IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 2, July 2024

Optimizing Number Theoretic Transform Techniques for Enhanced Lattice-Based Cryptography

Gauswami Rohitgiri Mahendragiri[1] and Dr. Rajeev Kumar [2]
Research Scholar, Department of Math[1]
Associate Professor, Department of Math[2]
Sunrise University, Alwar, Rajasthan, India

Abstract: *Conventional public key cryptography will be broken by a massive quantum computer. An alternative for safeguarding communications in the age of quantum computing is lattice-based cryptography. One appealing method for effectively handling polynomial multiplication is the Number Theory Transform (NTT).For many systems, including battery-operated devices and Internet of Things (IoT) gadgets, low power consumption is essential. However, further study is needed to develop NTTs that are low power and efficient. The suggested design may be implemented using inexpensive single-port RAM and only requires n log (n) clock cycles*

Keywords: Number Theoretic Transform (NTT), Modular Arithmetic, Polynomial Multiplication

I. INTRODUCTION

Public-key cryptography is the foundation for establishing secure communication between several parties. All forms of communication are at risk from quantum computers. One practical solution for defending communication channels against a quantum attack is post-quantum cryptography. The Fast Fourier Transform has a finite field variation called the NTT. Two polynomials are converted into the spectral domain so they may be multiplied point wise. The performance bottleneck of lattice-based encryption is circumvented by the NTT. It will be possible for a quantum computer to crack conventional public-key encryption. Lattice-based encryption has emerged as a substitute for traditional methods of communication security in the era of quantum computing. For instance, a common technique for rapidly multiplying polynomials is the Number Theoretic Transform. Post quantum cryptography is standardized by the National Institute of Standards and Technology and the National Security Agency. A group of cryptographic techniques known as QPC are impervious to known quantum computer attacks. Lattice-based encryption, which is based on difficult lattice problems, offers a reasonable trade-off between security and efficiency. Consequently, it is essential to optimize the NTT in order to enable and make feasible lattice-based post-quantum cryptography. With several NTT configuration settings, the NTT architecture is flexible. A useful method for making the multiplication of two large polynomials simpler is the Number Theoretic Transform. The NTT is a finite-field variation of the Fast Fourier Transform.

NTT

$$X(k) = \sum_{i=0}^{N-1} x(i) w^{ik} \pmod{M} \qquad k = 0,\ 1,\ \ldots N-1 \qquad \ldots 1$$

Inverse NTT

$$Y(k) = \sum_{k=0}^{N-1} x(k) w^{-ik} \pmod{M^{-1}} \qquad k = 0,\ 1,\ \ldots N-1 \qquad \ldots 2$$

This paper provides the first NTT ASIC design for fast, low-power, and secure lattice-based cryptography. Our proposed approach may be implemented with low-cost single-port RAM and only requires n log clock cycles for the forward and inverse NTT.

Copyright to IJARSCT
www.ijarsct.co.in
DOI: 10.48175/568

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 2, July 2024

II. LITERATURE REVIEW

Numerous signal processing applications, including as FIR filters, image filtering, and homomorphic image enhancement, have made use of the NTT. Furthermore, the NTT necessitates an extra reduction module and is utilized in lattice-based encryption to alter more important vectors.

Methodology

This section shows the methods employed in achieving the aim and objectives of this paper

Post-Quantum Cryptography (PQC)

The PQC methods are typically implemented utilizing Lattice-Based Cryptography, Code-Based Cryptography, Multivariate Cryptography Protocols, or Hash-Based Signature methods, as seen in Figure 1.Figure 1 will provide a quick discussion of the PQC methods.

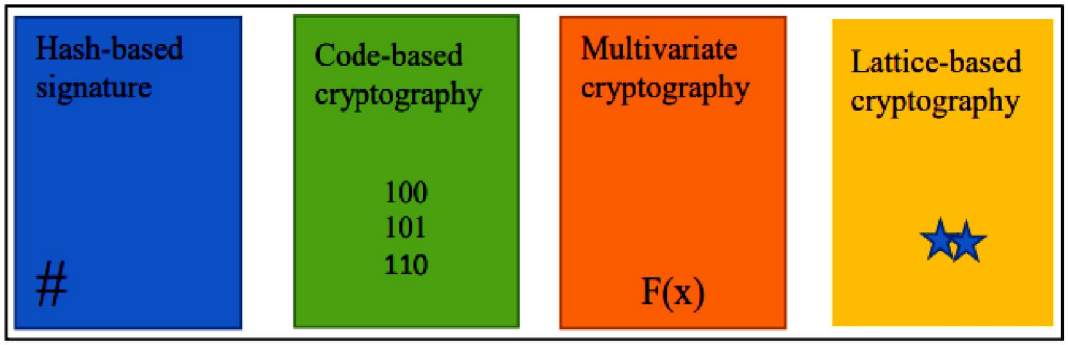

Figure 1: Implementation methods of four fundamental quantum secure algorithms

A hash-based signature

A one-time signature which requires that each key pair be used just once to sign a message, is the first step in a hash-based signature technique. But Merkle suggested creating a many-times signature method with a binary hash tree, which was eventually called the Merkle tree. The hash values of OTS public keys make up the leaves of a Merkle tree.The set of all OTS hidden keys becomes the secret key in a Merkle signature scheme whereas the root node of the Merkle tree becomes the public key. Random bit strings serve as the remote keys for hash-based OTS.

