MID-TERM EXAM

This exam consists of two independent parts (lattice-based and code-based crypto). We would be grateful if you could write each part on a different copy. Each part starts with easier questions, related to the course. You are highly encouraged to treat both parts (you do not have to finish one part fully before starting the other one).

1 Part I: Code-based cryptography

1. Show that the largest possible dimension k of a binary linear code of length $n = 16$ and minimum distance $d = 3$ is 10. Rule out the existence of a code of dimension 11 by considering its parity-check matrix.

2. *Recall that the finite field $\mathbb{F}_8$ on 8 elements is an extension of the binary field $\mathbb{F}_2$ that can be defined by element α satisfying $\alpha^3 + \alpha + 1 = 0$. We have $\alpha^7 = 1$ and the non-zero elements of $\mathbb{F}_8$ are all powers of α and can be expressed as:*

$$1, \alpha, \alpha^2, \alpha^3 = \alpha + 1, \alpha^4 = \alpha^2 + \alpha, \alpha^5 = \alpha^2 + \alpha + 1, \alpha^6 = \alpha^2 + 1.$$

To multiply field elements one may apply polynomial (in α) multiplication and then use $\alpha^3 = \alpha + 1$ to decrease degrees. Alternatively, one may use the above correspondence with powers of α: for example $(\alpha^2+\alpha+1)(\alpha^2+1)$ is equal to $\alpha^5.\alpha^6 = \alpha^{11} = \alpha^4 = \alpha^2 + \alpha$. Similarly, we have $\alpha^3 + \alpha^6 = \alpha^4$.

Let $\boldsymbol{\alpha} = [0, 1, \alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^5, \alpha^6]$. What can you say about the parameters (length, dimension, minimum distance) of the *binary* Goppa code $\Gamma(\boldsymbol{\alpha}, 1 + X + X^2)$ defined by the vector $\boldsymbol{\alpha}$ and the Goppa polynomial $1 + X + X^2$?

(To minimize confusion you may use an alternative notation for $\boldsymbol{\alpha}$, such as $\vec{\alpha}$ or $\underline{\alpha}$.)

3. Let $\mathbf{G}$ be the 4×8 matrix whose four rows are $\mathbf{1}$ (the all-one vector) and $\boldsymbol{\alpha}, \boldsymbol{\alpha}^2, \boldsymbol{\alpha}^3$. Let C be the code over $\mathbb{F}_8$ generated by $\mathbf{G}$.

   What is the dimension and the minimum distance of C ?

   Show that $C^\perp = C$ and that $\mathbf{G}$ is also a parity-check matrix for C.

4. Let $\mathbf{H}$ be the matrix

$$\mathbf{H} = \begin{bmatrix} \mathbf{1} \\ \boldsymbol{\alpha} \\ \boldsymbol{\alpha}^2 \end{bmatrix} = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & \alpha & \alpha^2 & \alpha^3 & \alpha^4 & \alpha^5 & \alpha^6 \\ 0 & 1 & \alpha^2 & \alpha^4 & \alpha^6 & \alpha & \alpha^3 & \alpha^5 \end{bmatrix}.$$

   Let L be the code generated by the rows of $\mathbf{H}$ which we also call ℓ_0, ℓ_1, ℓ_2. Let $\Pi = C * L$. Show that $\mathbf{H}$ is a parity-check matrix for Π.

5. Let $\mathbf{y} = \begin{bmatrix} 1 & \alpha^2 & 0 & 0 & 0 & 0 & 1 & \alpha^6 \end{bmatrix}$. This is a codeword of C with two errors. Compute the vectors

$$\mathbf{y}\ell_0, \mathbf{y}\ell_1, \mathbf{y}\ell_2.$$

6. Let σ be the syndrome function associated with the matrix $\mathbf{H}$. Compute $\sigma(\mathbf{y}\ell_0)$.

7. We are given

$$\sigma(\mathbf{y}\ell_1) = \begin{bmatrix} \alpha^2 \\ 1 \\ \alpha^6 \end{bmatrix} \quad \text{and} \quad \sigma(\mathbf{y}\ell_2) = \begin{bmatrix} 1 \\ \alpha^6 \\ \alpha^6 \end{bmatrix}$$

   Check that $\lambda_0 = 1, \lambda_1 = \alpha^4, \lambda_2 = \alpha^2$ is a solution of the linear system

$$\lambda_0 \sigma(\mathbf{y}\ell_0) + \lambda_1 \sigma(\mathbf{y}\ell_1) + \lambda_2 \sigma(\mathbf{y}\ell_2) = 0.$$

8. Give a codeword ℓ of L that has 0 values on the two positions where $\mathbf{y}$ is in error. What are those coordinate positions ?

