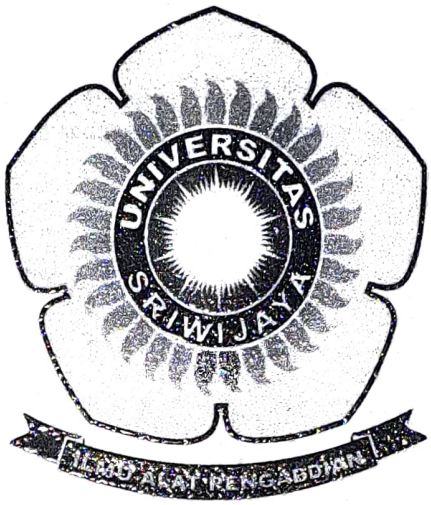
IMPLEMENTASI ALGORITMA POST-QUANTUM CRYPTOGRAPHY SEBAGAI ENKRIPSI PADA PESAN

SKRIPSI

Diajukan Untuk Melengkapi Salah Satu Syarat

Memperoleh Gelar Sarjana Komputer



OLEH:

Sa'ad Abdillah Waqas

09011281924070

JURUSAN SISTEM KOMPUTER

FAKULTAS ILMU KOMPUTER

UNIVERSITAS SRIWIJAYA

2025

HALAMAN PENGESAHAN

SKRIPSI

IMPLEMENTASI ALGORITMA POST-QUANTUM CRYPTOGRAPHY SEBAGAI ENKRIPSI PADA PESAN

Sebagai salah satu syarat untuk penyelesaian studi di

Program Studi S1 Sistem Komputer

Oleh:

SA'AD ABDILLAH WAQAS

09011281924070

Pembimbing 1 : **Dr. Ir. Ahmad Heryanto, M.T.**
NIP. 198701222015041002

Mengetahui

Ketua Jurusan Sistem Komputer

Dr. Ir. Sukemi, M.T

196612032006041001

HALAMAN PERSETUJUAN

Telah diuji dan lulus pada :

Hari : Senin

Tanggal : 30 Desember 2024

Tim Penguji :

1. **Ketua : Ahmad Fali Oklilas, M.T.**
2. **Penguji : Prof. Deris Stiawan, M.T., Ph.D.**
3. **Pembimbing : Dr. Ir. Ahmad Heryanto, M.T.**

Ketua Jurusan Sistem Komputer

Dr. Ir. Sukemi, M.T.

NIP. 196612032006041001

HALAMAN PERNYATAAN

Yang bertanda tangan dibawah ini:

Nama : Sa'ad Abdillah Waqas
NIM : 09011281924070
Judul : IMPLEMENTASI ALGORITMA POST-QUANTUM CRYPTOGRAPHY SEBAGAI ENKRIPSI PADA PESAN

Hasil Pengecekan Software IThentivate/Turnitin : 6%

Menyatakan bahwa laporan tugas akhir saya merupakan hasil karya sendiri dan bukan hasil penjiplakan atau plagiat. Apabila ditemukan unsur penjiplakan atau plagiat dalam laporan tugas akhir ini, maka saya bersedia menerima sanksi akademik dari Universitas Sriwijaya.

Demikian, pernyataan ini saya buat dalam keadaan sadar dan tidak dipaksakan.

Indralaya, Juni 2025

Penulis,

Sa'ad Abdillah Waqas

NIM. 09011281924070

HALAMAN PERSEMBAHAN

Dengan penuh rasa syukur kepada Tuhan Yang Maha Esa atas limpahan rahmat dan karunia-Nya, skripsi ini saya persembahkan kepada:

1. Kedua Orang Tua Tercinta

   Ayah dan Ibu, terima kasih atas cinta, doa, dukungan, dan pengorbanan yang tak pernah henti. Segala keberhasilan ini tidak lepas dari keikhlasan kalian.

2. Saudara dan Keluarga Besar

   Kakak/adik dan keluarga besar saya, terima kasih atas semangat, perhatian, dan doa yang selalu menguatkan.

3. Dosen Pembimbing dan Pengajar

   Terima kasih atas bimbingan, ilmu, dan kesabaran yang diberikan selama masa studi dan penyelesaian skripsi ini.

4. Sahabat-Sahabat

   Kepada teman-teman seperjuangan yang selalu mendukung, memberi semangat, dan menemani proses panjang ini dengan tawa serta kerja keras bersama.

5. Almamater Tercinta

   Tempat saya belajar, tumbuh, dan mendapatkan pengalaman berharga selama masa perkuliahan.

6. Untuk Diriku Sendiri

   Atas segala kerja keras, dedikasi, dan ketangguhan menghadapi tantangan, ini adalah hadiah kecil untuk perjalanan yang telah dilalui.

