Quantum Security

Zelalem.S, Dec
2025

Abstract— This paper comprehensively assesses the disruptive influence of **Quantum Cryptography** on existing algorithms and encryption methods, emphasizing the imperative to evolve security paradigms in the era of quantum computing. The research scrutinizes the robustness of quantum cryptographic techniques in ensuring security within communication protocols and key distribution. It also investigates post-quantum cryptography solutions to guarantee the security and resilience of communication systems and critical applications in a quantum empowered environment.

This synthesis provides a comprehensive overview of the state of quantum cryptography research, encompassing philosophical insights, practical implications, and the essential role it plays in shaping the future of secure communication while emphasizing the urgency of adapting to quantum threats.

Keywords: QKDP QC Qubit QKDP BB84 PNS

I. Introduction

Quantum technology is expected to become a reality in the near future, with vastly superior performance to existing computing methods. The advent of quantum computing has also changed the landscape of security and cryptography.

Quantum computing is poised to disrupt many aspects of technology, the following are some of the highlights.

- Examine how quantum cryptography will impact existing cryptographic methods.
- Overview implementation of quantum key distribution protocols.

This paper synthesizes the findings of different papers to provide a comprehensive overview of the impact of quantum computing on business. It also discusses the use of quantum key distribution (QKD) to share keys for message encryption and decryption. QKD is a secure method of communication that can be used to protect data from being intercepted by quantum computers.

II. Quantum Cryptography

According to Maneesh Yati [1], Quantum cryptography is based on the phenomena of quantum physics which allows secure data transmission between sender and receiver.

Quantum cryptography is novel in the field of cryptography [4]. This paper reviewed four related papers to find out their main strengths and weaknesses on the quantum security problem domain. The methodology they used and the problem they addressed is going to be discussed. And finally, we compare and contrast between papers based on their weakness and strength.

A. Quantum Advantage in Cryptography

Renato Renner and Ramona Wolf, from the Institute for Theoretical Physics at ETH Zurich [2], wrote paper titled ”Quantum Advantage in Cryptography” They discuss quantum cryptography's potential applications and limitations in cybersecurity. The paper explores the function of quantum cryptography within the broader framework of cybersecurity, as well as its potential uses and constraints.

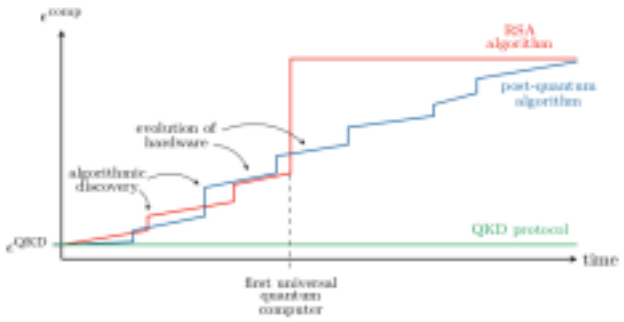

Fig. 1. Security of cryptographic protocols over time:image taken from paper

According to the authors, quantum cryptography enables the development of communication systems whose only physical rules and a few minimum requirements may ensure concealment presumption.

As depicted in the picture, it shows security of cryptography protocols over time for QKD,computational power,algorithmic discovery and evolution of hardware. It means when the first quantum starts RSA algorithm continues to exist through time with quantum computational efficiency. Then RSA is going to

be threatened from quantum leading to post quantum algorithms and quantum key distribution protocols.

And when we come to figure 2, the image shows what could be the possible threats of cryptography.Weather each one of the given safe or not starting from classical cryptography to no signaling cryptography.Parallel to hardware development, software development and developments in physical theories.

Accordingly, all are not safe for classical cryptography,only hardware development is safe in post quantum cryptography but the other two not. In quantum cryptography, two of them(hardware development and software development are safe) but development in physical theories is not safe. After all, for no signaling cryptography all are safe. No signaling is just the spatial separation of Alice and Bob to share keys with entanglement that means.

1) Strength:

- Its exploration of the different quantum-resistant cryptographic approaches that have been put forth, including hash-based, lattice-based, and code-based methods.

	Hardware developments	Software developments	Developments in physical theories
Classical cryptography	not safe	not safe	not safe
Post-quantum cryptography	safe	not safe	not safe
Quantum cryptography	safe	safe	not safe
Non-signaling cryptography	safe	safe	safe

Fig. 2. Possible threats for cryptography: image taken from paper

- It explains the current state of quantum computing and how it might one day be used to compromise encryption systems.
- It investigates initiatives being undertaken to create post quantum cryptography, which is impervious to assaults from quantum computers.

