TAYLOR'S UNIVERSITY
Wisdom · Integrity · Excellence

Bachelor of Computer Science (Hons)
Bachelor of Software Engineering (Hons)

ASSIGNMENT COVER SHEET

Module Code: **ITS64304**

Module Name: **Theory of Computation**

Students Name	**Students ID:**
1) Ishihara Satoaki	0354208
2) Basilia Sebastian	0353378
3) Syed Muhammad Taha Ali	0354100
4) Mohamed Fahad Farhan	0354487
5) Mohammad Sameed Khan	0353846
6)	

Assignment No. / Title	Assignment 2
Course Tutor/Lecturer	Assoc. Prof. Dr Raja

Declaration *(need to be signed by students. Otherwise, assignment will not be marked)*

We certify that this assignment is entirely our own work, except where we have given fully documented references to the work of others, and that the material contained in this assignment has not previously been submitted for assessment in any other formal course of study.

Signature of Students:

Marks:	**Evaluated by:**
Evaluator's Comments:	

Table of Contents

Introduction

In the realm of information security, cryptography plays an indispensable role in ensuring the confidentiality, integrity, and authenticity of sensitive data. However, with the advent of quantum computing, traditional cryptographic systems face unprecedented challenges that threaten their long-standing security guarantees. As quantum computers continue to advance, it becomes imperative to investigate the impact of quantum computing on cryptographic algorithms and develop new cryptographic solutions that are invulnerable to quantum attacks.

In this research report, we delve into the fascinating intersection of cryptography and quantum computing, aiming to explore the implications, challenges, and potential solutions for secure communication in the quantum era. By investigating the effects of quantum computing on cryptography, we seek to contribute to the development of the quantum-resistant cryptographic algorithms and prepare for a future landscape of secure communication.

The report is structured as follows:

1. **Background and Context**: We provide a concise overview of classical cryptography, its foundational principles, and its role in modern communication systems. Additionally, we introduce the fundamentals of quantum computing, explaining the unique properties of quantum bits (qubits) and their potential to revolutionise computation.

2. **Quantum Threats to Cryptography**: In this section, we examine the specific threats posed by quantum computing to traditional cryptographic systems. We discuss the potential of quantum algorithms, such as Shor's algorithm, to break widely used encryption schemes, highlighting the urgent need for post-quantum cryptography.

3. **Post-Quantum Cryptography**: In this section, we explore the emerging field of post-quantum cryptography that aims to develop cryptographic algorithms, which can oppose attacks caused by quantum computers. We investigate a wide variety of approaches such as lattice-based, code-based, multivariate cryptography, among others, assessing their security, efficiency, and feasibility for practical implementation.

4. **Quantum Key Distribution**: Quantum key distribution (QKD) is a promising technology that utilises the principles of quantum mechanics to establish secure

cryptographic keys. In this section, we delve into the principles and protocols of QKD, highlighting its potential as a quantum-resistant solution for secure key exchange.

5. **Bridging the Gap**: As the transition to post-quantum cryptography poses challenges for the existing infrastructure, we discuss strategies for bridging the gap between classical and quantum-safe cryptographic systems. We explore hybrid cryptography, quantum-safe algorithms, and the deployment challenges involved in ensuring a smooth and secure transition.

6. **Future Perspectives**: We conclude the report by discussing the future prospects and open research directions in the field of cryptography and quantum computing. We explore topics such as quantum-resistant standards, quantum key distribution networks, and the impact of quantum technologies beyond encryption, offering insights into the evolving landscape of secure communication.

Through this research report, we aim to contribute to the growing body of knowledge in the field of cryptography and quantum computing. By analysing the impact of quantum computing on cryptography and investigating potential quantum-resistant solutions, we strive to facilitate the development of secure communication protocols that can withstand the power of quantum computers, ensuring the confidentiality and integrity of sensitive information in the quantum era.

