National College of Ireland

A Novel Approach to Near Field Communication Using B92 Quantum Key Distribution Protocol

MSc Research Project
MSc Cyber Security

Neha Singh
Student ID: x22132759

School of Computing
National College of Ireland

Supervisor: Evgeniia Jayasekera

National College of Ireland

MSc Project Submission Sheet

School of Computing

Student Name: Neha Singh ……

Student ID: X22132759……

Programme: MSc Cyber Security …… **Year:** 1……..……..

Module: Academic Internship……..……

Supervisor: Evgeniia Jayasekera……..……

Submission Due Date: 14 December 2023 ……..……

Project Title: A Novel approach to Near Field Communication using B92 Quantum Key Distribution protocol

Word Count: 6282……**PageCount** 17……..……..

I hereby certify that the information contained in this (my submission) is information pertaining to research I conducted for this project. All information other than my own contribution will be fully referenced and listed in the relevant bibliography section at the rear of the project.
ALL internet material must be referenced in the bibliography section. Students are required to use the Referencing Standard specified in the report template. To use other author's written or electronic work is illegal (plagiarism) and may result in disciplinary action.

Signature: ……

Date: ……

PLEASE READ THE FOLLOWING INSTRUCTIONS AND CHECKLIST

Attach a completed copy of this sheet to each project (including multiple copies)	□
Attach a Moodle submission receipt of the online project submission, to each project (including multiple copies).	□
You must ensure that you retain a HARD COPY of the project, both for your own reference and in case a project is lost or mislaid. It is not sufficient to keep a copy on computer.	□

Assignments that are submitted to the Programme Coordinator Office must be placed into the assignment box located outside the office.

Office Use Only	
Signature:	
Date:	
Penalty Applied (if applicable):	

A Novel Approach to Near Field Communication Using B92 Quantum Key Distribution Protocol

Neha Singh
X22132759

Abstract

This report presents a method based on post quantum cryptography—the B92 Quantum Key Distribution (QKD) protocol—that can be integrated to improve the security of Near Field Communication (NFC) systems. Inspired by the growing risks that quantum computing presents to conventional cryptography methods, this work investigates quantum-resistant ways to protect NFC technology, specifically from weaknesses that allow for eavesdropping. This research uses several in-depth simulations to evaluate the viability and effectiveness of using the B92 procedure in a realistic setting. To assess the protocol's robustness, the study methodology combines theoretical analysis with realistic simulations, generating various scenarios with varying degrees of noise and the possibility of eavesdropping. The B92 protocol significantly improves NFC security and exhibits robustness against attacks utilising quantum computing. The study's conclusions address the pressing need for quantum-resistant cryptographic techniques in the age of growing cyber threats, and they further the field of post quantum cryptography in useful communication technologies. In addition to expanding the body of knowledge in this area, the thesis creates new opportunities for future study and real-world implementations, which could completely alter NFC and other digital communication systems' security requirements in the era of quantum computing.

1 Introduction

In the evolving landscape of digital transactions, the advent of technology has introduced us to the era of NFC. This communication protocol enables connection between two devices in proximity of 10cm (Al-Ofeishat & Rababah, 2012). To our concern, the financial sector is the primary user of NFC, providing a blend of convenience and speed. It is a prime target for cyber attacks due to the immediate monetary gains. However, as this technology gets deeper into our financial ecosystem, it faces increasing security challenges . This paper seeks to address one of the critical vulnerabilities in NFC technology – the susceptibility to eavesdropping attacks – by exploring the potential application of QKD, specifically the B92 protocol, in enhancing NFC security (Solat, 2017).

Since NFC is a crucial component of contactless payments, its security is critical. The present NFC security state-of-the-art primarily uses encryption techniques such as RSA and AES. The master card has recently announced its new quantum-safe card, but it also uses modern cryptography (Elliptical Curve Cryptography (ECC)), not quantum cryptography . With humankind's power, it is only a matter of time before modern cryptographic techniques can easily be broken with quantum computers. While resistant to traditional attacks, these strategies show weaknesses regarding sophisticated quantum computing technologies. This new vulnerability in NFC security emphasises the necessity of investigating quantum-resistant cryptography techniques (Fan & Gong, 2013).

The driving force behind this research is the rapidly developing field of quantum computing, which presents a severe challenge to established cryptographic norms. Eavesdropping vulnerability becomes more pertinent in NFC payments, where security lapses can have disastrous financial and privacy consequences (Brown & Thomas Diakos, 2013). One prospective answer to this problem is the B92 QKD protocol, which is renowned for its security assurance based on the concepts of quantum physics. This research aims to open the door for future-proof, quantum-resistant payment systems by examining their use in NFC.

This leads to the question **"How can the B92 QKD protocol enhance NFC security against eavesdropping?"**

The primary purpose of this study is to determine whether or not the B92 protocol is feasible and efficient to use in NFC systems. To respond to this main query, we examine how secure NFC is currently and how susceptible it is to quantum attacks. Moving forward, we create a simulation model to assess the B92 protocol, establish a simulated setting, and evaluate B92's ability to fend off eavesdropping attempts. Finally, we analyse how resilient the B92 protocol is to different simulated attacks, such as active listening and noise.

This research's primary contribution is thoroughly examining and simulating the B92 QKD protocol. This work substantially contributes to cybersecurity and digital payment systems, furthering academic knowledge of quantum-resistant cryptographic solutions and serving as fundamental work for future practical implementations.

This comprehensive report delves into applying the B92 protocol to enhance NFC security. It begins with an Introduction that sets the research context, followed by a Literature Review covering NFC security challenges and post quantum cryptography and protocols. The Research Methodology section details the design and analysis of simulations, while the Design Specification outlines the technical implementation of the B92 protocol. The Implementation section discusses its practical application, leading to an Evaluation through statistical analysis. The discussion critically evaluates the design, relating findings to existing research. Finally, the Conclusion and Future Work summarize the study and discuss implications, limitations, and future research pathways, all supported by comprehensive References. Through this thorough exploration, the report examines the role of the B92 protocol in enhancing NFC security.

2 Related Work

This literature review explores the promise of post-quantum cryptography, specifically QKD protocols such as B92, and its existing cryptographic security with a particular focus on NFC technology. It evaluates how susceptible NFC is to quantum attacks and investigates how post-quantum technologies can strengthen digital communications against constantly changing cybersecurity threats.