2) Weakness:

- Should show how quantum cryptography relates to the current status of quantum computing and cryptography,
- Does not provide enough (full) information to claim that the article is out-of-date or inadequate.
- It needs further exploration of the impact and advantage of quantum in cybersecurity.

B. Quantum Cryptography for the Future Internet and the Security Analysis

This paper explores the significance of quantum cryptography as a solution to the security challenges posed by the evolving landscape of the internet. It discusses the vulnerabilities of current encryption methods in the face of quantum computing advancements and introduces the concept of quantum key distribution (QKD) protocols. The paper emphasizes the unconditional security and eavesdropper detection properties of quantum cryptography, making it suitable for ensuring secure communication in the future Internet.

In the following Figure fig 3, if an eavesdropper monitors the quantum channel, for a bit of quantum information, he will choose the same measuring base with the sender with a 50 percent probability. Therefore, the eavesdropper will be detected at a 50 probability for a bit of quantum information. Note that, for the quantum information of n-bit is, the probability of the eavesdropper being detected is $1-(1/2)^n$ means 1/2 x 1/2 x 1/2=⅛. The more the number of transmission data the higher the probability of the eavesdropper being detected, no matter whether there is noise interference or not.The number of photons measured, whether noise free or not, eavesdropper is detected.

Figure 4 shows the eavesdropper being detected when he/she eavesdrops on the channel in different probability. In this picture, the purple line represents that the attacker monitors the channel in the possibility of 100 percent while the green line and the red line represent that the attacker monitors the channel in the possibility of 50 percent and 20 percent, respectively. From these three curves, we can observe that regardless of probability of the eavesdrop monitoring the

Results	Polarization	
	⊕	⊗
Bases		
↔	1	0: 50%; 1: 50%
↕	0	0: 50%; 1: 50%
↗	0: 50%; 1: 50%	0
↖	0: 50%; 1: 50%	1

Fig. 3. Measurement results

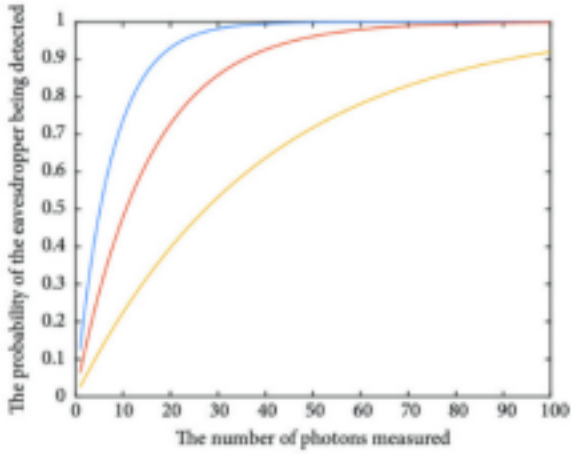

Fig. 4. The eavesdropper detects the channel with different probability.

channel, the probability of being detected is nearly 100 percent as the number of transmitted bits is rising.

1) Strength:

The paper does an excellent job of introducing and explaining the fundamental concepts of quantum information and communication. It provides a solid foundation for readers who may not be familiar with quantum mechanics, making the content accessible to a broader audience.

Comprehensive overview of various quantum crypto graphic protocols: The paper offers a comprehensive review of different quantum cryptographic protocols, such as Quantum Key Distribution (QKD), Quantum Oblivious Transfer (QOT), Quantum Authentication (QA), Quantum Bit Commitment (QBC), and Quantum Signature (QS) protocols.

This coverage provides a well-rounded understanding of the various ways in which quantum mechanics can enhance cryptographic security.

Through analysis of unconditional security and eavesdropper detection, this paper delves into the core strength of [1]. It explains how the properties of quantum information, such as the uncertainty principle and quantum no-cloning theory, ensure that any eavesdropping attempts are detectable. It also provided mathematical and conceptual explanations to support this claim.

2) Weakness:

Limited discussion on real-world applications and practical implementations: While the paper does an admirable job of explaining the theoretical concepts of quantum cryptography, it falls short in discussing real-world applications and practical implementation challenges. More examples or case studies illustrating how quantum cryptography can be applied in scenarios like the Internet of Things or secure communication systems would enhance the paper's relevance.

