CS8000 PROJECT REPORT

Investigate the impact of quantum computing on

Diffie-Hellman Key Exchange

Apurva Dattatraya Kolhe, Esha Bharat Acharya, Raghul S, Sachi Patel

**INTRODUCTION**

The Diffie-Hellman key exchange algorithm is a cryptographic protocol that allows two parties to establish a shared secret key over an insecure communication channel without any prior secrets. The algorithm is based on modular exponentiation and is reliable on the computational difficulty of calculating discrete logarithms in a finite field. The development of quantum computers could potentially compromise the security of the Diffie-Hellman Key Exchange algorithm. This is because the quantum computers can perform certain types of calculations, such as Shor's algorithm, that can break this computational difficulty and allow attackers to easily calculate private keys.

*Apurva:* As we approach the advent of quantum computing, we face the inevitability that many long-standing solutions in computer science will be broken. To demonstrate its impact, we will be working with the Diffie Hellman key exchange algorithm in cryptography. While I have worked with key exchange algorithms, I am new to the field of quantum computing. I am excited to learn about how these two domains intersect and affect each other. This project is of interest to me because it involves exploring ways to ensure that Diffie Hellman remains a useful and reliable algorithm even in the era of quantum computing. By identifying potential vulnerabilities introduced by quantum computing and assessing the effectiveness and feasibility of alternative methods of generating secure keys, this project has the potential to offer valuable insights into the impact of quantum computers on the security of cryptographic systems. Ultimately, this could lead to the development of more robust cryptographic protocols that can withstand attacks from quantum computers, which is an increasingly important area of research as this field continues to advance.

*Esha:* The impact of quantum computing on the security of the Diffie-Hellman key exchange algorithm is a critical topic in the field of cybersecurity. This is personally relevant to me, because as a cyber security enthusiast, it highlights the need to stay up to date with the latest advancements in technology and to be proactive in identifying potential security risks. In addition, I see the aim of using quantum computers to predict prime numbers as an important step in the development of quantum-resistant cryptography like Shor’s algorithm, and how it is applied in factoring integers. I will learn about the importance of polynomial time while studying the efficiency of such types of algorithms. It could lead to the development of new algorithms and protocols that can enhance security in various sectors. I will also get an opportunity to learn the key differences between classical asymmetric cryptography algorithms and quantum algorithms and I can question the significance of password length and whether the inclusion of distinct alpha-numeric and special characters reduce the probability of predicting keys with the use of quantum computing.

*Raghul:* I am always intrigued by the idea and the development of quantum computers and have always wondered how the quantum computers will break some of the current algorithms which are solely reliable on the difficulty of them being broken using a classical computer. One such

algorithm is Diffie-Hellman Key Exchange. As mentioned above, the quantum computers can perform certain types of calculations, such as Shor's algorithm, that can break this computational difficulty and allow attackers to easily calculate private keys. I am really interested in investigating how much of an impact this will be by simulating the quantum environment using certain tools and try to break the algorithm with various key sizes and see how many qubits would be required to break the security and how long will the quantum computers take to do these calculations.

*Sachi:* There are no limits when it comes learning about computer algorithms, since algorithms change through creative thinking and have something unique to offer every time through their computational problems. We use Privacy and security in our everyday lives, and we all know that when it comes to privacy and security, functioning systems rely on secure and structures cryptographic algorithms. It really interests me and pushes me to think that how Diffie-Hellman key exchange plays an important role when it comes to sharing secret information in a secure way between two different parties even over insecure communication platforms. From this project, I am really looking forward to learning and finding more about different functions and possible ways to encrypt information with the use of algorithms.

**ANALYSIS**

In this project, we investigated the potential impact of quantum computing on the security of the Diffie-Hellman Key Exchange algorithm, and explored alternative methods of generating secure keys that are resistant to quantum attacks. We used a combination of theoretical analysis and practical implementation to achieve our goals. We used Python programming language and the PyCryptodome library to implement and test the Diffie-Hellman Key Exchange algorithm and the RLWE-based key exchange algorithm.