2.1 NFC Technology Security Concerns

The operational modes and uses of NFC are thoroughly examined in this study by (Singh & Hassan, 2018), focusing on security flaws such as data corruption, eavesdropping, and denial-of-service attacks. It emphasises how crucial secure communication routes are to NFC, especially for programmes like MIDAS. However, it mainly focuses on theoretical issues and

provides no real-world case studies or experimental evidence to support the recommended solutions. According to a study (Tabet & Ayu, 2016), NFC security in payment systems provides insight into possible attacks and weaknesses. It discusses different cryptographic protocols and emphasises how crucial robust encryption techniques are for NFC. However, the study only looks at NFC payment systems and offers no case studies or empirical data to support its conclusions.

Likewise, (Chattha, 2014) thoroughly examines NFC vulnerabilities, such as data manipulation, eavesdropping, and man-in-the-middle attacks, and it promotes using secure channels as a defensive tactic. Although it offers valuable insights about NFC design, it concentrates more on finding weaknesses than investigating cutting-edge fixes or technological advancements to lessen these dangers. (Ozdenizci, et al., 2015) thoroughly explains the capabilities and security issues associated with various NFC applications. It covers a wide range of NFC modes and provides a solid basis for comprehending the fundamentals of the technology. However, it does not specifically address security concerns or sophisticated cryptographic solutions.

The lack of empirical support and the overemphasis on traditional encryption, identified in previous research, are the main areas for improvement in NFC security research that this work attempts to fill. It offers a unique, quantum-resistant solution by concentrating on the Quantum Key Distribution (QKD) B92 protocol, which goes beyond conventional cryptographic techniques. This study aims to compare the B92 protocol with existing cryptographic algorithms and assess how well it mitigates NFC vulnerabilities. By incorporating state-of-the-art quantum-resistant cryptography techniques, this all-encompassing method will greatly expand NFC security and contribute considerably to the sector in the era of quantum computing developments.

2.2 Current NFC Cryptography

(Ratnadewi, et al., 2016) Comprehensively analyses Data Encryption Standard (DES) and 3DES encryption methods in NFC-based systems, focusing on their implementation and performance. The strength of this research lies in its detailed explanation of the cryptographic processes and the empirical testing of these methods in NFC environments. It successfully demonstrates that DES and 3DES can be effectively implemented in NFC systems, with DES offering faster execution times compared to 3DES. However, the study's limitation is its narrow focus on DES and 3DES without considering more advanced encryption methods like AES or quantum-resistant algorithms. This focus may limit the applicability of the findings in environments where higher security standards are required.

Moving forward, (Wijaya, et al., 2017)’s study evaluates the Advanced Encryption Standard (AES-128) cryptography method within NFC systems, contrasting its performance with DES and 3DES. The paper's strength is its in-depth analysis of the AES-128 implementation and its detailed comparison with older cryptographic standards, highlighting AES-128's longer processing times despite its higher security level. This research is significant in illustrating the trade-offs between security and efficiency in cryptographic methods. However, the research must address newer or more advanced cryptographic techniques, especially those relevant to evolving quantum computing threats.

Mastercard's initiative to implement quantum-resistant encryption techniques in its new cards marks a significant advancement in payment security. Using ECC for authentication and

adherence to EMV contactless kernel specifications showcases a robust approach against common and quantum-based threats. The initiative's strength lies in its quick user authentication process and the attempt to future-proof against quantum attacks. However, the industry's mixed response to ECC's quantum resistance highlights a critical limitation. It underscores the need for thorough testing and validation of these quantum-resistant methods, considering the potential vulnerabilities that quantum computing might exploit (Day, 2022).

The reviewed literature demonstrates a focused exploration of cryptographic methods (DES, 3DES, AES-128, and ECC) in NFC-based systems, providing valuable insights into their implementation and performance trade-offs. However, these studies predominantly centre on conventional cryptographic methods and lack a detailed examination of emerging quantum-resistant technologies. This gap underscores the necessity of research like the proposed B92 QKD protocol study, which aims to address NFC vulnerabilities against more sophisticated threats, including quantum computing. The evolving landscape, as evidenced by Mastercard's initiative, necessitates exploring more advanced cryptographic solutions, balancing the demands of security, efficiency, and quantum resistance.

2.3 Post Quantum Cryptography and Quantum Key Distribution

A revolutionary development in secure communications, post quantum cryptography's QKD offers theoretical protection against computer advances, especially quantum computing. QKD protocols, like B92 and its variations, use the principles of quantum physics to guarantee the safe distribution of cryptographic keys. The security of QKD is based on the intrinsic qualities of quantum states, like superposition and entanglement, which make any attempt at listening obvious.

(Diamanti, et al., 2016)'s work thoroughly analyses the real-world difficulties that QKD systems encounter, including key rate, resilience, cost, and distance-related problems. It draws attention to the discrepancy between what QKD systems can perform today and what is needed to be widely used in practical applications. The study examines several strategies for addressing these issues, including network QKD, new QKD protocols, and hardware development. Although it acknowledges recent technological advances and offers a hopeful outlook for QKD, it also highlights the limitations imposed by fundamental physics and the need for additional innovation.

The applicability of QKD in cryptographic systems is assessed in this survey research (Alléaume, et al., 2014), which focuses on how well it integrates into the current communication infrastructures. The compatibility of QKD with contemporary cryptographic techniques is rigorously examined, as are the difficulties associated with its practical implementation, including scalability, interoperability, and affordability issues. The study highlights the need for hybrid systems that integrate classical and quantum cryptography methods to strike a compromise between usability and security.

As examined in these sources, the state of the art in QKD shows notable advancements in tackling the difficulties associated with using quantum cryptography systems in real-world applications, such as NFC payment systems. The literature also indicates that crucial rate, transmission distance, and integration with present communication networks remain issues for current solutions. These drawbacks make it necessary to do additional research, like the B92 protocol study that is being suggested, to strengthen the security of NFC payment systems against vulnerabilities like eavesdropping. The distinct benefits of post quantum cryptography

highlight the significance of furthering QKD research and development for valuable and safe communication systems, particularly considering new dangers in the quantum computer era.

2.4 QKD Protocols

A thorough theoretical analysis of several QKD protocols, such as BB84, B92, SARG04, and others, is presented in this study (Padmavathi, et al., 2016). It does an excellent job of explaining the fundamental ideas of quantum mechanics that underpin these protocols, which is essential to comprehending the secure communication they are built upon. However, it must be presented more when demonstrating various QKD methods' difficulties and practical applicability, particularly in real-world situations like NFC payment systems. Table 1 shows the comparative analysis of different QKD protocols (Jha, et al., 2019).