Semoga karya sederhana ini bermanfaat bagi semua yang membaca

KATA PENGANTAR

Puji dan syukur kepada Tuhan Yang Maha Esa, karena berkat Rahmat dan Karunia-nya lah sehingga penulis dapat menyelesaikan penyusunan Tugas Akhir ini dengan judul **"Implementasi Algoritma Post-Quantum Cryptography Sebagai Enkripsi Pada Pesan"**.

Laporan ini merupakan salah satu syarat untuk memenuhi sebagian kurikulum dan syarat untuk kelulusan Mata Kuliah Skripsi pada Jurusan Sistem Komputer di Universitas Sriwijaya.

Pada kesempatan ini, penulis ingin mengucapkan terima kasih kepada pihak yang telah memberikan bantuan, dorongan, motivasi, semangat, dan bimbingan dalam penyusunan proposal skripsi ini, yakni :

1. Kepada Tuhan Yang Maha Esa, yang telah melimpahkan Berkat dan Rahmat-Nya.
2. Keluarga saya yang menjadi salah satu penyemangat dalam penulisan tugas akhir.
3. Bapak Prof. Dr. Erwin, S.Si, M.Si selaku Dekan fakultas Ilmu Komputer Universitas Sriwijaya.
4. Bapak Dr. Ir. Sukemi, M.T. selaku Ketua Jurusan Sistem Komputer Universitas Sriwijaya.
5. Bapak Iman Saladin B. Azhar, S.Kom., M.MSi. selaku Dosen Pembimbing Akademik.
6. Bapak Dr. Ir. Ahmad Heryanto, M.T selaku Dosen Pembimbing Tugas Akhir.
7. Mbak Sari, Kak Yopi, dan Kak Angga selaku admin Jurusan Sistem Komputer.
8. Qory Amanah Putra dan Muhammad Sultan Alif yang selalu membersamai dan menyemangati di rumah kontrakan.

9. Teman-teman Sistem Komputer Indralaya
10. Kakak tingkat Sistem Komputer Universitas Sriwijaya yang lainnya.

Dalam penyusunan Skripsi ini saya menyadari sepenuhnya bahwa laporan ini masih jauh dari kata sempurna, oleh karena itu saya mengharapkan saran dan kritik dari semua pihak yang berkenan demi laporan yang lebih baik lagi.

Akhir kata, saya harap semoga Skripsi ini dapat bermanfaat serta dapat memberikan pengetahuan dan wawasan bagi semua pihak yang membutuhkannya.

Indralaya, Juni 2025

Sa'ad Abdillah Waqas

NIM. 09011281924070

IMPLEMENTASI ALGORITMA POST-QUANTUM CRYPTOGRAPHY SEBAGAI ENKRIPSI PADA PESAN

Sa'ad Abdillah Waqas (09011281924070)
Jurusan Sistem Komputer, Fakultas Ilmu Komputer, Universitas Sriwijaya
Email : saadabdillah42@gmail.com

ABSTRAK

Kemajuan teknologi komputasi kuantum telah menimbulkan ancaman serius terhadap keamanan sistem kriptografi konvensional seperti RSA dan ECC yang saat ini digunakan secara luas dalam aplikasi komunikasi. Sebagai respons terhadap tantangan ini, penelitian ini bertujuan untuk mengimplementasikan dan mengevaluasi algoritma *NTRU* sebagai solusi *Post-Quantum Cryptography* untuk pengamanan pesan. Hasil pengujian dalam aspek performa,menunjukkan bahwa waktu pemrosesan mencapai titik optimal pada nilai N yang relatif kecil (107-263), dengan karakteristik pertumbuhan waktu komputasi yang hampir linear seiring dengan peningkatan parameter. Ketika dikonfigurasi dengan parameter yang tepat algoritma *NTRU*, mampu menyediakan solusi enkripsi yang efisien dan aman untuk menghadapi ancaman yang muncul dari era komputasi kuantum.

Kata kunci : Post-quantum Cryptography, NTRU, Keamanan Komunikasi

IMPLEMENTATION OF POST-QUANTUM CRYPTOGRAPHY ALGORITHM AS MESSAGE ENCRYPTION

Sa'ad Abdillah Waqas (09011281924070)

Departement of Computer Systems, Faculty of Computer Science, Sriwijaya University

Email : saadabdillah42@gmail.com

ABSTRACT

The advancement of quantum computing technology has posed serious threats to the security of conventional cryptographic systems such as RSA and ECC, which are currently widely used in communication applications. In response to this challenge, this research aims to implement and evaluate the NTRU algorithm as a post-quantum cryptography solution for message security. In the research methodology, The test results in terms of performance show that the processing time reaches an optimal point at a relatively small value of N (107-263), with an almost linear growth of computation time as the parameter increases. When configured with the right parameters, the NTRU algorithm is able to provide an efficient and secure encryption solution to face the emerging threats of the quantum computing era.

