Cybersecurity and Quantum Computing: Challenges and Countermeasures

Nafee Ibn Sabah

B. Sc. In Software Engineering

DAFFODIL INTERNATIONAL UNIVERSITY

Approval Form

Department of Software Engineering

Faculty of Science and Information Technology

Supervisor Approval Form

Fall 2025	B.Sc. In SWE	Campus: DSC

Student Name	Student ID
Nafee Ibn Sabah	221-35-1002

Project/Thesis Information	
Project/Thesis Title	Cybersecurity and Quantum Computing: Challenges and Countermessures
Type of work	Qualitative and Quantitative Hybrid academic thesis.

Supervisor information	
Supervisor Name	MD Khaled Sohel
Supervisor Initial	MKS
Completed Credit till now	133
How many crediis this semester	12
Amount (Due)	Tobe Cleared by final.
Supervisor Consent	☑ Yes ☐ No

Supervisor Signature

APPROVAL FORM – FINAL DEFENSE

APPROVAL

This thesis titled on "**Cybersecurity and Quantum computing: Challenges and Countermeasures**", submitted by **Nafee Ibn Sabah (ID: 221-35-1002)** to the Department of Software Engineering, Daffodil International University has been accepted as satisfactory for the partial fulfillment of the requirements for the degree of Bachelor of Science in Software Engineering and approval as to its style and contents.

BOARD OF EXAMINERS

Chairman

Dr. A. H. M. Saifullah Sadi
Professor
Department of Software Engineering
Faculty of Science and Information Technology Daffodil International University

Internal Examiner 1

Dr. Rubaiyat Islam
Associate Professor
Department of Software Engineering
Faculty of Science and Information Technology
Daffodil International University

Internal Examiner 2

Dr. Md. Abdul Kader
Associate Professor
Department of Software Engineering
Faculty of Science and Information Technology
Daffodil International University

Internal Examiner 3

Nuruzzaman Faruqui
Assistant Professor
Department of Software Engineering
Faculty of Science and Information Technology
Daffodil International University

External Examiner

Md. Mostafiz Khan
Managing Director
Tecognize Solutions Limited

DAFFODIL INTERNATIONAL UNIVERSITY

DECLARATION OF THESIS AND COPYRIGHT

Author's Full Name	:	Nafee Ibn Sabah
Date of Birth	:	30th March 2002
Title	:	Undergraduate student
Academic Session	:	

I declare that this thesis is classified as:

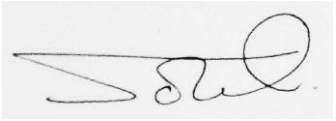
☐	CONFIDENTIAL	(Contains confidential information under the Official Secret Act 1997)*
☐	RESTRICTED	(Contains restricted information as specified by the organization where research was done)*
☐	OPEN ACCESS	I agree that my thesis to be published as online open access (Full Text)

I acknowledge that Daffodil International University reserves the following rights:

1. The Thesis is the Property of Daffodil International University.
2. The Library of Daffodil International University has the right to make copies of the thesis for the purpose of research only.
3. The Library of Daffodil International University has the right to make copies of the thesis for academic exchange.

Certified by:

_____
(Student's Signature)



_____
(Supervisor's Signature)

_____
Student ID 221-35-1002
Date: 27th November 2025

_____
Name of Supervisor Mr Md Khaled Sohel
Date: 24th December 2025

THESIS DECLARATION LETTER

Librarian,
Daffodil International University,
Daffodil Smart City,
Ashulia.Dhaka,Bangladesh

Dear Sir,

CLASSIFICATION OF THESIS AS CONFIDENTIAL

Please be informed that the following thesis is classified as CONFIDENTIAL for a period of three (3) years from the date of this letter. The reasons for this classification are as listed below.

Author's Name Nafee Ibn Sabah
Thesis Title Cybersecurity and Quantum Computing: Challenges and Countermeasures

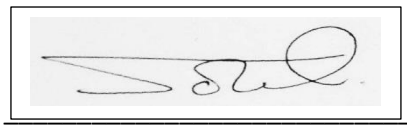
Reasons (i) Thesis contains sensitive data used in cyber security.

(ii)

(iii)

Thank you.

Yours faithfully,



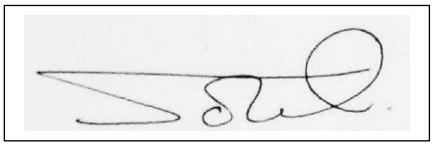
(Supervisor's Signature)

Date:

Stamp:

SUPERVISOR'S DECLARATION

I hereby declare that I/ have checked this thesis/ and in my opinion, this thesis is adequate in terms of scope and quality for the award of the degree of Bachelor of Science in Software Engineering



(Supervisor's Signature)

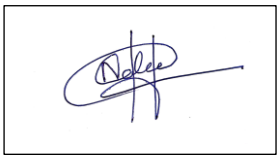
Full Name : MD Khaled Sohel

Position : Assistant Professor

Date : 24th December 2025

STUDENT'S DECLARATION

I hereby declare that the work in this thesis is based on my original work except for quotations and citations which have been duly acknowledged. I also declare that it has not been previously or concurrently submitted for any other degree at Daffodil International University or any other institution.



(Student's Signature)

Full Name : Nafee Ibn Sabah

ID Number : 221-35-1002

Date : 24th December 2025

Cybersecurity and Quantum Computing: Challenges and Countermeasures

Nafee Ibn Sabah

Thesis submitted in fulfillment of the requirements
for the award of the degree of
Bachelor of Science in Software Engineering

Department of Software Engineering (Major in Cyber Security)

DAFFODIL INTERNATIONAL UNIVERSITY

November 2025

ACKNOWLEDGEMENTS

This is to acknowledge the support and guidelines given to me while in the making of this thesis paper

I am profoundly thankful to my supervisor Mr. MD Khaled Sohel sir for his valuable feedback and much-needed guidelines which helped me make this thesis from start to finish. Their support meant that I also had proper directions and could make improvements upon my work from time to time.