Table 1: Comparison Table of QKD Protocols

Parameter	**BB84**	**B92**	**SARG04**	**S09**	**S13**
Founder	C.H Bennett and G Brassard	C.H Bennett	Scarani.V, A. Acin, Ribordy G, Gisin N	Eduin Esteban Hernadez Serna	Eduin Esteban Hernadez Serna
Year	1984	1992	2004	2009	2013
Number of States	4	2	4	Arbitrary states	4
Principal	Heisenberg	Heisenberg	Heisenberg	Public Private Key	Heisenberg
Polarization	Orthogonal	Non-Orthogonal	Orthogonal	Arbitrary	2 Orthogonal
Man- in- the-Middle	Vulnerable	Robust	Robust	Robust	N/A
Eavesdropping	Robust	Robust	Robust	Robust	Robust
Security	Average	Good	Average	Good	Average
Efficiency	Low	Best	Average	Good	Average

The authors of this paper provide a thorough analysis of many QKD procedures, including their theoretical foundations and historical evolution. This study offers an invaluable framework for comprehending the development of QKD protocols and their respective benefits and drawbacks (Elboukhari, et al., 2014). Like the first paper, it does not detail how these protocols are implemented in modern technologies like NFC systems; instead, it concentrates mainly on theoretical issues.

This study extends the scope by addressing recent advances in QKD protocols, such as the Coherent One-Way (COW) protocol and differential phase shift QKD. Including these more recent protocols provides an understanding of the dynamic and ever-evolving post quantum cryptography (Nurhadi & Syambas, 2018). Its utility for practical deployment guidance is limited since, despite its thorough coverage, the practical implementation of these protocols—especially in particular technologies like NFC—is not sufficiently addressed.

This article (Abushgra, 2022) investigates the adaptability and integration of several QKD techniques with traditional systems. Theoretical modifications of these protocols are covered, offering insights into possible real-world uses such as NFC payment systems. However, the

study focuses primarily on theoretical possibilities rather than delving into workable implementation solutions for these protocols in actual systems.

The studied material provides a solid theoretical basis for comprehending the principles of different QKD techniques. However, there needs to be more guidance on practical use, especially when integrating these protocols with real-world technology like NFC payment systems. This gap highlights the necessity for studies tackling QKD systems' theoretical stability and real-world implementation difficulties. Such a study is necessary to improve security in systems susceptible to problems like eavesdropping and to further the deployment of quantum cryptography in real-world communication technology.

2.5 QKD B92 Protocol

By contrasting multiple implementations, (ANGHEL, et al., 2022) thoroughly examine the B92 QKD protocol in this paper. The work is vital because it introduces the Quantum Bit Travel Time (QBTT) eavesdropper detection technique and comprehensively simulates the B92 protocol in various circumstances, including those with and without eavesdroppers. The Quantum Bit Error Rate (QBER) from the final key was dramatically decreased using this method, demonstrating how effective it is at improving security. Meanwhile, the study's dependence on simulations rather than actual implementations is one of its limitations because it might not adequately represent the difficulties and complexities of real-world applications. The results are essential for comprehending how well the B92 procedure works in various situations.

The implementation and optimisation of the B92 QKD protocol have been greatly enhanced by the work of (Gopal, 2022). The paper's most vital point is its thorough examination of the B92 protocol on actual quantum hardware and simulation under various circumstances, including varied key lengths and eavesdropper techniques. The work identifies the best circumstances for using the protocol and convincingly illustrates its promise in quantum cryptography. However, the study's emphasis on theoretical and simulated scenarios is a significant drawback since it needs to fully represent real-world application practical difficulties, including ambient influences on quantum hardware. This work addresses the resilience of the B92 protocol against eavesdropping, which is a significant concern in financial transactions and is especially pertinent to NFC payment systems.

The primary method used in both research is only the simulation of eavesdroppers, which might not accurately represent the intricacies of the real world, especially in NFC situations. This points to a research void in using B92 QKD in real-world NFC systems, where environmental noise is an essential consideration. To close these gaps, this study will apply the simulated and theoretical results with environmental noise, offering a more thorough comprehension of the B92 protocol's efficacy in realistic situations, particularly in financial transactions.

3 Research Methodology

This study mainly focused on modelling the B92 QKD protocol. The main goal was to examine the protocol's viability and effectiveness against attacks particularly noise interference and efforts to intercept communications. To understand the protocol's robustness under varying situations, scenarios were created to replicate several attack vectors, such as active listening, noise interference, and ideal scene without any noise or interception. Figure 1 illustrates that we will follow a three-phase method of simulating the B92 protocol.

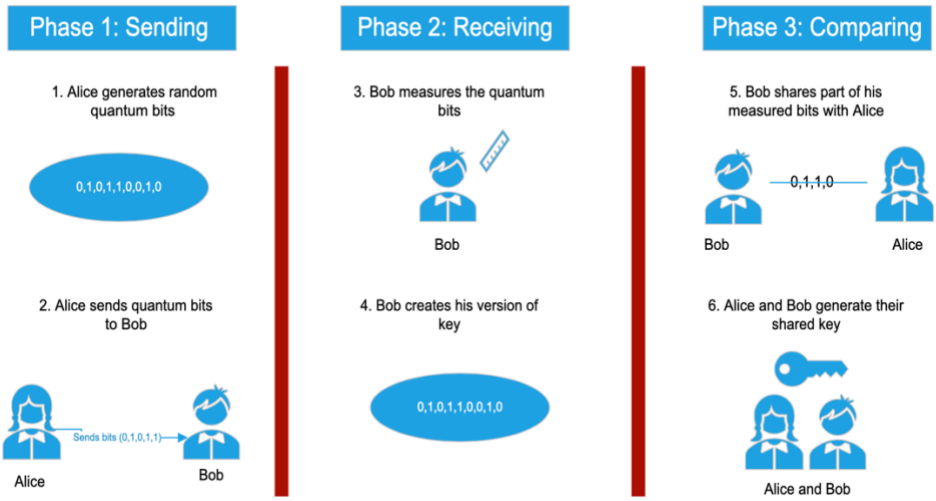

Figure 1: Methodology of the Proposed System

3.1 Phase 1: Alice Sending Bits

Alice generates a series of random bits (0s and 1s) to represent her portion of the quantum key. A random number generator is used to accomplish this. The length of the key, which represents the bits Alice plans to deliver to Bob is kept separately**.**

3.2 Phase 2: Bob Measuring Bits and Generating his Key

Bob measures bits by deciding whether to consider each bit from Alice based on whether noise and eavesdropping are present. Bob measures Alice's bits transferred while accounting for any possible channel noise if no one listens. This simulates the process of quantum measurement. The programme randomly determines whether Eve's measurement succeeds if she listens. The integrity of the key that Bob receives may be compromised by Eve's intervention, which can change the bits. Alice retains a copy of the key, interpreting the bits as successfully transferred without Eve.

