}{q} \cdot \frac{p}{2} && (\textit{Fact } 1) \\
=&\frac{p}{q} \cdot \left(\beta + \frac{m\beta^2}{2} + \frac{1}{2}\right) \\
\le&\frac{p}{q} \cdot m \cdot \beta^2 && (m \cdot \beta^2 \ge 2\beta + 2) \\
<&\frac{p}{2 \cdot m \cdot p \cdot \beta^2} \cdot m \cdot \beta^2 && (q > 2 \cdot m \cdot p \cdot \beta^2) \\
=&\frac{1}{2}.
\end{aligned}$$

(ii) Let $\underline{q}'(\ell, m, p, \beta) = \frac{1}{2} \cdot \ell \cdot m \cdot p^2 \cdot \beta^2$.

Fix any public key $(\mathbf{A}, \mathbf{v}) \in \mathbb{Z}_q^{n\times m} \times \mathbb{Z}_q^n$, messages $\mathbf{x} \in \mathbb{Z}_p^\ell$, and ciphertexts $(\mathbf{c}_{i,0}, c_{i,1}) \in \mathbb{Z}_q^m \times \mathbb{Z}_q$ with encryption randomness $(\mathbf{s}_i, \mathbf{e}_{i,0}, e_{i,1}) \in \mathbb{Z}_q^n \times \mathbb{Z}_\beta^m \times \mathbb{Z}_\beta$ for $i \in [\ell]$. For correctness to hold, we want

$$\left|\frac{p}{q} \cdot \left(\sum_{i=1}^{\ell} a_i \cdot \mathbf{c}_{i,1} - \left(\sum_{i=1}^{\ell} a_i \cdot \mathbf{c}_{i,0}\right)^{\mathtt{T}} \cdot \mathbf{u}\right) - \langle \mathbf{a}, \mathbf{x}\rangle\right| < \frac{1}{2}.$$

Observe that

$$\begin{aligned}
&\left|\frac{p}{q} \cdot \left(\sum_{i=1}^{\ell} a_i \cdot \mathbf{c}_{i,1} - \left(\sum_{i=1}^{\ell} a_i \cdot \mathbf{c}_{i,0}\right)^{\mathtt{T}} \cdot \mathbf{u}\right) - \langle \mathbf{a}, \mathbf{x}\rangle\right| \\
=&\left|\frac{p}{q} \cdot (\sum_{i=1}^{\ell} a_i \cdot e_{i,1} - (\sum_{i=1}^{\ell} a_i \cdot \mathbf{e}_{i,0})^{\mathtt{T}} \cdot \mathbf{u} + \lfloor q/p \rfloor \cdot \langle \mathbf{a}, \mathbf{x}\rangle) - \langle \mathbf{a}, \mathbf{x}\rangle\right| \\
\leq&\frac{p}{q} \cdot \left|\sum_{i=1}^{\ell} a_i \cdot e_{i,1}\right| + \frac{p}{q} \cdot \left|(\sum_{i=1}^{\ell} a_i \cdot \mathbf{e}_{i,0})^{\mathtt{T}} \cdot \mathbf{u}\right| + \left|\frac{p}{q} \cdot \left\lfloor \frac{q}{p} \right\rfloor - 1\right| \cdot |\langle \mathbf{a}, \mathbf{x}\rangle| && \text{(triangle inequality)} \\
\leq&\frac{p}{q} \cdot \ell \cdot \frac{p}{2} \cdot \frac{\beta}{2} + \frac{p}{q} \cdot \ell \cdot \frac{p}{2} \cdot m \cdot \frac{\beta^2}{4} + \frac{1}{q} \cdot \frac{p}{2} && (\mathit{Fact}\ 1) \\
=&\frac{p}{q} \cdot \left(\frac{\ell \cdot p \cdot \beta}{4} + \frac{\ell \cdot m \cdot p \cdot \beta^2}{8} + \frac{1}{2}\right) \\
\leq&\frac{p}{q} \cdot \frac{\ell \cdot m \cdot p \cdot \beta^2}{4} && (m \cdot \beta^2 \geq 2\beta + 2) \\
<&\frac{2 \cdot p}{\ell \cdot m \cdot p^2 \cdot \beta^2} \cdot \frac{\ell \cdot m \cdot p \cdot \beta^2}{4} && (q > 2 \cdot m \cdot p \cdot \beta^2) \\
=&\frac{1}{2}.
\end{aligned}$$

