**Enhancing Data Integrity: A** **Fast-Fourier Lattice-based Compact Signatures Over NTRU (FALCON) Post-quantum Cryptographic Signatures for Systems Data in the Provincial Government of Davao del Norte**



A Capstone Project Presented to the

Faculty of the Institute of Computing

Davao del Norte State College

New Visayas, Panabo City

**Emmanuel H. Otacan**

June 2025

**Chapter 1**

**INTRODUCTION**

**Background of the Study**

In the ever-evolving landscape of cybersecurity, a looming shadow emerges in the form of quantum computing, a technological force capable of unraveling the very fabric of modern cryptography's security [1][2][3][4]. When sharing information, it is crucial to prioritize implementing security measures. The fast improvement of information technology today has made it convenient for individuals to exchange data or information easily [5]. Addressing security issues in these choices and implementations is essential, especially because big data environments lack comprehensive data protection features, making them low-hanging fruits for attackers. Large amounts of data stored on the cloud are very sensitive [6]. Different strategies are being studied and incorporated to use subscription-based cloud for serving analytics systems [3]. Only secure cryptographic algorithms can safeguard data from potential attackers and provide security for big data in the cloud [7].

Public key cryptography plays a critical role in our modern communication infrastructure, including applications like mobile phones, internet commerce, and social networks. The security of these systems relies on cryptographic functionalities like public key encryption, digital signatures, and key exchange, which are currently implemented using specific mathematical problems. [8]. As quantum computing emerges, these existing cryptosystems are getting less secure [9][10][8]. The goal of post-quantum cryptography (PQC) is to develop cryptographic systems that are secure against both quantum and classical computers [8].

In March 2023, QuSecure, a quantum security provider, asserted that it had achieved the inaugural live, end-to-end quantum-resistant cryptographic communication satellite link in space. According to the company, this marked the first instance of safeguarding US satellite data transmissions from both classical and quantum decryption attacks using PQC. The quantum-secure communication from Earth to space and back was established through a Starlink satellite in collaboration with a leading global system integrator (GSI) and security provider. This development is noteworthy as data transmitted between satellites and ground stations has conventionally been susceptible to theft when traveling through the air, rendering satellite communications even more exposed than typical internet communications, as highlighted by the vendor [11].

In August 2023, Google revealed a significant initiative to enhance the security of web browsing against potential quantum threats by introducing Chrome support for quantum-resistant encryption. Termed X25519Kyber768, this novel quantum-resistant cryptography involves a hybrid mechanism that combines the outputs of two cryptographic algorithms to encrypt Transport Layer Security (TLS) sessions. The hybrid encryption method integrates X25519, an elliptic curve algorithm widely utilized for key agreement in current TLS implementations, and Kyber-768, a quantum-resistant Key Encapsulation Method (KEM). This advanced encryption has been incorporated into Chrome 116 and is accessible behind a flag in Chrome 115. Pareekh Jain, Chief Analyst at Pareekh Consulting, commented on Google's proactive approach, stating, "Google's announcement regarding the protection of encryption keys in Chrome from quantum computers demonstrates a forward-looking perspective. While widespread adoption of quantum computers is still a few years away, there is a present risk of messages being stored and decrypted later."[12].

In September 2023, a group consisting of technologists, researchers, and skilled practitioners introduced the PQC Coalition to advance widespread comprehension and public acceptance of PQC algorithms. IBM Quantum, Microsoft, MITRE, PQShield, SandboxAQ, and the University of Waterloo are among the founding members of the coalition. The PQC Coalition intends to leverage its combined technical knowledge and impact to promote the worldwide integration of PQC in both commercial and open-source technologies. Members of the coalition will utilize their expertise to encourage and progress interoperable standards and technical strategies. Additionally, they will actively engage as informed authorities, providing essential outreach and education to the public [13].

In the Philippines, there is a study that highlights the limited knowledge and challenges regarding cryptocurrencies and blockchain wallet access. The Philippines has legalized cryptocurrency use with approval from the Central Bank of the Philippines, and it is utilized by banks and money transfer outlets in the country. Popular cryptocurrencies in the Philippines, such as Bitcoin, Ethereum, XRP, and Bitcoin Cash, are widely accepted. The research notes the volatility in cryptocurrency prices, with fluctuations between high and low peaks. Additionally, it mentions that central organizations in the country are adopting this technology through centralized establishments [14]. The limited knowledge and challenges regarding cryptography are also the findings of another comprehensive study on the Feasibility and Suitability of Bitcoin in the Philippine Setting [9]. This study focuses on the feasibility and suitability of Bitcoin adoption in the Philippines. It emphasizes that cryptocurrencies, particularly Bitcoin, have gained substantial interest due to their trust-enhancing decentralized nature. The study explores the social aspects of Bitcoin adoption in the Philippines, utilizing surveys and interviews among Filipinos. The findings indicate that a significant portion of the population is aware of cryptocurrencies, but their overall knowledge, particularly regarding Bitcoin, remains relatively low. The research suggests that, while Bitcoin may be feasible in the Philippines, it is currently unsuitable due to insufficient cryptocurrency knowledge, financial literacy, and willingness to adopt it among the population [15].

In the Provincial Government of Davao del Norte, there is a need for the adoption of cryptographical technologies including the advancement of the use of post-quantum cryptography. The organization has already established its transactional systems. Transactional systems in the organization encompass the Executive Management System (EMIS), Financial Management Information System, Properties and Supplies Information Management Systems (PASIMS), and the Human Resource Management Information System (HRIS). One of the problems encountered in the organization is the increasing data volume in their transactional systems. Every year, a large amount of data is generated by these systems. The proposed solution for the expansion of data is the implementation and application of data warehousing for permanent data. In line with this innovative solution, another problem arises which is the verification and validation of the data to be stored in the data warehouse. This study proposes a solution for the verification, validation, and tamper-proofing of permanent data in preparation for the storage of data in the data warehouse by generating a hash digest of every record of the identified permanent data to be uploaded by the data owners which can be verified by solving the hashes in each record comparing it to the raw data of records. This work proposes the Fast-Fourier Lattice-based Compact Signatures Over NTRU (FALCON) to add a more secure feature that uses post-quantum cryptography in hashing the data. Quantum cryptography relies on the principles of quantum mechanics and the unique informational characteristics of quantum systems [16]. Quantum computing, originally conceptualized by Richard Feynman in 1982, poses a significant threat to both current asymmetric and symmetric cryptography. Researchers are working on quantum algorithms that can compromise the security of existing asymmetric encryption methods that rely on factors like prime numbers and discrete logarithms. Even the widely trusted elliptic curve cryptography is vulnerable to quantum computers. Consequently, there is a growing demand for cryptographic solutions that can resist the potential threats posed by quantum computing [17].

Aligned with the Sustainable Development Goals (SDGs) set by the United Nations, this study focuses on enhancing data integrity within the Provincial Government of Davao del Norte, the alignment with Goal 16 (Peace, Justice, and Strong Institutions) is evident. As this project aims to strengthen the integrity of systems data, it promotes the rule of law and equal access to justice, as outlined in Target 16.3. By safeguarding sensitive information and ensuring data protection, this project strengthens the foundations of a just and secure institution, fostering trust and accountability within the government's data management systems. Furthermore, Goal 17 (Partnerships for the Goals) plays a role in the project's collaborative nature. While not directly linked to a specific indicator, my capstone underscores the significance of partnerships, knowledge sharing, and cooperation in implementing robust data security measures. These collaborations are essential for achieving the project's objectives and furthering the principles of sustainable development.

**General Objectives**

This study aims to develop a Fast-Fourier Lattice-based Compact Signatures Over NTRU (FALCON) Post-quantum Cryptography for Systems Data in the Provincial Government of Davao del Norte.

**Specific Objectives**

In particular, the developer/researcher intends to establish a system with the capability to:

1. Develop a web application to access the system's user interface.
2. Generate public and private FALCON keys that bind to every user’s identity.
3. Generate FALCON digital signatures using the user’s private key of identified permanent data, files, or messages into the system.
4. Verify the authenticity of the data based on the user’s public key in comparison to the generated FALCON hash of records in the system.
5. View their authenticated/verified data in a dashboard.
6. Provide signatory and verification API access to other systems for integration services of the system.