3.3 Phase 3: Comparing the Keys

Bob and Alice compare a subset of their keys after transmission to look for differences. The program counts the differences between Alice and Bob's keys by comparing the corresponding bits. This comparison is essential for determining the integrity of the key transfer and identifying the existence of an eavesdropper (such as Eve). The Quantum Bit Error Rate (QBER) represents the discrepancy between the keys. The bits of the keys that remain after the comparison bits are eliminated are Alice and Bob's final keys.

The B92 protocol was evaluated in four different scenarios: in noisy environments, in the presence of eavesdropping, under ideal circumstances, where there was no noise or eavesdropping, and under the presence of both noise and eavesdropping. This aided in assessing the robustness and adaptability of the protocol. A critical analysis was conducted on the protocol's capacity to identify attempts at eavesdropping and preserve key integrity in various scenarios. The code also shows how to use the XOR method to encrypt and decrypt a message, illustrating a valuable use for the shared key. The XOR method was used for simplicity and it can be changed to any other encryption methods. Although it simplifies many aspects of the actual quantum physics involved in the B92 protocol, this simulation offers

insight into the dynamics of quantum key distribution in the face of real-world obstacles like noise and eavesdropping.

4 Design Specification

The primary goal of this project's design specification is to strengthen the security of NFC devices against eavesdropping by implementing the B92 QKD protocol. The B92 protocol is successfully implemented by the project to identify and stop eavesdropping during the key generation stage, which secures us from the actual information being intercepted. The use of this protocol for NFC communication has yet to be included in the current project's scope and is considered a future endeavour.

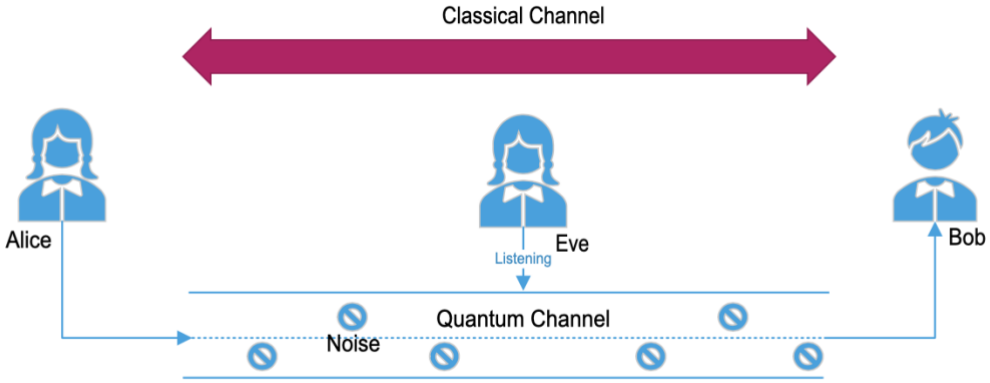

Figure 2: Basic QKD Model

4.1 Architecture and Framework

The B92 protocol uses two non-orthogonal quantum states to facilitate secure key exchange. Each bit of the key in B92 is encoded in one of two quantum states (0 and 1), such as photon polarisations, which are unstable when measured simultaneously because of quantum uncertainty. Since measuring the quantum state inevitably modifies it during transmission—a characteristic ensured by the no-cloning theorem and Heisenberg's uncertainty principle—any attempt at eavesdropping is observable (Haitjema, 2007). A subset of the communication is compared for key verification, and any differences point to possible eavesdropping. The QBER is used as a gauge of the integrity and security of this protocol, which takes advantage of the fundamental characteristics of quantum physics to provide secure communication.

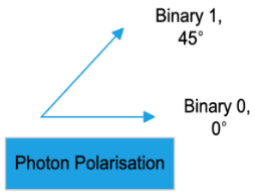

Figure 3: B92 Two Orthogonal States

The algorithm simulates the B92 protocol. It incorporates random noise effects and represents Alice's key generation, Eve's possible eavesdropping, and Bob's reception.

Algorithm Steps:

1. **Initialization:**
   - Define the length of the key to be generated (**keyLength**).
   - Initialize arrays for Alice's key (**keyAlice**), Bob's received bits (**keyBob**), and Eve's measurements (**keyEve**).
   - Set parameters for eavesdropping probability (**eveSpying**) and noise level (**noise**).
2. **Key Generation by Alice:**
   - Alice generates a random key of length **keyLength**, with each bit being either 0 or 1.
3. **Key Transmission and Eavesdropping Simulation:**
   - For each bit in Alice's key:
     - If Eve chooses not to eavesdrop (determined by **eveSpying**), proceed with standard transmission to Bob.
     - If Eve eavesdrops, Eve measures the bit (success determined randomly).
   - The bit may or may not be altered based on the simulation of eavesdropping success.
4. **Noise Simulation:**
   - Simulate noise in the transmission channel. Each bit has a probability (**noise**) of being flipped during transmission to Bob.
5. **Reception by Bob:**
   - Bob receives the transmitted bits, forming his version of the key.
6. **Key Comparison and Error Calculation:**
   - Compare a subset (**sampleSize**) of bits between Alice's and Bob's keys to check for discrepancies.
   - Calculate the number of discrepancies (errors) to evaluate the integrity of the key transmission.
   - Calculate the Quantum Bit Error R.
7. **Optional Encryption and Decryption:**
   - If the keys match sufficiently (based on a threshold of discrepancies), use the shared key for encrypting and decrypting a message.
8. **Visualization and Analysis:**
   - Visualize the impact of noise and eavesdropping using plots.
   - Compare Alice and Bob's final keys to highlight discrepancies.

Functions Used

- **encrypt_message(message, shared_key)**: Encrypts a message using the XOR operation with the shared quantum secret key.
- **decrypt_message(encrypted_message, shared_key)**: Decrypts the message by reversing the XOR operation.
- **noiseError():** Simulates the effect of noise on a bit during transmission. It modifies a bit's state to symbolise the noise effect in a quantum communication channel, indicating how outside interferences can cause a bit to flip, resulting in mistakes in the delivered data.
- **onlyAB():** Handles the transmission of bits from Alice to Bob when Eve is not eavesdropping. Considering the process's quantum mechanics, this function makes sure

that Bob receives the bits that Alice transmits precisely and considers the likelihood of transmission noise.