Question 2 (Normal-Form of LWE, Lindner-Peikert Encryption)**.** In this question, we study the "normal form" of the LWE assumption and use it to prove the security of the Lindner-Peikert encryption scheme. We first recall the ordinary LWE assumption and then state the normal-form variant.

Definition (Decision-Learning with Errors (LWE) Assumption)**.** Let $n, m, \log q \in \mathsf{poly}(\lambda)$ with $n \leq m$ and χ be a distribution over $\mathbb{Z}$ parametrised by λ. The Decision-$\mathsf{LWE}_{n,m,q,\chi}$ assumption states that for any PPT adversary $\mathcal{A}$

$$\left|\Pr\left[b = 1 \,\middle|\, \begin{array}{l} \mathbf{A} \leftarrow\$ \mathbb{Z}_q^{n\times m} \\ \mathbf{s} \leftarrow\$ \mathbb{Z}_q^n,\ \mathbf{e} \leftarrow\$ \chi^m \\ \mathbf{b}^{\mathtt{T}} := \mathbf{s}^{\mathtt{T}} \cdot \mathbf{A} + \mathbf{e}^{\mathtt{T}} \bmod q \\ b \leftarrow \mathcal{A}(\mathbf{A}, \mathbf{b}) \end{array}\right] - \Pr\left[b = 1 \,\middle|\, \begin{array}{l} \mathbf{A} \leftarrow\$ \mathbb{Z}_q^{n\times m} \\ \mathbf{b} \leftarrow\$ \mathbb{Z}_q^m \\ b \leftarrow \mathcal{A}(\mathbf{A}, \mathbf{b}) \end{array}\right]\right| \leq \mathsf{negl}(\lambda).$$

Definition (Normal-Form Decision-Learning with Errors (LWE) Assumption)**.** Let $n, m, \log q \in \mathsf{poly}(\lambda)$ with $n \leq m$ and χ be a distribution over $\mathbb{Z}$ parametrised by λ. The Normal-Form Decision-$\mathsf{LWE}_{n,m,q,\chi}$

assumption states that for any PPT adversary $\mathcal{A}$

$$\left| \Pr\left[b = 1 \,\middle|\, \begin{array}{l} \mathbf{A} \leftarrow\!\!\$\ \mathbb{Z}_q^{n \times m} \\ \mathbf{s} \leftarrow\!\!\$\ \chi^n,\ \mathbf{e} \leftarrow\!\!\$\ \chi^m \\ \mathbf{b}^{\mathsf{T}} := \mathbf{s}^{\mathsf{T}} \cdot \mathbf{A} + \mathbf{e}^{\mathsf{T}} \bmod q \\ b \leftarrow \mathcal{A}(\mathbf{A}, \mathbf{b}) \end{array} \right] - \Pr\left[b = 1 \,\middle|\, \begin{array}{l} \mathbf{A} \leftarrow\!\!\$\ \mathbb{Z}_q^{n \times m} \\ \mathbf{b} \leftarrow\!\!\$\ \mathbb{Z}_q^{m} \\ b \leftarrow \mathcal{A}(\mathbf{A}, \mathbf{b}) \end{array} \right] \right| \leq \mathsf{negl}(\lambda).$$

Note that in the normal-form variant the LWE secret $\mathbf{s}$ is also drawn from the error distribution χ.