I extend my sincere appreciation towards the faculty members of SWE, Daffodil International University, for giving me proper academic support and resources needed to make the study fun and worthwhile experience.

Special thanks to my batchmates and friends whose moral support and appreciation goes beyond words.

Lastly, I am eternally grateful to my family for believing in me and providing me with support which is akin to a cornerstone in my academic journey.

DEDICATION

This thesis is dedicated to my parents for their unconditional love and support which made this all possible. Their firm belief in my potential has been an invaluable motivation for this study.

This thesis is also dedicated to any future students who would like to study quantum computing and cryptography and would find this study helpful in understanding how it works.

ABSTRACT

It would be wrong to say classical computers are the future because now this is the age of “Quantum Computers”. This study aims to explain how it works, what are the issues with current cryptographic solutions that are vulnerable to quantum level attacks, provide case studies, performance and security trade offs along with challenges and discussions in case-by-case study. This entire paper aims to simplify the process and provides valuable insights into various available solutions. There isn’t a single one fit for all solution when it comes to cyber security and especially when it comes to Post Quantum Cryptography and as a result many different types of the PQC models are briefly studied to form an opinion on which one to use for which cases along with helpful benchmarks which ultimately helps in making a decision regarding which one to use depending on case by case scenario. This thesis also briefly studies on the economic implications on losses due to cybersecurity.

TABLE OF CONTENT

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

QKD	Quantum Key Distribution
PQC	Post Quantum Cryptography
HNDL	Harvest now, decrypt later
LWE	Learning with errors
ML-KEM	Module Lattice based Key Encapsulation Mechanism
ML-DSA	Module Lattice-based Digital Signature Algorithm
BD	Bangladesh

LIST OF APPENDICES

INTRODUCTION

Opening Statement

With the emergence of quantum computing, it's imperative that a proper quantum resistant environment is set up to counter it, not only that but also to make sure to minimize damage and use the best one for the best case, the main problem being the lack of information in one place as it is a new topic. While there are many existing solutions, many still needs improvements and must be studied upon to make a proper informed decision.

Quantum Computers

The quantum computers work in Qubits, which unlike the traditional bits consisting of 0s and 1s, it is a bit different. A qubit can be in a state of 0, 1 or both at the same time and as a result compared to classical computers, the mathematical computation possible while qubits are much faster and efficient in nature. (1) (3)

To fully understand how quantum computing works, we need to visit the elements of quantum mechanics which are superimposition, entanglement and quantum interference. To briefly explain each element, it would be as follows:

Quantum Superimposition: It's when a quantum element and in our case the qubit can exist in multiple state at the same time and as a result can be exponentially faster when thousands of qubits are formed and used to compute things. (2)

Quantum Entanglement: It's when two or more particles get linked in a such a way that one's state can influence the other and vice versa, it forms sometimes of tether-like connection despite the distance covered between them effecting each other's state. (2)

Quantum Interference: When quantum states overlap each other, they can also form and change depending on if its constructive interference or destructive interference. The overlap might affect other states involved and is best demonstrated on double slit experiment. (2)

Table 0.1 Classical Computer Vs Quantum Computer speed

Classical Algorithms with Exponential Runtime	Quantum Algorithm with Polynomial Runtime
10 seconds	1 minute
2 minutes	2 minutes
0.3K years	10 minutes
3.3K years	11 minutes
Around 13.8 billion years	Around 24 minutes

As we can see that while for very simple tasks like managing various spreadsheets or modifying documents as needed is where classical computers and their algorithms work the best as they are easy to compute, but for complex works like breaking encryption, training various AI models it's a clear win for quantum algorithms. (4)

There are many other areas that also benefit from such kind of quantum computing, but the focus of this thesis paper would be on the field of cybersecurity as it's one of the major areas now where modern solutions are not even considered without a quantum environment. There are many things that must be addressed first before we go into the technical details of the studies that are done over the years which resulted in fascinating finds which also includes Quantum key distribution also known as QKD. (1) (3) (5)

Cryptographic keys are used to identify, encrypt and decrypt data as needed, it is often used for digital security and in an essential element of Post Quantum Cryptography or PQC. (5) (6)

Classical Cryptographic system and PQC

In classical cryptographic systems such as RSA, Diffie-Hellman, ECC it is seen that due to its dependency on integer factorization and discrete logarithm they are strong against classical cryptographic system, however, they are weak against quantum algorithms where it was decrypted very easily. People depended on this kind of algiruthm for so long that it was thought to be almost indestructible and thus as a result was implemented almost everywhere possible. (8)

When developing their quantum environment one of the notable algorithms developed by IBM was Shor's algorithm which not only helped decrypt and decode RSA but also other current classical encryptions in place faster than even the classical supercomputers. Not only that, but the adversaries also responsible for stealing data attempted to follow the "HNDL" model which would yield stolen data that can be used when quantum computing reaches maturity and is available to a certain degree. This not only creates an issue with the existing security solution but also creates a new threat of cyber criminals stealing data as man in the middle attack being very common. Thus began the development of PQC which helped resist quantum level algorithms and also help create techniques such as using QKD to make sure key exchanges can be done safely.(9) (10) (11)

In order to make sure the keys shared are not being eavesdropped or being watched by anyone, QKD was formed also known as Quantum Key Distribution, it's a method where keys used in cryptographic operations are shared between the sender and receiver and if any middleman tries to spy on it the quantum state changes and alerts that the key is no longer secured for operation. It utilized quantum entanglement and any attempts to observe or measure it can disturb the system allowing it to be highly secured. (5)

QKD under normal status

Under normal circumstances any QKD type of cryptographic exchange would look like something like this:

Figure 0.1 *QKD under normal status*

Source: Self-made by Canva

As shown in figure 1.1 we can see that a typical key exchange is happening with no middleman or eavesdropping from someone else. As its a quantum state, it wont change as it is not observed while in transit thus maintaining its properties while also being fast and efficient.