Keywords: Post-quantum Cryptography, NTRU, Communication Security

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

DAFTAR LAMPIRAN

BAB I
PENDAHULUAN

1.1. Latar Belakang

Teknologi informasi telah memasuki hampir semua aspek kehidupan, mulai dari komunikasi dengan teman, hingga layanan keuangan dan pemerintahan. Oleh karena itu, menjaga kerahasiaan dan integritas data menjadi sangat penting, dan algoritma kriptografi memegang peranan fundamental yang sangat penting dalam keamanan siber. Fungsinya adalah untuk menjaga kerahasiaan informasi sehingga hanya pihak pengirim dan penerima yang dituju yang memiliki kemampuan untuk mengaksesnya [1].

Kriptografi merupakan sebuah ilmu yang mempelajari beberapa teknik untuk menjaga kerahasiaan sebuah informasi. Data yang dikirim melalui jaringan komputer ataupun media penyimpanan digital dapat diamankan menggunakan kriptografi. Terdapat dua jenis kriptografi yang umum digunakan, yaitu kriptografi simetris dan kriptografi asimetris. Kriptografi simetris merupakan kriptografi yang menggunakan satu kunci untuk mengamankan data, sedangkan kriptografi asimetris menggunakan sepasang kunci untuk mengamankan data, yaitu kunci publik dan kunci privat [2].

Keamanan informasi terus berkembang, dan tantangan baru terus muncul. Salah satu tantangan paling signifikan yang dihadapi oleh dunia keamanan informasi saat ini adalah kemajuan dalam komputasi kuantum [3] . Komputer kuantum adalah komputer yang menggunakan prinsip-prinsip mekanika kuantum untuk melakukan komputasi. Berbeda dengan komputer klasik yang menggunakan bit klasik sebagai unit informasi, komputer kuantum menggunakan qubit (quantum bit) yang dapat berada dalam keadaan superposisi [4] . Kemampuan ini memungkinkan pemrosesan informasi menjadi jauh lebih kompleks dan cepat. Komputer kuantum memiliki potensi besar untuk mengatasi masalah yang menantang dan rumit, termasuk dalam bidang pemodelan molekuler, optimisasi, dan faktorisasi bilangan besar. Algoritma-algoritma kriptografi konvensional sepenuhnya rentan terhadap komputer kuantum. Komputer kuantum memiliki potensi untuk mengeksekusi perhitungan yang sangat kompleks dengan

kecepatan yang jauh melampaui komputer konvensional saat ini. Kelemahan utama yang dihadapi oleh algoritma kriptografi konvensional adalah bahwa komputer kuantum dapat dengan mudah memecahkannya, terutama dalam hal faktorisasi bilangan bulat, dan logaritma diskrit [5].

Bukti efektivitas algoritma kuantum terhadap algoritma kriptografi klasik adalah uji algoritma untuk faktorisasi bilangan bulat menggunakan komputer kuantum milik IBM. Jika pada komputer konvensional, faktorisasi bilangan 129 bit memerlukan lebih dari delapan bulan, komputer kuantum ini dengan menggunakan algoritma *Shor* dapat mempercepat proses ini jutaan kali lipat. Sebagai contoh, sistem kriptografi *RSA* bergantung pada kesulitan komputasi dalam masalah faktorisasi bilangan besar dan menggunakan kunci publik, yang dihasilkan dari perkalian dua bilangan prima besar. Untuk meretas sistem kriptografi ini, cukup dengan menemukan faktor-faktor dari bilangan. Dengan bantuan komputer kuantum, algoritma *Shor* bisa memecahkan masalah faktorisasi ini dengan sangat cepat. Dengan kata lain, teknologi kuantum membuat banyak sistem kriptografi, termasuk *RSA*, menjadi tidak lagi aman [6].

Pada bidang komunikasi, kita menggunakan aplikasi seperti *WhatsApp*, Telegram, dan *Signal* yang mengandalkan teknologi enkripsi untuk melindungi privasi dan keamanan data pengguna. *WhatsApp* menggunakan Signal Protocol dengan implementasi AES-256, HMAC-SHA256, dan Curve25519 untuk menjamin kerahasiaan pesan *end-to-end*. Telegram memakai protokol MTProto 2.0 dengan kombinasi algoritma AES-256, RSA-2048, dan pertukaran kunci *Diffie-Hellman* untuk mengamankan komunikasi penggunanya [7] . Namun, dengan kemajuan teknologi dan munculnya komputer kuantum, infrastruktur kriptografi yang ada saat ini berpotensi menjadi rentan dan tidak lagi mampu menjamin keamanan data secara optimal. Hal ini memerlukan desain dan pengembangan algoritma kriptografi yang tahan terhadap serangan komputer kuantum. Kebutuhan ini melahirkan konsep *post-quantum cryptography (PQC)* sebagai solusi untuk menghadapi ancaman komputasi kuantum di masa depan. Bidang *post-quantum cryptography* merupakan area penelitian yang sedang berkembang pesat, yang bertujuan untuk merancang algoritma kriptografi yang

tidak hanya mampu bertahan dari ancaman komputasi kuantum, tetapi juga tetap efisien dalam penggunaan sumber daya komputasi konvensional. [8].