Next, let $n, \log p, \log q \in \mathsf{poly}(\lambda)$ with $p < q$, and χ be the uniform distribution over $\mathbb{Z}_\beta$, for some $\log \beta \in \mathsf{poly}(\lambda)$ with β being odd and $\beta < q$. We introduce the Lindner-Peikert encryption scheme:

$\mathsf{KGen}(1^\lambda)$	$\mathsf{Enc}(\mathsf{pk}, x \in \mathbb{Z}_p)$	$\mathsf{Dec}(\mathsf{sk}, \mathsf{ctxt})$
$\mathbf{A} \leftarrow\!\!\$\ \mathbb{Z}_q^{n \times n}$	Parse $(\mathbf{A}, \mathbf{b}) \leftarrow \mathsf{pk}$	Parse $(\mathbf{c}_0, c_1) \leftarrow \mathsf{ctxt}$
$\mathbf{s}, \mathbf{e} \leftarrow\!\!\$\ \chi^n$	$\mathbf{r}, \mathbf{e}_0 \leftarrow\!\!\$\ \chi^n$	$\mathbf{s} \leftarrow \mathsf{sk}$
$\mathbf{b}^{\mathsf{T}} := \mathbf{s}^{\mathsf{T}} \cdot \mathbf{A} + \mathbf{e}^{\mathsf{T}} \bmod q$	$e_1 \leftarrow\!\!\$\ \chi$	$\bar{x} := c_1 - \mathbf{s}^{\mathsf{T}} \cdot \mathbf{c}_0 \bmod q$
$\mathsf{pk} := (\mathbf{A}, \mathbf{b})$	$\mathbf{c}_0 := \mathbf{A} \cdot \mathbf{r} + \mathbf{e}_0 \bmod q$	**return** $\left\lfloor \frac{p}{q} \cdot \bar{x} \right\rceil$
$\mathsf{sk} := \mathbf{s}$	$c_1 := \mathbf{b}^{\mathsf{T}} \cdot \mathbf{r} + e_1 + \left\lfloor \frac{q}{p} \right\rfloor \cdot x \bmod q$	// rounding to nearest integer
return $(\mathsf{pk}, \mathsf{sk})$	$\mathsf{ctxt} := (\mathbf{c}_0, c_1)$	
	return ctxt	

Choose between answering either Part (a), or answering the two Parts (b) and (c).

(a) Let q be prime, $m \geq n + \lambda$, and χ be symmetric about 0, i.e. $\chi = -\chi$. Prove via a reduction that if the Decision-$\mathsf{LWE}_{n,m,q,\chi}$ assumption holds then the Normal-Form Decision-$\mathsf{LWE}_{n,m-n,q,\chi}$ assumption holds. [Hint: The analysis of normal-form SIS in the lecture notes. The level of detail of the answer should be on a similar level as the lecture notes.]

(b) Show that the Lindner-Peikert encryption scheme is correct when $q > 2 \cdot n \cdot p \cdot \beta^2$ and $n \cdot \beta^2 \geq \beta + 1$. [Hint: Read hint of Question 1 (b) (i)]

(c) Prove via a reduction that the Lindner-Peikert encryption scheme is IND-CPA-secure under the Normal-Form Decision-$\mathsf{LWE}_{n,n+1,q,\chi}$ assumption. [Hint: Read hint of Question 1 (b) (ii). The level of detail of the answer should be on a similar level as the lecture notes.]

(a) Given a PPT adversary $\mathcal{A}$ that can break the Normal-Form Decision-LWE, we construct a PPT adversary $\mathcal{B}$ that can break decision-LWE. (Chris: Maybe add parameters here later...) Let $\mathcal{B}$ be as follows on input $(\mathbf{A}, \mathbf{b})$:

- If $\mathbf{A}$ does not have linearly-independent rows, abort.
- Permute the columns of $\mathbf{A}$ so that the last n columns are linearly-independent.
- Parse $\mathbf{A}$ as $(\mathbf{A}_0 \| \mathbf{A}_1)$ and $\mathbf{b}^{\mathsf{T}}$ as $(\mathbf{b}_0^{\mathsf{T}} \| \mathbf{b}_1^{\mathsf{T}})$.
- Set $\bar{\mathbf{A}} := -\mathbf{A}_1^{-1} \cdot \mathbf{A}_0$.
- Set $\bar{\mathbf{b}} := \mathbf{b}_1^{\mathsf{T}} \cdot \bar{\mathbf{A}} + \mathbf{b}_0^{\mathsf{T}}$.
- Output whatever $\mathcal{A}(\bar{\mathbf{A}}, \bar{\mathbf{b}})$ outputs.

By Lemma 8.10 in Lecture 8, the probability that $\mathbf{A}$ does not have linearly-independent rows, i.e. not full-rank, is negligible in n. The following analysis is conditioned on $\mathbf{A}$ being full-rank.

If $(\mathbf{A}, \mathbf{b})$ is uniformly random, then $(\bar{\mathbf{A}}, \bar{\mathbf{b}})$ is also uniformly random.

If $(\mathbf{A}, \mathbf{b})$ consists of LWE samples, then we have

$$\mathbf{b}_0^{\mathtt{T}} = \mathbf{s}^{\mathtt{T}} \cdot \mathbf{A}_0 + \mathbf{e}_0^{\mathtt{T}} \bmod q \text{ and}$$
$$\mathbf{b}_1^{\mathtt{T}} = \mathbf{s}^{\mathtt{T}} \cdot \mathbf{A}_1 + \mathbf{e}_1^{\mathtt{T}} \bmod q$$

where $\mathbf{s} \leftarrow\$ \mathbb{Z}_q^n$, $\mathbf{e}_0 \leftarrow\$ \chi^{m-n}$, and $\mathbf{e}_1 \leftarrow\$ \chi^n$. It follows that

$$\begin{aligned}\bar{\mathbf{b}} &= \mathbf{b}_1^{\mathtt{T}} \cdot \bar{\mathbf{A}} + \mathbf{b}_0^{\mathtt{T}} \bmod q \\ &= -\mathbf{s}^{\mathtt{T}} \cdot \mathbf{A}_1 \cdot \mathbf{A}_1^{-1} \cdot \mathbf{A}_0 + \mathbf{e}_1^{\mathtt{T}} \cdot \bar{\mathbf{A}} + \mathbf{s}^{\mathtt{T}} \cdot \mathbf{A}_0 + \mathbf{e}_0^{\mathtt{T}} \bmod q \\ &= \mathbf{e}_1^{\mathtt{T}} \cdot \bar{\mathbf{A}} + \mathbf{e}_0^{\mathtt{T}} \bmod q,\end{aligned}$$

i.e. $(\bar{\mathbf{A}}, \bar{\mathbf{b}})$ consists of normal-form LWE samples.

Our adversary $\mathcal{B}$ therefore succeeds whenever $\mathcal{A}$ succeeds, except with negligible probability.

(b) Fix any public key $(\mathbf{A}, \mathbf{b}) \in \mathbb{Z}_q^{n\times n} \times \mathbb{Z}_q^n$, message $x \in \mathbb{Z}_p$, and ciphertext $(\mathbf{c}_0, c_1) \in \mathbb{Z}_q^n \times \mathbb{Z}_q$ with encryption randomness $(\mathbf{r}, \mathbf{e}_0, e_1) \in \mathbb{Z}_\beta^n \times \mathbb{Z}_\beta^n \times \mathbb{Z}_\beta$. For correctness to hold, we want $\left|\frac{p}{q} \cdot (\mathbf{c}_1 - \mathbf{s}^{\mathtt{T}} \cdot \mathbf{c}_0) - x\right| < \frac{1}{2}$. Observe that