- **calculate_qber(AliceKey, BobKey, sampleSize):** This function computes the QBER. It analyses a portion of the bits from Bob's and Alice's keys to assess the key transfer's integrity.

$$\text{QBER} = \frac{\text{Number of Discrepencies}}{\text{Total number of Compared bits}}$$

The user can change the algorithm's key length, eavesdropping probability, noise level, and sample size for comparison. The B92 QKD protocol can be simulated using this technique, focusing on noise effects, eavesdropping, key generation, and transmission. It establishes the groundwork for comprehending the dynamics of quantum key distribution in the face of practical difficulties like noise and eavesdropping.

5 Implementation

During the study's implementation phase, we created a detailed simulation model to simulate the B92 protocol realistically. Key generation, transmission procedures, noise and eavesdropping simulations, and the QBER computation are all included in this model. Python was chosen for this implementation due to its powerful standard library and simplicity of reading, especially the random module, which is essential for emulating the randomness found in quantum physics. A thorough explanation of the implementation is provided below, emphasising the methods employed:

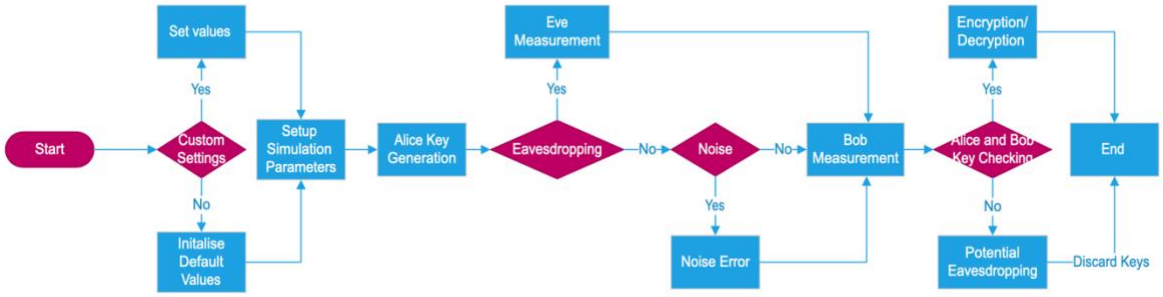

Figure 4: Flow Chart of the Project

1. **Initial Settings Configuration:** The script begins by initialising several parameters, including sample size for key verification, noise level, eavesdropping probability **(eveSpying),** and key length. If custom settings are selected, user input can override these settings.
2. **Handling User Input:** The input function in Python collects user preferences so that the program can be run with customised parameters. Additional data is gathered for the sample size, noise level, eavesdropping probability, and key length if selected.
3. **Random Key Generation (Alice's Key):** The Python random module creates Alice's key to replicate the stochastic aspect of quantum state preparation. Using **random.random(),** each bit of the key is created and then rounded to produce a binary result (0 or 1).
4. **Simulation of Quantum Transmission and Eavesdropping (Eve's Actions):** This simulation considers the possibility of interference from an eavesdropper, Eve, during

the quantum communication process. This determines whether Eve (using **eveSpying)** tries to intercept each bit and, if so, if her measurement succeeds.

5. **Noise Simulation:** The noise parameter influences the transmission of bits, with a certain probability of each bit being flipped, simulating environmental or system errors in quantum communication.
6. **Bob Measurement:** Bob measures the key sent by Alice and generates his version of the key (**keyBob**).
7. **Key Comparison and Verification:** To confirm the integrity of the key exchange, a portion of the key bits are compared between Alice and Bob. The **sampleSize** parameter determines how many bits to examine.
8. **Encryption and Decryption:** The programme moves on to the encryption and decryption stage if the key verification is successful. It illustrates a primary use of the shared key by encrypting and decrypting a message supplied by the user using a straightforward **XOR** technique for simplicity.
9. **Presentation of Outputs:** The user is shown several outputs during the simulation, such as the keys produced, the number of noise-affected bits, the success rate of eavesdropping attempts, and the final encrypted and decrypted communications.

Tools and Languages Used

1. **Python Programming Language:** Python3 was used to create the complete simulation because of its ease of use and efficiency in managing user interactions and random processes.
2. **Random Library:** The Random Module is an essential part of the Python standard library that simulates the randomness needed for the simulation's decision-making and quantum key generation procedures.
3. **Matplotlib Library:** The Matplotlib library was used to depict essential elements of the QKD simulation graphically. Matplotlib is a Python visualisation tool. It made it possible to plot data in pie charts and bar charts to clearly show variations and statistical insights.
4. **PyCharm IDE:** PyCharm was used for the script's development and debugging. PyCharm's extensive feature set considerably aided the development process, which includes an integrated debugger, an intelligent code editor, and error highlighting. Its integrated Python development tools and strong code navigation capabilities were beneficial in effectively managing and organising the script.

Output Produced

1. **Simulated Quantum Keys:** Keys that were generated to represent Alice, Bob, and Eve's respective roles in the distribution of quantum keys.
2. **Encrypted and Decrypted Messages:** Illustrating how the shared key is used in real-world scenarios.
3. **Statistical Data with visual representation:** Details regarding the key distribution's efficacy, including its effects on noise and the success of eavesdropping.

The section outlines the ultimate phase of the B92 protocol simulation, providing in-depth coverage of its essential elements, utilized tools, and generated outcomes. It highlights the pragmatic use of the shared key in encryption and decryption processes, alongside the accomplished simulation of diverse quantum cryptography scenarios.

6 Evaluation

In the context of NFC security, the B92 protocol was evaluated with an emphasis on its robustness against eavesdropping and its capacity to preserve integrity in the face of noise. The following are the simulation's main conclusions:

6.1 Performance Analysis Under Normal Conditions

The QKD protocol performs exceptionally well in a perfect setting with no noise and no listening. This scenario demonstrates the intrinsic robustness and trustworthiness of the protocol. It shows that, in the right circumstances, it can permit flawless key agreement between communicating parties—a noteworthy accomplishment in quantum cryptography. Figure 4 shows how well the QKD procedure performs in these circumstances.