**Significance of the Study**

The chosen organization, the Provincial Government of Davao del Norte, can anticipate several significant benefits from the proposed **Enhancing Data Integrity: A Fast-Fourier Lattice-based Compact Signatures Over NTRU (FALCON) Post-quantum Cryptography for Systems Data in the Provincial Government of Davao del Norte**. This system addresses the critical challenge of managing the increasing volume of data generated by their transactional systems. By providing a tamper-proofing mechanism for data warehousing and verification, the organization can ensure the safe storage of sensitive information. Furthermore, the system's integration capabilities through an API and a user-friendly dashboard will empower the following specific end users:

**Data Owners:** Data owners within the Provincial Government of Davao del Norte would be primary end users. They can verify the authenticity of identified permanent data/tables/records in the system, access the system through an API for integration services, view their uploaded data in a dashboard, and verify the authenticity of their data based on the generated hash of records. These users are likely to be individuals responsible for the data within the organization.

**Administrators and IT Personnel**: IT personnel or administrators responsible for managing and maintaining the system would be end users as well. They would ensure the smooth operation of the system, manage user access, and oversee the technical aspects of the Fast-Fourier Lattice-based Compact Signatures Over NTRU (FALCON) Post-quantum Cryptography system.

**External and Internal Auditors and Regulators**: External auditors and regulatory bodies, especially the Commission on Audit (COA), may use the system to verify the data integrity and security measures in place within the organization. This is especially relevant in the context of government organizations that need to comply with various regulations and standards.

**Citizens and the General Public:** Depending on the nature of the data stored by the Provincial Government of Davao del Norte, the public or citizens may indirectly benefit from enhanced data security and integrity, as it can lead to more transparent and accountable government operations.

**Researchers and Academics:** Researchers and academics in the field of post-quantum cryptography, data security, and information technology may find the study significant for academic and research purposes. They can use the findings and methodologies for further research and education.

The result is improved data management, organization, and security, essential for an institution's efficiency and accountability. Additionally, the collaborative nature of the project nurtures knowledge sharing and cooperation, which are crucial for implementing strong data integrity measures. Ultimately, the organization stands to gain enhanced integrity, ensuring the reliability and trustworthiness of its data management systems.

**Scope and Limitations**

This study is conducted exclusively for the benefit of the Provincial Government of Davao del Norte, focusing on enhancing data integrity within the organization's information systems. Several factors constrain the scope of this project. Firstly, the pilot testing of the proposed security measures will be limited to one core system, namely the Properties and Supplies Information Management System (PASIMS). While this system serves as a representative case, the findings and recommendations may not directly apply to other systems within the organization. The primary users of the study will be the system process owners, who will be involved in the implementation and maintenance of the security measures. The study will exclusively utilize the FALCON-generated hash for data verification. The system platform for implementation will be a web application and API services for integration purposes.

**Definition of Terms**

**Cryptographic Hash Function**: A function that takes an input (or message) and returns a fixed-size string of bytes, which is typically a hexadecimal number. The output, known as the hash value, should be unique to the input data and computationally infeasible to reverse.

**SHA-256:** Secure Hash Algorithm 256-bit. SHA-256 is a specific implementation of a cryptographic hash function that produces a 256-bit (32-byte) hash value.

**Hash Value:** The output of a hash function, a fixed-length string of characters, is typically represented in hexadecimal format. In the case of SHA-256, it's a 64-character hexadecimal string.

**Hash Digest or Message Digest:** Another term for the hash value produced by a cryptographic hash function. It is often used interchangeably with "hash value."

**Discrete Fourier Transform (DFT):** is a mathematical transformation that transforms a sequence of complex numbers (or real numbers) into another sequence of complex numbers.

**Fast Fourier Transform (FFT):** is an algorithm for efficiently computing the discrete Fourier transform (DFT) and its inverse. A mathematical algorithm that transforms a function of time (or space) into a function of frequency, is widely used in signal processing and cryptography.

**Lattice:** a lattice is a discrete set of points that spans a mathematical space in a regular, repeating pattern.

**Lattice-Based Cryptography:** A cryptographic approach that relies on the mathematical structure of lattices, particularly resistant to attacks by quantum computers.

**Compact Signatures:** Efficient and concise representations of digital signatures, reducing the size of cryptographic signatures for improved efficiency.

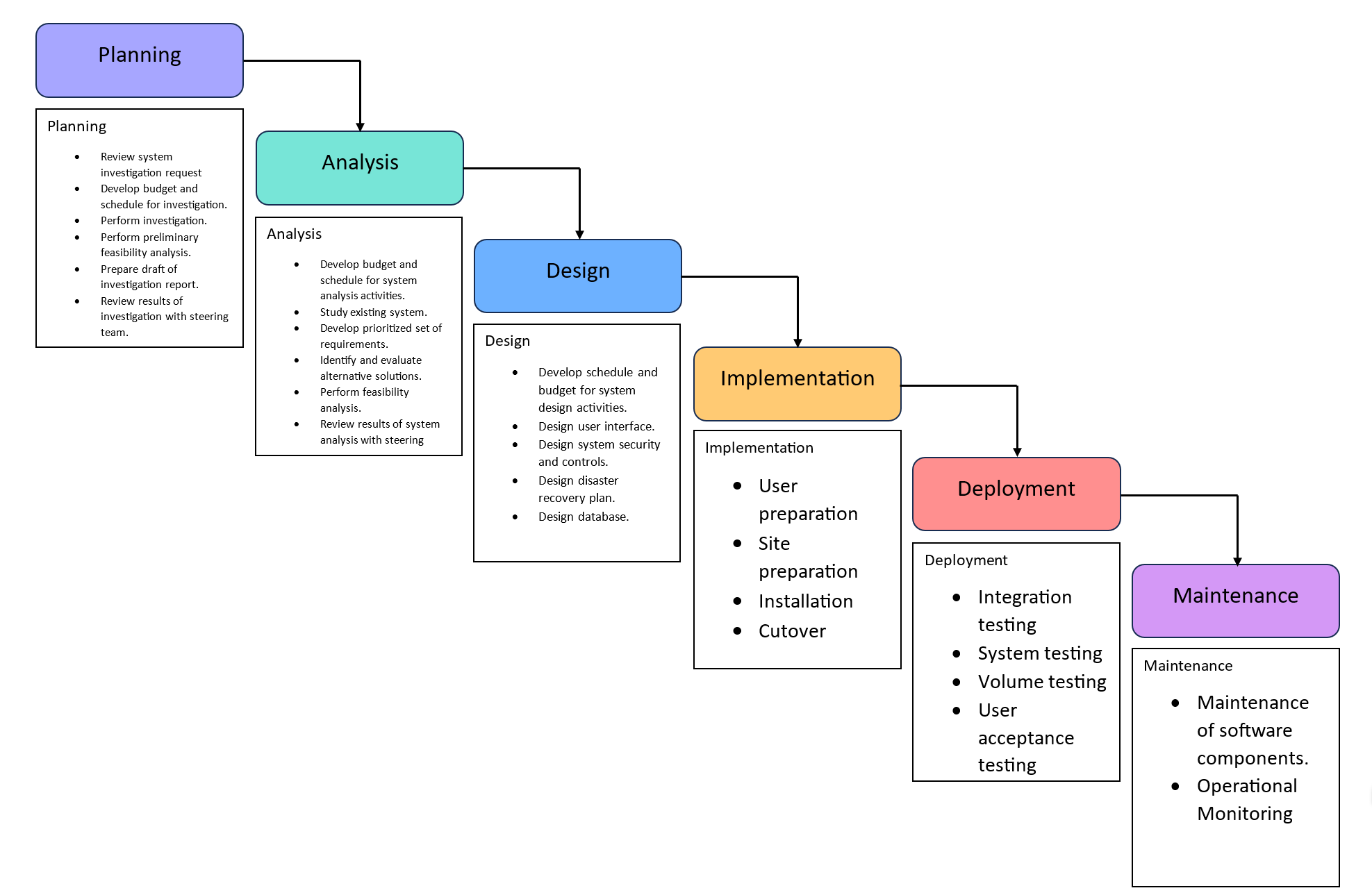
**N-th degree Truncated polynomial Ring Units (NTRU):** an open-source public-key cryptosystem that uses lattice-based cryptography to encrypt and decrypt data.