The first step in our analysis was to review the literature on the topic of quantum computing and its potential impact on cryptographic algorithms. We used the read papers to gain knowledge to understand the mathematical concepts and algorithms behind quantum computing, including quantum gates, qubits, and quantum algorithms such as Shor's algorithm. We reviewed the principles of classical cryptography, including symmetric key cryptography and public key cryptography, as well as the limitations of these methods when faced with quantum attacks.

Using the knowledge, we gained from CS 5800, we focused on the Diffie-Hellman Key Exchange algorithm and its vulnerability to quantum attacks. We analyzed the security of the algorithm and its susceptibility to attacks by quantum computers. We explained how the algorithm works, and showed how it can be compromised by attackers using quantum computers to perform discrete logarithm calculations. We also reviewed the current state of research on post-quantum cryptography, and explored alternative methods of generating secure keys that are resistant to quantum attacks.

We implemented the Diffie-Hellman Key Exchange algorithm in Python, using the PyCryptodome library to generate random prime numbers and to perform modular exponentiation. We tested the algorithm by simulating two parties exchanging public keys and deriving the shared secret key, and we verified that the key was the same in both parties.

Then we implemented the Shor’s algorithm using Python by simulating a quantum environment on the system using IBM Qiskit to prove that this algorithm can break the Diffie-Hellman by calculating the private key’s. This serves as proof that quantum computers can break the Diffie-Hellman algorithm which poses a great security thread for today’s world. Hence, we need to find an alternative way to generate the keys and we proceed with our next step.

To implement and test our alternative key generation method, we chose the Ring Learning with Errors (RLWE) algorithm, which is a lattice-based post-quantum cryptographic algorithm. We used the knowledge gained from the CS 5800 module on algorithms to understand the mathematical principles behind the RLWE algorithm and its implementation.

We then implemented the RLWE-based key exchange algorithm in Python, using the PyCryptodome library to generate random polynomials, to perform polynomial multiplication and addition, and to sample from a Gaussian distribution. We tested the algorithm by simulating two parties exchanging public keys and deriving the shared secret key, and we verified that the key was the same in both parties.

Finally, we compared the security and performance of the Diffie-Hellman Key Exchange algorithm and the RLWE-based key exchange algorithm. We discussed the advantages and disadvantages of each algorithm in terms of resistance to quantum attacks, key size, computational complexity, and memory requirements.

Overall, our analysis showed that quantum computing poses a significant threat to the security of classical cryptographic algorithms such as Diffie-Hellman Key Exchange. However, by adopting post-quantum cryptographic methods such as the RLWE algorithm, it is possible to generate secure keys that are resistant to quantum attacks. Our practical implementation and testing of the RLWE algorithm demonstrated its effectiveness in generating secure keys, making it a viable alternative to traditional cryptographic algorithms.

**POST QUANTUM CRYPTOGRAPHY**

Lattice-based cryptography and code-based cryptography are two post-quantum cryptography schemes that are being explored as potential replacements for currently used public-key cryptographic algorithms such as RSA and ECC, which are vulnerable to attacks by quantum computers.

Lattice-based cryptography involves using the geometry of high-dimensional spaces to create cryptographic schemes that are believed to be resistant to quantum attacks. The security of lattice-based cryptography is based on the difficulty of solving certain problems in high-dimensional spaces, such as the Shortest Vector Problem (SVP) or the Closest Vector Problem (CVP).

Code-based cryptography, on the other hand, is based on the difficulty of decoding linear error-correcting codes. In code-based cryptography, the encryption key is based on a linear error-correcting code, while the decryption key is based on the secret knowledge of how to decode that code. This secret knowledge is used to recover the original message from the received message, even if some errors have occurred during transmission.

Both lattice-based cryptography and code-based cryptography have their own strengths and weaknesses, and ongoing research is being conducted to improve their efficiency and security.