This is just an example of the first QKD type of technique used in development as there are various other types as of which many are still under experimentation and development which would also require further testing documentation. Different type of techniques has different types of weaknesses and strengths, in that case depending on use case the best algorithm is selected.

QKD during middleman attack

We already know that when observed, the quantum states change and as a result this can be utilized to make sure nothing is observed while the keys are in transit, a common type of attack named man in the middle is when someone steals data in transit or spies on them, sometimes depending on the situation they can even impersonate one of them for additional information. To avoid that, QKD helps as it changes drastically when observed by an unintentional third-party during data transit or key exchanges.

Figure 0.2 *QKD under observed status*

Source: Self-made by Canva

With only a small change due to state shifting while being observed the entire key changes drastically alerting the ones that the key has been observed and thus the data transit has been compromised by someone who is observing them. (7)

Table 0.2 Classical Cryptography Vs PQC

Classical	Quantum
Based on mathematical computation	Based on Quantum mechanics
Straightforward	Sophisticated
Huge scope	Limited scope as of this moment
Well established and tested	Early stage of development
Less Expensive	Much more expensive
Bound by computational power and its limitations	Bound by laws of physics so needs no upgrades

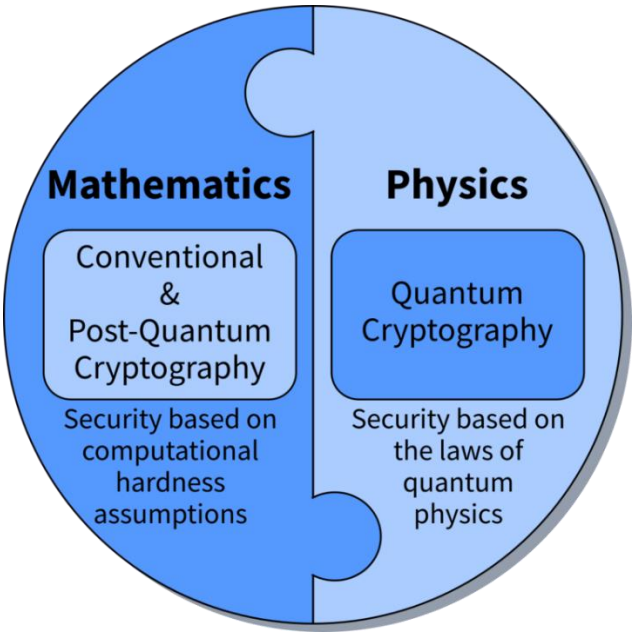


Figure 0.3 Yin & Yang representation of PQC and CC

Source: (12)

Due to the lack of cybersecurity, the world can lose up to an estimation of around 10.5 trillion USD or equivalent up to 2025 and that amount is shockingly high as even after so many security measures are in place, the cybercriminals always finding ways to circumvent the system security and thus creating crisis among people. This clearly means not a lot of people are still aware or care about their digital wellbeing as a recent survey suggested that phishing is still one of the major ways money is lost due to people falling victims to cybercrime. (13)

Table 0.3 Global Cost Timeline

Year	Amount in trillions

2019	3.21
2021	6.00
2023	8.10
2025	10.5

The shocking part of the data is by the end of 2025 at a loss of 10.5 trillion it boils down to a loss of around 330,000 USD per minute or even 5.5K per second, despite so many security in place, in a world without security the amount could have easily tripled with no way of getting back lost funds due to the presence of cryptocurrency .

This thesis aims to provide both exhaustive and properly structured analysis of various types of algorithms present within the current post quantum cryptography and help analyse different trade-offs that might be present between the types, their implementation and use cases depending on various their efficiency and performance.

CHAPTER 2

Literature Review

Table 21 Literature Review

Serial Number	Author-Year	Title	Contribution	Limitaiton
1.	Bernstein et al. (2009)	Introduction to post-quantum cryptography	Introduction to PQC	Many information old and outdated now as better solutions exist. (14)
2.	Buchmann et al. (2017)	Postquantum Cryptography—State of the Art	Unique Key System	Using unique key systems also used only one key per message so it was slow. (16)
3.	Hülsing (2013)	Shorter Signatures for Hash-Based signature schemes	Reduced signature size	Each key was one time only which used more resources. (15)
4.	Bernstein et al. (2015)	SPHINCS: Practical Stateless Hash-Based Signatures.	Introduced stateless hash-based signatures.	Cannot be used for key reuse as the signature size is big. (17)

Serial Number	Author-Year	Title	Contribution	Limitaiton
5.	Shahid et al. (2020)	WOTS-S: A Quantum Secure Compact Signature Scheme for Distributed Ledger.	Secure Blockchain.	Onetime key usage. (18)
6.	Sjöberg (2017)	Post-Quantum Algorithms for Digital Signing in PKI.	PQC algorithms.	Theoretical Information only (19)
7.	Suhail et al. (2021)	On the Role of Hash-Based Signatures in Quantum-Safe IoT.	Hash based signatures in IoT.	Lacked proper algorithm with real world applications. (20)
8.	Hegde, Jamuar, and Kulkarni (2023)	Post Quantum Implications on Private and Public Key Cryptography.	Used multiple keys	Very high computational overhead (21)
9.	Chambers, J. (2023)	What should we be doing with	A very business focused	No actual plans for planning on what to prepare

Serial Number	Author-Year	Title	Contribution	Limitaiton
		quantum computing?	article showing importance of waiting for quantum computing to mature.	for once PQC reaches maturity. (4)
10.	IBM (2024)	Shor's Algorithm	Can speed up exponentially	Sometimes unstable and has errors that needs further testing. (9)
11.	Khalil. M. (2025)	The cost of cybercrime statistics is projected to be $10.5 trillion annually by 2025	Depicts some of the highest level of financial loss for 2025 due to quantum attacks	No preventive measures or backup plans talked about. (13)
12.	Regenscheid, A. (2024)	Transition to Post-Quantum cryptography standards	Talks about migrating current infrastructures and system to PQC	Lack of demographic-based research needs to cover wider areas. (11)
13.	Sanghadia, P. (2025)	Understanding Quantum Key	Security in form of QKD	Still in experimental

