TTM4135 Worksheet 9: Post-Quantum Cryptography

Tjerand Silde and Emil August Hovd Olaisen
{tjerand.silde, emil.august.olaisen}@ntnu.no

Spring 2026

This exercise is an extension of Worksheet 7, with additional tasks about post-quantum cryptography. The tasks dive deeper into the mathematics of lattice-based cryptography. In particular, we explore two schemes: a public-key encryption scheme closely resembling ML-KEM / CRYSTALS-Kyber, and a digital signature algorithm closely resembling ML-DSA / CRYSTALS-Dilithium.

The tasks are somewhat more demanding. If you struggle, feel free to skip certain parts. The questions are designed so that you can still use results from previous tasks you have not completed. This worksheet is intended to help you better understand lattice-based cryptography, but it will not be directly relevant for the exam.

Outline:

- Task 1: properties of the polynomial ring $R_{q,d}$,
- Task 2: a module-based public-key encryption scheme,
- Task 3: communication costs,
- Task 4: computational efficiency,
- Task 5: motivation for using modules,
- Task 6: a module-based digital signature scheme.

The ring $R_{q,d}$. An element $a \in R_{q,d}$ is a vector

$$a = (a_0, a_1, \ldots, a_{d-1}), \quad a_i \in \mathbb{Z}_q.$$

Addition is component-wise. Multiplication is defined using matrix multiplication:

$$a \cdot b = \begin{bmatrix} a_0 & -a_{d-1} & \ldots & -a_1 \\ a_1 & a_0 & \ldots & -a_2 \\ \vdots & \vdots & \ddots & \vdots \\ a_{d-1} & a_{d-2} & \ldots & a_0 \end{bmatrix} \begin{bmatrix} b_0 \\ b_1 \\ \vdots \\ b_{d-1} \end{bmatrix}.$$

Equivalently,

$$(a \cdot b)_i = \sum_{j=0}^{i} a_{i-j} b_j - \sum_{j=i+1}^{d-1} a_{d+i-j} b_j.$$

You may assume the following properties without proof:

$$a \cdot b = b \cdot a, \tag{1}$$
$$a \cdot (b \cdot c) = (a \cdot b) \cdot c, \tag{2}$$
$$a \cdot (b + c) = a \cdot b + a \cdot c. \tag{3}$$

Thus $(R_{q,d}, +, \cdot)$ is a commutative ring. Vectors and matrices over $R_{q,d}$ behave exactly as over the integers. We write $\mathbf{s} \in [\beta]^n$ to mean that each coefficient of every entry $s_i \in R_{q,d}$ lies in $\{-\beta, \ldots, \beta\}$.

1. (a) Show that computing $a \cdot b$ for $a, b \in R_{q,d}$ requires d^2 multiplications and $d(d-1)$ additions in $\mathbb{Z}_q$.
   (b) Let $s, e \in [\beta]$. Show that $se \in [d\beta^2]$.
   (c) Let $\mathbf{s}, \mathbf{e} \in [\beta]^n$. Show that $\mathbf{se} \in [dn\beta^2]$.

Public-key encryption over modules. We use $R_{q,d}$ to encrypt messages $M \in \{0,1\}^d$ by interpreting M as a polynomial with binary coefficients.

KGen: sample $\mathbf{s}, \mathbf{e}_1 \leftarrow\!\$\ [\beta]^n$ and output

$$\mathsf{sk} = \mathbf{s}, \qquad \mathsf{pk} = (\mathbf{A} \leftarrow\!\$\ R_{q,d}^{n\times n},\ \mathbf{t} = \mathbf{As} + \mathbf{e}_1).$$

Enc(pk, M): sample $\mathbf{r}, \mathbf{e}_2 \leftarrow\!\$\ [\beta]^n$, $e_3 \leftarrow\!\$\ [\beta]$, and output

$$\mathbf{u}^\intercal = \mathbf{r}^\intercal \mathbf{A} + \mathbf{e}_2^\intercal, \quad v = \mathbf{r}^\intercal \mathbf{t} + e_3 + M\lfloor q/2 \rfloor.$$

Dec(sk, c): output $M' = v - \mathbf{u}^\intercal \mathbf{s}$.

2. (a) Show that
$$M' = \mathbf{r}^\intercal \mathbf{e}_1 - \mathbf{e}_2^\intercal \mathbf{s} + e_3 + M\lfloor q/2 \rfloor.$$
   (b) Show that $M' = e + M\lfloor q/2 \rfloor$ with
$$e \in [2dn\beta^2 + \beta].$$
   (c) Explain why each coefficient of M can be recovered correctly if
$$2dn\beta^2 + \beta < \frac{q}{4}.$$
   (d) Define an explicit decoding function
$$\mathsf{Decode} : \mathbb{Z}_q \to \{0,1\},$$
   and explain how it is applied coefficient-wise to recover M from M'.