Background and Context

Cryptography secures sensitive information in modern communication systems using mathematical principles to transform plaintext into unreadable ciphertext. The discipline has a rich history, starting with the Caesar cipher used by Julius Caesar. Later, more complex techniques, like the Vigenère cipher, were developed. However, classical cryptography faced vulnerabilities with the advent of computers, leading to more secure symmetric and asymmetric-key algorithms. Despite its effectiveness, quantum computing presents new challenges that could render existing cryptographic systems insecure.

Qubits have unique properties that allow quantum computers to cope with specific problems much more instantly than classical bit computers. This has significant implications for cryptography, as many widely used cryptographic algorithms rely on computational problems that are difficult to solve classically. For example, factorization of large numbers is the basis for the security of RSA and other public-key encryption schemes.

Shor's algorithm, formulated by Peter Shor in 1994, enables rapid factorization of large numbers on a quantum computer by leveraging the inherent quantum properties of qubits to determine the prime factors of a composite number. This groundbreaking discovery gave rise to the field of post-quantum cryptography, which focuses on the development of cryptographic algorithms that maintain their security even in the presence of quantum computers. Researchers are currently investigating various methodologies, including lattice-based, code-based, multivariate, and hash-based cryptography. These approaches utilise mathematical problems that are believed to be arduous for both classical and quantum computers to solve.

Recently, researchers have focused on standardising post-quantum cryptographic algorithms to transition smoothly to quantum-resistant cryptography. Initiatives and competitions by organisations like NIST help select new algorithms that can withstand quantum attacks.

As we develop and deploy post-quantum algorithms, we also need to consider existing classical cryptography. Hybrid cryptography combines classical and quantum-resistant algorithms to bridge the gap between classical and quantum-safe systems. Quantum key distribution (QKD) is another potential solution to securely distribute cryptographic keys.

Quantum Threats to Cryptography

Quantum computing poses a major threat to classical cryptographic systems, which rely on difficult mathematical problems for security. The significant computational power of quantum computers, particularly for certain algorithms like Shor's, can compromise the security provided by classical cryptographic algorithms. Shor's algorithm, developed in 1994, is one of the most notable quantum algorithms that threatens traditional cryptography by efficiently factoring large numbers and solving the discrete logarithm problem. This algorithm can break the mathematical foundations of widely-used cryptographic systems like RSA and Diffie-Hellman key exchange, leaving them vulnerable to quantum attacks.

Shor's algorithm has a significant impact on cryptography. It can factorise large numbers on a quantum computer, making RSA and Diffie-Hellman key exchange vulnerable to quantum attacks. Grover's algorithm also poses a threat to specific cryptographic systems by reducing the effective key sizes of symmetric cryptographic algorithms. Although it does not directly break encryption schemes, it can perform an exhaustive search of the key space in roughly the square root of the classical time, weakening the security margin of symmetric encryption schemes.

The rise of quantum attacks targeting conventional cryptographic systems emphasises the pressing need to develop post-quantum cryptographic algorithms. These algorithms are specifically crafted to withstand attacks from both classical and quantum computers. By delving into alternative mathematical problems deemed challenging for quantum computers, post-quantum cryptography strives to ensure secure communication amidst the imminent advent of quantum computing.

Post-Quantum Cryptography

Post-quantum cryptography is an emerging field that focuses on developing cryptographic algorithms capable of resisting attacks from both classical and quantum computers. As quantum computing advances, it poses a significant threat to traditional cryptographic systems, necessitating the exploration of alternative cryptographic approaches. This section explores post-quantum cryptography, examining different strategies and evaluating their security, efficiency, and practical feasibility.

Lattice-based cryptography stands out as a promising avenue for post-quantum cryptographic solutions. It relies on mathematical lattice problems and offers strong security guarantees even against quantum attacks. Notable lattice-based schemes include Learning With Errors (LWE), Ring Learning With Errors (RLWE), and NTRU encryption and signature schemes (Peikert, 2016).

Code-based cryptography is another approach that employs error-correcting codes. These codes introduce redundancy to detect and correct errors during data transmission. Code-based cryptographic systems, like the McEliece cryptosystem, resist attacks from quantum computers due to the complexity of decoding linear codes. However, their efficiency and key sizes can pose challenges for practical implementation (Misoczki et al., 2019).