**Fast-Fourier Lattice-based Compact Signatures Over NTRU** **(FALCON):** Falcon is a cryptographic signature algorithm submitted to the NIST Post-Quantum Cryptography Project on November 30th, 2017.

**Chapter 2**

**METHODOLOGY**

For the implementation of the Fast-Fourier Lattice-based Compact Signatures Over NTRU (FALCON) Verification and Validation of systems data in the Provincial Government of Davao del Norte, the Waterfall methodology proves to be a suitable choice. Given the project's specific objectives, scope, and focus on enhancing data integrity within a well-defined organization, the Waterfall approach aligns with the structured and linear nature of the project. In the Waterfall methodology, the project sequentially progresses through distinct phases, including requirements gathering, system design, implementation, testing, deployment, and maintenance. This sequential flow ensures that each phase is completed before moving on to the next, which is particularly beneficial for a project with defined and specific objectives. The Waterfall model allows for clear documentation, systematic testing of each component, and comprehensive verification and validation, which are essential for a project focused on data security. Moreover, the project's scope and limitations, such as the focus on a single core system (PASIMS) and a limited number of records for processing, align well with the Waterfall model's structured approach. This methodology will enable a systematic and controlled development process for the Secure Hash Algorithm Verification and Validation system, ensuring that the objectives are met efficiently, and that the system is ready to enhance data integrity within the organization. Figure 1 Shows the Waterfall Methodology in the development of the system.



**Figure 1**. Modified Waterfall Model

**System Planning**

In the initial phase, the project begins with a thorough review of the system investigation request, pointing to understanding the specific needs and objectives of the Provincial Government of Davao del Norte. During this phase, a budget and schedule for the investigation are meticulously developed, ensuring that the project's financial and temporal aspects are well-defined. The core activities include performing the investigation itself, collecting vital data and information to inform subsequent project stages, and conducting a preliminary feasibility analysis to assess the practicality of the proposed solution. This phase culminates in the preparation of a draft investigation report, summarizing the findings and insights gathered. The results of the investigation are presented to the steering team, providing an opportunity for review and validation, ensuring alignment with the project's objectives, and initiating the groundwork for subsequent phases of the project.

*Work Breakdown Structure (WBS)*

The utilization of the Work Breakdown Structure (WBS) in this project is of paramount importance to ensure a systematic and well-structured approach to project management. The WBS serves as the project's foundational framework. By hierarchically decomposing the project into smaller, more manageable components, the WBS enhances project clarity and transparency, enabling the developer and stakeholders to track progress, identify dependencies, and allocate resources efficiently. Figure 2 shows the Work Breakdown Structure of the project.

A diagram with colorful text

Description automatically generated with medium confidence

**Figure 2.** Work Breakdown Structure

*Project Schedule*

A Gantt chart, employed as a project management instrument, helped the developer in organizing and arranging project activities. This chart visually represents the names of tasks, timelines for different project components, and the durations associated with each task and its subtasks. Figure 3 shows the project schedule in a Gantt chart.

A graph with a chart and a graph

Description automatically generated with medium confidence

**Figure 3.** The Gantt Chart

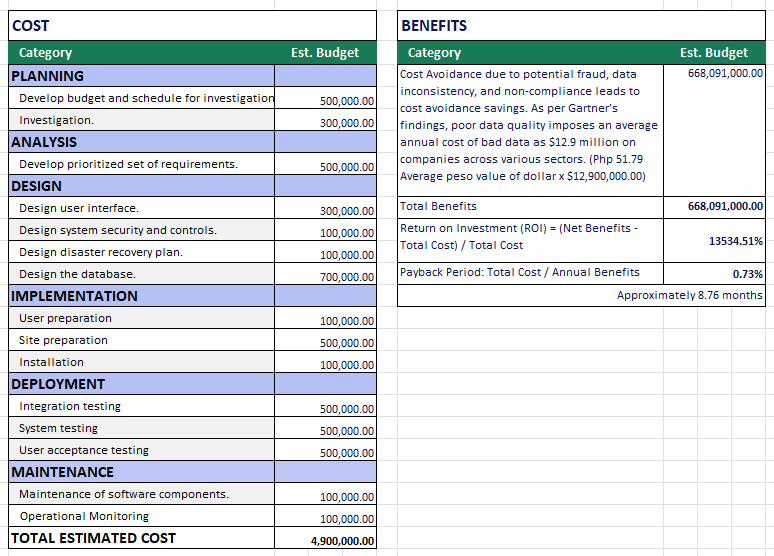
**Feasibility Study**

The feasibility study in this project plays an essential role in evaluating the practicality and viability of implementing the Fast-Fourier Lattice-based Compact Signatures Over NTRU (FALCON) Post-quantum Cryptography system within the Provincial Government of Davao del Norte. It encompasses a systematic and in-depth analysis of various aspects, including technical, financial, operational, and organizational feasibility. Technical feasibility assesses the project's compatibility with existing systems, technology requirements, and the capability of the proposed solution to meet the organization's needs. Financial feasibility involves budget and cost-benefit analyses, ensuring that the project can be executed within the allocated budget and that the benefits justify the investment. Operational feasibility evaluates the potential impact on day-to-day operations, identifying any disruptions and proposing mitigation strategies. Lastly, organizational feasibility examines whether the project aligns with the government's strategic goals, considers the available human resources, and ensures the organization's readiness for the proposed changes.

*Economic Feasibility*

The following economic feasibility study serves as a basis for informed decision-making, ensuring that the project aligns with the organization's financial objectives and delivers a favorable return on investment. As data security and integrity are paramount in modern governance, the economic feasibility assessment underscores the project's potential to yield not only financial gains but also to safeguard against potential losses and risks associated with data breaches or errors, ultimately contributing to the organization's long-term fiscal stability and operational effectiveness. The proposed project is estimated to gain a Return on Investment (ROI) of 0.73% in 8.7 months after deployment.

**Table 1.** Economic Feasibility



*Technical Feasibility*

To evaluate the project’s compatibility with the existing system, the developer created a technical feasibility of the readiness of the software and hardware infrastructure and the capability of the Fast-Fourier Lattice-based Compact Signatures Over NTRU (FACLON). It delves into the technical challenges, risks, and opportunities that may arise during project execution, ensuring that the necessary technological components are in place to support the project's objectives. Table 2 shows the Hardware requirements of the system.

* Hardware Requirements

**Table 2.** Hardware Requirements

A screenshot of a computer hardware requirements

Description automatically generated

To accommodate existing infrastructure while maintaining the computational capabilities necessary for the successful execution of the Fast-Fourier Lattice-based Compact Signatures Over NTRU (FALCON) Post-quantum Cryptography. The developer Identified the minimum hardware requirement for the system entails a standard desktop computer with an Intel® Core® i5-8259U processor operating at a base frequency of 2.3 GHz, with TurboBoost disabled. This specification ensures that the system can function optimally on a widely available and cost-effective hardware configuration [insert Falcon reference here].

**Table 3.** The FALCON’s Performance Based on the Minimum Hardware Requirements

A screenshot of a computer

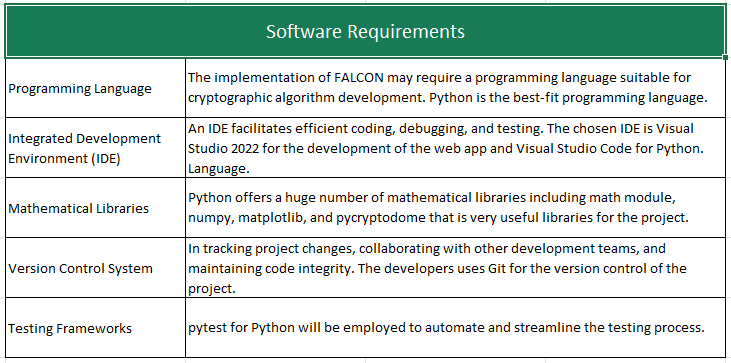
Description automatically generated

Table 3 shows the dimensions of FALCON's performance metrics, encompassing key generation RAM usage, public key size, and signature size, which are quantified in bytes. The time required for key generation is presented in milliseconds. While the private key size is not explicitly stated in the table, it is approximately three times that of a signature.

* Software Requirements

The software requirements for the development of the project are carefully selected to ensure efficiency, reliability, and security throughout the development lifecycle. Table 4 shows the general software requirements of the system.