Post-quantum cryptography bertujuan mengembangkan sistem kriptografi yang dapat menahan ancaman potensial yang ditimbulkan oleh komputer kuantum. Karena metode enkripsi tradisional seperti *RSA, ECC, AES* dan *DES* rentan terhadap serangan kuantum, transisi ke *PQC* sangat penting untuk mengamankan komunikasi dan integritas data di masa depan [9] . Algoritma kriptografi pasca-kuantum dibagi menjadi beberapa kategori utama, yaitu *Lattice*-based, *Code-based, Multivariate Polynomial, Hash-based dan Isogeny-based* [10].

Dalam bidang komunikasi, telah dilakukan penelitian dan pengembangan untuk mengimplementasikan algoritma *post-quantum cryptography* pada pesan seperti pada penelitian [11]. Peneliti mengusulkan protokol baru untuk pengiriman pesan grup yang aman yang memastikan kerahasiaan, keterlacakan, dan pengurutan pesan. Penelitian ini menggunakan protokol *isogeny-based eliptic curve* yang disebutnya *double rachet* untuk komunikasi grup. Protokol ini dirancang untuk menahan serangan kuantum, memberikan keamanan yang lebih baik untuk komunikasi grup. Penelitian ini menyoroti kebutuhan pesan instan yang aman dalam konteks meningkatnya kemampuan komputasi kuantum.

Pada penelitian [12] juga menggunakan algoritma *isogeny-based* untuk mengembangkan algoritma seperti *Diffie-Hellman key exchange* dengan menggunakan kunci simetrik sebagai *shared key*. Penelitian ini menunjukkan bahwa protokol pertukaran kunci yang mirip dengan *Diffie-Hellman based post-quantum* dapat berfungsi secara praktis. Sedangkan pada penelitian [13] dilakukan analisis kemungkinan penerapan skema tanda tangan dengan metode code based *post-quantum cryptography* untuk tujuan otentikasi pesan. Pada penelitian ini digaris bawahi bahwa terdapat beberapa masalah yang muncul seperti pertumbuhan eksponensial dalam waktu pembuatan kunci dan tanda tangan bergantung pada peningkatan kemampuan koreksi. Ini membatasi rentang parameter yang bisa digunakan menjadi lebih kecil, sehingga mempersempit area aplikasi.

Pada penelitian [8] membahas tentang pengembangan dan implementasi algoritma *RSA* berbasis kisi-kisi (*Lattice-based RSA*). Penelitian ini bertujuan

untuk mengatasi kelemahan algoritma RSA konvensional terhadap serangan kuantum. Algoritma yang diusulkan ini diuji dalam dimensi 60 dengan ukuran kunci sekitar 1.152×10^5 bit. Proses komputasi yang intensif dalam pembuatan dan penggunaan kunci besar memerlukan energi yang lebih tinggi, namun hal ini diimbangi dengan keamanan yang lebih tinggi terhadap serangan kuantum. Selain itu juga pada penelitian [14] menggunakan pendekatan tinjauan dan tutorial untuk menganalisis skema *Bit Flipping Key Encapsulation* (*BIKE*). Pendekatan ini melibatkan pemahaman prinsip kerja dasar sistem kriptografi *McEliece* dan variasi modernnya berdasarkan *QC-MDPC*. Penelitian ini menyimpulkan bahwa BIKE adalah kandidat kuat untuk kriptografi pasca-kuantum yang sedang dalam tahap akhir proses standarisasi *NIST*. Namun, penelitian juga menemukan beberapa tantangan utama, seperti ukuran kunci yang besar, kompleksitas desain, dan adanya masalah kunci lemah yang dapat mempengaruhi tingkat keamanan.

Salah satu algoritma yang menjanjikan dalam *post-quantum cryptography* adalah algoritma *NTRU*. Algoritma ini merupakan sistem kriptografi kunci publik yang didasarkan pada teori bilangan bulat dan aljabar cincin *(ring theory)*. Sistem ini dirancang untuk memberikan keamanan yang kuat dengan ukuran kunci yang relatif kecil dibandingkan dengan beberapa sistem kriptografi kunci publik lainnya seperti *RSA* atau *ECC* [15]. *NTRU* didasarkan pada teori matematis yang kuat yang melibatkan konsep struktur aljabar seperti jaringan *Lattice*. Keunggulan *NTRU* adalah kemampuannya untuk memberikan tingkat keamanan yang tinggi sambil mempertahankan efisiensi yang baik dalam penggunaan sumber daya komputasi [16]. Algoritma ini diharapkan dapat menjadi solusi yang efektif untuk menghadapi tantangan keamanan dari komputasi kuantum yang semakin maju. Oleh karena itu, penelitian ini bertujuan untuk mengimplementasikan algoritma *post-quantum cryptography* terutama *NTRU*, dalam pengamanan pesan dan untuk menguji efektivitas serta kekuatannya dalam melindungi data dalam era komputasi kuantum yang semakin relevan dan kompleks.