How can protocols address specific threats and vulnerabilities that emerge with the evolution of the Internet? clarifies connections can make the paper more impactful.

The paper occasionally jumps between concepts without a smooth transition, which can make it challenging for readers to follow the logical flow of the argument. Improved organization and clearer signposting would rather enhance readability.

C. Quantum Cryptography

Maneesh Yati [1], of deakin university published the minor thesis quantum leap, thesis Quantum Cryptography,in November 2020. This thesis paper examines how quantum cryptography impacts the existing cryptography techniques.Its processing power increment with a factor 2^nwhich handles large asymmetric keys while classical one n^2factor.

Processing fast where number of qubits 53 for google and 500 d-wave will achieve able quantum supremacy.Classical encryption strategies are unsafe as quantum computers can decode data present in classical keys easily and the public keys will no longer be safer.

Majority security breaches occurred due to unauthorized data access by technical advancement of intruders and automated attacks.That's why quantum cryptography is introduced to ensure secure communication between networks.Uncertainty principle and Quantum No-cloning makes this happen with its limitations such as zero decoherence and absolute zero temperature.

If use of quantum gadgets become a reality it opens a wide range of new attacks like side channel attacks although quantum technology uses millions of small particles present in light to transfer their encrypted keys and even it detects eavesdropping and can prevent hacking. Quantum keys are used instead of secret keys to transfer information. Quantum key distribution channel is used to transfer data securely even on an insecure network.Key distribution protocols utilize quantum mechanics to distribute session keys and check for eavesdroppers and verify the correctness of a session key.

When eavesdropper tries to measure qubit before message receiver, there is a very high chance that there will be a change in qubit state.If the information is accessed by an attacker or an intruder, distorted information will be received by receiver and it will take to break laws of quantum physics to access the information.

Classic key distribution approach has many challenges.But quantum key distribution addresses these problems.Key related quantum computing has many applications which makes it extremely powerful and useful.But poorly designed

key distribution protocols suffer from security problems.Hence,quantum key distribution protocol designing is the utmost priority in a communication system.

From the figure the aim of the QKD protocol is to identify the change in Qubit's state.

1) Strength:

- Simple and easy explanation to understand it with a real world scenario.
- Quantum key distribution protocol implementation methods are convincing graphically teller including Qskit demo code to show the low level(code level) im plementation.
- Well defined design of Qubits mathematically and logi cally illustrated easily like that of current logic gates.But

```
qc = QuantumCircuit(1,1)
# Alice prepares qubit in state |+>
qc.h(0)
qc.barrier()
qc.h(0)
qc.measure(0,0)

# Draw and simulate circuit
display(qc.draw())
sim = Aer.get_backend('qasm_simulator')
out = execute(qc, sim)
plot_histogram(out.result().get_counts())
```

Fig. 5. Protocol Overview:using Qiskit

```
qc = QuantumCircuit(1,1)
# Alice prepares qubit in state |+>
qc.h(0)
qc.measure(0, 0)
qc.barrier()
# Eve then passes this on to Bob
# who measures it in the X-basis
qc.h(0)
qc.measure(0,0)

# Draw and simulate circuit
display(qc.draw())
sim = Aer.get_backend('qasm_simulator')
out = execute(qc, sim)
plot_histogram(out.result().get_counts())
```

Fig. 6. Qiskit eavesdropper demo code

this gives more clue how logic gates are designed in circut level.

It explores quantum key application areas of the future adding the efficiency and security, it adds quantum bit sizes referring to IBM submit and D wave for cloud functions.

2) Weakness:

- It does not focus on specific quantum cryptography rather assesses a wide area of application and use.
- Discusses more about quantum computer applications in Artificial Intelligence, health, corona.
- Bench marked Quantum Leap and other researches to cover wide contents and pivoted it as a referencing it as a minor thesis.

If Alice sends a qubit to Bob, and an eavesdropper (Eve) tries to measure it before Bob does, there is a very high chances that there will be a change in qubit. Alice sends qubit to Bob which is measured in X axis. Alice sends qubit to Bob but eve intervened and tried to read it.

