An Introduction to Number Theoretic Transform in Post-Quantum Lattice Cryptography

EE5163 Advanced Digital Signal Processing: Final Report

Lo-Chun, Chou
R13922136 [1]

[1]Department of Computer Science, National Taiwan University

June 10, 2025

Abstract

In the domain of post-quantum cryptography (PQC), lattice-based cryptography stands out as one of the most promising approaches due to its balanced performance between security and efficiency. A key computational task in these schemes is polynomial multiplication, where Number Theoretic Transform (NTT) is particularly effective for this task. NTT achieves quasilinear time complexity$O(n \log n)$, similar to the Fast Fourier Transform (FFT), but operates entirely over integers, thus avoiding rounding errors from floating-point arithmetic. In this report, we explore the foundations of NTT, drawing from some recent research papers, and provide an overview of its principles, implementation strategies, and applications in lattice-based cryptographic systems.

1 Introduction

1.1 Motivation

While both Number Theoretic Transform (NTT) and Fast Fourier Transform (FFT) are used in polynomial multiplication, NTT is a relative new approach, which is often not covered in the textbooks. This lack of accessible resources is also noted in the reference work *A Beginner's Guide to Number Theoretic Transforms (NTTs)*, where the authors mentioned that the lack of guidance and tutorial available in one place is the main obstacle for learning NTT[4], which is also the reason why they wrote the material.

While the beginner's guide offers a solid introduction to the basic ideas of NTT, it occasionally assumes familiarity with advanced mathematical concepts. Therefore, we expand upon its foundation by including additional mathematical background, clarifying essential concepts such as rings, primitive roots, and modular arithmetic, so all mathematical backgrounds that are needed but unfamiliar to a non-math-major would be covered.

Furthermore, we conclude with a brief example introducing the applications of NTT in real-world scenarios, so that we can move beyond the theoretical part, gaining a full picture of the concept of NTT.

1.2 Polynomial Multiplication in Cryptographic Systems

1.3 Report Structure

2 Preliminaries: Mathematical Foundations of the Number Theoretic Transform

2.1 Rings and quotient rings

To properly define primitive roots and illustrate the structure of the Number Theoretic Transform (NTT), it is necessary to first introduce the concepts of rings, ideals, and quotient rings.

These algebraic structures are needed because they provide the foundation for polynomial multiplication in NTT, since in order to do polynomial multiplication for polynomials $G(x)$ and $H(x)$, both of them must belong to the same quotient ring. Due to the fact that quotient rings are constructed on the notions of rings and ideals, we begin by briefly reviewing these foundational concepts.

Definition 2.1 (Ring, [3], pp. 85–86)**.** *A set R is called a **ring** if it has two binary operations, written as addition and multiplication, satisfying the following axioms for all $a, b, c \in R$:*

1. $a + b = b + a$.
2. $a + (b + c) = (a + b) + c$.
3. *An element* 0 *in* R *exists such that* $0 + a = a$ *for all* a.
4. *For each* $a \in R$ *an element* $-a \in R$ *exists such that* $a + (-a) = 0$.
5. $a(bc) = (ab)c$.
6. *An element* 1 *in* R *exists such that* $1 \cdot a = a = a \cdot 1$ *for all* a.
7. $a(b + c) = ab + ac$ *and* $(b + c)a = ba + ca$.

Definition 2.2 (Ideal, [2], p. 1)**.** *A subset A of a ring R (commutative, with 1) is said to be an **ideal** if*

1. $0 \in A$ *and* $a, b \in A \Rightarrow a + b, -a \in A$ *(so A is an additive subgroup of R).*

2. $(a \in A, r \in R)\ ra \in A$.

Intuitively, an ideal is a special subset of a ring, which includes the zero element and is closed under addition, also, it would satisfy that every multiple of an element in A is also in A.

Definition 2.3 (Quotient Ring, [2], p. 3)**.** *Let A be an ideal in the ring R. The* ***quotient ring*** *R/A is defined as follows:*

$$\begin{aligned} \mathit{Set} &\coloneqq \{r + A \mid r \in R\} \qquad \textit{(additive cosets)} \\ 0 &\coloneqq A \\ 1 &\coloneqq 1 + A \\ (r + A) + (s + A) &\coloneqq (r + s) + A \\ (r + A)(s + A) &\coloneqq (rs) + A \end{aligned}$$

where $r, s \in R$.

To be simple, a quotient ring R/A is formed by grouping elements of the ring R into disjoint sets called cosets, where each coset has the form $r + A = \{r + a \mid r \in R\}$. These cosets partition the ring in a way that reflects the structure of the ideal A.

One may wonder why quotient rings are introduced in the literature of NTT. The idea is that, we treat every element in the same coset as "equivalent", just like in modular arithmetic.

