Quantum-Enhanced Secure Communication via One-Time Pad and & Key Distribution

Thesis submitted in partial fulfilment

of the requirements of the degree of

Bachelor of Technology

in

Cloud Technology and Information Security

by

Princy Kshirsagar (2021-B-06102003)

Deekshant Wankhade (2021-B-21041999)

Rutuja Balwade (2022-B-08092002)

Under the Supervision of

Prof. Jayashree Mahale

May 2025

School of Engineering

Ajeenkya DY Patil University, Pune

Quantum-Enhanced Secure Communication via One-Time Pad and & Key Distribution

Princy kshirsagar
2021-B-06102003
BTech CTIS

Deekshant Wankhade
2021-B-21041999
BTech CTIS

Rutuja Balwade
2021-B-21041999
BTech CTIS

AJEENKYA
D Y PATIL UNIVERSITY
THE INNOVATION UNIVERSITY

School of Engineering

AJEENKYA D Y PATIL UNIVERSITY
THE INNOVATION UNIVERSITY
School of Engineering

26 May, 2025

CERTIFICATE

This is to certify that the dissertation **"Quantum-Enhanced Secure Communication via One-Time Pad and Key Distribution"** is a bonafide work of "**Princy Kshirsagar (2021-B- 06102003), Deekshant Wankhade (2021-B-21041999), Rutuja Balwade (2022-B-08092002)",** submitted to the School of Engineering, Ajeenkya D Y Patil University, Pune in partial fulfilment of the requirement for the award of the degree of **"Bachelor of Technology in Cloud Technology and Information Security"**.

Prof. Jayashree Mahale
Supervisor

Internal-Examiner/s

External Examiner

Dr. Prashant Kumbharkar
Dean-School of Engineering

AJEENKYA D Y PATIL UNIVERSITY
THE INNOVATION UNIVERSITY
School of Engineering

26 May, 2025

Supervisor's Certificate

This is to certify that the dissertation entitled **"Quantum-Enhanced Secure Communication via One-Time Pad and Key Distribution"** submitted by **Princy Kshirsagar (2021-B- 06102003), Deekshant Wankhade (2021-B-21041999), Rutuja Balwade (2022-B-08092002),** is a record of original work carried out by him/her under my supervision and guidance in partial fulfilment of the requirements of the degree of **Bachelor of Technology in Cloud Technology and Information Security** at **School of Engineering**, **Ajeenkya DY Patil University, Pune, Maharashtra-412105**. Neither this dissertation nor any part of it has been submitted earlier for any degree or diploma to any institute or university in India or abroad.

Prof. Jayashree Mahale
Supervisor

AJEENKYA D Y PATIL UNIVERSITY
THE INNOVATION UNIVERSITY
School of Engineering

Declaration of Originality

We*, *Princy Kshirsagar (2021-B- 06102003), Deekshant Wankhade (2021-B-21041999), Rutuja Balwade (2022-B-08092002), hereby declare that this dissertation entitled "***Quantum-Enhanced Secure Communication via One-Time Pad and Key Distribution"*** presents my original work carried out as a bachelor student of School of Engineering, Ajeenkya D Y Patil University, Pune, Maharashtra. To the best of my knowledge, this dissertation contains no material previously published or written by another person, nor any material presented by me for the award of any degree or diploma of Ajeenkya D Y Patil University, Pune or any other institution. Any contribution made to this research by others, with whom we have worked at Ajeenkya D Y Patil University, Pune or elsewhere, is explicitly acknowledged in the dissertation. Works of other authors cited in this dissertation have been duly acknowledged under the sections "Reference" or "Bibliography". we also declare that we have adhered to all principles of academic honesty and integrity and have not misrepresented or fabricated or falsified any idea/data/fact/source in my submission.

We are fully aware that in case of any non-compliance detected in future, the Academic Council of Ajeenkya D Y Patil University, Pune may withdraw the degree awarded to me on the basis of the present dissertation.

Date: 26 May 2025

Place: Lohegaon, Pune

Princy Kshirsagar

Deekshant Wankhade

Rutuja Balwade

Acknowledgement

On behalf of ourselves, we want to extend our sincere thanks to Prof. Jayashree Mahale Grant-in-Aid for to enlighten us through her profound suggestions and vigilant comments with the entire journey of this research. The guidance she has given us has been foundational in shaping our perspective and grounding us for good results. We are, in the deepest sense, very grateful to Dr. Prashant Kumbharkar- our de-an of this university for developing a warm and fertile academic soil which furnished us the requisite resources to do this work. A warm thanks to all of the participants in our survey for their time and willingness to answer the questions in good faith which this research could not have been possible without your contributions. We are extremely thankful to the reviewers and the editors who work in is publication process for their positive comments which improved us constructive suggestions for the quality of our entire work as well. We are thankful to the families and friends for their continuous support, patience, and emotional backing of ours throughout the way, entirely. Their faith in us helped us get through all phases of this journey.