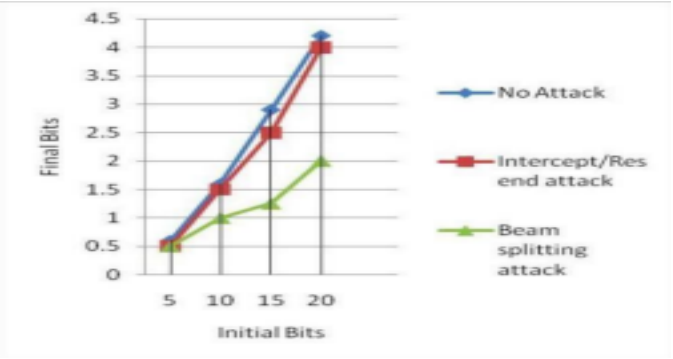

Fig. 7. Initial vs Final Bits Length

D. The Impact of Quantum Computing on Present Cryptog raphy

The paper titled "The Impact of Quantum Computing on Present Cryptography" by Vasileios Mavroeidis et al [4] ex plores the potential effects of quantum computing on current cryptographic methods.

It delves into the vulnerabilities that quantum computing poses to both symmetric and asymmetric cryptographic algorithms, discussing how methods like Shor's algorithm and Grover's algorithm can break encryption techniques that rely on large prime factorization and discrete logarithm problems.

The paper emphasizes the need for post quantum cryptographic solutions that can withstand the computational power of quantum computers. It covers quantum key distribution methods and mathematical-based approaches like lattice-based cryptography, multivariate-based cryptography, hash-based signatures, and code-based cryptography. While the paper is comprehensive in its coverage, it might lack detailed explanations of quantum concepts and could benefit from more recent developments in the rapidly evolving field of quantum computing.

1) Strength:

The paper comprehensively analyzes how quantum computing affects current cryptography, covering both symmetric and asymmetric methods

The paper effectively outlines vulnerabilities in existing cryptography due to quantum algorithms, particularly large prime factorization and discrete logarithm problems.

The paper's introduction of Shor's and Grover's algorithms adds technical depth to the discussion, enhancing readers' understanding of their impact on cryptography.

Cryptographic Algorithm	Type	Purpose	Impact From Quantum Computer
AES-256	Symmetric key	Encryption	Secure
SHA-256, SHA-3	–	Hash functions	Secure
RSA	Public key	Signatures, key establishment	No longer secure
ECDSA, ECDH (Elliptic Curve Cryptography)	Public key	Signatures, key exchange	No longer secure
DSA (Finite Field Cryptography)	Public key	Signatures, key exchange	No longer secure

Fig. 8. Encryption impact analysis

From here we can observe that AES-256 and SHA-256, SHA-3 are secure but RSA,ECDSA, ECDH (Elliptic Curve Cryptography) and DSA (Finite Field Cryptography) are no longer secure.

Crypto Scheme	Key Size	Effective Key Strength/Security Level (in bits)	
		Classical Computing	Quantum Computing
RSA-1024	1024	80	0
RSA-2048	2048	112	0
ECC-256	256	128	0
ECC-384	384	256	0
AES-128	**128**	**128**	**64**
AES-256	**256**	**256**	**128**

Fig. 9. Security levels in key length for most used cryptographic schems All public key algorithms used today are based on two mathematical problems, the aforementioned factorization of large numbers like RSA and the calculation of discrete logarithms like DSA since they have a similar mathematical structure ECC also breakable.

Advanced Encryption Standard (AES) is considered to be one of the cryptographic primitives that is resilient in quantum computations, but only when is used with key sizes of 192 or 256 bits.Key sizes of 192 and 256 for AES, T

The paper addresses the need for quantum-resistant solutions.

2) Weakness:

• should include more information on how quantum cryptography relates to the current status of quantum computing and cryptography.

Overall, the study gives an overview of quantum cryptography's current condition,advantages, possible uses, and drawbacks in cybersecurity..

III. Algorithms

A. Vulnerable to Quantum Algorithms

Shor's Algorithm in Asymmetric Cryptography is affected as it uses Large prime integer factorization and the discrete logarithm problem so it can be broken with Shor's algorithm rapidly even.

Grover's algorithm in Symmetric Cryptography crack Data Encryption Standard (DES), which relies its security on a 56-bit key. The authors remarked that the algorithm needs only 185 searches to find the key for database searching. Grover's algorithm can be utilized to find a collision in a hash function in square root steps of its original length. So, all under listed encryption schemes are affected.