Code-based cryptography

Today's public-key cryptosystems, the majority of which depend on the intricacy of either factorization or the discrete logarithm problem, are seeing competition from code-based encryption. The foundation of code-based encryption, in contrast to public-key techniques, is the NP-hard issue of decoding unknown error-correcting codes. Two basic code-based cryptography systems have been named after the people who invented them. Both have the disadvantage of having huge vital lengths, which makes them problematic to implement on embedded devices with limited resources as compared to more conventional cryptosystems like RSA. Therefore, by embedding a message or introducing random mistakes, the input message is changed into a code word for plain text encryption.

Multivariate cryptography

The problem of solving non-linear equation structures over finite fields is the foundation of multivariate cryptography approaches. Patarin's Secret Fields, which generalizes a proposal by Matsumoto and Imai, is one of the special cases. Since multivariate polynomials over a finite field are the foundation of all Multivariate Public-Key Cryptosystems they all share the same basic design. Multivariate quadratic polynomials are still considered NP-hard, nonetheless, since the majority of polynomial equations are of degree two. Since Shor's algorithm doesn't rely on any of the intricate issues that Shor's methods can resolve, it cannot be solved more easily with Shor's methods than with a conventional computer.

Lattice-based cryptographic

The majority of lattice-based cryptographic algorithms employ cryptographic builders that provide security proofs based on worst-case hardness and are comparatively simple and time-efficient. One of the few algorithms that shows promise as potential candidates for post-quantum cryptography is lattice-based cryptography. These protocols are

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 2, July 2024

supported by certain encryption algorithms, such as RSA, Diffie-Hellman, and the elliptic curve, which are categorized as asymmetric cryptographic primitives since they are based on challenging mathematical problems. because current asymmetric encryption primitives can be swiftly solved by quantum computers employing Shor's factorization quantum approach.

General Description of NTT and Inverse NTT

The hardware description of NTT and inverse NTT is displayed in the image below. A polynomial x's n coefficients are transformed into the spectral domain by the NTT. To maintain the NTT's flexibility, the NTT-1 returns the pre-calculated values needed for the NTT and NTT-1 to the normal environment by transforming the coefficients of the result vector ^x.

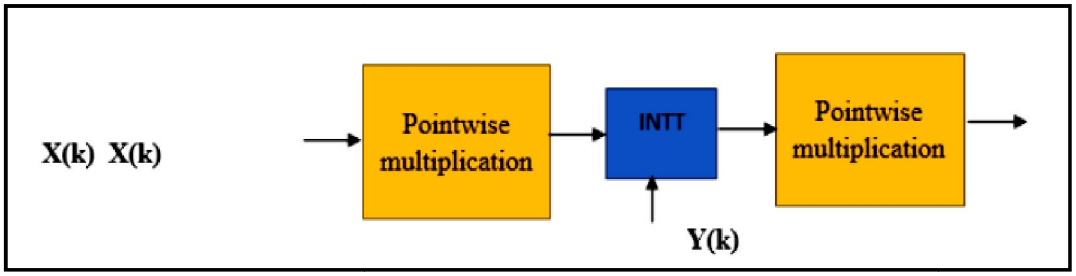

Figure 2: NTT and NTT−1 input/output description.

A finite field extension of the conventional Discrete Fourier Transform is the Number Theoretic Function. With a lot of work, it ensures success by enabling quick convolutions on integer sequences without round-off mistakes. Convolutions are useful for multiplying lengthy polynomials or large integers. We may multiply the components in those rings more effectively by using the NTT, a ring-based transformation. Arithmetic or number-theoretic operations are made up of complex-valued functions that are specified for all positive integers. Using the Fast Fourier Transform approach instead of floating-point numbers or complex arithmetic, the NTT is a non-trivial number theory that represents a finite field of polynomials.

NTT

$$X(k) = \sum_{i=0}^{N-1} x(i) w^{ik} \pmod{M} \qquad k = 0,\ 1,\ \ldots N-1 \qquad \ldots 1$$

Inverse NTT

$$Y(k) = \sum_{k=0}^{N-1} x(k) w^{-ik} \pmod{M^{-1}} \qquad k = 0,\ 1,\ \ldots N-1 \qquad \ldots 2$$

Where w = Nth primitive root of unity in Z and N = transform length, and the primitive element.