Multivariate cryptography builds upon multivariate polynomials to create cryptographic systems. The security of these schemes relies on the complexity of solving systems of multivariate equations. Examples include the Hidden Field Equations (HFE) and Rainbow signature scheme. While multivariate cryptography shows promise against quantum attacks, issues such as key sizes and efficiency remain (Ding et al., 2019).

Hash-based cryptography utilises hash functions as the foundation for post-quantum cryptographic systems. These schemes leverage the collision resistance of hash functions to provide security. The Merkle signature scheme and Lamport signature scheme are notable examples. While hash-based cryptography offers strong security, limitations in terms of key sizes and efficiency may arise (Bernstein et al., 2012).

Additional approaches in post-quantum cryptography include isogeny-based cryptography, which employs mathematical properties of elliptic curves and isogenies, and code-based encryption schemes such as the Niederreiter cryptosystem. These approaches provide

alternative avenues for exploring post-quantum security (Jao and De Feo, 2011; Bernstein et al., 2017).

Quantum Key Distribution

Quantum Key Distribution (QKD) represents a highly promising technology that capitalises on the tenets of quantum mechanics to establish secure cryptographic keys. Unlike classical key exchange protocols that rely on computational assumptions, QKD exploits the inherent properties of quantum mechanics to ensure the utmost security in key distribution. This section delves into the principles and protocols of QKD, emphasising its potential as an impervious solution for quantum-resistant secure key exchange.

At the heart of QKD lies the Heisenberg uncertainty principle, which asserts the impossibility of precisely measuring certain pairs of physical properties of a quantum system simultaneously. QKD protocols exploit this principle to detect any illicit eavesdropping attempts on the communication channel. Among the extensively studied and implemented QKD protocols, the BB84 protocol, introduced by Bennett and Brassard in 1984, stands as a prominent example (Bennett & Brassard, 1984).

In the BB84 protocol, the sender, commonly referred to as Alice, encodes the secret key information using quantum states, typically individual photons, in different quantum bases. The receiver, commonly referred to as Bob, measures the received quantum states in randomly chosen bases. Both Alice and Bob publicly announce their bases for a subset of the transmitted quantum states and use this information to establish a secure key through classical post-processing techniques. The security of QKD protocols lies in the fact that any attempt by an eavesdropper, commonly referred to as Eve, to intercept the quantum states would introduce detectable errors, allowing Alice and Bob to detect the presence of an adversary.

Various improvements and variations of the BB84 protocol have been proposed to enhance the security and efficiency of QKD. These include the use of entangled states, such as in the Ekert protocol (Ekert, 1991), and the development of practical implementations, such as the decoy-state method (Hwang, 2003). Moreover, researchers continue to explore novel QKD protocols, such as measurement-device-independent QKD (Lo et al., 2012), which aim to further strengthen the security guarantees of QKD.

While QKD offers strong security guarantees based on the laws of physics, its practical implementation faces challenges. These challenges include the limited transmission distance of QKD systems due to the attenuation and noise introduced in the communication channel.

Additionally, the integration of QKD with existing communication infrastructure and the development of practical and scalable QKD devices pose significant engineering and deployment challenges.

Bridging the Gap

As the field of cryptography transitions from classical to post-quantum systems, it poses challenges for the existing infrastructure and cryptographic protocols. This section explores strategies for bridging the gap between classical and quantum-safe cryptographic systems, ensuring a smooth and secure transition. We will explore hybrid cryptography, quantum-safe algorithms, and the deployment challenges involved in this process.

1. **Hybrid Cryptography**: One approach to bridging the gap is through hybrid cryptography, which combines classical and post-quantum cryptographic algorithms. In this paradigm, classical cryptographic algorithms are used alongside quantum-safe algorithms to provide a layered defence against attacks from both classical and quantum adversaries. By employing hybrid schemes, organisations can maintain compatibility with existing infrastructure while gradually integrating quantum-safe algorithms into their systems. The National Institute of Standards and Technology (NIST) recommends considering hybrid cryptography as a transitional solution.

