

Final exam

Exercises and questions can be answered in any order. Please write the number of the answered question.

Preliminaries.

- If S is a set, $x \leftarrow_{\S} S$ means that x is sampled uniformly at random from S . If χ is a distribution over S , χ^n denotes the distribution over S^n obtained by sampling n elements from χ independently.
- The dot product of two vectors $\vec{v}$, $\vec{w}$ is written $\langle \vec{v} | \vec{w} \rangle$.
- Throughout, $p > 2$ is a prime number. We identify $\mathbb{Z}_p = \mathbb{Z}/p\mathbb{Z}$ with the integers $\{-p + \lceil p/2 \rceil + 1, \dots, 0, \dots, \lceil p/2 \rceil\}$. An element of $\mathbb{Z}_p$ is considered “small” if its integer representative is close to 0.
- Let χ be a distribution over $\mathbb{Z}_p$. Let $\vec{s} \in \mathbb{Z}_p^n$. The *LWE distribution* of parameters n, p, χ and secret $\vec{s}$ is the distribution of pairs $(\vec{a}, \langle \vec{a} | \vec{s} \rangle + e)$, where $\vec{a}$ is sampled uniformly from $\mathbb{Z}_p^n$, and e is sampled from χ . The *decisional LWE problem* is the problem of distinguishing samples $(\vec{a}, \langle \vec{a} | \vec{s} \rangle + e)$ from the LWE distribution (for a fixed secret $\vec{s}$, sampled uniformly at the start) from uniform samples $(\vec{a}, \vec{b}) \in \mathbb{Z}_p^n \times \mathbb{Z}_p$.

Exercise 1. Fully Homomorphic Encryption using eigenvalues.

In a modernization effort, the ACME corporation wants to invent a fully homomorphic secret-key encryption scheme. Here is their idea. Let p be a prime number, and n a (non-zero) integer.

- The **secret key** is a uniformly random non-zero vector $\vec{s} \in \mathbb{Z}_p^n$.
- An **encryption** of a message $\mu \in \mathbb{Z}_p$ is a matrix $M \in \mathbb{Z}_p^{n \times n}$ chosen uniformly at random among matrices that satisfy $M\vec{s} = \mu\vec{s}$. We write $M \leftarrow \text{Enc}_{\vec{s}}(\mu)$.
- To **decrypt** a matrix $M \in \mathbb{Z}_p^{n \times n}$, if $\vec{s}$ is an eigenvector, compute the eigenvalue $\mu = \text{Dec}_{\vec{s}}(M)$ such that $M\vec{s} = \mu\vec{s}$. If $\vec{s}$ is not an eigenvector, then M is not a valid encryption, and $\text{Dec}_{\vec{s}}(M) = \perp$.

Question 1.1. Given only $M_1 \leftarrow \text{Enc}_{\vec{s}}(\mu_1)$ and $M_2 \leftarrow \text{Enc}_{\vec{s}}(\mu_2)$, without knowing the secret key $\vec{s}$, show that it is possible to compute a valid encryption of the messages $\mu_1 + \mu_2$, $\mu_1 \cdot \mu_2$, and $\mu_1 + c$ for any constant $c \in \mathbb{Z}_p$ (all computations are in $\mathbb{Z}_p$).

Question 1.2. Deduce that the scheme is fully homomorphic: given $M_i \leftarrow \text{Enc}_{\vec{s}}(\mu_i)$ for $1 \leq i \leq k$, and *any* function $f : \mathbb{Z}_p^k \rightarrow \mathbb{Z}_p$ (given in a suitable form), without knowing the secret key $\vec{s}$, show that it is possible to compute a valid encryption of $f(\mu_1, \dots, \mu_k)$.

Question 1.3. Show that the scheme is not secure: given a few encryptions of known (or chosen, if you prefer) messages, an adversary can find the secret key in polynomial time with a non-negligible probability of success. *Details.* As usual in cryptography, it is implicitly assumed that Enc and Dec are polynomial-time; in particular, n and $\log p$ must be polynomial. The probability of success of the adversary is not the focus of the question: sketching why it is non-negligible is enough, but don't spend too much time on it.