• Shor's Algorithm in Asymmetric Cryptography • Grover's algorithm in Symmetric Cryptography • Asymmetric Encryption Schemes Affected

• Symmetric Encryption Schemes Affected

• Hash Functions Affected

IV. Post Quantum Problems

1) Quantum Key Distribution:BB84 protocol: exploits the polarization of light for creating random sequence of qubits (key) that are transmitted through a quantum channel Secure key sequence can be generated whenever the channel bit error rate is less than about 7 percent.BB84 exploits the polarization of light for creating random sequence of qubits (key) that are transmitted through a quantum channel. 2) Photon Number Splitting Attack: the disturbed channel or middle attack. In addition to noise in the quantum channel, the equipment is impractical to produce and detect single pho tons. Therefore, in practice, laser pulses are used. Producing multiple photons opens up a new attack known as Photon Number Splitting (PNS) attack. In PNS attack, an attacker (Eve) deterministically splits a photon off of the signal and stores it in a quantum memory which does not modify the polarisation of the photons. The remaining photons are allowed to pass and are transmitted to the receiver (Bob). Next, Bob measures the photons and the sender (Alice) has to reveal the encoding bases. Eve will then be able to measure all captured photons on a correct basis. Consequently, Eve will obtain information about the secret key from all signals containing more than one photon without being noticed. 3)Mathematical Problems: There are many alternative mathematical problems to those used in RSA, DH and ECDSA that have already been implemented as public key cryptography schemes discussed above in figure 8 and figure 9.

V. Solutions

A. Quantum Key Distribution:BB84 protocol Solutions 1. Quantum key distribution (QKD) exploits the polarization of light to create a random sequence of qubits (quantum bits), which are then transmitted through a quantum channel. This method can mitigate blinding attacks, in which an eavesdropper (Eve) tries to learn the key by shining a bright light on the quantum channel.

2. Photon number splitting (PNS) attack is a type of attack that Eve can use to try to learn the key in quantum key distribution (QKD). In this attack, Eve splits the photons in the quantum channel and measures them. This allows Eve to learn some information about the key, but it also leaves a signature that can be detected by the legitimate users (Alice and Bob).

Eavesdropper detection can be used to defend against PNS attacks. Alice and Bob can use decoy states to send a random number of photons to each other. If Eve is present, she will not be able to distinguish between the decoy states and the real states, and this will allow Alice and Bob to detect her presence.

The rate of the detection is important because it determines how likely it is that Eve will be caught. A higher detection rate means that Eve is less likely to be successful. B. Mathematical based Solutions:

Lattice-based cryptography is a form of public key cryptography that avoids the weaknesses of RSA. Rather than multiplying primes, lattice-based encryption schemes involve multiplying matrices. This makes them more resistant to attack by quantum computers. Multivariate-based cryptography is another form of public key cryptography that is resistant to attack by quantum computers. It uses polynomials to encrypt and decrypt messages. Hash-based signatures are a type of digital signature that uses a hash function to create a fingerprint of a message. The hash function is a mathematical algorithm that converts a message into a fixed-length string of characters. The signature is created by encrypting the hash of the message with the private key. The public key can then be used to verify the signature. Code-based cryptography is a type of cryptography that uses error-correcting codes to encrypt and decrypt messages. Error-correcting codes are used to detect and correct errors that occur when data is transmitted. Code-based cryptography is resistant to attack by quantum computers because it is based on problems that are believed to be difficult for quantum computers to solve. Symmetric encryption schemes, such as AES, are not as vulnerable to quantum attacks as asymmetric encryption schemes, such as RSA. However, they are still vulnerable to quantum brute force attacks, which can be performed by a quantum computer using Grover's algorithm.

Grover's algorithm is a quantum algorithm that can search an unstructured database much faster than any classical algorithm. This means that a quantum computer could use Grover's algorithm to break a symmetric encryption scheme with a 128- bit key in a time that is polynomial in the size of the key.

To make symmetric encryption schemes quantum-safe, it is necessary to increase the length of the keys. For example, the AES scheme with a 256-bit key is considered quantum safe because it would take a quantum computer a time that is exponential in the size of the key to break it.

The goal of post-quantum cryptography is to find algorithms that are difficult to break, even by quantum computers. This is a challenging task, as quantum computers are capable of solving many problems that are considered difficult for classical computers.

One approach to post-quantum cryptography is to use algorithms that are based on problems that are believed to be difficult for quantum computers. For example, lattice-based cryptography uses problems related to the shortest vector problem, which is believed to be difficult for quantum computers.

Another approach is to use algorithms that are based on problems that are difficult for both classical and quantum computers. For example, hash-based cryptography uses hash functions, which are mathematical functions that are difficult to invert.