1.2. Tujuan dan Manfaat

1.2.1. Tujuan

Tujuan dari penulisan Tugas Akhir ini, yaitu :

1. Dapat mengimplementasikan algoritma *post-quantum cryptography* sebagai enkripsi pada pesan.
2. Mendapatkan hasil analisa kinerja algoritma *post-quantum cryptography* pada proses enkripsi dan dekripsi pada pesan.

1.2.2. Manfaat

Manfaat dari penulisan Tugas Akhir ini, yaitu :

1. Mengetahui keamanan pada pesan dengan menggunakan algoritma *post-quantum cryptography*.
2. Mengetahui kinerja algoritma *post-quantum cryptography* sebagai enkripsi pada pesan.

1.3. Perumusan dan Batasan Masalah

1.3.1. Perumusan Masalah

Berdasarkan permasalahan yang telah dijabarkan sebelumnya, maka penulis merumuskan sebuah masalah dalam penelitian ini, yaitu :

1. Bagaimana algoritma *post-quantum cryptography* diterapkan pada enkripsi pesan ?
2. Bagaimana kinerja algoritma *post-quantum cryptography* ?

1.3.2. Batasan Masalah

Berikut batasan masalah pada Tugas Akhir ini, yaitu :

1. Penelitian ini hanya akan berfokus pada satu algoritma *post-quantum cryptography* yaitu algoritma *NTRU*.
2. Penelitian ini akan menguji kinerja algoritma *post-quantum cryptography* sebagai enkripsi pada pesan.

3. Penelitian ini tidak akan mencakup implementasi penuh dari semua aspek infrastruktur keamanan, tetapi akan lebih berfokus pada implementasi algoritma *post-quantum cryptography* itu sendiri.

1.4. Metodologi Penelitian

Pada Tugas Akhir ini, metodologi yang digunakan adalah sebagai berikut :

1.4.1. Metode Studi Pustaka dan Literatur

Pada metode ini, dilakukan pencarian dan pengumpulan referensi berupa literatur yang terdapat pada buku dan internet mengenai Tugas Akhir yang sedang dikerjakan.

1.4.2. Metode Konsultasi

Dalam metode ini penulis melakukan konsultasi secara langsung dan atau tidak langsung kepada semua pihak narasumber yang memiliki pengetahuan serta wawasan yang baik dalam mengatasi permasalahan yang ditemui pada penulisan Tugas Akhir ini.

1.4.3. Metode Pembuatan Model

Metode selanjutnya adalah membuat suatu perancangan pemodelan dengan menggunakan program.

1.4.4. Metode Pengujian

Pengujian terhadap sistem yang telah dibuat perlu dilakukan untuk melihat batasan-batasan kinerja sistem tersebut dapat menghasilkan nilai akurasi yang baik atau sebaliknya.

1.4.5. Metode Hasil dan Analisa

Hasil dari pengujian pada Tugas Akhir ini akan di analisa seluruh kelebihan serta kekurangannya, sehingga diharapkan dapat digunakan sebagai referensi yang baik untuk penelitian selanjutnya.

1.4.6. Metode Penarikan Kesimpulan dan Saran

Metode ini merupakan tahap akhir dari Metodologi Penelitian, berdasarkan hasil dan analisis penelitian yang dilakukan maka akan didapatkan kesimpulan dan saran untuk penelitian selanjutnya.

1.5. Sistematika Penulisan

Dalam mempermudah penyusunan Tugas Akhir ini dan juga membuat isi dari setiap bab yang ada pada Tugas Akhir ini lebih jelas, maka dibuat sistematika penulisan sebagai berikut :

BAB I – PENDAHULUAN

Sebagai fondasi penelitian, bab ini membahas tentang Latar Belakang Masalah, Tujuan dan Manfaat, Perumusan dan Batasan Masalah, Metode Penelitian, dan Sistematika Penulisan dari penelitian yang dilakukan.

BAB II – TINJAUAN PUSTAKA

Bab selanjutnya merupakan penjelasan Dasar Teori, Konsep dan Prinsip Dasar yang dibutuhkan untuk memecahkan masalah dalam penelitian yang dilakukan.

BAB III – METODOLOGI

Metodologi yang digunakan akan dibahas secara rinci tentang teknik, metode, dan alur proses yang dilakukan dalam penelitian.

BAB IV – HASIL DAN ANALISA

Bab empat merupakan hasil pengujian dan analisis yang diperoleh dari penelitian serta pembahasan terhadap hasil yang telah dicapai meliputi kelebihan dan kekurangan dari penelitian yang telah dilakukan.

