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 $(\mathbf{c}_0, c_1) \leftarrow \mathsf{ctxt}$
$\mathbf{u} \leftarrow\!\!\$\ \chi^m$	$\mathbf{s} \leftarrow\!\!\$\ \mathbb{Z}_q^n$	$\mathbf{u} \leftarrow \mathsf{sk}$
$\mathbf{v} := \mathbf{A} \cdot \mathbf{u} \bmod q$	$\mathbf{e}_0 \leftarrow\!\!\$\ \chi^m$	$\bar{x} := c_1 - \mathbf{c}_0^\intercal \cdot \mathbf{u} \bmod q$
$\mathsf{pk} := (\mathbf{A}, \mathbf{v})$	$e_1 \leftarrow\!\!\$\ \chi$	**return** $\left\lfloor \frac{p}{q} \cdot \bar{x} \right\rceil$
$\mathsf{sk} := \mathbf{u}$	$\mathbf{c}_0^\intercal := \mathbf{s}^\intercal \cdot \mathbf{A} + \mathbf{e}_0^\intercal \bmod q$	
return $(\mathsf{pk}, \mathsf{sk})$	$c_1 := \mathbf{s}^\intercal \cdot \mathbf{v} + e_1 + \lfloor q/p \rfloor \cdot x \bmod q$	// rounding to nearest integer
	$\mathsf{ctxt} := (\mathbf{c}_0, c_1)$	
	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 $q > \underline{q}'(\ell, m, p, \beta)$.

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 $\mathcal{A}$

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

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 $(\mathbf{A}, \mathbf{v}) \leftarrow \mathsf{pk}$	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.]

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

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

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

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