$$\begin{aligned}
&\left|\frac{p}{q} \cdot (\mathbf{c}_1 - \mathbf{s}^{\mathtt{T}} \cdot \mathbf{c}_0) - x\right| \\
=&\left|\frac{p}{q} \cdot (e_1 + \mathbf{e}^{\mathtt{T}} \cdot \mathbf{r} - \mathbf{s}^{\mathtt{T}} \cdot \mathbf{e}_0 + \lfloor q/p \rfloor \cdot x) - x\right| \\
\leq&\frac{p}{q} \cdot |e_1| + \frac{p}{q} \cdot \left|\mathbf{e}^{\mathtt{T}} \cdot \mathbf{r}\right| + \frac{p}{q} \cdot \left|\mathbf{e}_0^{\mathtt{T}} \cdot \mathbf{u}\right| + \left|\frac{p}{q} \cdot \left\lfloor \frac{q}{p} \right\rfloor - 1\right| \cdot |x| && \text{(triangle inequality)} \\
\leq&\frac{q}{p} \cdot \frac{\beta}{2} + \frac{q}{p} \cdot n \cdot \frac{\beta^2}{4} + \frac{q}{p} \cdot n \cdot \frac{\beta^2}{4} + \frac{1}{q} \cdot \frac{p}{2} && \text{(Fact 1)} \\
=&\frac{p}{q} \cdot \left(\frac{\beta}{2} + \frac{n\beta^2}{2} + \frac{1}{2}\right) \\
\leq&\frac{p}{q} \cdot n \cdot \beta^2 && (n \cdot \beta^2 \geq \beta + 1) \\
<&\frac{p}{2 \cdot n \cdot p \cdot \beta^2} \cdot n \cdot \beta^2 && (q > 2 \cdot n \cdot p \cdot \beta^2) \\
=&\frac{1}{2}.
\end{aligned}$$

(c) Let Π denote the Lindner-Peikert public-key encryption scheme and let $\mathcal{A}$ be any PPT adversary. As for Question 1 (ii), the proof proceeds by game-hopping, also known as *hybrid argument*. That means, we define a sequence of hybrid security experiments where the first is identical to $\text{IND-CPA}_{\Pi,\mathcal{A}}^0$ and the last is identical to $\text{IND-CPA}_{\Pi,\mathcal{A}}^1$, and show that any two consecutive experiments are computationally or statistically indistinguishable from each other. Consequently, we have that $\text{IND-CPA}_{\Pi,\mathcal{A}}^0$ and $\text{IND-CPA}_{\Pi,\mathcal{A}}^1$ are computationally indistinguishable from each other, as desired.

The sequence of hybrids are as follows.

- Hyb_0: This experiment is identical to $\text{IND-CPA}^0_{\Pi,\mathcal{A}}$.
- Hyb_1: This experiment is almost identical to Hyb_0, except that for the public key $\mathsf{pk} = (\mathbf{A}, \mathbf{v})$, the vector $\mathbf{b}^\mathsf{T}$ is now sampled uniformly from $\mathbb{Z}_q^n$ and not computed as $\mathbf{b}^\mathsf{T}\mathbf{s}^\mathsf{T} \cdot \mathbf{A} + \mathbf{e}^\mathsf{T} \bmod q$ anymore.
- Hyb_2: This experiment is almost identical to Hyb_1, except that in the challenge ciphertext, the term $\mathbf{A} \cdot \mathbf{r} + \mathbf{e}_0 \bmod q$ is replaced by a uniform sample from $\mathbb{Z}_q^n$ and $\mathbf{b}^\mathsf{T} \cdot \mathbf{r} + e_1 \bmod q$ is replaced by a uniform sample from $\mathbb{Z}_q$.
- Hyb_3: This experiment is almost identical to Hyb_2, except that the message being encrypted is changed from x_0 to x_1.
- Hyb_4: This experiment is almost identical to Hyb_3, except that the challenge ciphertext is computed as in $\mathsf{Enc}(\mathsf{pk}, x_1)$.
- Hyb_5: This experiment is almost identical to Hyb_4, except that the public key $\mathsf{pk} = (\mathbf{A}, \mathbf{b})$ is sampled as in $\mathsf{KGen}(1^\lambda)$. This experiment is identical to $\text{IND-CPA}^1_{\Pi,\mathcal{A}}$.