Ring: - is a set of real numbers ($\mathbb{R}$) with two operands (+ and *) and satisfying the following properties:

- $\mathbb{R}$ is an abelian group under +.
- Associativity of x – For every a, b, c $\in \mathbb{R}$

a * (b * c) = (a * b) x*c

- Distributive Properties For every a, b, c $\in \mathbb{R}$the following identities hold:

a * (b + c) = (a * b) + (a * c) and (b + c) * a = b *a + c * a.

Field: -is a set of elements F with two operands (+ and *)and satisfying the following properties:

- F is an abelian group under + and
- F – {0} (the set F without the additive identity 0) is an abelian group under *.

Generators

Unit g $\in \mathbb{Z}n*$ is called a generator or primitive root of $\mathbb{Z}n*$ if for every a$\in \mathbb{Z}n*$ therefore, g^k=w for some integer k. In other words, if we start with g, and keep multiplying by g, eventually, we see every element.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 2, July 2024

Modular Arithmetic

Assuming that the value of n is positive. The set [0, n−1] can thus be represented as ℤn. Assuming that two integers, a and b, are the same, we may express this as a = b (mod n) and state that x and y are congruent modulo n if a and b vary by a multiple of n. When the context makes it obvious, we can omit. In Zn, each integer an is congruent to some y. It is said to decrease an integer a modulo n when multiples of n are added or subtracted from it to get some b ∈ℤn, where b is the residue.

The roots of compliance with the nth multiplicative order are known as primitive nth roots of unity. They serve as the roots of the nth cyclotomic polynomial, for instance, and are crucial to many areas of number theory, especially algebraic number theory.

Roots of Unity

The primitive root n is an integer g such that every integer relative to n is congruent to the power of g mod n.

Procedure in calculating/finding NTT:

i. Have a vector sequence of an nth non-negative number

ii. Choose a working modulus, say M.

iii. Select an integer k≥1 and define N=kn +1. A value of k that will make N a prime

iv. Define w = g^k mod M

Even though lattice-based cryptography has been around for almost two decades, it is still considered a new approach to cryptographic design. This is because only the NTT component uses arithmetic operations, especially in systems where floating-point units are more significant and slower than integer arithmetic units.

Optimizing The Use of Power

Careful resource management can significantly lower dynamic power consumption when several embedded system components activate low-power modes. An operating system may, for instance, recognize a load or get explicit indications from apps to switch the computer to a lower-power and, consequently, lower-performance state. Any advantages of doing so, though, have to be balanced against the ongoing power consumption. This study employs silicon on insulator and clock gating as two methods to reduce the dynamic power consumption of the NTT.

Clock Gating

Usually, the clock signal needs a lot of dynamic power since it has a lot of fan-out. One efficient way to reduce power consumption in synchronous circuits is by clock gating. It is not necessarily necessary to use every functional unit in a design for every clock cycle. The purpose of clock gating is to only activate the clock signal for those components that need to be in operation. When registers are idle, their dynamic power consumption is zero, hence the only power consumption to be concerned about is static power consumption. The clock gating idea is shown in Figure 3. During the clock gating optimization, the registers that have the same enabled signal are grouped together. The logic used to generate the enable signal is then inverted.

Silicon on Insulator (SOI)

One type of insulator that has been used in CMOS circuits is silicon on insulator. It is composed of two different kinds of insulators. The benefit of both sapphire and SiO2 is that they both reduce capacitance between the source and the drain. Another advantage is the decreased diffusion capacitance, which lowers subthre shold leakage in circuits and, thus, further reduces power consumption. There are two different kinds of SOI techniques: FDSOI and PDSOI. Due to technological limitations, the PDSOI approach is typically used even though FDSOI helps reduce tunneling currents in CMOS.

III. RESULTS AND DISCUSSIONS

The results of the article are presented in this subsection along with a commentary. The research of lattice-based post-quantum cryptography is still in its infancy. The Xilinx Zynq-7000 on the Zed board was utilized to implement our FPGA hardware design. Some parallel NTT architectures are only suitable for applications requiring high throughput and small n values. Because the authors of advise computing the Twiddle factors at run-time, the memory use was much reduced. Between 200 and 300 slices are used for n = 256, n = 512, and n = 1024.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 2, July 2024

Power measurement

UMC 65 nm technology was used to develop the ASIC design. To minimize leakage currents, a low-level library with a high threshold voltage was employed. The static power consumption is independent of the parameter set as the same architecture is employed for all setups. Clock gating is expected to provide in considerable power savings because the NTT is not constantly operating. The cryptographic technique employed and the amount of time dedicated to particular operations affect how much power is saved. To significantly lower overall power consumption, just a few more gates are required. The operand separation strategy increased the number of cells by 145 in addition to the design clock gating. However, because unnecessary signal transmission was blocked, the system's switching activity was greatly decreased. Consequently, a 0.03W decrease in overall power consumption was achieved.