**Table 4.** Software Requirements



**Table 5.** Comparison Among Programming Languages

A table with green and white text

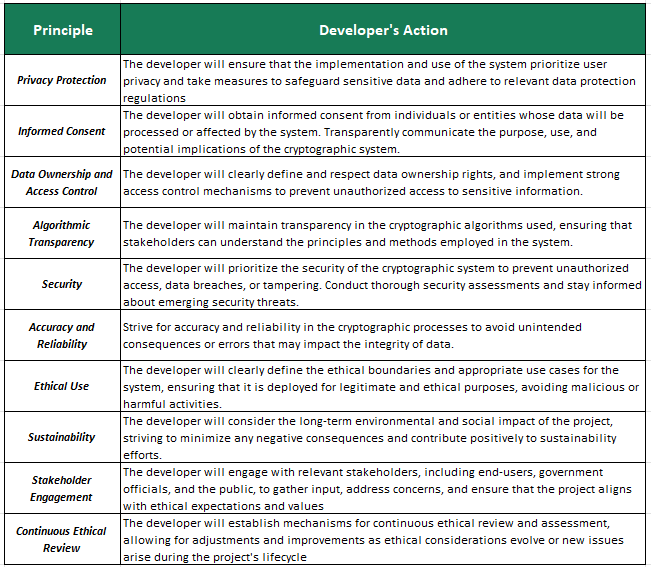
Description automatically generated

Python stands out as the optimal programming language for cryptographic algorithm development due to its versatility and extensive library support. The chosen Integrated Development Environment (IDE) combination, comprising Visual Studio 2022 for web app development and Visual Studio Code for Python, provides a strong platform for efficient coding, debugging, and testing. Python's rich ecosystem includes mathematical libraries such as the math module, numpy, matplotlib, and pycryptodome, providing comprehensive support for the complex mathematical operations inherent in cryptographic algorithms. The project employs Git as the Version Control System, facilitating seamless collaboration, change tracking, and code integrity maintenance. For testing, the pytest framework for Python is utilized, automating, and streamlining the testing process to ensure the reliability and correctness of the FALCON system. Together, these software requirements form a well-integrated and cohesive development environment, laying the foundation for a secure and effective implementation of the FALCON Post-quantum Cryptography system. and Table 5 shows that the Python and C# programming languages are the best combination of coding environment for the project.

* Ethical Considerations

In the development of the system, a conscientious approach to ethical considerations is important. Firstly, utmost priority is given to privacy protection, ensuring that user data is handled with the utmost care and in compliance with data protection regulations. Obtaining informed consent from individuals or entities affected by the system is a fundamental ethical practice, promoting transparency regarding the system's purpose and potential implications. The project places a strong emphasis on algorithmic transparency, striving to maintain openness in cryptographic processes to allow stakeholders to understand the methods employed. Ethical use and defining appropriate boundaries for the system's application are critical, ensuring that FALCON is deployed only for legitimate and ethical purposes, steering clear of malicious activities. Throughout development, a commitment to fairness, accuracy, and reliability is upheld, minimizing biases and errors that may impact data integrity. Stakeholder engagement is actively pursued to gather diverse perspectives, and accessibility is prioritized to create an inclusive system. The project also recognizes the importance of legal compliance, sustainability, and continuous ethical review to adapt to evolving ethical standards and emerging challenges, encouraging a responsible and ethical development approach for the FALCON system. Table 6 summarizes the ethical considerations of the developer in the implementation of the system.

**Table 6.** The Project Ethical Considerations



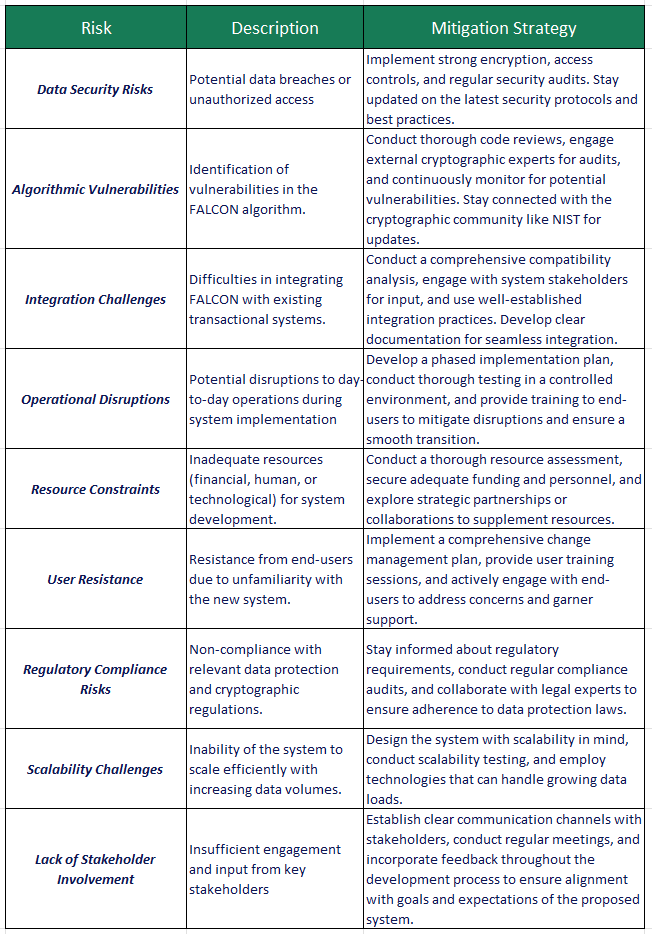
*Operational Feasibility*

Operational feasibility in the development of the proposed system is a critical aspect that addresses the practicality and effectiveness of integrating the solution into the operational framework of the Provincial Government of Davao del Norte. The project acknowledges the existing transactional systems within the organization, including the Executive Management System (EMIS), Financial Management Information System, Properties and Supplies Information Management Systems (PASIMS), and the Human Resource Management Information System (HRIS). The proposed system must seamlessly align with these established systems to ensure a smooth and coherent integration process. As the organization faces challenges related to the increasing data volume generated by these systems, the operational feasibility study aims to validate the viability of the proposed solution, considering aspects such as data verification, validation, and tamper-proofing for permanent data storage. The success of the proposed system hinges on its ability to enhance operational efficiency, streamline data management processes, and provide user-friendly interfaces for data owners. Additionally, the project's commitment to utilizing an API for integration services and creating graphical dashboards demonstrates a forward-looking approach to operational feasibility, ensuring that the system is adaptable, user-friendly, and aligned with the operational requirements and goals of the Provincial Government of Davao del Norte.

*Risk Assessment and Mitigation*

Risk assessment and mitigation in developing the proposed system is a meticulous process designed to identify, evaluate, and address potential challenges that could impact the project's success. One primary risk involves data security, where strong encryption, effective access controls, and continuous security audits are implemented to counter the risk of data breaches. Algorithmic vulnerabilities are addressed through rigorous code reviews, external cryptographic expert audits, and vigilant monitoring for potential weaknesses. Integration challenges are managed through thorough compatibility analyses and the creation of clear documentation, ensuring a smooth integration with existing transactional systems. Operational disruptions are minimized with a phased implementation plan, extensive testing, and user training sessions. Resource constraints are addressed by conducting a thorough resource assessment, securing adequate funding and personnel, and exploring strategic partnerships. User resistance is mitigated through a well-structured change management plan and continuous user engagement. Regulatory compliance risks are managed by staying informed about relevant regulations and conducting regular compliance audits. Scalability challenges are addressed by designing the system with scalability in mind and conducting thorough scalability testing, while the lack of stakeholder involvement is minimized through clear communication channels and regular stakeholder engagement. This comprehensive approach to risk assessment and mitigation ensures that the development of the proposed system progresses with a keen awareness of potential challenges and effective strategies to address them. Table 7 shows the tabular presentation for the Risk Assessment and Mitigation of the proposed system.