By the Normal-Form Decision-$\mathsf{LWE}_{n,n,q,\chi}$, which is implied by the Normal-Form Decision-$\mathsf{LWE}_{n,n+1,q,\chi}$ assumption, we have

$$\left|\Pr\left[\mathsf{Hyb}_0(1^\lambda) = 1\right] - \Pr\left[\mathsf{Hyb}_1(1^\lambda) = 1\right]\right| \leq \mathsf{negl}(\lambda)$$

and

$$\left|\Pr\left[\mathsf{Hyb}_4(1^\lambda) = 1\right] - \Pr\left[\mathsf{Hyb}_5(1^\lambda) = 1\right]\right| \leq \mathsf{negl}(\lambda).$$

For the following two game-hops, we can build a reduction to the Normal-Form Decision-$\mathsf{LWE}_{n,n+1,q,\chi}$ assumption, by observing that $\mathbf{A}' := \mathbf{A}||\mathbf{b}^\mathsf{T}$ is a uniformly random matrix. We then obtain that

$$\left|\Pr\left[\mathsf{Hyb}_1(1^\lambda) = 1\right] - \Pr\left[\mathsf{Hyb}_2(1^\lambda) = 1\right]\right| \leq \mathsf{negl}(\lambda)$$

and

$$\left|\Pr\left[\mathsf{Hyb}_3(1^\lambda) = 1\right] - \Pr\left[\mathsf{Hyb}_4(1^\lambda) = 1\right]\right| \leq \mathsf{negl}(\lambda).$$

Finally, we realise that statistically, $\Pr\left[\mathsf{Hyb}_2(1^\lambda) = 1\right] = \Pr\left[\mathsf{Hyb}_3(1^\lambda) = 1\right]$. Using triangle inequality, we thus obtain that

$$\begin{aligned}
&\left|\Pr\left[\text{IND-CPA}^0_{\Pi,\mathcal{A}}(1^\lambda) = 1\right] - \Pr\left[\text{IND-CPA}^1_{\Pi,\mathcal{A}}(1^\lambda) = 1\right]\right| \\
=&\left|\Pr\left[\mathsf{Hyb}_0(1^\lambda) = 1\right] - \Pr\left[\mathsf{Hyb}_1(1^\lambda) = 1\right]\right| \\
\leq& \,\mathsf{negl}(\lambda) + \mathsf{negl}(\lambda) + \mathsf{negl}(\lambda) + \mathsf{negl}(\lambda),
\end{aligned}$$

and the sum of 4 negligible functions is negligible.

Question 3 (SIS Commitments)**.** In this question, we study a basic lattice-based commitment scheme. First, we introduce the concept of commitments.

Definition (Commitments)**.** A commitment scheme for message space $\mathcal{X}$ is a tuple of PPT algorithms $\Gamma = (\mathsf{Setup}, \mathsf{Com})$ with the following syntax:

- $\mathsf{pp} \leftarrow \mathsf{Setup}(1^\lambda, 1^\ell)$: The setup algorithm inputs the security parameter $\lambda \in \mathbb{N}$ and a length parameter $\ell \in \mathbb{N}$. It outputs the public parameters pp (also known as the commitment key).
- $\mathsf{com} \leftarrow \mathsf{Com}(\mathsf{pp}, \mathbf{x} \in \mathcal{X}^\ell; r)$: The commitment algorithm inputs the public parameters pp, a message $\mathbf{x} \in \mathcal{X}^\ell$, and some randomness r (from some randomness space). It outputs a commitment com. By

default, the randomness r is assumed to be sampled uniformly at random from the randomness space, and is omitted from the input.