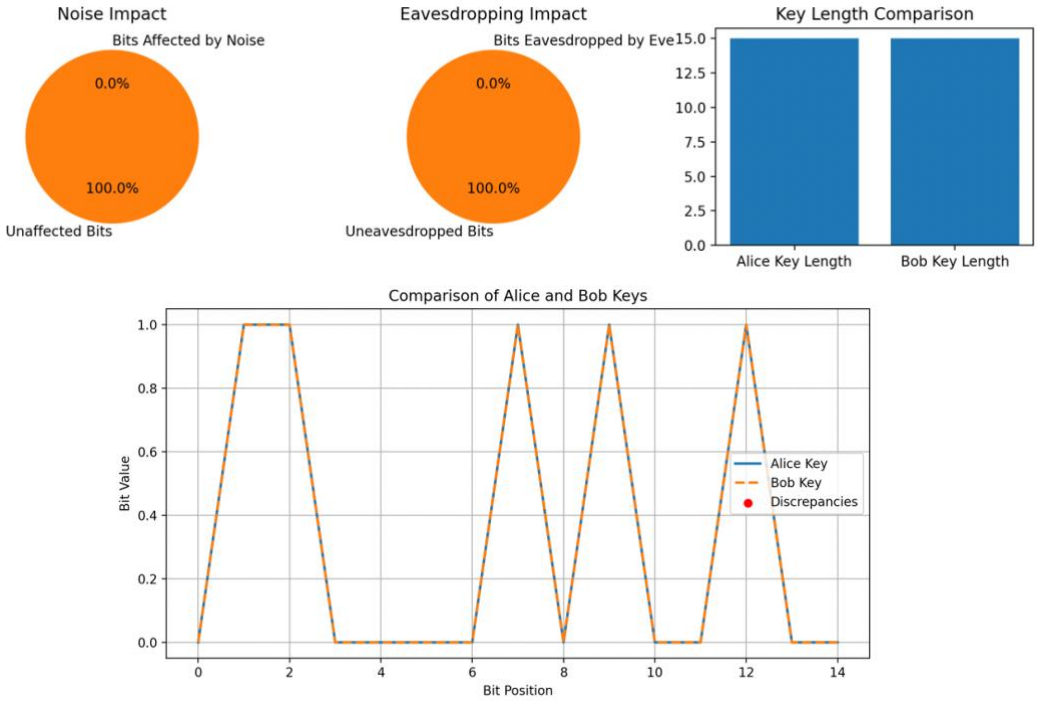

Figure 5: Normal Condition

6.2 Evaluation in Noisy Environment

Despite the noise in the surrounding environment, the QKD system can still generate many valid key bits. The protocol's adaptation and durability in less-than-ideal settings are demonstrated in this situation, which has promise for real-world applications where some degree of noise is unavoidable. The flexibility and resilience of the protocol under challenging circumstances are emphasised in Figure 5, which is a crucial feature for practical NFC applications.

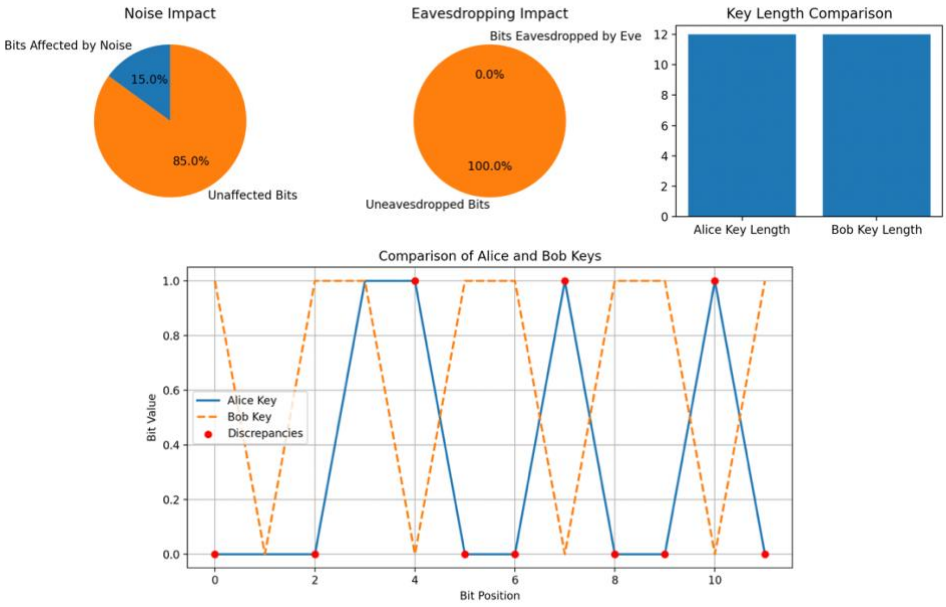

Figure 6: Noise

6.3 Assessing Security Against Eavesdropping

The QKD protocol demonstrates its strong eavesdropping detection capabilities by identifying inconsistencies with significant eavesdropping. This is an essential component of any secure communication system since it shows how the protocol can protect against unwanted interceptions, a critical need for secure communications. The effectiveness of the protocol in preventing unauthorised interceptions—a crucial prerequisite for secure NFC communications—is illustrated in Figure 6.