Timing Result

The number of clock cycles needed for the NTT and NTT-1 is equal to n log when one clock cycle is assumed and a single port RAM is used. Unlike previous studies, post-processing doesn't need any more clock cycles.

IV. CONCLUSION

This study proposes a fast, flexible, and secure low-power NTT ASIC architecture. The versatility of the architecture makes it possible to employ a wide range of cryptographic methods. Activities can be rescheduled, and efficient modulo-reduction techniques can be used to speed up the design process. One appealing method for effectively handling polynomial multiplication is the Number Theory Transform. For many systems, including battery-operated devices and Internet of Things gadgets, low power consumption is essential.

REFERENCES

[1]. Paludo, Rogério, and Leonel Sousa. "Number Theoretic Transform Architecture suitable to Lattice-based Fully-Homomorphic Encryption." 2021 IEEE 32nd International Conference on Application-specific Systems, Architectures and Processors (ASAP). IEEE, 2021.
[2]. Mert, Ahmet Can, et al. "An extensive study of flexible design methods for the number theoretic transform." IEEE Transactions on Computers (2020).
[3]. Fritzmann, Tim, and Johanna Sepúlveda. "Efficient and flexible low-power NTT for lattice-based cryptography." 2019 IEEE International Symposium on Hardware Oriented Security and Trust (HOST). IEEE, 2019.
[4]. Longa, Patrick, and Michael Naehrig. "Speeding up the number theoretic transform for faster ideal lattice-based cryptography." International Conference on Cryptology and Network Security. Springer, Cham, 2016.
[5]. Karabulut, Emre, and Aydin Aysu. "RANT: A RISC-V architecture extension for the number theoretic transform." 2020 30th International Conference on Field-Programmable Logic and Applications (FPL). IEEE, 2020.
[6]. Pessl, Peter, and Robert Primas. "More practical single-trace attacks on the number theoretic transform." International Conference on Cryptology and Information Security in Latin America. Springer, Cham, 2019.
[7]. Nejatollahi, Hamid, Rosario Cammarota, and Nikil Dutt. "Flexible ntt accelerators for rlwe lattice-based cryptography." 2019 IEEE 37th International Conference on Computer Design (ICCD). IEEE, 2019.
[8]. Özerk, Özgün, et al. "Efficient number theoretic transform implementation on GPU for homomorphic encryption." The Journal of Supercomputing 78.2 (2022): 2840-2872.
[9]. Banerjee, Utsav, Tenzin S. Ukyab, and Anantha P. Chandrakasan. "Sapphire: A configurable crypto-processor for post-quantum lattice-based protocols." arXiv preprint arXiv:1910.07557 (2019).
[10]. Zhang, Neng, et al. "Highly efficient architecture of NewHope-NIST on FPGA using low-complexity NTT/INTT." IACR Transactions on Cryptographic Hardware and Embedded Systems (2020): 49-72.
[11]. Mert, Ahmet Can, ErdinçÖztürk, and ErkaySavaş. "Design and implement encryption/decryption architectures for bfv homomorphic encryption scheme." IEEE Transactions on Very Large-Scale Integration (VLSI) Systems 28.2 (2019): 353-362.
[12]. Fritzmann, Tim, et al. "Masked accelerators and instruction set extensions for post-quantum cryptography." IACR Transactions on Cryptographic Hardware and Embedded Systems 2022.1 (2021): 414-460.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 2, July 2024

[13]. Mert, Ahmet Can, et al. "An extensive study of flexible design methods for the number theoretic transform." IEEE Transactions on Computers (2020).
[14]. Mert, Ahmet Can, et al. "A flexible and scalable NTT hardware: Applications from homomorphically encrypted deep learning to post-quantum cryptography." 2020 Design, Automation & Test in Europe Conference & Exhibition (DATE). IEEE, 2020.
[15]. Reparaz, Oscar, et al. "Masking ring-LWE." Journal of Cryptographic Engineering 6.2 (2016): 139-153.
[16]. Bache, Florian, et al. "High-speed masking for polynomial comparison in lattice-based kems." IACR Transactions on Cryptographic Hardware and Embedded Systems (2020): 483-507.
[17]. Aysu, Aydin, Cameron Patterson, and Patrick Schaumont. "Low-cost and area-efficient FPGA implementations of lattice-based cryptography." 2013 IEEE international symposium on hardware-oriented security and trust (HOST). IEEE, 2013.