Serial Number	Author-Year	Title	Contribution	Limitaiton
		Distribution (QKD)	unbound by classic hardware limitation.	phase and needs further testing (7)
14.	Sharma, A., & Naik, G. M. (2025).	A case study on the implementation of Caesar, ViGenere, and RSA Ciphers.	Discusses various classic ciphers in modern settings.	Without modern implementation and modification, will eventually be toppled by Quantum computers. (8)
15.	Demir et al. (2025)	Performance Analysis and Industry Deployment of Post-Quantum Cryptography Algorithms	Vast study on PQC and NIST standard CRYSTALS-Kyber and CRYSTALS-Dilithium	Relies on specific CPU architecture. (22)
16.	Scrivano (2025)	A Comparative Study of Classical and Post-Quantum	Practical use of Hybrid structure in PQC with	

Serial Number	Author-Year	Title	Contribution	Limitaiton
		Cryptographic Algorithms in the Era of Quantum Computing. ArXiv.org.	studies to critical threat model. (23)	
17.				
18.				
19.				

CHAPTER 3

METHODOLOGY

Methodology Principles and step by step guide:

Proper methodology principles were followed to make sure this paper is both insightful and useful in terms of both academia and personal knowledge in this field. Data was collected through fair means and proper citations were given where appropriate.

1) First relevant literature works in forms of papers, journals, internet articles, eBooks were read to get relevant knowledge needed for this study, all the things in this thesis under citations are mentioned in the reference page with valid information.

2) Then each work is properly analysed while taking relevant notes and data collection starts.

3) In case on unavailable data, data is simulated or collected from other reliable sources.

Sample methodology of a custom hashing algorithm and how it works

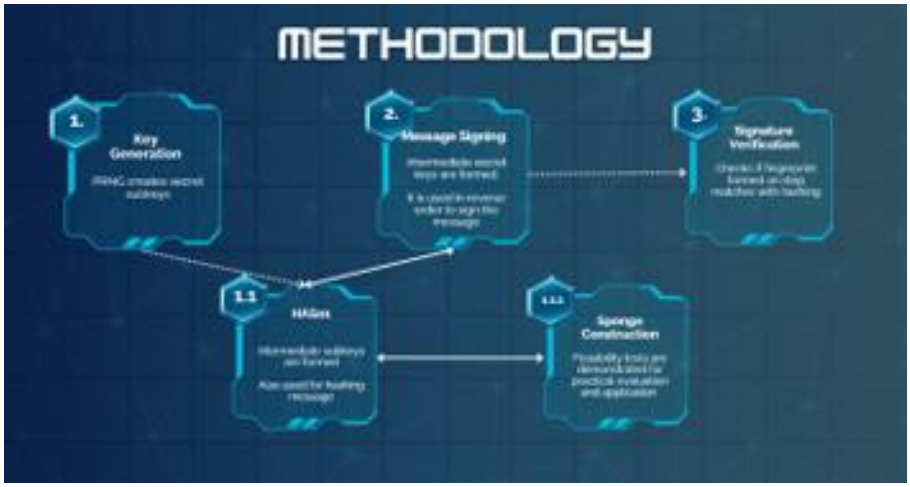


Figure 3.1 Methodology of a HAS01 algorithm, modified Syrga 1. Source: Self-made on canva

Step 1: Key Generation:

A pseudorandom number generator creates a set of secret subkeys which later combines to form secret main key. Later it goes through HAS01 algorithm multiple times to create intermediate subkeys and then finally after multiple hashing public key is formed.

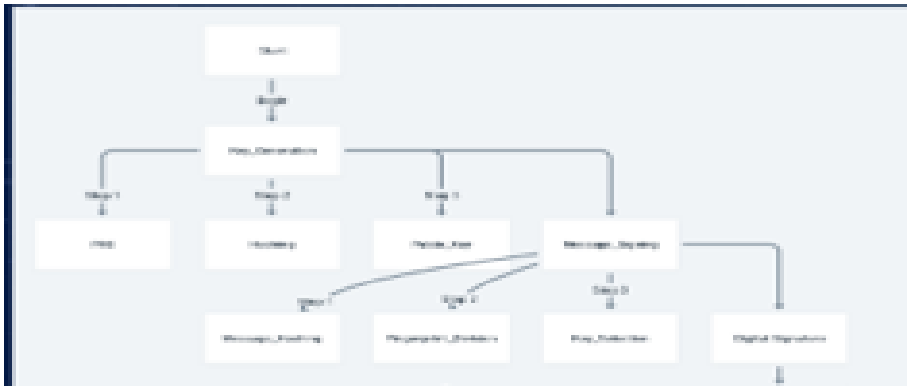


Figure 3.2 Another representation of HAS01

Figure 3.3 Hash-based algorithm methodology and workflow
Source Made on canva

Step 2: Signing message:

Hashing the message using HAS01 while creating a fingerprint and then it is divided into 32 smaller bits. Each part selects a segment from one of the intermediate secret keys. A digital signature is created using the selected elements and another hashing round is done in reverse order. The algorithm uses the intermediate secret keys in reverse order for subsequent messages which make sure each secret key is used once. The final hashed value combined with data like how many rounds forms the digital signature.

Step 3: Signature Verification:

Receiver gets the message, signature and the public key. Receiver hashes the message and checks if fingerprint matches and processes the rest using the public key.

CHAPTER 4
RESULTS AND DISCUSSION

4.1 Test Results:

Table 4.1: Comparing various results after studying following methodology

Algorithm Type	Mathematical Background	Key Size	Signature	Efficiency	Security
Lattice-Matrix	LWE	Small	Medium	Hugh	High
Code-based	Syndrome Decoding Problem	Large	Small	Medium	High
Hash-based	Collision Resistance	Medium	Large	Medium	Very high
Mutli-variate	Solving various multi variate equations	Medium	Medium	Medium	Medium

These results show the following conclusion:

Lattice based algorithm: Strong performance with moderate number of resources needed.