2. **Quantum-Safe Algorithms**: Another approach involves the implementation of quantum-safe algorithms capable of withstanding attacks from quantum computers. The domain of post-quantum cryptography encompasses diverse cryptographic primitives that are resistant to quantum threats, such as lattice-based, code-based, multivariate, hash-based, and isogeny-based schemes, among others. These algorithms are purposefully designed to withstand attacks from both classical and quantum computers. To evaluate and establish standardised quantum-safe algorithms, the National Institute of Standards and Technology (NIST) has launched the Post-Quantum Cryptography Standardization project.

3. **Deployment Challenges**: The deployment of post-quantum cryptography poses several challenges. One major concern is the efficiency and performance of quantum-safe algorithms. As post-quantum algorithms often exhibit higher computational costs compared to classical algorithms, their implementation should be optimised to ensure acceptable performance in real-world scenarios. Additionally, the integration of quantum-safe algorithms into existing protocols and systems may require substantial modifications, including changes to cryptographic libraries, key management practices, and network infrastructure.

Future Perspectives

In this section, we discuss the future prospects and open research directions in the field of cryptography and quantum computing. We explore various topics that shed light on the evolving landscape of secure communication and the impact of quantum technologies beyond encryption.

1. **Quantum-Resistant Standards**: As the realm of post-quantum cryptography progresses, it is imperative to establish robust standards that can withstand quantum attacks. These standards will serve as essential benchmarks for the development, assessment, and adoption of cryptographic algorithms that remain secure in the face of quantum computing. Prominent entities like the National Institute of Standards and Technology (NIST) actively participate in standardisation endeavours, aiming to identify and endorse quantum-resistant algorithms that can form the bedrock of secure communication in the quantum era.

2. **Quantum Key Distribution Networks**: Quantum key distribution (QKD) offers a promising approach for secure key exchange. In the future, the deployment of QKD networks is anticipated to become more widespread, enabling secure communication across large-scale infrastructures. Research efforts are focused on developing efficient protocols, optimising network architectures, and addressing practical challenges such as long-distance transmission, scalability, and compatibility with existing network technologies. The establishment of robust QKD networks will be instrumental in achieving quantum-resistant secure communication.

3. **Impact of Quantum Technologies Beyond Encryption**: While cryptography is a primary application of quantum computing, the impact of quantum technologies extends beyond encryption. Quantum computing has the potential to revolutionise fields such as optimization, simulation, machine learning, and drug discovery. As quantum computers become more powerful, exploring the implications and developing quantum-inspired algorithms in these domains will be essential. The convergence of cryptography and quantum computing opens up new avenues for innovation and interdisciplinary research.

Personal Contributions

Student Name	Contribution made:
1) Ishihara Satoaki	• Introduction (Entirely) • Background and Context (Entirely) • Quantum Threats to Cryptography (Entirely) • Post-Quantum Cryptography (Entirely) • Quantum Key Distribution (Entirely) • Bridging the Gap (Entirely) • Future Perspectives (Entirely) • References (Entirely)
2) Basilia Sebastian	
3) Mohamed Fahad Farhan	
4) Mohammad Sameed Khan	
5) Syed Muhammad Taha Ali	• Introduction (partially) • Background and Context (partially) • Future Perspectives (partially
6)	

References

[1] Stallings, W. (2017). *CRYPTOGRAPHY AND NETWORK SECURITY PRINCIPLES AND PRACTICE SEVENTH EDITION GLOBAL EDITION*. [online] Pearson. Available at: https://www.cs.vsb.cz/ochodkova/courses/kpb/cryptography-and-network-security_-principles-and-practice-7th-global-edition.pdf. [Accessed 20 May. 2023].

[2] Bernstein, D.J., Buchmann, J. and Dahmen, E. (2009). *Post-Quantum Cryptography*. [online] *Google Books*, Springer Science & Business Media. Available at: https://www.google.com.my/books/edition/Post_Quantum_Cryptography/VB598lO47NAC?hl=en&gbpv=0. [Accessed 20 May. 2023].