An important example would be $\mathbb{Z}/n\mathbb{Z}$, which represents the ring of integers modulo n, where all numbers differed by a multiple of n are considered the same. In the same way, a quotient ring allows us to "mod out" an ideal A and treat every element in A as zero, simplifying the structure of the ring and allowing new algebraic manipulations.

To illustrate what this means, we can consider the following example:

If given $R = \mathbb{Z}$ and $A = 2\mathbb{Z}$, which means that we have the ring of integers and ideal of even numbers, respectively. Then $R/A = \mathbb{Z}/2\mathbb{Z}$ would be defined as having the set:

$$\{r + 2\mathbb{Z} \mid r \in \mathbb{Z}\}$$

Some of its cosets would be:

$$\begin{aligned} \{1 + 2\mathbb{Z}\} &= \{1, 3, 5, 7, \ldots\} \\ \{2 + 2\mathbb{Z}\} &= \{2, 4, 6, 8, \ldots\} \\ \{3 + 2\mathbb{Z}\} &= \{3, 5, 7, 9, \ldots\} \\ &\vdots \end{aligned}$$

However, we can see that $\{1 + 2\mathbb{Z}\}$ and $\{3 + 2\mathbb{Z}\}$ are the same, thus there would actually be only two cosets:

$$\{0 + 2\mathbb{Z}\} = \{0, 2, 4, 6, \ldots\}$$
$$\{1 + 2\mathbb{Z}\} = \{1, 3, 5, 7, \ldots\}$$

Thus, if we have two elements r_1 and r_2 in the same coset, say $0 + 2\mathbb{Z}$, then we can write:

$$r_1 = 0 + 2z_1 \quad \text{for some } z_1 \in \mathbb{Z}$$
$$r_2 = 0 + 2z_2 \quad \text{for some } z_2 \in \mathbb{Z}$$

and we can see that $r_1 \equiv r_2 \pmod{2\mathbb{Z}}$ since $r_1 - r_2 = 2(z_1 - z_2) \in 2\mathbb{Z}$. This can also be written as $r_1 - r_2 \equiv 0 \pmod{2\mathbb{Z}}$, and $r_1 - r_2 \in 2\mathbb{Z}$. What this means is that, for any element in the ideal $2\mathbb{Z}$, it would be treated as equivalent to 0 in the quotient ring $\mathbb{Z}/2\mathbb{Z}$.

2.2 Modular Arithmetic and Roots of Unity

In this subsection, we first introduce the concept of residue class modulo n, in order to be used in defining $\mathbb{Z}_n$, then we further define the order of an integer under modulo n, so that primitive root can be defined. The reason why primitive root is needed is that it is used to construct the NTT matrix, which we would talk about the details in the next subsection.

Definition 2.4 (Residue Class Modulo n, [3], p. 30)**.** *If a is an integer, its equivalent class $[a]$ with respect to congruence modulo n is called its* ***residue class modulo*** *n, and we write $\overline{a} = [a]$ for convenience:*

$$\overline{a} = [a] = \{x \in \mathbb{Z} \mid x \equiv a \pmod{n}\}.$$

Intuitively saying, after we selected an integer n to be the modulus, we can divide all the integers into n classes, each class is a set of integers that having the same remainder when divided by n.

Therefore, for any integer n, there are n residue classes modulo n, which are $\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{n-1}$, if we collect all of these residue classes as a set, then we get the set of integers modulo n, which is defined as follows:

Definition 2.5 (Integers Modulo n, [3], p. 30)**.** *The set of all residue classes modulo n is denoted*

$$\mathbb{Z}_n = \{\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{n-1}\}.$$

and is called the set of ***integers modulo*** *n.*

Before introducing the definition of primitive root, we first define the order of an integer modulo n as follows:

Definition 2.6 (Order of an Integer Modulo n , [1], p. 147)**.** *Let $n > 1$ and $\gcd(a, n) = 1$. The **order of** a **modulo** n is the smallest positive integer k such that*

$$a^k \equiv 1 \pmod{n}.$$

Using the definition of order, we can then define the primitive root as follows:

Definition 2.7 (Primitive Root, [1], p. 150)**.** *If $\gcd(a, n) = 1$ and a is of order $\varphi(n)$ modulo n, then a is called a **primitive root** of the integer n. Equivalently, a is a primitive root modulo n if*

$$a^{\varphi(n)} \equiv 1 \pmod{n} \quad \textit{but} \quad a^k \not\equiv 1 \pmod{n} \quad \forall\ 1 \leq k < \varphi(n).$$

Note that the primitive root may not be unique, and since we use the primitive root to construct the NTT matrix, the NTT of a polynomial may not be unique and would depend on the choice of the primitive root. [4, pp. 5–6]

In the context of NTT, we choose the modulus n to be a prime number, let it be denoted as q, and under the assumption that our polynomials $G(x)$ and $H(x)$ are of degree $n - 1$, we try to find primitive roots ω that would satisfy:

$$\omega^n \equiv 1 \pmod{q} \quad \text{and} \quad \omega^k \not\equiv 1 \pmod{q} \quad \forall\ 1 \leq k < n.$$

Which means that if we're trying to do convolution of polynomials of degree 3, then we should find a primitive root that would be congruent to 1 when raised to the power of 4, under some choice of modulus q.