BAB V – KESIMPULAN DAN SARAN

Pada bab terakhir berisi kesimpulan yang bersumber dari hasil penelitian yang dilakukan serta saran untuk penelitian selanjutnya khususnya tentang Tugas Akhir yang dikerjakan.

Daftar Pustaka

[1] M. Kumar, “Post-quantum cryptography Algorithm’s standardization and performance analysis,” *Array*, vol. 15, Sep. 2022, doi: 10.1016/j.array.2022.100242.

[2] S. K. Singh, “A Comparative Study of Cryptography Techniques Used in Wireless Networks,” *International Journal of Computer Applications* , vol. 179, pp. 7–12, 2021.

[3] V. Mavroeidis, K. Vishi, M. D. Zych, and A. Jøsang, “The Impact of Quantum Computing on Present Cryptography,” Mar. 2018, doi: 10.14569/IJACSA.2018.090354.

[4] M. Vogel, “Quantum Computation and Quantum Information, by M.A. Nielsen and I.L. Chuang,” *Contemp Phys*, vol. 52, no. 6, pp. 604–605, Nov. 2011, doi: 10.1080/00107514.2011.587535.

[5] M. Jobair, H. Faruk, S. Tahora’, M. Tasnim’, H. Shahriar’, and N. Sakib’, “A Review of Quantum Cybersecurity: Threats, Risks and Opportunities.”

[6] L. Cherckesova, O. Safaryan, P. Razumov, V. Kravchenko, S. Morozov, and A. Popov, “Post-Quantum Cryptosystem NTRUEnCrypt and Its Advantage over Pre - Quantum Cryptosystem RSA,” in *E3S Web of Conferences*, EDP Sciences, Dec. 2020. doi: 10.1051/e3sconf/202022401037.

[7] C.-E. Bogos, R. Mocanu, and E. Simion, “A security analysis comparison between Signal, WhatsApp and Telegram,” 2023.

[8] I. Mustafa *et al.*, “A Lightweight Post-Quantum Lattice-Based RSA for Secure Communications,” *IEEE Access*, vol. 8, pp. 99273–99285, 2020, doi: 10.1109/ACCESS.2020.2995801.

[9] R. Bavdekar, E. J. Chopde, A. Bhatia, K. Tiwari, S. J. Daniel, and Atul, “Post Quantum Cryptography: Techniques, Challenges, Standardization, and Directions for Future Research,” Feb. 2022, [Online]. Available: http://arxiv.org/abs/2202.02826

[10] K. Basu, D. Soni, M. Nabeel, and R. Karri, “NIST Post-Quantum Cryptography-A Hardware Evaluation Study.” [Online]. Available: http://cyber.nyu.edu

[11] J. Bobrysheva and S. Zapechnikov, “Post-quantum Secure Group Messaging,” in *Proceedings of the 2021 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering, ElConRus 2021*, Institute of Electrical and Electronics Engineers Inc., Jan. 2021, pp. 2323–2326. doi: 10.1109/ElConRus51938.2021.9396513.

[12] Bobrysheva Julia and Zapechnikov Sergey, *Post-Quantum Security of Communication and Messaging Protocols: Achievements, Challenges and New Perspectives 2019*.

[13] Y. Gorbenko, I. Svatovskiy, and O. Shevtsov, *Post-Quantum Message Authentication Cryptography Based on Error-Correcting Codes*.

[14] M. R. Nosouhi, S. W. A. Shah, L. Pan, and R. Doss, “Bit Flipping Key Encapsulation for the Post-Quantum Era,” 2023, *Institute of Electrical and Electronics Engineers Inc.* doi: 10.1109/ACCESS.2023.3282928.

[15] D. Buell, “Lattice-Based Cryptography and NTRU,” pp. 205–221, 2021, doi: 10.1007/978-3-030-73492-3_15.

[16] J. Senor, J. Portilla, and G. Mujica, “Analysis of the NTRU Post-Quantum Cryptographic Scheme in Constrained IoT Edge Devices,” *IEEE Internet Things J*, vol. 9, no. 19, pp. 18778–18790, Oct. 2022, doi: 10.1109/JIOT.2022.3162254.

[17] S. Glisic, “Quantum vs post-quantum security for future networks: Survey,” Jan. 01, 2024, *KeAi Communications Co.* doi: 10.1016/j.csa.2024.100039.

[18] A. Levina, V. Kadykov, and M. R. Valluri, “Security Analysis of Hybrid Attack for NTRU-Class Encryption Schemes,” *IEEE Access*, vol. 11, pp. 109939–109952, 2023, doi: 10.1109/ACCESS.2023.3321693.

[19] N. Yue, Y. Wang, and M. Wang, “Identity-Based Proxy Re-encryption over NTRU Lattices for Cloud Computing,” in *Procedia Computer Science*, Elsevier B.V., 2021, pp. 264–269. doi: 10.1016/j.procs.2021.04.061.