A commitment scheme could satisfy the hiding and binding properties defined as follows:

(Statistically) Hiding For any $\ell \in \mathbb{N}$, any $\mathbf{x}, \mathbf{y} \in \mathcal{X}^\ell$, the statistical distance between the following distributions are negligible in λ:

$$\left\{ (\mathsf{pp}, \mathsf{com}) : \begin{array}{l} \mathsf{pp} \leftarrow \mathsf{Setup}(1^\lambda, 1^\ell) \\ \mathsf{com} \leftarrow \mathsf{Com}(\mathsf{pp}, \mathbf{x}) \end{array} \right\} \quad \text{and} \quad \left\{ (\mathsf{pp}, \mathsf{com}) : \begin{array}{l} \mathsf{pp} \leftarrow \mathsf{Setup}(1^\lambda, 1^\ell) \\ \mathsf{com} \leftarrow \mathsf{Com}(\mathsf{pp}, \mathbf{y}) \end{array} \right\}.$$

(Computationally) Binding For any $\ell \in \mathbb{N}$ and any PPT adversary $\mathcal{A}$, it holds that

$$\Pr\left[\begin{array}{l} \quad \mathsf{Com}(\mathsf{pp}, \mathbf{x}; r) = \mathsf{Com}(\mathsf{pp}, \mathbf{y}; s) \\ \wedge\, \mathbf{x} \neq \mathbf{y} \end{array} \middle| \begin{array}{l} \mathsf{pp} \leftarrow \mathsf{Setup}(1^\lambda, 1^\ell) \\ ((\mathbf{x}, r), (\mathbf{y}, s)) \leftarrow \mathcal{A}(\mathsf{pp}) \end{array} \right] \leq \mathsf{negl}(\lambda).$$

Let $n, m, \log p, \log q = \mathsf{poly}(\lambda)$ with $p < q$. Consider the following commitment scheme construction for the message space $\mathbb{Z}_p$:

$\underline{\mathsf{Setup}(1^\lambda, 1^\ell)}$	$\underline{\mathsf{Com}(\mathsf{pp}, \mathbf{x} \in \mathbb{Z}_p^\ell; \mathbf{r} \in \mathbb{Z}_p^m)}$
$\mathbf{A} \leftarrow\!\$\ \mathbb{Z}_q^{n \times m}$	$\mathbf{c} := \mathbf{A} \cdot \mathbf{r} + \mathbf{B} \cdot \mathbf{x} \bmod q$
$\mathbf{B} \leftarrow\!\$\ \mathbb{Z}_q^{n \times \ell}$	$\mathsf{com} := \mathbf{c}$
$\mathsf{pp} := (\mathbf{A}, \mathbf{B})$	**return** com
return pp	

(a) Prove that the above commitment scheme is statistically hiding if $m > n \cdot \log_p q + \omega(\log n)$. The level of detail of the answer should be on a similar level as the lecture notes.

(b) Prove that the above commitment scheme is computationally binding under the $\mathsf{SIS}_{n,m+\ell,p,q}$ assumption. The level of detail of the answer should be on a similar level as the lecture notes.

(a) We want to show that the distributions

$$\mathcal{D}_{\mathbf{x}} := \left\{ (\mathbf{A}, \mathbf{B}, \mathbf{c}) : \begin{array}{c} \mathbf{A} \leftarrow\!\$\ \mathbb{Z}_q^{n \times m} \\ \mathbf{B} \leftarrow\!\$\ \mathbb{Z}_q^{n \times \ell} \\ \mathbf{r} \leftarrow\!\$\ \mathbb{Z}_p^m \\ \mathbf{c} := \mathbf{A} \cdot \mathbf{r} + \mathbf{B} \cdot \mathbf{x} \bmod q \end{array} \right\} \quad \text{and} \quad \mathcal{D}_{\mathbf{y}} := \left\{ (\mathbf{A}, \mathbf{B}, \mathbf{c}) : \begin{array}{c} \mathbf{A} \leftarrow\!\$\ \mathbb{Z}_q^{n \times m} \\ \mathbf{B} \leftarrow\!\$\ \mathbb{Z}_q^{n \times \ell} \\ \mathbf{s} \leftarrow\!\$\ \mathbb{Z}_p^m \\ \mathbf{c} := \mathbf{A} \cdot \mathbf{s} + \mathbf{B} \cdot \mathbf{y} \bmod q \end{array} \right\}$$

are statistically close.