**Table 7.** Risk Assessment and Mitigation of the proposed system



**Requirements Specification**

The requirements specification for the proposed system involves critical elements derived from user needs. The user profile is a foundational requirement, outlining the important details and attributes of individuals interacting with the system. User credentials, comprising unique identifiers and authentication information, are crucial for secure access and user verification. The key pair itself, composed of a private and public key, is fundamental to cryptographic operations, facilitating secure data transactions. Importantly, the key pair serves as a binding mechanism, associating the identity of the user with the generated keys. This linkage is important as it signifies the user's authority and responsibility for validating the authenticity and integrity of the associated data, contributing to the general security and trustworthiness of the proposed system. To determine the necessary details about the process of digital signatures and non-repudiation of user’s actions, a literature review was conducted.

Key Generation

A diagram of a computer program

Description automatically generated with medium confidence

**Figure 4.** The Process of Digital Signature Attachment

A diagram of a document

Description automatically generated

**Figure 5.** The Process of Digital Signature Verification

**System Analysis**

To gain a clear understanding of the specifics of the problem to solve or the opportunities to address, a system investigation is performed. First, a preliminary statement of the problem is refined. It is identified that there is a need for data warehousing of systems data in the Provincial Government of Davao del Norte to reduce the load from systems servers by transferring permanent systems data into a data warehouse. In line with the first identified problem, the main problem arises the data verification and validation. The following conceptual framework of the system is created by performing an initial system investigation.

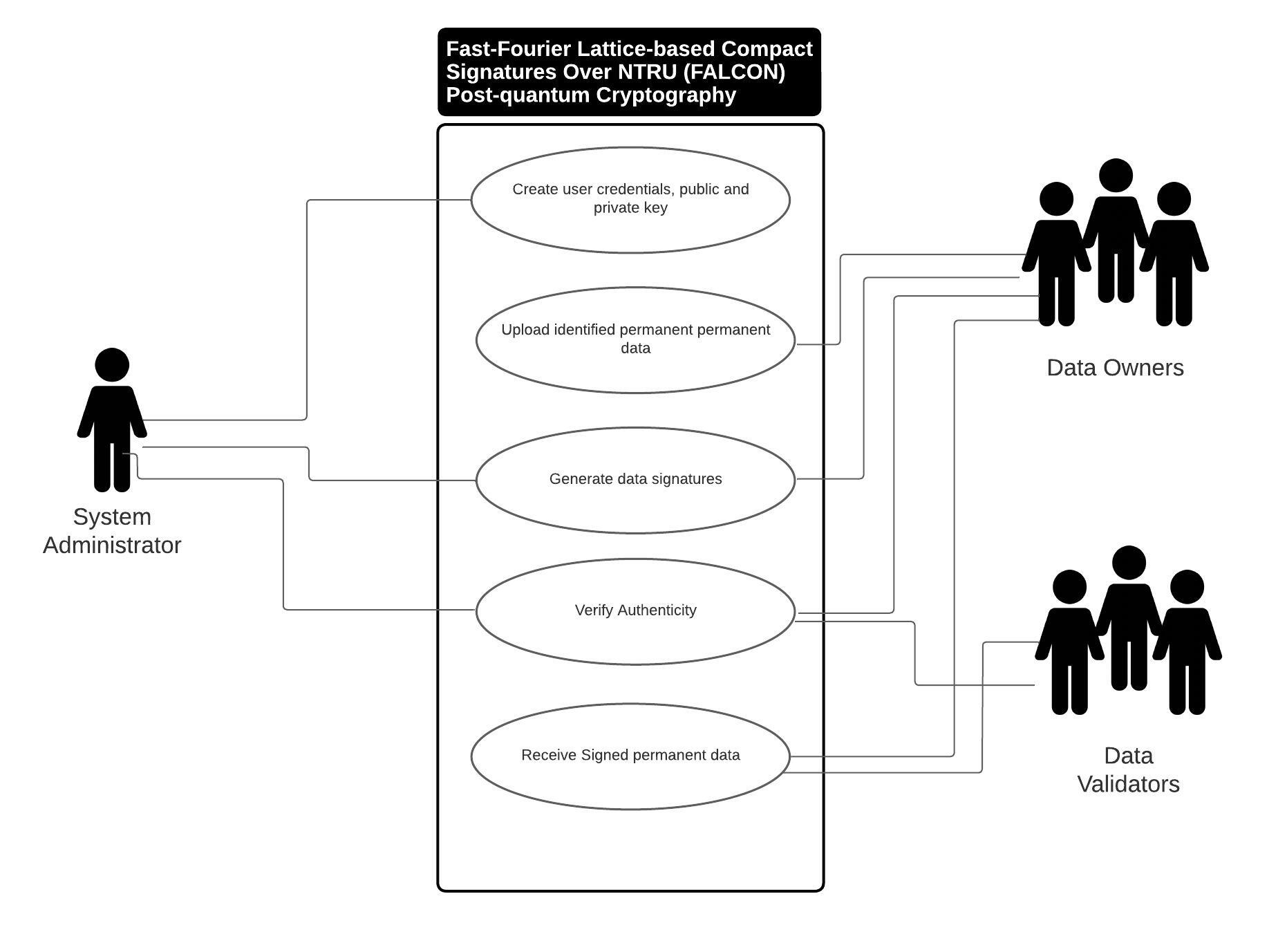
**A diagram of a computer

Description automatically generated**

**Figure 6.** The Conceptual Framework

The initial step in the system process involves identifying the user's permanent data, which is then converted into a byte string. The user's digital signature, generated during the user registration process, is also associated with this data. Permanent data, which can encompass various types such as text, images, files, and records, serves as input for hash generation within the system. Users interact with the system through a web app interface, and upon uploading data, the web app triggers an API call for data signature generation. The API, in turn, produces a hash digest or data signature corresponding to the input data. Subsequently, this data signature is appended to the original data, serving to verify its authenticity. Users can validate the data either through the web application or by utilizing the web API.

*Use Case Diagram*



**Figure 7.** Use Case Diagram

Figure 4 shows the use case diagram of the proposed system. Three identified users have access to the major functionality of the system. The system administrator is the one who is responsible for the creation of user credentials and the generation of the user’s public and private keys. After a user profile is created, users can now have access to the web application for them to upload their identified permanent data in the system. The generation of data signatures can be done by both System Administrator and Data Owners. The verification of the authenticity of data signatures can be done by the data owners themselves, the system administrator, and the data validators.

**System Design**

The proposed system is designed in ASP.net C# utilizing the Model View Controller (MVC) design pattern. The model(M) serves as the application’s data and business logic. It is responsible for retrieving and storing data, as well as defining the rules that govern the manipulation of that data. In ASP.NET, models are often represented as classes that interact with a database or other data sources. The view(V) is responsible for displaying the data to the user. The view utilizes AngularJS, HTML, and Bootstrap for the design. The controller(C) is responsible for handling user input, processing it, and updating the model and/or view accordingly. In the context of ASP.NET, controllers handle incoming HTTP requests, interact with the model to retrieve, or update data, and then determine which view should be used to present the response to the user. Furthermore, the FALCON’s main functionality is implemented in a Python environment. The major challenge in designing this system is integrating FALCON’s Python code into the controller side of the web application.

**Technologies Concept and Theories**

The following summarizes the applications used in developing the Fast-Fourier Lattice-based Compact Signatures Over NTRU (FALCON) Post-quantum Cryptography for Systems Data in the Provincial Government of Davao del Norte.

**Technologies Applied**

*Fast-Fourier Lattice-based Compact Signatures Over NTRU (FALCON)*

Falcon stands out as the most compact among all post-quantum signature schemes, showing an efficient and concise design that minimizes computational overhead. Not only does Falcon excel in compactness, but it also demonstrates commendable speed, making it a compelling choice for cryptographic applications that require both efficiency and security. Notably, the implementation of the signature component, referred to as Sign, introduces a delicate process involving Fast Fourier Sampling. This intricacy underscores the precision and sophistication required to execute this important element of the Falcon algorithm.

* **Cyclotomic Ring**

The Cyclotomic ring is employed for the falcon’s algorithm. A cyclotomic ring is a mathematical structure that arises in the study of algebraic number theory. This ring is constructed by taking polynomials with coefficients in the finite field *Zq* and quotient out by the ideal generated by *x + 1*. This construction can have applications in various areas of mathematics, such as algebraic number theory, coding theory, or cryptography, depending on the context in which it is used.