Despite the difficulties involved in developing post-quantum cryptography, it has a crucial advantage over classical cryptography: it does not have to fear the development of a more powerful machine. This is because a universal quantum computer is already the worst-case scenario, at least within the theory of quantum mechanics.

The gradual improvement of hardware may make it necessary to adjust the length of the keys used in post-quantum algorithms from time to time. However, the development of a universal quantum computer will not make these algorithms immediately insecure.

VI. Discussion

Maneesh Yati[1] designed QKDP implementation methods in BB84:Protocol and eavesdropper detection.It uses channel disturbance and Eavesdropper scenario based implementation solve the problem using Qiskit which is a code based implementation of the quantum protocol.The main strength is scenario based simple approach with clear methods in QDP. But the main weakness is that it touches many areas and unnecessary details that it lacks specificity. Compared to paper D[3] in terms of specificity details, the D one is much more specific.But this paper is simple and clear in stating quantum cryptography illustrating with methods and scenario based approaches to reach the audience.

ianqi Zhou, Jian Shen, Xiong Li, Chen Wang and Jun Shen[4] simply described for a general problem nature to be understandable for the general audience specifically on the detection of eavesdropper probability.They made analysis of security issues that quantum brings in the near future.But high level abstraction without detail methodology only focusing the detection and analysis part.Compared to paper A[2], in simplicity and generalization it is somewhat similar but the former one is more wider and complex.But it is quite different from C[1] and D[3] following specific methodologies to check QKD or post quantum problem solutions.

vasileim, kamerv, mateusdz and josang[3] focused on algo rithms and implementations of post quantum techniques.Even though it does not well abstracted to readers(it lacks simplic ity) to understand what QC is and how it affects the existing and the post quantum problem nature.This paper is more targeted to technical individuals since it needs a mathematical understanding of algorithms.But still it indicated quantum safe(post quantum algorithms) that how to develop quantum resistant mechanisms in the field of cryptography.This paper can be a little similar to paper in C[1] but they follow different approaches for the methodology but this paper is a detail on algorithms and post quantum cryptography technicality.

Renato Renner and Ramona Wolf[2] described the general theory of quantum cryptography and its complexity.Strengths are listed but the main strength of the paper is that it theorizes

quantum cryptography in relation with quantum physics problem nature.But the main weakness relative to the other three is that it lacks specificity (narrowing its scope of coverage).Over all, compared to the other three, this paper abstracts overall quantum phenomena broadly.

VII. Conclusion

Quantum cryptography will disrupt existing technology both positively and negatively.The positive impact that it will bring is quantum cryptography will transform the existing cryptography encryption and communications schemes in to a new technology shift. In which the existing can be seen as classical(old) like that of classical physics.But doing this will negatively impact the current technology and systems, algorithms, encryption mechanisms, existing researches to be shifted to know quantum philosophy that needs an understanding of quantum physics, entanglement, and the devices to work with it.

Encryption algorithms, communication protocols and key distribution mechanisms of the current system will have no value.It will completely break security algorithms of existing logic, intrude easily into existing business critical information to take it away.

This paper's main intention was to systematically review quantum cryptography research papers on how it will impact the existing security schemes and know the problem domain to forward a research discourse on associated security challenges.

Based on this, we recommend to implement quantum resistant solutions or adapt the new technology are options left as gaps. Quantum cryptography will come with a convincing and promising security avoiding bottlenecks of current cryptography and security as assessed from the papers.

It does not mean quantum is un hackable as demonstrated in the paper, but it does mean it is both the theory of quantum physics and QKDP assures that the law of physics keeps its state no information is lost in between sender Alice and receiver Bob.

REFERENCES

[1] Maneesh Yati ”Quantum Cryptography”, Minor Thesis Quantum Leap, Deakin university, November 2020.

[2] Renato Renner and Ramona Wolf ”Quantum Advantage in

Cryptography

Theoretical Physics, ETH Zurich, 8093 Z ¨ urich, ¨ Switzerland, 11 Jan 2023.

[3] Vasileios Mavroeidis, Kamer Vishi, Mateusz D. Zych, Audun Jøsang ”The Impact of Quantum Computing on Present Cryptography”, University of Oslo, Norway, November 3, 2018.

[4] Tianqi Zhou, Jian Shen, Xiong Li, Chen Wang, Jun Shen ”Quantum Cryptography for the Future Internet and the Security Analysis”,Jiangsu Engineering Center of Network Monitoring, Nanjing University of Information Science and Technology, Nanjing, China, 21 Feb 2018.