Princy Kshirsagar

Deekshant Wankhade

Rutuja Balwade

Abstract

In the future, cloud services will remain a key focus of IT and digitalization.' The use of cloud services for data collection, processing, and storage is on the rise in various industries, including healthcare systems to smart devices. Additionally, agriculture technology can also be used to drive these applications. In these cloud-based environments, high availability and efficient operations without interruption are crucial, but the main objective is to maintain a high level of data security. The post-quantum world presents significant challenges for contemporary cryptographic techniques to achieve this. Quantum attacks are a common issue with classical encryption methods, particularly those that prioritize computational complexity.

The paper investigates the use of quantum-safe key exchange protocols to incorporate the theoretically unbreakable one-time pad (OTP). Our integration of Quantum Key Distribution (QKD) and post- quantum cryptographic techniques provides a robust foundation for secure communication in the quantum domain.

Index Terms - Automation, Cloud Audit, Cloud Computing, Security

Contents

Contents

List of Figures

List of Tables

List of Abbreviations

QKD -	QKD - Quantum Key Distribution
OTP -	One Time Pad
RSA -	Rivest-Shamir-Adleman (Cryptosystem)
ECC -	ECC - Elliptic Curve Cryptography
BB84 -	BB84 - Bennett and Brassard 1984 Protocol
PRNG -	PRNG - Pseudo-Random Number Generator
AWS -	Amazon Web Services
ANUQRNG -	Australian National University Quantum Random number generator
HMAC -	Hash-Based Message Authentication Code
MAC -	MAC - Message Authentication Code
DUHK -	DUHK - Don’t Use Hardcoded Keys
PKI -	PKI - Public Key Infrastructure
SSL -	SSL - Secure Sockets Layer
TLS -	TLS - Transport Layer Security
VPN	VPN - Virtual Private Network
FTPS -	FTPS - File Transfer Protocol Secure
SFTP -	SFTP - Secure File Transfer Protocol
QKD -	Quantum Key Distribution
OTP -	OTP - One-Time Pad
RSA	RSA - Rivest-Shamir-Adleman
ECC -	ECC - Elliptic Curve Cryptography
BB84 -	BB84 - Bennett and Brassard 1984 Protocol
PRNG -	Pseudo-Random Number Generator

CHAPTER 1

INTRODUCTION

1.1 QUANTUM COMPUTING AND THE FUTURE OF SECURE COMMUNICATION

The security of today cryptographic systems faces a very serious threat as quantum computing technology advances rapidly. Currently, conventional encryption methods like RSA and Elliptic Curve Cryptography (ECC) are built on the hardness of mathematical problems, namely factoring large numbers and solving discrete logarithms. Quantum algorithms such as Shor's can supposedly solve these problems much faster than classical computers. However, this will fundamentally break the cryptographic mechanisms built on these. Moreover, Grover's algorithm makes brute force symmetric encryption vulnerable, in essence making the security of such systems effectively double. The emergence of these vulnerabilities indicates the increasing emergence of cryptographic frameworks to protect against quantum-based attack.

All quantum computers work, fundamentally on principles different from classical computing as they are based on quantum mechanics. Classical bits (the most basic computer entities) can have only two values − either zero or one; however, quantum bit or qubit can be in a superposition form which means it simultaneously represents not just 0 and 1 but also both. This ability has enabled quantum machines to process and analyse large sets of system data with complex algorithms in a far more effective manner than classical computers ever could. Besides that, qubits can be entangled; thus, a relationship is created so that the state of one qubit appears to influence another qubit no matter how far apart they are. Novel quantum effects provide remarkable solutions to cryptographic problems such as encryption that is faster, and also provides stronger security against certain classes of attack — in particular those facilitated by quantum computers.

A promising post-quantum strategy for communication security combines one-time pad encryption with the well-known BB84 quantum key distribution protocol (QKD) for quantum-liked security.

The one-time pad, when used with a perfectly random key of the same length as the message and only the message itself, is provably unbreakable in theory. But its main drawback is regarding a secure way of sending that encryption key. That is exactly where BB84 comes in with a novel solution. BB84 utilizes known quantum mechanical properties (superposition and entanglement) to securely transmit cryptographic keys.