***R = Zq[x] / (x + 1)***

1. ***Zq***: This typically denotes the finite field of order *q*. The elements in this field are integers modulo ***q***. The field has ***q*** elements, where ***q*** is a prime power.
2. ***Zq[x]***: This is the polynomial ring over the finite field ***Zq****.* It consists of polynomials whose coefficients are elements of ***Zq****.*
3. ***(x + 1)***: Is an ideal in the polynomial ring ***Zq[x]****.* The ideal generated by ***x + 1***consists of all polynomials that have ***x + 1***as a factor.
4. ***Zq[x]/(x + 1)***: This represents the quotient ring obtained by dividing ***Zq[x]*** by the ideal ***(x + 1)***. In other words, it's the set of equivalence classes of polynomials in ***Zq[x]***, where two polynomials are considered equivalent if their difference is in the ideal ***(x + 1)***. This is also known as the quotient ring or residue class ring.
5. Cyclotomic Ring ***R***: The quotient ring ***Zq[x] / (x+1)*** is referred to as a cyclotomic ring. The term "cyclotomic" often comes up in the context of rings obtained by adjoining roots of unity.

* **Key Generation Algorithm (*Keygen()*)**

**A white background with black text

Description automatically generated**

**Figure 9.** ProcessPseudo Code of Key Generation Algorithm

Step 1:

**Generate Matrices *A, B* with Coefficients in *R*:**

Two matrices, ***A*** and ***B***, are generated. The coefficients of these matrices belong to the cyclotomic ring ***R***. Additionally, the matrices are chosen in such a way that product ***B A*** results in the zero matrix. This property is often crucial for the security of cryptographic systems.

**Note:**

The condition ***B A = 0*** implies that the rows of ***B*** are orthogonal to the columns of ***A***, which is a common property in cryptographic schemes.

**Note:**

The use of matrices over the cyclotomic ring suggests a connection to lattice-based cryptography, where problems related to lattices are utilized for cryptographic security.

**Additional Condition on Matrix** ***B***: The matrix ***B*** is specified to have small coefficients. This condition is likely related to the hardness assumptions or security properties of the Falcon.

Step 2:

**Public Key (*pk*):**

The public key (***pk***) is set to be matrix ***A.***

Step 3:

**Secret Key (*sk*):**

The secret key (***sk***) is set to be matrix ***B.***

The key generation algorithm involves the generation of matrices ***A*** and B over the cyclotomic ring ***R***, with specific properties related to their product and the size of coefficients in ***B***. The public key ***(pk)*** is then set to be matrix ***A***, and the secret key ***(sk)*** is set to be matrix ***B***. The use of a cyclotomic ring in this context may be motivated by the cryptographic properties it offers, and the specific structure of ***R*** may be exploited for security.

* **Signing a Message (*m*)**

***A black text on a white background

Description automatically generated***

**Figure 10.** Process Pseudo Code of Signing a Message

Step 1:

**Compute *c* such that *cA = H(m)***:

Here, ***A*** is a matrix from the public key, and ***H(m)*** represents a hash of the message ***m***. The goal is to find a vector ***c*** such that multiplying it by matrix ***A*** results in a value close to the hash of the message. This step is often related to the challenge-response mechanism used in digital signatures.

Step 2:

**Select *V ←* "a vector in the lattice *Λ(B)*, close to *c*"**:

This step involves selecting a vector (***v*** from the lattice ***Λ(B)***, which is related to the secret key ***B*** in the public-key scheme. The vector ***v*** is chosen to be close to the computed vector ***c***.

* + **Lattice:** In lattice-based cryptography, a lattice is a discrete set of points with a certain structure. The lattice ***Λ(B)*** is associated with the secret key matrix ***B***.
  + **Selecting *v* close to *c***: The choice of a vector ***v*** close to ***c*** is likely part of a mechanism to introduce randomness and enhance the security of the signature scheme. The closeness of ***v*** to ***c*** is a measure of how well the signer can hide the actual value of ***c***.

Step 3:

**Generate the signature *s*** ***←c−v***:

The signature s is then computed as the difference between the vector c and the chosen vector v.

* + **Interpretation:** This subtraction is a way to blind the value of ***c***, making it difficult for an adversary to recover ***c*** from the signature ***s***. The resulting ***s*** is part of the signature for the message ***m***.
  + **The Signature *s*:** The final signature is represented as a tuple ***s = (s1, s2)***, where ***s1***​ and ***s2***​ are components of the vector ***s***.

In summary, the signing process involves computing a vector c that is related to the hash of the message, selecting a vector ***v*** from the lattice ***Λ(B)*** close to ***c***, and then computing the signature ***s*** as the difference between ***c*** and ***v***. This process likely leverages the hardness of lattice problems for security, a common approach in lattice-based cryptography.

* **Verifying the message and the signature using the public key *Verify (m, pk sig)***

This function takes three parameters: a message ***m***, a public key ***pk***, and a signature ***sig***. The purpose of this function is to verify whether the signature ***sig*** is valid for the given message ***m*** and public key ***pk***.

**A black and white text

Description automatically generated**

**Figure 11.** Process Pseudo Code of Message Verification

Step 1:

**Accept if *s* is short**:

The length or size of the signature ***s*** should be relatively short. This condition is often desirable in practical applications as shorter signatures lead to more efficient communication and storage.

* + **Short Signature Requirement**: This requirement may be imposed to achieve efficiency in terms of bandwidth, storage, and computation. Short signatures are desirable for many practical applications, especially in resource-constrained environments.

Step 2:

**Accept if *sA = H(m)*:**

Multiply the signature vector s by the public key matrix ***A***, and the result should be equal to the hash of the message ***H(m)***. In other words, verify that the linear combination of the signature vector ***s*** and the public key matrix ***A*** corresponds to the hash of the message.

* **Linear Combination Verification**: The equation ***sA=H(m)*** represents a key equation in the verification process. This equation ensures that the signature was generated using the private key corresponding to the given public key and that it corresponds to the hash of the message. The linear combination involving matrix multiplication is a common structure in cryptographic schemes, especially in lattice-based cryptography.
* **Rejection Criteria**: If either of the conditions is not satisfied, the verification process should reject the signature. This rejection is important for ensuring the integrity and authenticity of the signed messages.

In summary, the verification process checks the length of the signature and verifies that the linear combination of the signature and the public key matches the hash of the message. If both conditions are met, the signature is accepted as valid; otherwise, it is rejected.

*Python*

Python is a programming language that is interpreted, interactive, and follows an object-oriented paradigm. It comes equipped with high-level data structures like lists and dictionaries, dynamic typing, dynamic binding, modules, classes, exceptions, and automatic memory management. Despite its remarkably simple and elegant syntax, Python is a potent and versatile programming language suitable for various purposes. Guido van Rossum designed it in 1990. Like many other scripting languages, Python is freely available for both personal and commercial use and is compatible with virtually any modern computer. When a Python program is executed, the interpreter automatically compiles it into platform-independent bytecode, which is then interpreted [18] [20] [21].

*AngularJS*

The front-end functionalities of the Fast-Fourier Lattice-based Compact Signatures Over NTRU (FALCON) are designed using the AngularJS framework. AngularJS is a JavaScript-based open-source front-end web application framework. It was developed and maintained by Google. AngularJS is designed to make both the development and testing of such applications easier by providing a framework for client-side model-view-controller (MVC) architecture and other common components used in web development [22].