[20] S. Saha, A. Hota, B. Choudhury, A. Nag, and S. Nandi, “NTRU and Secret Sharing Based Secure Group Communication for IoT Applications,” *IEEE Access*, vol. 11, pp. 117341–117350, 2023, doi: 10.1109/ACCESS.2023.3325305.

[21] K. Dey, S. K. Debnath, P. Stˇ, and V. Srivastava, “A Post-Quantum Signcryption Scheme Using Isogeny Based Cryptography.”

[22] G. Yalamuri, P. Honnavalli, and S. Eswaran, “A Review of the Present Cryptographic Arsenal to Deal with Post-Quantum Threats,” in *Procedia Computer Science*, Elsevier B.V., 2022, pp. 834–845. doi: 10.1016/j.procs.2022.12.086.

[23] J. Senor, J. Portilla, and G. Mujica, “Analysis of the NTRU Post-Quantum Cryptographic Scheme in Constrained IoT Edge Devices,” *IEEE Internet Things J*, vol. 9, no. 19, pp. 18778–18790, Oct. 2022, doi: 10.1109/JIOT.2022.3162254.

[24] J. Bi and L. Han, “Lattice Attacks on NTRU Revisited,” *IEEE Access*, vol. 9, pp. 66218–66222, 2021, doi: 10.1109/ACCESS.2021.3076598.

[25] C. Balamurugan, K. Singh, G. Ganesan, and M. Rajarajan, “Code-based Post-Quantum Cryptography-Source link Code-based Post-Quantum Cryptography,” 2021, doi: 10.20944/PREPRINTS202104.0734.V1.

[26] J. Bobrysheva and S. Zapechnikov, “On the key composition for post-quantum group messaging and file exchange,” in *Procedia Computer Science*, Elsevier B.V., Jul. 2021, pp. 102–106. doi: 10.1016/j.procs.2021.06.012.

[27] F. Borges, P. R. Reis, and D. Pereira, “A Comparison of Security and its Performance for Key Agreements in Post-Quantum Cryptography,” *IEEE Access*, vol. 8, pp. 142413–142422, 2020, doi: 10.1109/ACCESS.2020.3013250.

[28] J. Krämer and P. Struck, “Encryption Schemes using Random Oracles: from Classical to Post-Quantum Security.”

[29] L. Shuai, H. Xu, L. Miao, and X. Zhou, “A Group-Based NTRU-Like Public-Key Cryptosystem for IoT,” *IEEE Access*, vol. 7, pp. 75732–75740, 2019, doi: 10.1109/ACCESS.2019.2920860.

[30] K. K. Soni and A. Rasool, “Cryptographic Attack Possibilities over RSA Algorithm through Classical and Quantum Computation,” 2018.

[31] V. Mavroeidis, K. Vishi, M. D. Zych, and A. Jøsang, “The Impact of Quantum Computing on Present Cryptography,” Mar. 2018, doi: 10.14569/IJACSA.2018.090354.

[32] F. Maqsood, M. Ahmed, M. Mumtaz Ali, and M. Ali Shah, “Cryptography: A Comparative Analysis for Modern Techniques,” 2017. [Online]. Available: www.ijacsa.thesai.org

[33] V. D. Badoni and Mr. A. jain, “Chip Implementation of Text Encryption and Decryption Algorithms,” *IOSR J Comput Eng*, vol. 16, no. 3, pp. 56–61, 2014, doi: 10.9790/0661-16365661.

[34] D. Thilagavathy, P. S. Babu, Adhiyamaan College of Engineering, Institute of Electrical and Electronics Engineers. Madras Section, and Institute of Electrical and Electronics Engineers, *2014 International Conference on Electronics, Communication and Computational Engineering (ICECCE) : 17 & 18 November 2014, venue, Adhiyamaan College of Engineering*.

[35] M. J. Hornos Barranco, “Learning the basics of cryptography with practical examples”.

[36] A. Sigov, L. Ratkin, and L. A. Ivanov, “Quantum Information Technology,” *J Ind Inf Integr*, vol. 28, p. 100365, Jul. 2022, doi: 10.1016/J.JII.2022.100365.

[37] Y. Huang, Z. Zhang, and X. Wang, “Quantum Computing: Principles and Recent Advances,” *Journal of Quantum Information Science*, vol. 12, pp. 145–162, 2022.

[38] Z. Chen, W. Li, and Q. Liu, “Shor’s Algorithm and Its Cryptographic Implications in Quantum Computing,” *Quantum Inf Process*, vol. 20, pp. 1–21, 2021.

[39] Q. Zhang, L. Wang, and S. Liu, “Error Correction for Quantum Computers: Recent Advances and Challenges,” *Quantum Sci Technol*, vol. 5, pp. 1–18, 2020.