Every break in the quantum states being transmitted signals to both the sender and receiver, that an intruder is listening. Using the one-time pad's perfect secrecy together with BB84's secure key delivery, one can create a robust, scalable and secure communication framework against any quantum attack. Together, this double tracking ensures that when quantum computers powerful enough to break all traditional encryption methods are invented and built (one should note properly secured communications in the quantum system even then), those systems stacked with hybrids will keep it impossible. BB84 can detect a key interception, so we can guarantee confidentiality and integrity of exchanged information owing to semi classical signal properties.

Most importantly, as quantum computing capabilities improve, it becomes critical that we incorporate a much more resilient cryptographic model at scale in order to keep mission critical data safe for the long-term privacy and security of an equally changing digital domain.

1.2 CURRENT METHODOLOGIES EMPLOYED IN OUR PROJECT

1.2.1. QUANTUM MECHANICS AND THE POWER OF QUBITS

Quantum mechanics and the weird behavior of minuscule particles like atoms, electrons, and photons are the premises of quantum computing; it is a branch of physics that analyses properties of matter at smallest scales. Qubits are the quantum computing hardware instead of classical computers' bits qubits; they are different from the ordinary bits because they can be 0, 1 or both at the same time Whereas qubits have very peculiar properties that enable quantum machines to beat classical machines at certain tasks. Superposition and entanglement are the two most fundamental features of qubits. Simply put, a qubit is able to be many values all at once – both 0 and 1 at the same time. What that implies is that a quantum computer can do many calculations at the same

time, making quantum computers extremely powerful processors. For example, a classical system of 3 bits can represent one of eight possible combinations at any instant but there are three qubits in superposition, all eight combinations at the same time. Such parallelism is what allows quantum computers to solve specific difficult problems — such as factoring very large numbers — exponentially faster than classical computers. Entanglement is also a very useful quantum phenomenon that comes directly from quantum mechanics. Entanglement means that when qubits are entangled the state is non-separable, a change in one qubit causes an instantaneous change on the other regardless of how far apart they are. It makes shared and coordinated information to run so efficiently in a quantum computer. It improves processing speed and synchronism, through which quantum systems can manage some tasks more efficiently than classical computers.

These incredible capabilities allow quantum computers to tackle problems which would be virtually impossible or infeasible for classical computers. Shor's algorithm, an iconic quantum algorithm (factoring $N = n \cdot n$ quickly vs classical inexact technique a sufficient condition for cryptanalysis breaking RSA) for example. Grover's algorithm applies to un-ordered databases and

it searches through them much faster than normal algorithms, in the order of root N operations. These advances may be enough to plough a path in which quantum computing revolutionizes cryptography, optimization and data analysis and even simulation of science.

With qubits, there are also other advantages besides computational (quantum cryptography) to make communications secure. QKD stands for Quantum key distribution, which is a quantum protocol for secure exchange of encryption keys using qubits. With a key interception by an unauthorised party disturbing the quantum state of the qubits, which provides an immediate notification that a third party is trying to gain access. This renders eavesdropping completely inactive without revelation, the security level of data transmission is at a new peak.

Qubits purport to have enormous utility, although they are hard to work with technologically. They are very fragile and suffer from the ever present evil of decoherence, in which they are disrupted by practically anything in their vicinity. Every little bit of noise, heat, or a jostling by nearby other machinery which can lead qubits leave from their quantum state. However, quantum computers are usually run at almost absolute-zero temperatures to help moderating this and error-correction is working on stabilising the situation of instability as well as quantum noise. Today, these barriers

prevent IQFT (Indistinguishable qubits with quantum feedback) from scaling and being practical as a general-purpose tool. Over time, the future will be quantum computing without these limitations with robust and fault-tolerant qubits, scalable architecture. Key players like IBM, Google (among others) are pouring resources in quantum technologies and running experiments that include superconducting circuits, trapped ions. With these developments having legs, quantum computers will eventually move past the reach of classical systems to facilitate leaps in artificial intelligence, cybersecurity and pharmaceuticals among others. Finally, the qubit is the heart of of why quantum computing might one day explode. Quantum mechanics has sure opened to the most (though never maintaining their delicate quantum states, their ability for parallel computation and computing in a short time can change technology) In the coming years, we will hopefully see quantum computing born from more and better research & innovation and revolutionary changes in industry that redefine our understanding of computer capabilities.