Define an intermediate distribution

$$\mathcal{D} := \left\{ (\mathbf{A}, \mathbf{B}, \mathbf{c}) : \begin{array}{c} \mathbf{A} \leftarrow\!\$\ \mathbb{Z}_q^{n \times m} \\ \mathbf{B} \leftarrow\!\$\ \mathbb{Z}_q^{n \times \ell} \\ \mathbf{c} \leftarrow\!\$\ \mathbb{Z}_q^n \end{array} \right\}.$$

By the leftover hash lemma (Lecture 8, Lemma 8.8), the following distributions are statistically close:

$$\left\{ (\mathbf{A}, \mathbf{v}) : \begin{array}{c} \mathbf{A} \leftarrow\!\!\$\, \mathbb{Z}_q^{n\times m} \\ \mathbf{u} \leftarrow\!\!\$\, \mathbb{Z}_p^m \\ \mathbf{v} := \mathbf{A} \cdot \mathbf{u} \bmod q \end{array} \right\} \quad \text{and} \quad \left\{ (\mathbf{A}, \mathbf{v}) : \begin{array}{c} \mathbf{A} \leftarrow\!\!\$\, \mathbb{Z}_q^{n\times m} \\ \mathbf{v} \leftarrow\!\!\$\, \mathbb{Z}_q^n \end{array} \right\}$$

It follows that both $\mathcal{D}_{\mathbf{x}}$ and $\mathcal{D}_{\mathbf{y}}$ are statistically close to $\mathcal{D}$, and therefore statistically close to each other.

(b) Suppose the commitment scheme is not computationally binding, then there exists $\mathcal{A}$ which, on input $(\mathbf{A}, \mathbf{B})$, can find distinct $(\mathbf{x}, \mathbf{r}) \in \mathbb{Z}_p^\ell \times \mathbb{Z}_p^m$ and $(\mathbf{y}, \mathbf{s}) \in \mathbb{Z}_p^\ell \times \mathbb{Z}_p^m$ such that $\mathbf{Ar} + \mathbf{Bx} = \mathbf{As} + \mathbf{By} \bmod q$ with non-negligible probability. We construct an adversary $\mathcal{B}$ against $\mathsf{SIS}_{n,m+\ell,p,q}$ as follows.

On input an instance $(\mathbf{A} \| \mathbf{B}) \in \mathbb{Z}_q^{n\times(m+\ell)}$, $\mathcal{B}$ passes $(\mathbf{A}, \mathbf{B})$ to $\mathcal{A}$ and receives from it $((\mathbf{x}, \mathbf{r}), (\mathbf{y}, \mathbf{s}))$. It then returns $((\mathbf{r} - \mathbf{s})^\mathsf{T} \| (\mathbf{x} - \mathbf{y})^\mathsf{T})$.

By our assumption on $\mathcal{A}$, with non-negligible probability, we have $\mathbf{A}(\mathbf{r} - \mathbf{s}) + \mathbf{B}(\mathbf{x} - \mathbf{y}) = \mathbf{0} \bmod q$, where $\|\mathbf{r} - \mathbf{s}\| \leq p$ and $\|\mathbf{x} - \mathbf{y}\| \leq p$, i.e. $((\mathbf{r} - \mathbf{s})^\mathsf{T} \| (\mathbf{x} - \mathbf{y})^\mathsf{T})$ is a valid solution to the $\mathsf{SIS}_{n,m+\ell,p,q}$ instance $(\mathbf{A} \| \mathbf{B})$.