Code based: Huge key sizes which are more suitable for high-capacity storage units.

Hash-based: Highest security but also needs high storage and bandwidth to match.

Table 4.2 Some benchmark scores on different platforms

Algorithm	Key Size (KB)	Encryption (ms)	Decryption (ms)	Signature Size (byte)	Signature Time (ms)	Verif(ication (ms)
ML-KEM-768	1.2	0.01	0.02	N/A	N/A	N/A
Falcon-512	0.9	N/A	N/A	666	0.18	0.05
SPHINCS+-128f	0.03	N/A	N/A	17088	15.45	0.22
Classic McEliece	261	0.22	12.81	N/A	N/A	N/A

From this set of data, we can deduce:

ML-KEM and ML-DSA: Best used where there is a very high frequency of transactions happening all at once and digital signatures.

SPHINCS: Best used for long term planning in archival.

Lattice-based: For maximum schemes of efficiency with firmware.

ICT shares: Bangladesh ICT shares are dominated by large companies

Global annual loss vs BD loss: Annually by the end of 2025, global losses can get up to 10.5 Trillion USD, to compare if BD has 1% of the economic weight that would be 105 Billion at base, now if we take in the factor of BD not being a primary target and reduce the amount of loss to 77 Billion, Bangladesh having an estimated worth of 450 Billion is still losing 16.38% on cyber-attacks.

4.2 Challenges:

1) Side channel attacks or SCAs: During the study the quantum environment is vulnerable to various kinds of physical leakage like Power, EM emissions, timing etc to recover keys which leaves them vulnerable, further studies might help develop something that will fix the issue in the future.

2) Financial burden: Some hardware and maintenance can be extremely cost prohibitive as quantum technology is new and not fully matured yet to the point of proper understanding. As a result, sometimes the cost can way overweight the return in case of smaller scenarios where PQC might not be viable yet.

3) Complexity: Coding in a proper and secured way while also making sure proper controls are in place in case of anomaly as sometimes due to compiler optimization issues or specific hardware issues that might lead to something worse, further studies need to be done to make sure nothing happens.

4) Transition Risk: Sometimes transitions from classical to PQC is not fully done so a hybrid approach is taken which sometimes is not perfect and can be exploited.

5) Operational Risks: PQC and Quantum computing in general is still new and as a result there will always be some sort of operational risk if handled by untrained users. So, both caution and carefulness must be maintained at all costs.

6) Due to various hardware and software limitations, implementing it into BD infrastructure might become harder than it should be as many of the existing systems are old

7) Financial Burden: Many small to medium companies are unwilling to implement a portion of their budget into this technology making it harder to convince potential stakeholders to prioritize security on the long run.

CHAPTER 5

CONCLUSION

Concluding discussions:

While no clear one fix for all exists in this PQC environment it is still very much dependent on lot of factors like area, hardware, requirements, likelihood of being attacked by a quantum computer etc. However, hash-based algorithms seemed to have a perfect combination of security and performance which will allow us to implement into broader spectrum of devices.

Further studies and testing might also yield greater results for which more time and resources are needed as this entire topic although new but very quickly evolving and we should evolve wit it as well. But overall a hash based algorithm would be the best suit for most of the things in BD infrastructure.

REFERENCES

1) *Superposition & entanglement*. (2025, January 23). Quantum Inspire. https://www.quantum-inspire.com/kbase/superposition-and-entanglement/

2) The basics of Quantum Computing. (2025, January 20). Quantum Inspire. https://www.quantum-inspire.com/kbase/introduction-to-quantum-computing/

3) Wendin, G., & Wendin, G. (2017). Quantum information processing with superconducting circuits: a review. Reports on Progress in Physics, 80(10), 106001. https://doi.org/10.1088/1361-6633/aa7e1a

4) Chambers, J. (2023, August 2). What should we be doing with quantum computing? - JC2 Ventures. JC2 Ventures. https://www.jc2ventures.com/blog/2022/what-should-we-be-doing-with-quantum-computing

5) Wikipedia contributors. (2025, November 23). Quantum key distribution. Wikipedia. https://en.wikipedia.org/wiki/Quantum_key_distribution

6) Wikipedia contributors. (2025b, November 28). Key (cryptography). Wikipedia. https://en.wikipedia.org/wiki/Key_(cryptography)

7) Sanghadia, P. (2025, April 29). Understanding Quantum Key Distribution (QKD): Promise and Limitations. https://www.linkedin.com/pulse/understanding-quantum-key-distribution-qkd-promise-pranav-sanghadia-5xr9c

8) Sharma, A., & Naik, G. M. (2025). A case study on the implementation of Caesar, ViGenere, and RSA Ciphers. Zenodo (CERN European Organization for Nuclear Research). https://doi.org/10.5281/zenodo.17722861

9) Shor's algorithm | IBM Quantum Documentation. (n.d.). IBM Quantum Documentation. https://quantum.cloud.ibm.com/docs/en/tutorials/shors-algorithm

10) Mastercard R&D (October 20, 2025) Preparing for a post-quantum world: Quantum-safe technology

11) Regenscheid, A. (2024). Transition to post-Quantum cryptography standards. https://doi.org/10.6028/nist.ir.8547.ipd

12) Quantum communication – stobinska-group.eu. (n.d.). https://www.stobinska-group.eu/en/research-scope/quantum-communication/

13) Khalil, M. (2025, September 28). The cost of cybercrime statistics is projected to be $10.5 trillion annually by 2025. DeepStrike. https://deepstrike.io/blog/cybercrime-statistics-2025

14) Bernstein, D. J., Buchmann, J., & Dahmen, E. (Eds.). (2009). Post-Quantum Cryptography. Springer. https://link.springer.com/book/10.1007/978-3-540-88702-7

15) Hülsing, A. (2013). W-OTS+ – Shorter Signatures for Hash-Based signature schemes. In Lecture notes in computer science (pp. 173–188). https://doi.org/10.1007/978-3-642-38553-7_10

16) Postquantum Cryptography—State of the art. (2017). IEEE Journals & Magazine | IEEE Xplore. https://ieeexplore.ieee.org/document/8012288

17) Bernstein, D. J., Hopwood, D., Hülsing, A., Lange, T., Niederhagen, R., Papachristodoulou, L., Schneider, M., Schwabe, P., & Wilcox-O'Hearn, Z. (2015). SPHINCS: Practical Stateless Hash-Based Signatures. In Lecture notes in computer science (pp. 368–397). https://doi.org/10.1007/978-3-662-46800-5_15

18) Furqan Shahid, Abid Khan, Saif Ur Rehman Malik, Kim-Kwang Raymond Choo, (2020), WOTS-S: A Quantum Secure Compact Signature Scheme for Distributed Ledger, https://doi.org/10.1016/j.ins.2020.05.024.