1.2.2. QUANTUM MECHANICS AND THE POWER OF QUBITS

Quantum mechanics-based quantum-safe communication systems are used to protect data by researchers against the security threats from quantum computers. One of the most efficient portfolio combinations is in the field where BB84 quantum key distribution (QKD) protocol overlapped with one-time pad (OTP) cryptographic method. Put together, they form a communication system theoretically immune to classical and quantum cyberattacks.

A. The One-Time Pad: A Cipher of Absolute Security

The one-time pad is a cryptographic technique renowned for offering perfect secrecy when its strict criteria are followed. It operates based on these key principles:

1. **Complete Randomness:** The encryption key must be truly random, free from any patterns or predictability.
2. **Key Length:** The key must be equal to or longer than the message it encrypts.
3. **Single Use:** Each key is used only once and then discarded

If used properly, one-time pad encrypts ciphertexts almost impossible to decrypt without the key being plaintext. The encryption is usually a very simple bitwise XOR of the plaintext and the random key, producing data which is indistinguishable from random.

The biggest issue with the one-time pad is distributing the encryption key between communicating parties in a secure manner. Physical delivery or even digital transfers raise security red flags. This is where BB84 protocol becomes reversible and a quantum-based method for secure key distribution.

B. The BB84 Protocol: Quantum-Assured Key Distribution

Introduced in 1984 by Charles Bennett and Gilles Brassard, the BB84 protocol was the first quantum key distribution protocol to be operational. This protocol leverages two basic principles from quantum physics: photons have unique properties that allow them to transmit cryptographic keys over a quantum channel. It works like this:

1. The sender, usually named Alice sending random bits onto single photons by choosing one polarisation basis out of two.
2. The Receiver Bob checks the bases of received photons randomly.
3. Alice and Bob do a pub comparison on which bases they used, publicly with each other but not the bit themselves after the transmission.

If the eavesdropper in a nutshell, frequently denominated Eve tries to spy or measure photons—she will disturb these quantum states in order to cause errors in the key process. It permits Alice and Bob to know whether there was an eavesdropping on their channel. If the error rate is not above threshold, they can extract a common shared secret key without any further use and keep on doing this. One of the things that make BB84 so strong is its dependence on very basic quantum phenomena such as superposition and the uncertainty principle. These principles ensure that even any eavesdropping would introduce observable perturbations to the key and hence making undetected surveillance impossible.

C. The Combined Strength of BB84 and the One-Time Pad

When paired, BB84 and the one-time pad form a formidable, quantum-resistant communication system with several crucial advantages:

1. **Perfect Encryption:** The one-time pad provides absolute secrecy when paired with a truly random, one-time-use key.

2. **Quantum-Safe Key Distribution:** BB84 uses quantum mechanical principles to securely distribute the encryption key while detecting any interception attempts.

3. **Long-Term Security:** As quantum computing technology evolves, this combination ensures future-proof, secure communications by mitigating both classical and quantum threats.

In essence, the integration of the BB84 protocol with the one-time pad offers a highly secure, resilient framework for communication in the quantum computing era. This combined approach not only overcomes the limitations of conventional encryption systems but also addresses the unique challenges posed by powerful quantum machines, safeguarding sensitive information well into the future.

1.3 OBJECTIVES OF THE PROJECT

The main goal of the project is to tackle the urgent issue of breaking current cryptographic systems by the emerging quantum computing [as fast] as possible in comparison to established systems. This project is about the weaknesses in classical encryption with classical algorithms e.g RSA & ECC when shaken under quantum algorithms Shor's & Grover's algorithms. It explains basic quantum ideas such as superpositions and entanglement, and why they are powerful tools which enable Quantum Computers to sub crack classical encryption methods. Counter to this, the project suggests a quantum-safe (from both classical and quantum attacks) secure communication for the quantum era based on BB84 quantum key distribution (QKD) protocol and one-time pad encryption. The aim of this combined strategy is to provide a future-looking, post-quantum secure solution which withstands classical and quantum invasive attacks on information secrecy/integrity.

1.4 SCOPE OF THE PROJECT

The project is consequently focused on the development and implementation of a scalable, post-quantum future-proof communication infrastructure able to cope with threats coming by the new quantum computing. It is followed by a comprehensive study of quantum-safe cryptographic techniques, specifically how BB84 quantum key distribution protocol and one- time pad encryption can be implemented. Based on the fundamental postulates of quantum mechanics (superposition, entanglement), the project aims the forge a secure

Tolerance high security weakest link in the chain: communication system able to withstand current and upcoming cyber threats Established as well is the difficulty of secure key distribution; what will be problems found, and then solve them with some novel efficient pattern Ultimately, this should lead to an implementable and persistent solution that can secure sensitive data in a world that is quickly going to be flooded by quantum technologies.