[3] Shor, P.W. (1994). Algorithms for quantum computation: discrete logarithms and factoring. *Proceedings 35th Annual Symposium on Foundations of Computer Science*, [online] 11. doi:https://doi.org/10.1109/sfcs.1994.365700. [Accessed 20 May. 2023].

[4] Menezes, A.J., van Oorschot , P.C. and Vanstone, S.A. (1996). HANDBOOK of APPLIED CRYPTOGRAPHY. *www.academia.edu*, [online] 794. Available at: https://www.academia.edu/33795500/HANDBOOK_of_APPLIED_CRYPTOGRAPHY [Accessed 20 May. 2023].

[5] Grover, L.K. (1996). A fast quantum mechanical algorithm for database search. *Proceedings of the twenty-eighth annual ACM symposium on Theory of computing - STOC '96*, 8, pp.212–219. doi:https://doi.org/10.1145/237814.237866. [Accessed 30 May. 2023].

[6] Boneh, D. and Lipton, R.B. (1996). Algorithms for Black-Box Fields and their Application to Cryptography. *Algorithms for Black-Box Fields and their Application to Cryptography*, [online] 15, pp.283–297. doi:https://doi.org/10.1007/3-540-68697-5_22. [Accessed 30 May. 2023].

[7] Pelkert, C. (2016). *A Decade of Lattice Cryptography*. [online] ieeexplore.ieee.org. Available at: https://ieeexplore.ieee.org/document/8187288 [Accessed 30 May. 2023].

[8] Bernstein, D.J., Lange, T. and Peters, C. (2008). Attacking and Defending the McEliece Cryptosystem. *Post-Quantum Cryptography*, [online] 16, pp.31–46. doi:https://doi.org/10.1007/978-3-540-88403-3_3. [Accessed 30 May. 2023].

[9] Jao, D., De Feo, L. and Plut, J. (2011). Towards Quantum-Resistant Cryptosystems from Supersingular Elliptic Curve Isogenies. *Springer*, [online] 24, pp.19–34. doi:https://doi.org/10.1007/978-3-642-25405-5_2. [Accessed 3 Jun. 2023].

[10] Bennett, C.H. and Brassard, G. (1984). *Quantum cryptography: Public key distribution and coin tossing*. [online] ResearchGate. Available at: https://www.researchgate.net/publication/228109483_WITHDRAWN_Quantum_cryptography_Public_key_distribution_and_coin_tossing. [Accessed 3 Jun. 2023].

[11] Ekert, A. (1991). Quantum cryptography based on Bell's theorem. *Physical review letters*, [online] 67(6), pp.661–663. doi:https://doi.org/10.1103/PhysRevLett.67.661. [Accessed 5 Jun. 2023].

[12] Hwang, W.-Y. (2003). Quantum Key Distribution with High Loss: Toward Global Secure Communication. *Physical Review Letters*, 91(5). doi:https://doi.org/10.1103/physrevlett.91.057901. [Accessed 5 Jun. 2023].

[13] Lo, H.-K., Curty, M. and Qi, B. (2012). Measurement-Device-Independent Quantum Key Distribution. *Physical Review Letters*, 108(13). doi:https://doi.org/10.1103/physrevlett.108.130503. [Accessed 5 Jun. 2023].

[14] Chen, L., Jordan, S., Liu, Y.-K., Moody, D., Peralta, R., Perlner, R. and Smith-Tone, D. (2016). Report on Post-Quantum Cryptography. *Report on Post-Quantum Cryptography*. [online] doi:https://doi.org/10.6028/nist.ir.8105. [Accessed 5 Jun. 2023].

[15] Scarani, V., Bechmann-Pasquinucci, H., Cerf, N.J., Dušek, M., Lütkenhaus, N. and Peev, M. (2009). The security of practical quantum key distribution. *Reviews of Modern Physics*, [online] 81(3), pp.1301–1350. doi:https://doi.org/10.1103/revmodphys.81.1301. [Accessed 5 Jun. 2023].