19) Sjöberg (2017), Post-Quantum Algorithms for Digital Signing in PKI http://kth.diva-portal.org/smash/record.jsf?pid=diva2:1121030

20) On the Role of Hash-Based Signatures in Quantum-Safe Internet of Things: Current Solutions and Future Directions. (2021, January 1). IEEE Journals & Magazine | IEEE Xplore. https://ieeexplore.ieee.org/document/9152977

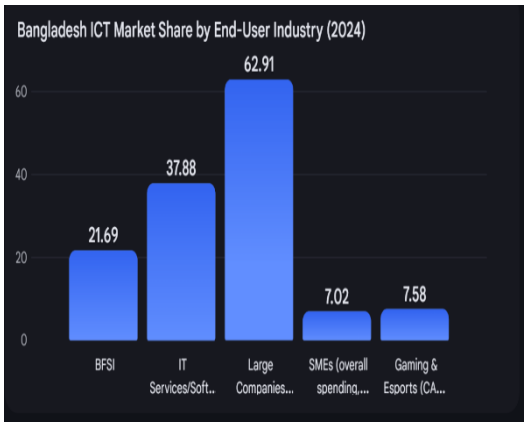
21) Post quantum implications on private and public key cryptography. (2023b, July 7). IEEE Conference Publication | IEEE Xplore. https://ieeexplore.ieee.org/document/10199503

22) Demir, E. D., Bilgin, B., & Onbaşlı, M. C. (2025, March). Performance Analysis and Industry Deployment of Post-Quantum Cryptography Algorithms. ArXiv.org. https://arxiv.org/abs/2503.12952

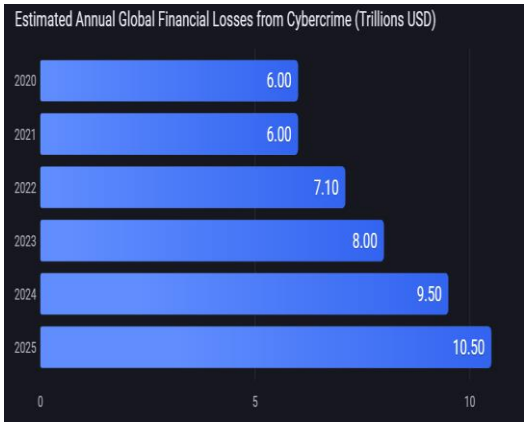
23) Scrivano, A. (2025, August 5). A Comparative Study of Classical and Post-Quantum Cryptographic Algorithms in the Era of Quantum Computing. ArXiv.org.

Appendices

A



BD economic sector in IT



Global losses due to cyber security

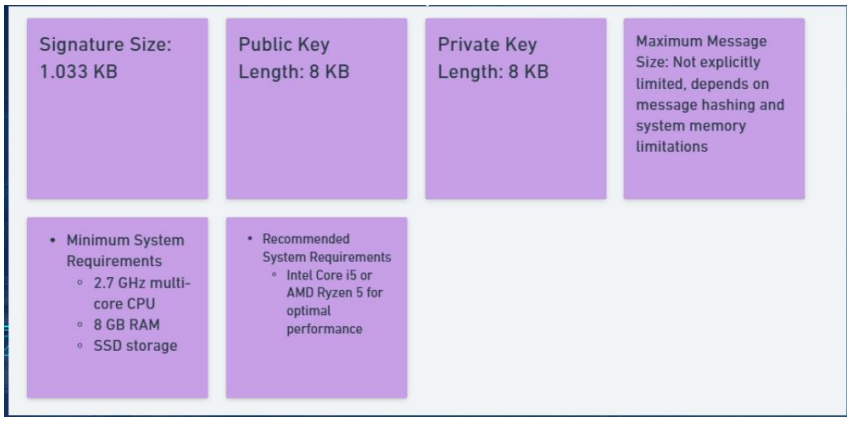
B

Scheme	Formulas	Parameters	Security Level, b
Syrga-1 Modified version	$b = k(\log(t/k))$	$k = 32, t = 256$	96
HORS [26]	$b = k(\log(t/kr))$	$k = 16, t = 2^{10}, r = 1$	96
W-OTS+ [19]	$b = n - \log(w^2 l + w)$, here $l = l_1 + l_2,\ l_1 = \left\lceil \frac{m}{\log w} \right\rceil, l_2 = \left\lfloor \frac{\log(l_1(w-1))}{\log w} \right\rfloor + 1$	$n = 128, w = 21, m = 256$	113
W-OTS^{PRF} [19]	$b = n - w - 1 - \log(lw)$, here $l = l_1 + l_2,\ l_1 = \left\lceil \frac{m}{\log w} \right\rceil, l_2 = \left\lfloor \frac{\log(l_1(w-1))}{\log w} \right\rfloor + 1$	$n = 128, w = 8, m = 256$	100