2 Part II: Lattice-based cryptography

2.1 Course questions

Let $\mathcal{L} \subset \mathbb{Z}^2$ be the lattice generated by (the columns of) the basis $B = \begin{pmatrix} 14 & -6 \\ -2 & 1 \end{pmatrix}$.

1. Show that $B' = \begin{pmatrix} -2 & 0 \\ 0 & 1 \end{pmatrix}$ is another basis of $\mathcal{L}$.
2. What are $\lambda_1(\mathcal{L})$ and $\lambda_2(\mathcal{L})$?
3. Give a basis of the dual lattice $\widehat{\mathcal{L}}$.
4. Let $X = \mathbb{F}_5^2$. Let D_1 be the distribution over X obtained by sampling $z \leftarrow \text{Uniform}(\mathbb{F}_5^2)$ and returning $x = B_1 \cdot z \in X$, for $B_1 = \begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix} \in \mathbb{F}_5^{2\times 2}$. And let D_2 be the distribution over X obtained by sampling $z \leftarrow \text{Uniform}(\mathbb{F}_5^2)$ and returning $x = B_2 \cdot z \in X$, for $B_2 = \begin{pmatrix} 1 & 2 \\ 1 & 3 \end{pmatrix} \in \mathbb{F}_5^{2\times 2}$. Describe a polynomial time algorithm that distinguishes between D_1 and D_2 with advantage at least $4/5$.
   Recall that the advantage of some algorithm $\mathcal{A}$ in distinguishing between D_1 and D_2 is defined as

$$\text{Adv}_{D_1,D_2}(\mathcal{A}) := \left|\Pr_{x\leftarrow D_1}(\mathcal{A}(x) = 1) - \Pr_{x\leftarrow D_2}(\mathcal{A}(x) = 1)\right|.$$

2.2 Image and kernel lattices

Let $q \geqslant 2$ be a prime integer, $m \geqslant r \geqslant 1$ be integers, and $A \in (\mathbb{Z}/q\mathbb{Z})^{m\times r}$. Recall that the image and kernel lattices of A are defined by

$$\Lambda(A) = \{v \in \mathbb{Z}^m \mid \exists w \in \mathbb{Z}^r,\ v = Aw \bmod q\}$$
$$\Lambda^\perp(A) = \{v \in \mathbb{Z}^m \mid v^T A = 0 \bmod q\}.$$

1. *What is $\text{rk}(\Lambda(A))$ and $\text{rk}(\Lambda^\perp(A))$? (justify your answer)*
2. *Assume that A has rank r, exhibit a matrix $H \in (\mathbb{Z}/q\mathbb{Z})^{m\times(m-r)}$ such that $\Lambda(A) = \Lambda^\perp(H)$.*

2.3 Learning with errors

Let q be some prime integer, $m \geqslant r \geqslant 1$ and $1 \leqslant B < q/2$ be integers, and let us fix some matrix $A \in (\mathbb{Z}/q\mathbb{Z})^{m\times r}$. Define the LWE distribution with matrix A (written $D_{\text{LWE}}(A)$) as the distribution over $(\mathbb{Z}/q\mathbb{Z})^m$ obtained by sampling s uniformly in $(\mathbb{Z}/q\mathbb{Z})^r$ and e uniformly in $\{-B,\dots,B\}^m$ and outputting $b = As + e \bmod q$. The objective of the exercise it to show that the knowledge of a short vector in $\Lambda^\perp(A)$ allows to distinguish the distribution $D_{\text{LWE}}(A)$ from the uniform distribution over $(\mathbb{Z}/q\mathbb{Z})^m$.

1. *Let $w \in \mathbb{Z}^m$ be a non-zero vector in $\Lambda^\perp(A)$. Assume that $|\langle w, e\rangle| \leqslant q/4 - 1$ for all $e \in \{-B,\dots,B\}^m$. Describe a polynomial time algorithm $\mathcal{A}$ that uses w to distinguish between the distributions $D_{\text{LWE}}(A)$ and $\text{Uniform}((\mathbb{Z}/q\mathbb{Z})^m)$ with advantage at least $1/2$.*
2. *Give an upper bound on $\|w\|$ (depending on (some of) the LWE parameters q, m, r and B) that ensures that $|\langle w, e\rangle| \leqslant q/4 - 1$ for all $e \in \{-B,\dots,B\}^m$.*