[40] Y. Wu, X. Li, and Z. Wang, “Recent Advances in Superconducting Quantum Computing: Architectures and Applications,” *Front Phys*, vol. 7, p. 198, 2019.

[41] L. Zhao, M. Xu, and H. Zhang, “Efficient Quantum Algorithms: A Comprehensive Review,” *Quantum Inf Process*, vol. 17, pp. 1–32, 2018.

[42] Q. Zhang, X. Liu, and Y. Wang, “Advances in Quantum Error Correction: Approaches and Challenges,” *Phys Rev A (Coll Park)*, vol. 97, no. 2, p. 022309, 2023.

[43] Y. Huang, Z. Li, and W. Chen, “Scalability Challenges and Solutions in Quantum Computing,” *Quantum Sci Technol*, vol. 8, no. 4, pp. 1–17, 2023.

[44] J. Smith, R. Johnson, and M. Davis, “Classical-Quantum Hybrid Computing: Opportunities and Challenges,” *IEEE Transactions on Computers*, vol. 71, no. 6, pp. 789–803, 2022.

[45] D. J. Bernstein and T. Lange, “Post-quantum cryptography,” Sep. 13, 2017, *Nature Publishing Group*. doi: 10.1038/nature23461.

[46] S. R. Chowdhury and S. Pradhan, “On the Generalizations of Grover algorithm,” 2022.

[47] G. Kumar Rajput, “Cryptanalysis of pre-quantum and post-quantum cryptography,” *INTERNATIONAL JOURNAL OF ADVANCE RESEARCH IN MULTIDISCIPLINARY*, vol. 1, doi: 10.5281/zenodo.13643131.

[48] T. M. Fernandez-Carames, “From Pre-Quantum to Post-Quantum IoT Security: A Survey on Quantum-Resistant Cryptosystems for the Internet of Things,” Jul. 01, 2020, *Institute of Electrical and Electronics Engineers Inc.* doi: 10.1109/JIOT.2019.2958788.

[49] H. Sababa, “Cryptography in the Post-Quantum Era: The evolution of cryptography and quantum mechanics and their intersection in the Post-Quantum Era.” [Online]. Available: https://www.researchgate.net/publication/322662995

[50] S. K. Sahu and K. Mazumdar, “State-of-the-art analysis of quantum cryptography: applications and future prospects,” 2024, *Frontiers Media SA*. doi: 10.3389/fphy.2024.1456491.

[51] M. Richter, M. Bertram, J. Seidensticker, and A. Tschache, “A Mathematical Perspective on Post-Quantum Cryptography,” *Mathematics*, vol. 10, no. 15, Aug. 2022, doi: 10.3390/math10152579.

[52] A. Mariano, T. Laarhoven, F. Correia, M. Rodrigues, and G. Falcao, “A Practical View of the State-of-the-Art of Lattice-Based Cryptanalysis,” *IEEE Access*, vol. 5, pp. 24184–24202, Aug. 2017, doi: 10.1109/ACCESS.2017.2748179.

[53] H. Bandara, Y. Herath, T. Weerasundara, and J. Alawatugoda, “On Advances of Lattice-Based Cryptographic Schemes and Their Implementations,” *Cryptography 2022, Vol. 6, Page 56*, vol. 6, no. 4, p. 56, Nov. 2022, doi: 10.3390/CRYPTOGRAPHY6040056.

[54] J. Hoffstein, J. Pipher, and J. H. Silverman, “NTRU: A Ring-Based Public Key Cryptosystem.”

[55] Z. Zheng, K. Tian, and F. Liu, “A Generalization of NTRUencrypt,” 2023, pp. 175–188. doi: 10.1007/978-981-19-7644-5_7.

[56] M. Praveen, P. Korni, R. Kalekar, and R. Kashyap, “DESIGN OF EFFICIENT MULTI CLIENT-SINGLE SERVER APPLICATION USING SOCKET PROGRAMMING.” [Online]. Available: www.tojdel.net

[57] N. Salaheddin ELGHERIANI and S. Salem DKHILA, “CLIENT/SERVER CHATTING PROGRAM [USING TCP/UDP DATAGRAMS],” *MINAR International Journal of Applied Sciences and Technology*, vol. 05, no. 03, pp. 89–109, Sep. 2023, doi: 10.47832/2717-8234.16.6.

[58] A. Mccluskey, B. Mb, C. Frca, A. Ghaaliq, and L. Mb, “Statistics II: Central tendency and spread of data,” *Continuing Education in Anaesthesia Critical Care & Pain*, vol. 7, no. 4, pp. 127–130, Aug. 2007, doi: 10.1093/BJACEACCP/MKM020.

[59] J. Hoffstein, J. Pipher, J. M. Schanck, J. H. Silverman, W. Whyte, and Z. Zhang, “Choosing Parameters for NTRUEncrypt.”