Syrga Data and formula

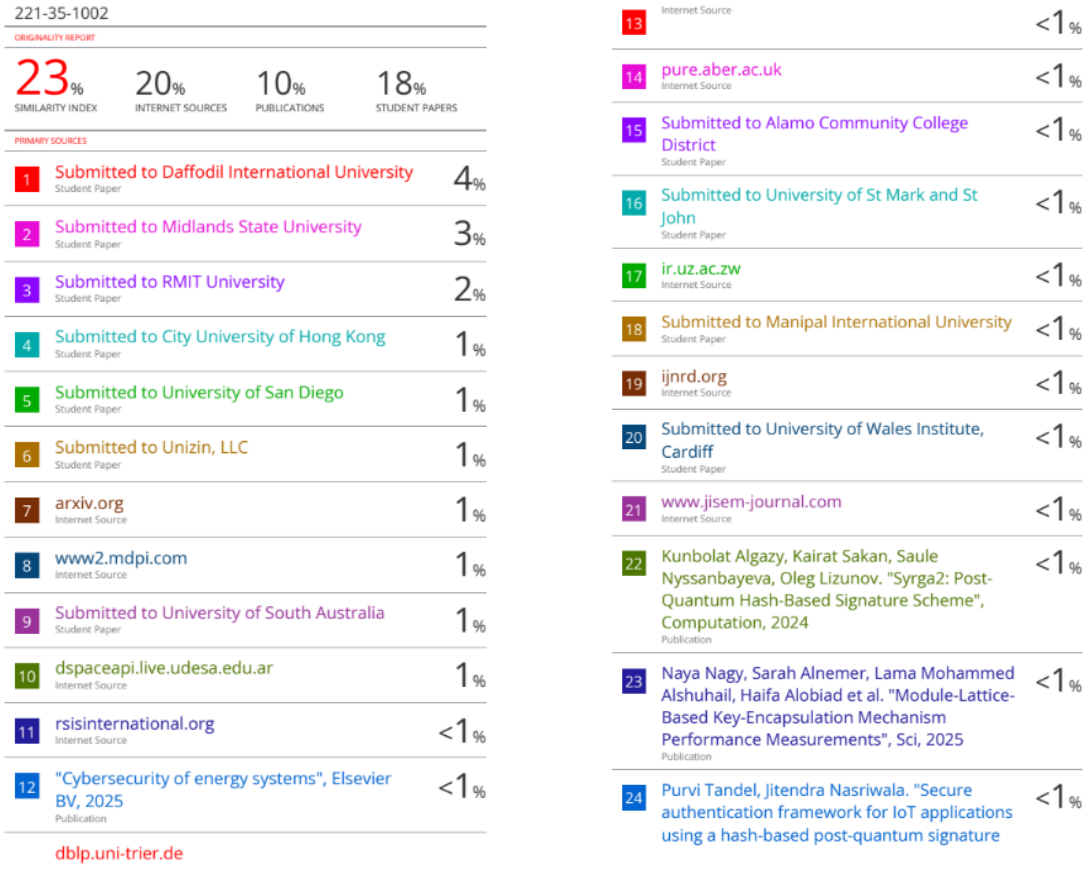
Scheme	Key Size (KB)	Signature Size (KB)	Key Usage
WOTS [7]	4.8	4.8	One time
WOTS+ [7]	3.7	3.2	One time
WOTS^{PRF} [7]	3.2	3.2	One time
HORS [7]	3.1MB	1.2	Few time
Syrga-1	8	1.033	Few time

Length Hash Value	Classical Security Level, (bit)		Quantum Security Level, (bit)	
	Preimage	Collision	Preimage	Collision
160-bit	160	80	80	53
256-bit	256	128	128	85
384-bit	384	192	192	128
512-bit	512	256	256	171