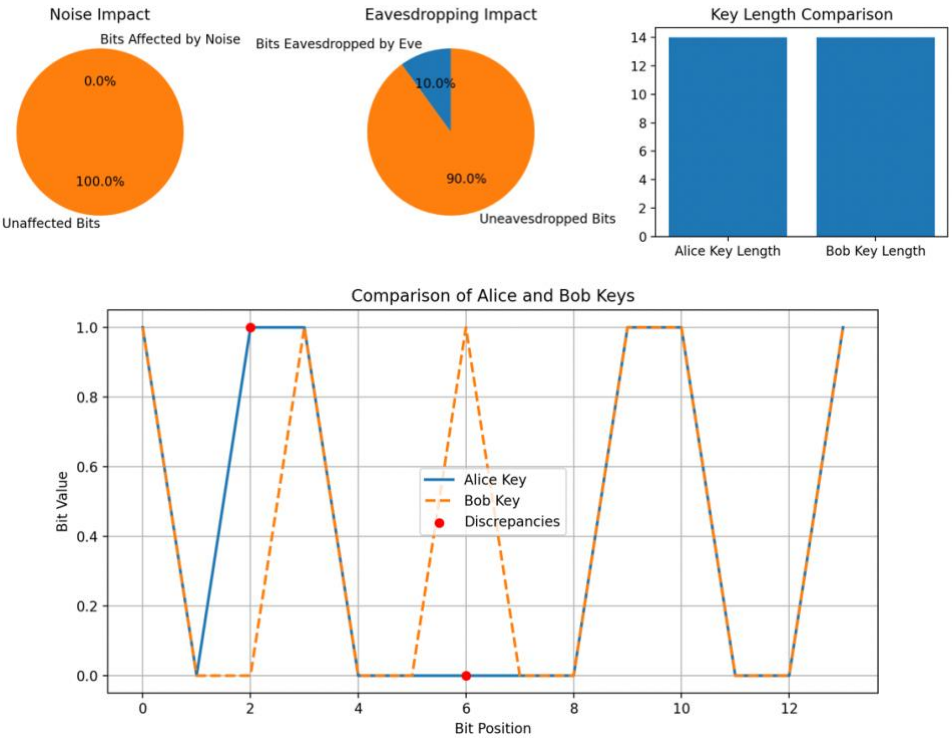

Figure 7: Eavesdropping

6.4 Evaluating with both Noise and Eavesdropping

Even though maximum eavesdropping and noise are extremely difficult, the protocol's performance in these scenarios offers essential insights into its limitations and possible areas for improvement. This scenario pushes the boundaries of quantum cryptography research and development to unprecedented heights. Figure 7 provides information about the protocol's shortcomings and possible areas for enhancement in harsh environments.

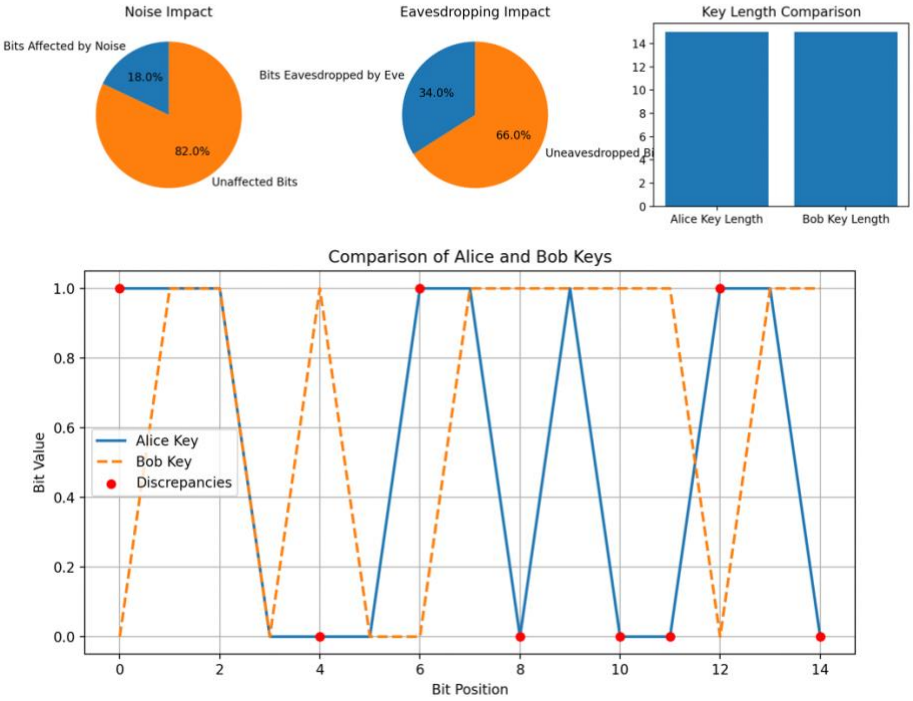

Figure 8: Noise and Eavesdropping

The QBER is a quantitative indicator of the protocol's security level that was computed under several conditions. Lower QBER values suggested higher security in noisy and eavesdropping environments and vice versa. By illustrating the usefulness and constraints of the B92 protocol in NFC systems, the study adds to the corpus of knowledge in post quantum cryptography. It creates opportunities for more research, especially in improving the protocol's resistance to noise and prying eyes in practical settings. In the age of quantum computing, the study emphasizes the significance of quantum-resistant cryptographic approaches for cybersecurity professionals. It sheds light on how post quantum cryptography can be used in NFC payment systems, which is a crucial issue for financial security.

The QKD protocol shows excellent promise for secure communication in the quantum world. It is impressive that it can identify eavesdropping and keep key integrity in various situations. The protocol's performance under optimal conditions is notable, which validates its theoretical robustness. Even though there are difficulties in noisy surroundings, these situations present essential learning opportunities and open the door to improvements that will further strengthen the dependability of the protocol in real-world conditions. The protocol's key advantages are its ability to detect eavesdropping in the key generation phase and its optimal performance. Difficulties in noisy workplaces are opportunities for continued innovation and advancement rather than failures. This thesis contributes to the subject by outlining QKD's accomplishments

and future development areas, emphasising the technology's critical role in developing secure quantum communications.

7 Discussion

We evaluated the B92 protocol's efficacy in strengthening NFC security against risks associated with quantum computing. The QBER study showed that the protocol had remarkable robustness against noise and eavesdropping. The B92 protocol demonstrated decreased QBER under typical circumstances, indicating efficient, secure communication; nevertheless, this rate rose in high-noise or eavesdropping situations, exposing certain drawbacks.

A comparison with conventional cryptography techniques like DES (Ratnadewi, et al., 2016), AES (Wijaya, et al., 2017), and ECC (Fan & Gong, 2013) demonstrated how much more resilient the B92 protocol is against quantum assaults. However, because quantum processes are complex, their computational efficiency and speed could have been better than those of techniques like AES. The B92 protocol also needs greater processing power, highlighting the difficulties in implementing it.

Table 2: Comparison with conventional cryptogrpahy

Factor / Criteria	B92 Protocol	DES	AES	ECC
Security Against Quantum Attacks	High (Quantum-Resistant)	Low (Vulnerable to brute-force attacks, potentially more susceptible to quantum attacks)	Moderate (Currently secure, but potentially vulnerable to future quantum attacks)	Moderate (Currently secure, but potentially vulnerable to future quantum attacks)
Resilience to Eavesdropping	High (Inherent to the quantum nature of the protocol)	Low (Vulnerable due to shorter key length)	Moderate (Robust against known eavesdropping techniques)	Moderate (Robust against known eavesdropping techniques)
Speed and Efficiency	High (Demands significant quantum computational resources)	Low to Moderate (Less efficient due to older algorithm, slower than AES)	High (Faster, more efficient for large data sets)	High (Efficient, especially for smaller data sizes)
Computational Requirements	Moderate (Complex quantum operations may slow down the process)	Moderate (Less complex, but limited by 56-bit key size)	Low to Moderate (Efficient algorithms)	Moderate (Efficient but requires curve calculations)
Real-World Applicability	Moderate (Promising but requires further real-world testing and implementation)	Low (Outdated and no longer recommended for secure applications)	High (Widely adopted for secure data encryption)	High (Increasingly used, especially in digital signatures)
Suitability for NFC Transactions	Moderate to High (Effective but needs real-world NFC system validation)	Low (Not recommended due to security concerns)	High (Efficient for quick transactions)	High (Suitable for secure transactions with efficiency)

We recognised the shortcomings of simulation-based approaches and recommended the necessity for more varied simulation scenarios and preliminary research with actual NFC systems. This method highlights the significance of creating cryptographic algorithms resistant

to improvements in quantum computing and connects the theoretical features of post-quantum cryptography with real-world NFC implementations. In summary, our study makes a substantial contribution to quantum cryptography by laying the groundwork for upcoming advancements in NFC security and highlighting the continued need for changes in cryptographic security.