3. (a) How many bits are required to store elements of $R_{q,d}$, $R_{q,d}^n$, and $R_{q,d}^{n\times n}$? Use this to compute the sizes of the public key, secret key, and ciphertext.

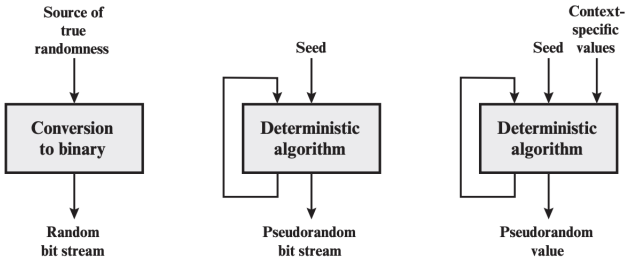

Figure 8.1 Random and Pseudorandom Number Generators

Figure 1: Generating random values from a seed using a TRNG, PRNG, and PRF.

   (b) Recall Figure 1. Explain how the public key can be compressed by transmitting a seed instead of $\mathbf{A}$. Why can this not be done for $\mathbf{t}$? What about the secret key and ciphertext?

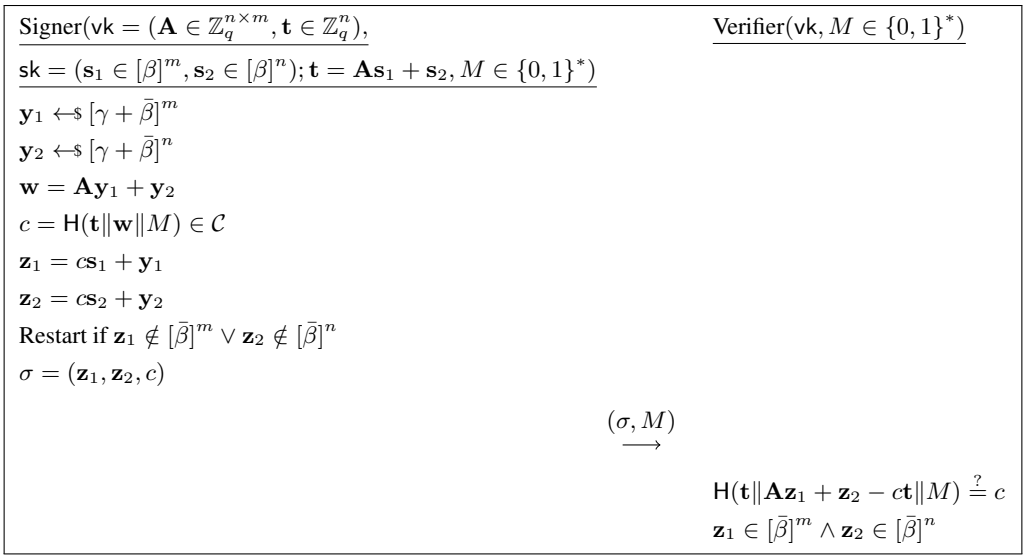

Figure 2: A lattice-based Schnorr-type signature.

(c) Assume $\mathsf{LWE}_{n_1,q,\beta}$ and $\mathsf{MLWE}_{n_2,d,q,\beta}$ are equally hard when $n_1 = n_2 d$. Explain how increasing d and decreasing n affects the transmission size and message length.

4. (a) Count the number of multiplications in $\mathbb{Z}_q$ required to compute:
   - $\mathbf{ab}$ for $\mathbf{a}, \mathbf{b} \in R_{q,d}^n$,
   - $\mathbf{Ab}$ for $\mathbf{A} \in R_{q,d}^{n\times n}$.

   (b) Count the number of vector and matrix-vector multiplications in KGen, Enc, and Dec.

   (c) What is the total cost (in $\mathbb{Z}_q$ multiplications) per bit of M?

5. Let $\beta = 1$ and $q = 3329$. Assume $\mathsf{LWE}_{602,q,\beta}$ is secure and we wish to exchange a 256-bit key.

   (a) Explain why choosing $n = 3$ and $d = 256$ is reasonable.

   (b) Show that correct decryption is not unconditionally guaranteed.

   (c) Estimate the probability that decryption fails.

6. Consider the lattice-based Schnorr-type signature scheme in Figure 2.

   (a) Show that the signature scheme is correct when it does not reject the signature.

   (b) What is the size of the challenge space $\mathcal{C}$, defined as the subset of polynomials in $[1]^d$ in which η elements are non-zero, and how does this impact security?

   (c) Explain why $\mathbf{z}_1$ and $\mathbf{z}_2$ are bounded before rejection and by what values.