Hashing algorithms parameters from papers

Plagiarism Report 0% AI



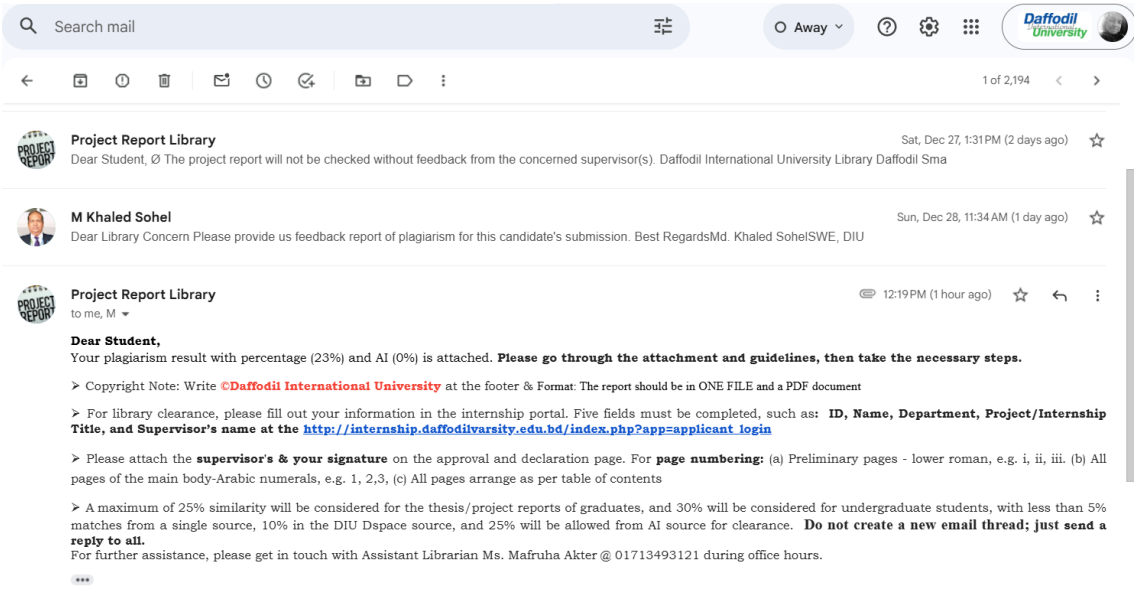
221-35-1002

ORIGINALITY REPORT

23%	20%	10%	18%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	Submitted to Daffodil International University Student Paper	4%
2	Submitted to Midlands State University Student Paper	3%
3	Submitted to RMIT University Student Paper	2%
4	Submitted to City University of Hong Kong Student Paper	1%
5	Submitted to University of San Diego Student Paper	1%
6	Submitted to Unizin, LLC Student Paper	1%
7	arxiv.org Internet Source	1%
8	www2.mdpi.com Internet Source	1%
9	Submitted to University of South Australia Student Paper	1%
10	dspaceapi.live.udesa.edu.ar Internet Source	1%
11	rsisinternational.org Internet Source	<1%
12	"Cybersecurity of energy systems", Elsevier BV, 2025 Publication	<1%
	dblp.uni-trier.de	
13	Internet Source	<1%
14	pure.aber.ac.uk Internet Source	<1%
15	Submitted to Alamo Community College District Student Paper	<1%
16	Submitted to University of St Mark and St John Student Paper	<1%
17	ir.uz.ac.zw Internet Source	<1%
18	Submitted to Manipal International University Student Paper	<1%
19	ijnrd.org Internet Source	<1%
20	Submitted to University of Wales Institute, Cardiff Student Paper	<1%
21	www.jisem-journal.com Internet Source	<1%
22	Kunbolat Algazy, Kairat Sakan, Saule Nyssanbayeva, Oleg Lizunov. "Syrga2: Post-Quantum Hash-Based Signature Scheme", Computation, 2024 Publication	<1%
23	Naya Nagy, Sarah Alnemer, Lama Mohammed Alshuhail, Haifa Alobiad et al. "Module-Lattice-Based Key-Encapsulation Mechanism Performance Measurements", Sci, 2025 Publication	<1%
24	Purvi Tandel, Jitendra Nasriwala. "Secure authentication framework for IoT applications using a hash-based post-quantum signature	<1%



Search mail

Away

Daffodil International University

1 of 2,194

Project Report Library — Sat, Dec 27, 1:31 PM (2 days ago)
Dear Student, Ø The project report will not be checked without feedback from the concerned supervisor(s). Daffodil International University Library Daffodil Sma

M Khaled Sohel — Sun, Dec 28, 11:34 AM (1 day ago)
Dear Library Concern Please provide us feedback report of plagiarism for this candidate's submission. Best RegardsMd. Khaled SohelSWE, DIU

Project Report Library — 12:19 PM (1 hour ago)
to me, M

Dear Student,
Your plagiarism result with percentage (23%) and AI (0%) is attached. **Please go through the attachment and guidelines, then take the necessary steps.**

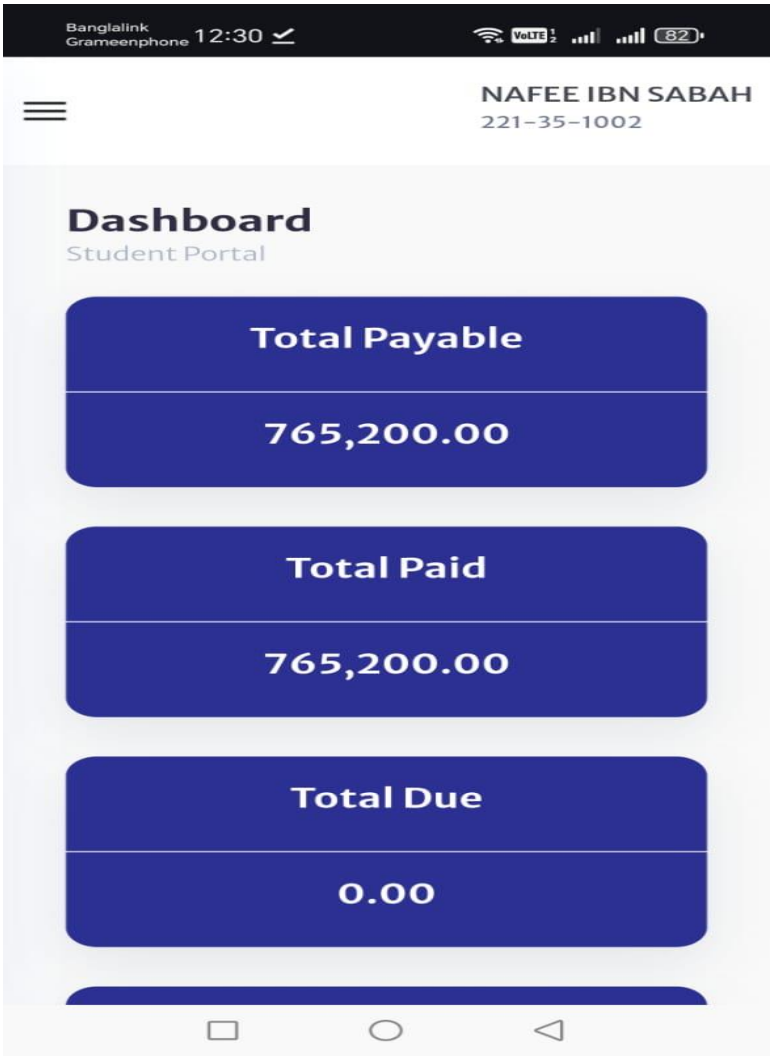
➢ Copyright Note: Write **©Daffodil International University** at the footer & Format: The report should be in ONE FILE and a PDF document

➢ For library clearance, please fill out your information in the internship portal. Five fields must be completed, such as: **ID, Name, Department, Project/Internship Title, and Supervisor's name at the** **http://internship.daffodilvarsity.edu.bd/index.php?app=applicant_login**

➢ Please attach the **supervisor's & your signature** on the approval and declaration page. For **page numbering:** (a) Preliminary pages - lower roman, e.g. i, ii, iii. (b) All pages of the main body-Arabic numerals, e.g. 1, 2,3, (c) All pages arrange as per table of contents

➢ A maximum of 25% similarity will be considered for the thesis/project reports of graduates, and 30% will be considered for undergraduate students, with less than 5% matches from a single source, 10% in the DIU Dspace source, and 25% will be allowed from AI source for clearance. **Do not create a new email thread; just send a reply to all.**
For further assistance, please get in touch with Assistant Librarian Ms. Mafruha Akter @ 01713493121 during office hours.

ACCOUNT CLEARANCE



Library Clearence