8 Conclusion and Future Work

This study aimed to assess the applicability and efficacy of the B92 protocol in strengthening the security of NFC systems, specifically against risks posed by quantum computing. To evaluate the B92 protocol's resilience to noise and eavesdropping and to compare its efficacy with more conventional cryptographic methods, the study entailed simulating the protocol under various circumstances. The study successfully illustrated the protocol's capabilities in a theoretical NFC environment through many simulations, highlighting its potential to safeguard communications from quantum attacks. A quantitative assessment of the security of the protocol under various conditions was given by the Quantum Bit Error Rate (QBER) analysis.

The outcomes showed that the B92 protocol provides good resilience against eavesdropping and modest resistance to noise interference. These results imply the requirement and viability of quantum-resistant cryptographic techniques in the age of increasing quantum computing, which is essential for NFC security and the development of post-quantum cryptography. The study recognised the shortcomings of simulation-based approaches, which might not accurately reflect real-world difficulties, but it also emphasised the potential of quantum cryptography to improve NFC security.

Future research ought to include the B92 protocol into functional NFC systems for pragmatic assessment to understand practical implementation and performance issues. Further research into the protocol's interoperability with other quantum-resistant cryptography techniques may result in more reliable NFC and digital communications security protocols. Additionally, we could also examine the B92 protocol's scalability with existing NFC hardware, how it affects transaction efficiency, and how integrating quantum cryptography into NFC systems would affect user experience.

To sum up, this research achieves its goals. It paves the way for future investigation, enhancing our knowledge of post-quantum cryptography in NFC applications and guaranteeing that advances in quantum computing are accompanied by robust security solutions for NFC.

References

Abushgra, A. A., 2022. Variations of QKD Protocols Based on Conventional System Measurements: A Literature Review. *Cryptography 2022,* 6(12).

Alléaume, R. et al., 2014. Using quantum key distribution for cryptographic purposes: A survey. *Theoretical Computer Science,* 560(2014), p. 62–81.

Al-Ofeishat, H. A. & Rababah, M. A., 2012. Near Field Communication. *International Journal of Computer Science and Network Security,* 12(2), pp. 93-99.

ANGHEL, C., ISTRATE, A. & VLASE, M., 2022. *A Comparison of Several Implementations of B92 Quantum Key Distribution Protocol.* Sinaia, Romania, IEEE.

Brown, T. W. C. & Thomas Diakos, J. A. B., 2013. *Evaluating the Eavesdropping Range of Varying Magnetic Field Strengths in NFC Standards.* Surrey, European Conference on Antennas and Propagation (EuCAP).

Chattha, N. A., 2014. *NFC — Vulnerabilities and defense.* Rawalpindi, Pakistan, IEEE.

Day, L., 2022. *MASTERCARD'S NEW CARD: SAFER FROM QUANTUM ATTACKS?.* [Online] Available at: https://hackaday.com/2022/10/25/mastercards-new-card-safer-from-quantum-attacks/ [Accessed 08 12 2023].

Diamanti, E., Lo, H.-K., Qi, B. & Yuan, Z., 2016. *Practical challenges in quantum key distribution.* s.l., npj Quantum Information.

Elboukhari, M., Azizi, M. & Azizi, A., 2014. Quantum Key Distribution Protocols: A Survey. *International Journal of Universal Computer Sciences,* 1-2010(2), pp. 59-67.

Fan, X. & Gong, G., 2013. *Securing NFC with Elliptical Curve Cryptography - Challenges and Solutions.* Ontario, Canda, Department of Electrical and Computer Engineering.

Gopal, A., 2022. Experiments with B92 Quantum Key Distribution Algorithm Implementation. *Preprints,* 2022070279(1).

Haitjema, M., 2007. A Survey of the Prominent Quantum Key Distribution Protocols.

Jha, M. S., Maity, S. K., Nirmal, M. M. & Krishna, J., 2019. A survey on quantum cryptography and quantum key distribution protocols. *International Journal of Advance Research, Ideas and Innovations in Technology,* Volume 5, pp. 144-147.

Nurhadi, A. I. & Syambas, N. R., 2018. *Quantum Key Distribution (QKD) Protocols: A Survey.* Nusa Dua, Bali, Indonesia, IEEE.

Ozdenizci, B., Ok, K. & Coskun, V., 2015. The Survey on Near Field Communication. *Sensors (Basel),* 15(6), p. 13348–13405.

Padmavathi, M. V., Vardhan, D. B. V. & Krishna, D. A. V. N., 2016. *Quantum Cryptography and Quantum Key Distribution Protocols: A Survey.* Bhimavaram, India, IEEE.

Ratnadewi, et al., 2016. *Implementation Cryptography Data Encryption Standard (DES) and Triple Data Encryption Standard (3DES) Method in Communication System Based Near Field Communication (NFC).* Makassar, Indonesia, Journal of Physics.

Singh, M. (. M. & Hassan, R., 2018. Near Field Communication (NFC) Technology Security Vulnerabilities and Countermeasures. *International Journal of Engineering and Technology,* 7(4.31), pp. 298-305.

Solat, S., 2017. *Security of Electronic Payment Systems: A Comprehensive Survey* . Paris, National Centre for Scientific Research CNRS.

Tabet, N. E. & Ayu, M. A., 2016. *Analysing the Security of NFC Based Payment Systems.* Mataram, Indonesia, International Conference on Informatics and Computing (ICIC), IEEE.

Wijaya, D. et al., 2017. Implementation and performance analysis of AES-128 cryptography method in an NFC-based communication system. *World Transactions on Engineering and Technology Education,* 15(2), pp. 178-183.