As mentioned before, Lattice-based cryptography relies on the hardness of certain mathematical problems related to lattices. A lattice is a set of points in space that are arranged in a periodic pattern, like the points on a lattice fence. In lattice-based cryptography, the difficulty of certain mathematical problems involving lattices is used to create cryptographic keys that are believed to be secure against attacks from both classical and quantum computers.

One of the main problems used in lattice-based cryptography is called the Ring Learning with Errors (RLWE) problem. The problem involves finding a short vector in a certain type of lattice, given noisy versions of some of the lattice points. This problem is believed to be computationally hard even for quantum computers, meaning that it would take an impractical amount of time and resources for a quantum computer to solve it.

**LWE**

LWE stands for Learning with Errors, which is a computational problem in cryptography related to the hardness of decoding random linear equations modulo a prime number. In this problem, given a set of noisy linear equations of the form a\_i⋅s + b\_i ≡ c\_i (mod q), where a\_i, s, b\_i, and c\_i are randomly chosen integers modulo q and the noise term e is chosen from a small distribution, the goal is to recover the secret vector s.

LWE forms the basis of several cryptographic constructions, including encryption schemes, key exchange protocols, and digital signatures, among others. It is considered to be one of the most promising candidates for post-quantum cryptography, as it is believed to be resistant to attacks by quantum computers.

**RLWE**

The RLWE (Ring Learning with Errors) problem is a specific type of LWE problem that is used as a basis for constructing cryptographic algorithms. In lattice-based cryptography, the security of the cryptographic scheme is based on the difficulty of certain mathematical problems in the theory of lattices.

This serves as the basis for a type of post-quantum cryptographic algorithm. It is based on the properties of a mathematical structure known as a ring. The problem of RLWE is to find the coefficients of a polynomial that is randomly sampled from a ring, given only noisy evaluations of the polynomial at a number of points.

RLWE can be used to construct cryptographic algorithms that are believed to be resistant to attacks by quantum computers. In particular, RLWE can be used to construct public-key encryption schemes and digital signature schemes. These schemes have been extensively studied and have been shown to be secure against a variety of attacks, including attacks by quantum computers.

**DIFFIE HELLMAN ALTERNATIVE**

The New Hope key exchange protocol is a specific example of a lattice-based key exchange protocol that uses the RLWE problem. It is said to be the alternative to Diffie-Hellman key exchange. It is a key exchange protocol based on a variant of the Ring Learning with Errors (RLWE) problem, which is a type of problem in lattice-based cryptography. New Hope provides similar security guarantees to Diffie-Hellman key exchange but is believed to be resistant to attacks by quantum computers, making it a potential replacement for the traditional key exchange protocol in a post-quantum world.

The protocol works by allowing two parties to agree on a shared secret key using public and private keys generated from the RLWE problem. The protocol is believed to be secure against attacks from both classical and quantum computers, because the RLWE problem is believed to be hard for both types of computers.

In contrast, the Diffie-Hellman key exchange protocol is vulnerable to attacks from quantum computers using Shor's algorithm, which can efficiently compute discrete logarithms in certain groups, including the group used in Diffie-Hellman. This means that if an attacker has a large enough quantum computer, they could use Shor's algorithm to efficiently break the Diffie-Hellman key exchange protocol and obtain the shared secret key.

**ALTERNATE APPROACH**

Code-based cryptography is another approach to post-quantum cryptography. It is based on error-correcting codes, which are used to detect and correct errors in data transmissions. In code-based cryptography, public keys are generated from specific types of codes, and private keys are generated from the corresponding decoding algorithm. The McEliece cryptosystem is a well-known code-based cryptosystem that is believed to be secure against quantum attacks. It is based on the problem of decoding a linear code with a random error distribution. But this is less preferred when compared to the previous one.