And such ω is called the **primitive n-th root of unity** in the ring $\mathbb{Z}_q$. [4, p. 4]

2.3 Cyclotomic Polynomials

From the previous subsections, we have already defined the quotient ring and the primitive root. We then introduce the concept of cyclotomic polynomials, which is chosen to construct the ideal of the quotient ring. [**?**, p. 3]

Definition 2.8 (Cyclotomic Polynomial, [**?**], p. 11)**.** *The n-th **cyclotomic polynomial** $\Phi_n(x)$ is defined by*

$$\Phi_n(x) = \prod_{\omega \in P(n)} (x - \omega)$$

where $P(n)$ denotes the set of all primitive n-th roots of unity.

But how do we connect the n-th cyclotomic polynomial to construct the ideal of the quotient ring? To answer this question, we first introduce our focus, the two widely used rings in lattice-based schemes are:

$$\mathbb{Z}_q[x]/(x^n - 1) \quad \text{and} \quad \mathbb{Z}_q[x]/(x^n + 1)$$

[?, p. 3]

Here we could see that the ideals of the quotient rings are $(x^n - 1)$ and $(x^n + 1)$, respectively. To construct these two ideals, we need the following proposition:

Proposition 2.1 (Fundamental Relation, [?], p. 12)**.** *For any positive integer n,*

$$x^n - 1 = \prod_{d|n} \Phi_d(x)$$

The above proposition shows that, if we are to choose the ideal with the form $(x^n - 1)$, then we could construct it by finding all the factors d that could divide n, then multiply all the d-th cyclotomic polynomials together.

To see how this works, we can consider the example of having $n = 4$, with the aid of the following table:

n	$\Phi_n(x)$	n	$\Phi_n(x)$
1	$x - 1$	6	$x^2 - x + 1$
2	$x + 1$	7	$x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$
3	$x^2 + x + 1$	8	$x^4 + 1$
4	$x^2 + 1$	9	$x^6 + x^3 + 1$
5	$x^4 + x^3 + x^2 + x + 1$	10	$x^4 - x^3 + x^2 - x + 1$

Table 1.1: The first ten cyclotomic polynomials.

Figure 1: Cyclotomic Table. Source: [?, p. 11]

We can see that, for $n = 4$, the factors of n are $1, 2, 4$, and the corresponding cyclotomic polynomials are:

$$\Phi_1(x) = x - 1$$
$$\Phi_2(x) = x + 1$$
$$\Phi_4(x) = x^2 + 1$$

According to the fundamental relation, we have:

$$\begin{aligned} x^4 - 1 &= \prod_{d|4} \Phi_d(x) \\ &= \Phi_1(x)\Phi_2(x)\Phi_4(x) \\ &= (x-1)(x+1)(x^2+1) \\ &= (x^2-1)(x^2+1) \\ &= x^4 - 1 \end{aligned}$$

which matches the result in the table.

This could easily be generalized to the case when we choose the ideal with the form $(x^n + 1)$. Observe that:

$$x^{2n} + 1 = (x^n + 1)(x^n - 1)$$

So we have:

$$x^n + 1 = \frac{x^{2n} + 1}{x^n - 1}$$

Using the proposition of the fundamental relation, we have:

$$\begin{aligned} x^{2n} - 1 &= \prod_{d|2n} \Phi_d(x) \\ x^n - 1 &= \prod_{d|n} \Phi_d(x) \end{aligned}$$

Therefore, we can rewrite the above equation* as:

$$x^n + 1 = \frac{x^{2n} + 1}{x^n - 1} = \frac{\prod_{d|2n} \Phi_d(x)}{\prod_{d|n} \Phi_d(x)} = \prod_{d \nmid n,\ d|2n} \Phi_d(x)$$

This means that, if we are to choose the ideal with the form $(x^n + 1)$, then we could construct it by finding all the factors d that could divide $2n$ but not n, then multiply all the d-th cyclotomic polynomials together.

In particular, if n is of the special form:

$$n = 2^k \qquad \text{for some } k \in \mathbb{N}$$

then we have:

$$x^{2^k} + 1 = \prod_{d \nmid 2^k,\ d|2^{k+1}} \Phi_d(x) = \Phi_{2^{k+1}}(x) = \Phi_{2n}(x)$$

Therefore, we arrived at the conclusion that, if we are to choose the ideal with the form $(x^n + 1)$ with $n = 2^k, \quad k \in \mathbb{N}$, then we could construct it by finding the $2n$-th cyclotomic polynomial $\Phi_{2n}(x)$.