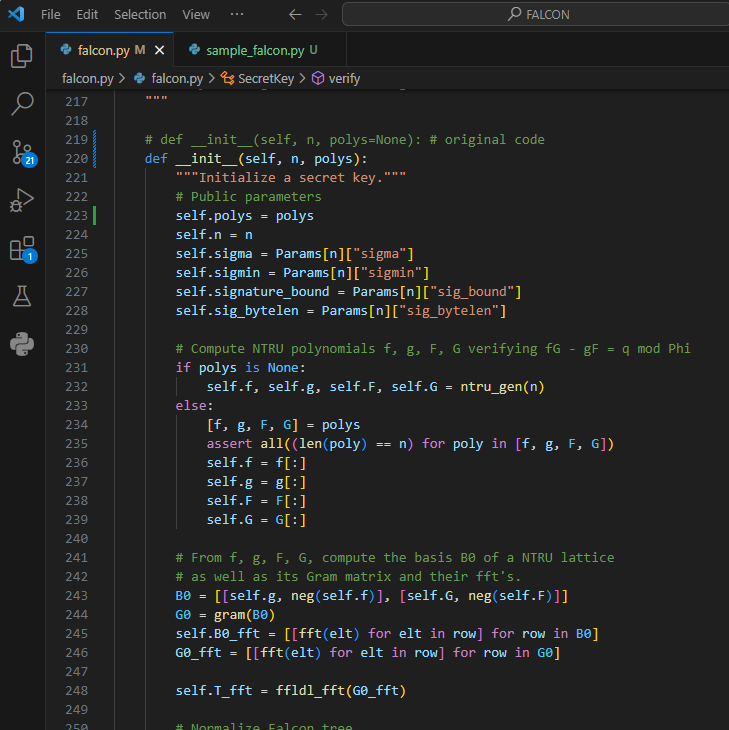
**Concepts and Theories**

*Fast Fourier Transform (FFT)*

The Fast Fourier Transform (FFT) is an algorithmic method for efficiently computing the Discrete Fourier Transform (DFT) and its inverse. The Fourier Transform is a mathematical technique that transforms a signal or function from its original domain (usually time or space) into a representation in the frequency domain. This transformation reveals the frequency components present in the signal. The FFT is particularly significant because it dramatically reduces the computation time required for the Fourier Transform, especially for large datasets. The standard DFT computation involves *O(N2)* operations, where *N* is the number of data points. In contrast, the FFT algorithm reduces this to *O(N* log *N),* making it much more efficient, especially for tasks like signal processing and spectrum analysis [23] [24]

*FALCON*

Fast-Fourier Lattice-based Compact Signatures Over NTRU (FALCON) On November 30th, 2017, Falcon, a cryptographic signature algorithm, was submitted to the NIST Post-Quantum Cryptography Project. It was developed by a team consisting of Pierre-Alain Fouque, Jeffrey Hoffstein, Paul Kirchner, Vadim Lyubashevsky, Thomas Pornin, Thomas Prest, Thomas Ricosset, Gregor Seiler, William Whyte, and Zhenfei Zhang. Falcon is grounded in the theoretical framework proposed by Gentry, Peikert, and Vaikuntanathan for lattice-based signature schemes. The researchers implement this framework using NTRU lattices and a trapdoor sampler known as "fast Fourier sampling." The fundamental computational challenge addressed by Falcon is the short integer solution problem (SIS) over NTRU lattices. As of now, there is no known efficient algorithm for solving this problem in the general case, even with the assistance of quantum computers [25]. Figure 4 shows a Python code snippet implementation of FALCON.



**Figure 12.** Code snippet of FALCON implementation in Python

**System Implementation and Testing**

The Fast-Fourier Lattice-based Compact Signatures Over NTRU (FALCON) Post-quantum Cryptography project follows a rigorous testing approach to ensure the smooth functioning of the system. An integral part of this process is the system testing phase, where the complete system is evaluated against its specified requirements. The testing covers various components such as public and private key generation, signature generation, and signature verification. It involves conducting comprehensive tests to validate the system's ability to handle different user inputs, identify and address potential errors, and respond appropriately. Emphasis is also placed on security testing to verify the strength of cryptographic protocols and protect against potential vulnerabilities. Figure 9 shows a simple implementation of the major functionalities of the FALCON algorithm and Figure 10 shows the sample output of the sample implementation.

A screen shot of a computer program

Description automatically generated

**Figure 13.** Sample FALCON implementation in Python

A screenshot of a computer program

Description automatically generated

**Figure 14.** Sample FALCON implementation results in Python

By running a simple and straight implementation of FALCON, the results showed that the code implementation in Python generated a public and private key for *n = 64.* The generated private key consists of the polynomial (*f, g, F, G)* while the public key for *n = 64* is *h.* By calling the function *pk.verify()* the algorithm returns *True* for the verification result which means that the original message is equivalent to its message signature.

**System Deployment**

To get the most out of the new system, The system will be deployed in 1 month duration. The implementation of the FALCON system involves its utilization under various operating conditions. Maximizing the system's performance during operation is a critical aspect of the organization. Many companies establish formal help desks to offer user support, comprising computer systems, technical experts, and resources to address problems and provide accurate information. The developer will act as the primary helpdesk of the system. Monitoring, a crucial process, measures system performance by tracking errors, memory usage, CPU time, and other indicators. System review is essential for analyzing whether the system operates as intended, comparing its designed performance and benefits with its actual operation.

**System Maintenance**

System maintenance for FALCON is an integral phase in its development lifecycle, focusing on adapting and improving the system to better align with user and organizational objectives. Various factors drive the need for program maintenance, including addressing issues such as slow response times for frequent transactions, bugs, or errors in the program, and technical or hardware challenges. Additionally, changes in business processes, evolving needs of system stakeholders, users, and managers, and external factors like corporate mergers, acquisitions, changes in government regulations, or alterations in the underlying operating system or hardware all contribute to the necessity for ongoing maintenance efforts. This stage ensures that FALCON remains resilient and responsive to the dynamic landscape of user requirements and external factors, sustaining its effectiveness in meeting the cryptographic and security needs of the Provincial Government of Davao del Norte.

**References:**

[1] V. Hassija et al., “Present landscape of quantum computing,” IET Quantum Communication, vol. 1, no. 2, pp. 42–48, Dec. 2020, doi: 10.1049/iet-qtc.2020.0027.

[2] “Zach Kirsch Quantum Computing: The Risk to Existing Encryption Methods”.

[3] W. Cui, T. Dou, and S. Yan, “Threats and Opportunities: Blockchain meets Quantum Computation,” in 2020 39th Chinese Control Conference (CCC), Jul. 2020. doi: 10.23919/ccc50068.2020.9189608.

[4] T. Niraula, A. Pokharel, A. Phuyal, P. Palikhel, and M. Pokharel, “Quantum Computers’ threat on Current Cryptographic Measures and Possible Solutions,” International Journal of Wireless and Microwave Technologies, vol. 12, no. 5, pp. 10–20, Oct. 2022, doi: 10.5815/ijwmt.2022.05.02.

[5] E. V. Haryannto, M. Zulfadly, Daifiria, M. B. Akbar, and I. Lazuly, “Implementation of Nihilist Cipher Algorithm in Securing Text Data With Md5 Verification,” Journal of Physics: Conference Series, vol. 1361, no. 1, p. 012020, Nov. 2019, doi: 10.1088/1742-6596/1361/1/012020.

[6] S. S. Moghadam and A. Fayoumi, “Toward Securing Cloud-Based Data Analytics: A Discussion on Current Solutions and Open Issues,” IEEE Access, vol. 7, pp. 45632–45650, 2019, doi: 10.1109/access.2019.2908761.

[7] S. S. Moghadam and A. Fayoumi, “Toward Securing Cloud-Based Data Analytics: A Discussion on Current Solutions and Open Issues,” IEEE Access, vol. 7, pp. 45632–45650, 2019, doi: 10.1109/access.2019.2908761.

[8] R. Sumithra and R. Parameswari, “Data privacy and data protection security algorithms for big data in cloud,” International journal of health sciences, pp. 7613–7621, May 2022, doi: 10.53730/ijhs.v6ns2.6834.

[9] L. Chen et al., “Report on Post-Quantum Cryptography,” National Institute of Standards, techreport, Apr. 2016. doi: 10.6028/nist.ir.8105.

[10] D. J. Bernstein and T. Lange, “Post-quantum cryptography,” Nature, vol. 549, no. 7671, pp. 188–194, Sep. 2017, doi: 10.1038/nature23461.

[11] M. Zhandry, “CRYPTOGRAPHY IN THE AGE OF QUANTUM COMPUTERS A DISSERTATION SUBMITTED TO THE DEPARTMENT OF COMPUTER SCIENCE AND THE COMMITTEE ON GRADUATE STUDIES OF STANFORD UNIVERSITY IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE DEGREE OF DOCTOR OF PHILOSOPHY”.