You have been hired to repair the scheme invented by ACME so that it is actually secure. To that end, let $\ell = \lceil \log_2 p \rceil$, and let $h : \mathbb{Z}_p \rightarrow \mathbb{Z}_p^\ell$ be the map that sends $x \in \mathbb{Z}_p$ to the vector encoding the binary decomposition of x viewed this time as an element of $\{0, \dots, p-1\}$ (least significant bit first). For example, if $p = 7$, we have $\ell = 3$, and:

$$h(3) = (1, 1, 0) \text{ because } 3 = 1 \cdot 2^0 + 1 \cdot 2^1 + 0 \cdot 2^2.$$

Let $H : \mathbb{Z}_p^{m \times m'} \rightarrow \mathbb{Z}_p^{m \times m' \ell}$ be the map that applies h to each coefficient of the input matrix, for example:

$$H \begin{pmatrix} 3 & 0 & 0 \\ 2 & 1 & 5 \end{pmatrix} = \begin{pmatrix} 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 \end{pmatrix}.$$

We also define a special matrix $G \in \mathbb{Z}_p^{m' \ell \times m'}$ via its transpose G^T :

$$G^T = \begin{pmatrix} 1 & 2 & \dots & 2^{\ell-1} & 0 & 0 & \dots & 0 & \dots & 0 & 0 & \dots & 0 \\ 0 & 0 & \dots & 0 & 1 & 2 & \dots & 2^{\ell-1} & \dots & 0 & 0 & \dots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \dots & 0 & 0 & 0 & \dots & 0 & \dots & 1 & 2 & \dots & 2^{\ell-1} \end{pmatrix}.$$

Question 1.4. Show that for all $M \in \mathbb{Z}_p^{m \times m'}$, $H(M)G = M$.

In the remainder, pick a dimension n , prime p , and a noise distribution χ over $\mathbb{Z}_p$ so that the decisional LWE problem is difficult (cf. preliminaries). We now introduce a modified fully-homomorphic encryption scheme, as follows. Set $m = (n + 1)\ell$ and $m' = n + 1$.

- As before, the secret key is a non-zero vector $\vec{s} \in \mathbb{Z}_p^n$, sampled uniformly at random. Let $\vec{s}' = (\vec{s} \parallel -1) \in \mathbb{Z}_p^{n+1}$ denote $\vec{s}$ concatenated with -1 .
- To **encrypt** a message $\mu \in \mathbb{Z}_2$ (identified with $\{0, 1\}$), sample $A \in \mathbb{Z}_p^{m \times n}$ uniformly, and sample $\vec{e} \in \mathbb{Z}_p^m$ from χ^m . Let $B = (A \parallel A\vec{s} + \vec{e}) \in \mathbb{Z}_p^{m \times (n+1)}$ denote A concatenated with the column $A\vec{s} + \vec{e}$. The encryption of μ is:

$$\text{Enc}_{\vec{s}}(\mu) = B + \mu G \in \mathbb{Z}_p^{m \times (n+1)}.$$

- To **decrypt** a matrix $M \in \mathbb{Z}_p^{m \times (n+1)}$, return 0 if every coordinate of $M\vec{s}'$ is less than $p/4$, 1 otherwise.

Question 1.5. Show that the scheme is correct: assuming χ is concentrated on small values, then:

$$\text{Dec}_{\vec{s}}(\text{Enc}_{\vec{s}}(\mu)) = \mu$$

holds with high probability. Concretely, we may assume $\Pr[|e| > p/4]$ is negligible when e is sampled from χ .

Question 1.6. Argue that the encryption of a message μ is indistinguishable from a uniformly random matrix in $\mathbb{Z}_p^{m \times (n+1)}$, based on the indistinguishability of the underlying decisional LWE problem.

Question 1.7. Given $M_1 \leftarrow \text{Enc}_{\vec{s}}(\mu_1)$ and $M_2 \leftarrow \text{Enc}_{\vec{s}}(\mu_2)$, show how to compute an encryption of $\mu_1 \cdot \mu_2$, without knowledge of $\vec{s}$. (We may assume without elaboration that a sum of a polynomial number of “small” values, such as those coming from χ , or $\{-1, 0, 1\}$, remains small.)