This property is quite useful, so in the context of PQC, the chosen ring is mostly $\mathbb{Z}_q[x]/(x^n + 1)$ instead of $\mathbb{Z}_q[x]/(x^n - 1)$. [4, p. 8] And we further denote the $2n$-th root of unity as ψ, with the detailed definition shown below:

Definition 2.9 ($2n$-th Root of Unity, [4], p. 8)**.** *Let $\mathbb{Z}_q$ be an integer ring modulo q, and $n-1$ is the polynomial degree of $G(x)$ and $H(x)$ and ω is the primitive n-th root of unity. Define ψ as the* ***primitive*** *$2n$-**th root of unity***

$$\iff \psi^2 \equiv \omega \pmod{q} \quad \textit{and} \quad \psi^n \equiv -1 \pmod{q}$$

With all of these defined, we can then move on to the next section, where the definition of the Number Theoretic Transform (NTT) would be introduced based on the above definitions.

3 The Number Theoretic Transform (NTT)

3.1 Definition of Forward and Inverse NTT

In the previous subsection, we introduced the formulation of the two widely used quotient rings in lattice-based schemes, if we focus on the case that the ideal is chosen to be of the form $(x^n + 1)$, we then denote them by R and R_q, respectively:

$$R = \mathbb{Z}[x]/(x^n + 1) \quad \text{and} \quad R_q = \mathbb{Z}_q[x]/(x^n + 1)$$

Assume the special case where $n = 2^k$, and consider ω to be a primitive n-th root of unity in $\mathbb{Z}_q$ which

$$\omega^n \equiv 1 \pmod{q} \quad \text{where} \quad q \equiv 1 \pmod{2n},\ q : \text{prime}$$

we could define the NTT of a polynomial $G(x) \in R_q$ as:

$$\hat{G} = \mathbf{NTT}(G(x)) = \sum_{i=0}^{n-1} G[i]\omega^{ij} \pmod{q}$$

where $\mathbf{NTT}_q$ is the NTT operator in the ring $\mathbb{Z}_q$.

3.2 Types of Convolutions and Equivalent NTTs

3.3 Comparison with Fast Fourier Transform (FFT)

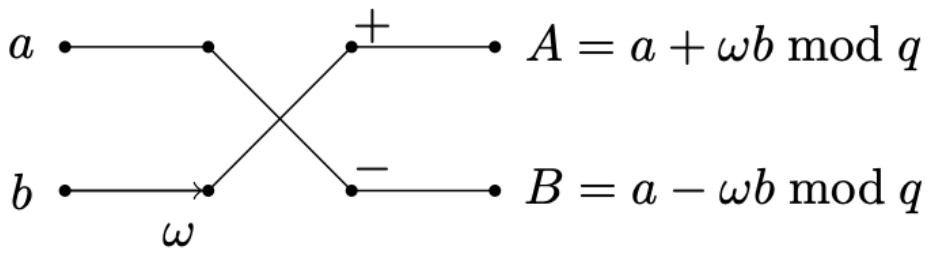
4 Limitations of NTT

4.1 Parameter Restrictions and Ring Compatibility

4.2 Negative Wrapped Convolution and Modulus Conditions

4.3 Hardware Bottlenecks and Communication Overheads

In hardware implementations of the Number Theoretic Transform (NTT), one major source of inefficiency arises from the intricate data communication between adjacent computation stages.



(a) Cooley-Tukey butterfly

Figure 2: Butterfly Diagram of the Cooley–Tukey NTT Algorithm. Source: `https://k.rypto.cafe/assets/images/misc/ct_butterfly.png`

As visualized in the butterfly diagram of the Cooley–Tukey NTT algorithm, multiple stages are required to process even small-length inputs, and each stage introduces data dependencies that result in extensive data movement. This leads to increased wiring complexity and higher area and energy overhead when deploying NTT on ASIC or FPGA-based accelerators. For in-memory computing architectures, these inefficiencies translate into additional shift operations to align data with memory bitlines, further increasing latency and hardware cost.

References

[1] D.M. Burton. *Elementary Number Theory.* Tata McGraw-Hill Publishing Company Limited, 2006.

[2] E.V. Flynn. Rings & arithmetic 3: Ideals and quotient rings. Lecture notes, University of Oxford, 2005. Lectures for Part A of Oxford FHS in Mathematics and Joint Schools.

[3] W. Keith Nicholson. *Introduction to Abstract Algebra.* Wiley Publishing, 4th edition, 2012.

[4] Ardianto Satriawan, Rella Mareta, and Hanho Lee. A complete beginner guide to the number theoretic transform (ntt), 2024. Last accessed 9 June 2025.