[12] I. News, “QuSecure launches live end-to-end satellite quantum resilient link through space.” https://www.helpnetsecurity.com/2023/03/11/qusecure-quantum-resilient-cryptographic-communications-satellite-link/, p. 3, Mar. 10, 2023. [Online]. Available: https://www.helpnetsecurity.com/2023/03/11/qusecure-quantum-resilient-cryptographic-communications-satellite-link/

[13] “Google readies Chrome for distant quantum attacks with new support.” https://www.csoonline.com/article/649480/google-readies-chrome-for-distant-quantum-attacks-with-new-support.html, p. 1. [Online]. Available: https://www.csoonline.com/article/649480/google-readies-chrome-for-distant-quantum-attacks-with-new-support.html

[14] J. R. Jeffrey and Yasay, “The Dawn of Digital Coins: A Literature Review on Cryptocurrency in the Philippines”.

[15] J. R. Jeffrey and Yasay, “The Dawn of Digital Coins: A Literature Review on Cryptocurrency in the Philippines”.

[16] M. Ricci et al., “A Comprehensive Study on the Feasibility and Suitability of Bitcoin in the Philippine Setting”.

[17] F. M. Ablayev and A. V. Vasiliev, “Cryptographic quantum hashing,” Laser Physics Letters, vol. 11, no. 2, p. 025202, Dec. 2013, doi: 10.1088/1612-2011/11/2/025202.

[18] V. Mavroeidis, K. Vishi, M. D., and A. Jøsang, “The Impact of Quantum Computing on Present Cryptography,” International Journal of Advanced Computer Science and Applications, vol. 9, no. 3, 2018, doi: 10.14569/ijacsa.2018.090354.

[19] M. F. Sanner, “PYTHON: A PROGRAMMING LANGUAGE FOR SOFTWARE INTEGRATION AND DEVELOPMENT”.

[20] K. R. Srinath, “Python -The Fastest Growing Programming Language”.

[21] A. J. Dhruv, R. Patel, and N. Doshi, “Python: The Most Advanced Programming Language for Computer Science Applications,” in Proceedings of the International Conference on Culture Heritage, Education, Sustainable Tourism, and Innovation Technologies, 2020. doi: 10.5220/0010307902920299.

[22] W. Chansuwath and T. Senivongse, “A model-driven development of web applications using AngularJS framework,” in 2016 IEEE/ACIS 15th International Conference on Computer and Information Science (ICIS), Jun. 2016. doi: 10.1109/icis.2016.7550838.

[23] “Fourier Transforms and the Fast Fourier Transform (FFT) Algorithm”.

[24] P. Duhamel and M. Vetterli, “FAST FOURIER TRANSFORMS: A TUTORIAL REVIEW AND A STATE OF THE ART”.

[25] P.-A. Fouque et al., “Falcon: Fast-Fourier Lattice-based Compact Signatures over NTRU Specification v1.2 -01/10/2020”.

[6] S. S. Moghadam and A. Fayoumi, “Toward Securing Cloud-Based Data Analytics: A Discussion on Current Solutions and Open Issues,” *IEEE Access*, vol. 7, pp. 45632–45650, 2019, doi: 10.1109/access.2019.2908761.

[14] J. R. Jeffrey and Yasay, “The Dawn of Digital Coins: A Literature Review on Cryptocurrency in the Philippines”.

[1]V. Hassija *et al.*, “Present landscape of quantum computing,” *IET Quantum Communication*, vol. 1, no. 2, pp. 42–48, Dec. 2020, doi: 10.1049/iet-qtc.2020.0027.   
[2]“Zach Kirsch Quantum Computing: The Risk to Existing Encryption Methods”.   
[3]W. Cui, T. Dou, and S. Yan, “Threats and Opportunities: Blockchain meets Quantum Computation,” in *2020 39th Chinese Control Conference (CCC)*, Jul. 2020. doi: 10.23919/ccc50068.2020.9189608.   
[4]T. Niraula, A. Pokharel, A. Phuyal, P. Palikhel, and M. Pokharel, “Quantum Computers’ threat on Current Cryptographic Measures and Possible Solutions,” *International Journal of Wireless and Microwave Technologies*, vol. 12, no. 5, pp. 10–20, Oct. 2022, doi: 10.5815/ijwmt.2022.05.02.   
[5]E. V. Haryannto, M. Zulfadly, Daifiria, M. B. Akbar, and I. Lazuly, “Implementation of Nihilist Cipher Algorithm in Securing Text Data With Md5 Verification,” *Journal of Physics: Conference Series*, vol. 1361, no. 1, p. 012020, Nov. 2019, doi: 10.1088/1742-6596/1361/1/012020.   
[6].   
[7]S. S. Moghadam and A. Fayoumi, “Toward Securing Cloud-Based Data Analytics: A Discussion on Current Solutions and Open Issues,” *IEEE Access*, vol. 7, pp. 45632–45650, 2019, doi: 10.1109/access.2019.2908761.   
[8]R. Sumithra and R. Parameswari, “Data privacy and data protection security algorithms for big data in cloud,” *International journal of health sciences*, pp. 7613–7621, May 2022, doi: 10.53730/ijhs.v6ns2.6834.   
[9]L. Chen *et al.*, “Report on Post-Quantum Cryptography,” National Institute of Standards, techreport, Apr. 2016. doi: 10.6028/nist.ir.8105.   
[10]D. J. Bernstein and T. Lange, “Post-quantum cryptography,” *Nature*, vol. 549, no. 7671, pp. 188–194, Sep. 2017, doi: 10.1038/nature23461.   
[11]M. Zhandry, “CRYPTOGRAPHY IN THE AGE OF QUANTUM COMPUTERS A DISSERTATION SUBMITTED TO THE DEPARTMENT OF COMPUTER SCIENCE AND THE COMMITTEE ON GRADUATE STUDIES OF STANFORD UNIVERSITY IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE DEGREE OF DOCTOR OF PHILOSOPHY”.   
[12]I. News, “QuSecure launches live end-to-end satellite quantum resilient link through space.” https://www.helpnetsecurity.com/2023/03/11/qusecure-quantum-resilient-cryptographic-communications-satellite-link/, p. 3, Mar. 10, 2023. [Online]. Available: https://www.helpnetsecurity.com/2023/03/11/qusecure-quantum-resilient-cryptographic-communications-satellite-link/   
[13]“Google readies Chrome for distant quantum attacks with new support.” https://www.csoonline.com/article/649480/google-readies-chrome-for-distant-quantum-attacks-with-new-support.html, p. 1. [Online]. Available: https://www.csoonline.com/article/649480/google-readies-chrome-for-distant-quantum-attacks-with-new-support.html   
[14].   
[15]J. R. Jeffrey and Yasay, “The Dawn of Digital Coins: A Literature Review on Cryptocurrency in the Philippines”.   
[16]M. Ricci *et al.*, “A Comprehensive Study on the Feasibility and Suitability of Bitcoin in the Philippine Setting”.   
[17]F. M. Ablayev and A. V. Vasiliev, “Cryptographic quantum hashing,” *Laser Physics Letters*, vol. 11, no. 2, p. 025202, Dec. 2013, doi: 10.1088/1612-2011/11/2/025202.   
[18]V. Mavroeidis, K. Vishi, M. D., and A. Jøsang, “The Impact of Quantum Computing on Present Cryptography,” *International Journal of Advanced Computer Science and Applications*, vol. 9, no. 3, 2018, doi: 10.14569/ijacsa.2018.090354.   
[19]M. F. Sanner, “PYTHON: A PROGRAMMING LANGUAGE FOR SOFTWARE INTEGRATION AND DEVELOPMENT”.   
[20]K. R. Srinath, “Python -The Fastest Growing Programming Language”.   
[21]A. J. Dhruv, R. Patel, and N. Doshi, “Python: The Most Advanced Programming Language for Computer Science Applications,” in *Proceedings of the International Conference on Culture Heritage, Education, Sustainable Tourism, and Innovation Technologies*, 2020. doi: 10.5220/0010307902920299.   
[22]W. Chansuwath and T. Senivongse, “A model-driven development of web applications using AngularJS framework,” in *2016 IEEE/ACIS 15th International Conference on Computer and Information Science (ICIS)*, Jun. 2016. doi: 10.1109/icis.2016.7550838.   
[23]“Fourier Transforms and the Fast Fourier Transform (FFT) Algorithm”.   
[24]P. Duhamel and M. Vetterli, “FAST FOURIER TRANSFORMS: A TUTORIAL REVIEW AND A STATE OF THE ART”.   
[25]P.-A. Fouque *et al.*, “Falcon: Fast-Fourier Lattice-based Compact Signatures over NTRU Specification v1.2 -01/10/2020”.