Hint: use H , otherwise similar to the original ACME scheme.

Question 1.8. Assuming we know how to perform additions homomorphically, is the scheme fully homomorphic, in the sense of question 1.2? If not, how can we transform it into a fully homomorphic encryption scheme?

Exercise 2. Authentication with LWE.

The ACME corporation is now designing an authentication system composed of a card and contactless receptor able to recognize the card. This system may be targeted by various adversaries. A *passive* adversary stealthily records all interactions between the card and receptor during its normal use. This adversary is able to observe as many interactions as desired. An *active* adversary has the same capabilities, but has also stolen the card, and is able to interact with the card in an arbitrary way. A *man-in-the-middle* attacker has stolen both the card and receptor, and can freely interact with both. This includes the ability to relay (and potentially tamper with) messages from one to the other. In all cases, the adversary’s goal is to recover the secret key stored within the card.

Basic protocol. Since the card is only able to perform very simple computations, the engineers at ACME decide to use LWE: after all, LWE only requires linear computations. Assume that the card and receptor both know an LWE secret $\vec{s}$, associated to parameters n, p, χ (cf. preliminaries). Let $m \geq n$ be an integer. The engineers first consider the following protocol.

1. The receptor sends to the card $A \leftarrow_{\$} \mathbb{Z}_p^{m \times n}$.
2. The card draws $\vec{e} \leftarrow \chi^m$ and sends back $\vec{b} = A\vec{s} + \vec{e}$.
3. The receptor accepts the card (with a green light) iff all coordinates of $\vec{b} - A\vec{s}$ are smaller than β for some bound $\beta < p/2$.

Question 2.1. Show that this protocol is secure against a passive adversary.

Question 2.2. Describe an attack by an active adversary.

Question 2.3. Propose a small modification of the protocol such that it achieves security against an active adversary, using a hash function in the Random Oracle Model. (A detailed proof is not required.)

Security against an active adversary. Since the card is very limited in computational abilities, the ACME engineers would like to avoid the use of a hash function. They design the following protocol. The common secret shared by the card and receptor now consists of two LWE secrets s_1, s_2 in $\mathbb{Z}_p^n$.

1. The card sends to the receptor $A_1 \leftarrow_{\$} \mathbb{Z}_p^{m \times n}$.
2. The receptor replies with $A_2 \leftarrow_{\$} \mathbb{Z}_p^{m \times n}$.
3. The card draws $\vec{e} \leftarrow \chi^m$ and sends $\vec{b} = A_1 \vec{s}_1 + A_2 \vec{s}_2 + \vec{e}$.
4. The receptor accepts iff all coordinates of $\vec{b} - A_1 \vec{s}_1 - A_2 \vec{s}_2$ are smaller than some bound $\beta < p/2$.

Question 2.4. Show that this protocol is secure against an active adversary.

Question 2.5. Show that it is insecure against a man-in-the-middle attacker.

Question 2.6. If we ignore the computational limitations of the card, and can use any cryptographic tool at our disposal, propose an authentication protocol that is secure against a man-in-the-middle attacker (no justification is required). Here, the adversary's goal is to “duplicate” the card, that is, to produce a new card that is also able to pass the authentication test.

An optimization by ACME™. After the fact, the ACME engineers realize that sampling from a discrete Gaussian χ is expensive on an embedded chip. The solution is simple: for χ , use the uniform distribution over $\{0, 1\} \subset \mathbb{Z}_p$. Let us go back to the original protocol, which only targets a passive adversary.

Question 2.7. Show that each time a passive adversary observes a transcript $A, A\vec{s} + \vec{e}$, they can deduce m quadratic equations over the coordinates $(s_1, \dots, s_n)$ of $\vec{s}$.

Hint: if e is sampled from χ , then it is a root of a simple quadratic equation.

Question 2.8. Using the previous question, show that a passive adversary that observes a polynomial number of transcripts can recover the secret $\vec{s}$.

Hint: a quadratic equation over unknowns $s_1, \dots, s_n$ is a linear equation over the monomials of degree at most 2 over the same unknowns. There is only a polynomial number of such monomials.