**CONCLUSION**

In conclusion, we investigated the impact of quantum computing on the security of the Diffie-Hellman key exchange algorithm and explored the potential of lattice-based cryptography, specifically the Ring-Learning with Errors (RLWE) algorithm, as a post-quantum alternative. Our analysis showed that while quantum computing poses a significant threat to the security of traditional cryptographic algorithms like Diffie-Hellman, RLWE-based cryptosystems are resistant to quantum attacks and can provide a secure alternative.

However, our project has some limitations. One limitation of our project is the reliance on current assumptions in the field of post-quantum cryptography. While RLWE-based cryptography has shown promising resistance to quantum attacks, there is still ongoing research into the potential vulnerabilities of these systems. Additionally, our analysis focused solely on the mathematical and theoretical aspects of the algorithm and did not consider the potential practical limitations of implementing such a system in real-world scenarios. Further research could explore these limitations and provide more insight into the feasibility and effectiveness of RLWE-based key exchange in practical applications. Furthermore, our analysis only considered a specific type of quantum attack, and other types of quantum attacks may still pose a threat to RLWE-based cryptosystems.

For future research, it would be interesting to implement a practical RLWE-based cryptosystem and evaluate its performance and security in practice. Additionally, exploring other post-quantum cryptographic alternatives and their comparative analysis with RLWE can also be a fruitful avenue for research.

*Raghul:* Through this project, I learned a lot about the challenges and potential solutions related to secure key exchange in a post-quantum computing era. Specifically, I gained a deeper understanding of the Diffie-Hellman Key Exchange algorithm and its vulnerabilities to quantum attacks, as well as the promising alternative of RLWE-based cryptography. This report will be of great value to me in future courses related to cryptography or security, and it has also sparked my interest in exploring this topic further in my future career as a computer scientist and we hope to apply the knowledge gained from this project to our future academic and professional endeavors.

*Esha:* This project gave me an opportunity to explore the potential impact on Diffie-Hellman Key Exchange algorithm and to investigate alternative methods of generating secure keys that cannot be easily decoded by quantum computers. I learnt about theoretical analysis as well as practical implementation, including Python Programming, especially PyCryptodome library. I studied Lattice-based and code-based cryptography which are post-quantum cryptographic schemes that are being explored as potential replacement for RSA. Since, Shor’s algorithm is simulated to break the Diffie Hellman algorithm, this analysis showed me that quantum computing poses a significant threat to classical cryptographic algorithms, but post-quantum cryptographic methods like the RLWE algorithm offer viable alternatives. While RLWE shows promising potential, it has piqued my interest as a security enthusiast, to further explore its limitations and ensure its effectiveness in practical applications.

*Esha:* This project explored the potential impact of quantum computing on the Diffie-Hellman Key Exchange algorithm and investigated alternative methods of generating secure keys. The study used theoretical analysis and practical implementation, including Python programming and the PyCryptodome library. The analysis showed that quantum computing poses a significant threat to classical cryptographic algorithms, but post-quantum cryptographic methods like the RLWE algorithm offer viable alternatives. Lattice-based and code-based cryptography are other post-quantum cryptographic schemes that are being explored as potential replacements for RSA and ECC. RLWE, which involves finding a short vector in a certain type of lattice, is believed to be computationally hard even for quantum computers.

Top of Form

Bottom of Form

**REFERENCES**

1. "Diffie-Hellman Key Exchange" by Khan Academy: <https://www.khanacademy.org/computing/computer-science/cryptography/modern-crypt/v/diffie-hellman-key-exchange-part-1>
2. "Quantum Computing for the Very Curious" by Michael Nielsen: <https://quantum.country/qcvc>
3. “Quantum Diffie-Hellman Key Exchange” by Dirk Fisher: <https://eprint.iacr.org/2021/1279.pdf>
4. Shor’s Algorithm: <https://en.wikipedia.org/wiki/Shor%27s_algorithm>
5. "Introduction to Quantum Computing" by IBM:

<https://quantum-computing.ibm.com/composer/docs/iqx>