1.5 IMPORTANCE OF THE PROJECT

The emergence of quantum computing from the research lab into functional real-world applications, means that the demand for strong, future-proof cryptographic capabilities is seriously urgent. Conventional cryptographic systems, e.g., RSA, ECC and even many symmetric algorithms currently applied to protect financial transactions, confidential communications, national infrastructures are heading towards oblivion as they succumb to quantum algorithms that can break them within practical time scales.

This project is fundamental in seeing how emerging security problems could be identified and solving by introducing a classical and quantum hybrid system of BB84 quantum key distribution protocol to the one-time pad encryption decoding. Using quantum phenomena such as superposition and the no-cloning theorem, BB84 enables strong security for key exchange and a one-time pad with un-broken truly random keys can achieve perfect secrecy indeed, something which no classical encryption scheme can do.

While the work is of highly theoretical nature, this paper provides a realistic roadmap for organizations and governments to secure their most sensitive data against current cyber threats as well as representative quantum opponents. In addition, it provides a strategic basis for embedding quantum-resistant facilities in existing communication infrastructures and thus fostering the future quantum-safe transition. In the end this research better equips the entire cyber security landscape with defences for asymmetric cryptosystems years before they are rendered obsolete.

CHAPTER 2

LITERATURE REVIEW

In this section, we analyse spectrum of the tools that researchers as well as cybersecurity professionals use to maintain the security of their cloud operates in general with a detailed look on Automated Audit tools. Review Here we analyze the architecture, implementation steps and inherent pros/cons of those tools to get a precise understanding of how well these solutions work in different scenarios. This is due to provide a balanced view on how these technology play against vulnerabilities in order to help secure cloud infrastructure.

2.1 QUANTUM COMPUTING THREATS

Quantum computing technology is rapidly evolving and evolving rapidly, which raises large questions to the current digital security system. Quantum computers, in contrast to classical computers that operate on binary (on and off) states, use quantum bits (qubits) which can be in superposition states and accomplish complex calculations far faster than classical systems. This computational capability is a direct threat to common cryptographic platforms such as RSA and Elliptic Curve Cryptography (ECC), which within many (online banking, secure email services, digital signatures/blockchain apps/public key infrastructures) are broadly used.

Quantum algorithms in particular, such as Shor's algorithm for integer factorisation and Grover's search algorithm for unstructured databases, have shown the ability to subvert classical cryptography protocols and make secure data protection methods void. The collapse of these systems could result in disastrous results such as the breach of national security, commercial espionage or massive data surveillance on personal information.

Consequently, an international race has intensified to find quantum-resistant cryptographic algorithms urgently. Next generation algorithms are expected to withstand attacks from quantum computers but not necessarily from classical computers as well. In the case of a rapid advancement

in these areas, sharing of knowledge, resources and best practices between international communities is essential to foster the development of dependable digital infrastructure through collaborative efforts. It is also called an international efforts for governments and private sector to get involved with cybersecurity research, especially in the quantum resilient solutions field.

Quantum-inspired education campaigns for the public, and advanced digital security solutions in tandem, are critical in preparing personal and organizational data storage for the coming quantum computing age.

2.2 AWS BRAKET

Amazon AWS (Amazon Web Services) Quantum Computing: AWS Braket is a quantum compute service in the cloud, which allows researchers and developers to apply quantum hardware and simulators from premier providers: D-Wave, IonQ, Rigetti..., etc. As service, this allow you to try quantum algorithms and experiment with hybridization of quantum-classical chances in order to overcome hard computational problems.

One important difference of AWS Braket is that is hybrid algorithms support where it allows to run quantum heterogeneity and classical computing resources. It works best for optimization, cryptography, machine learning problems, and material science which go well beyond the abilities or the capabilities offering of traditional systems. Amazon Braket from AWS also provides a complete development environment to run quantum research, integration with AWS services like Amazon S3 and Amazon SageMaker creates the complete toolbox. AWS Braket simplifies quantum programming with a software development kits (SDKs) and a lower-level console interface powered by AWS. So, developers can simply create, simulate and execute quantum programs on different backends with a rich set of the larger AWS ecosystem to store and analyse results. In the near term, as quantum-classical hybrid systems become increasingly necessary to solve problems that classical computers cannot fully solve we need such services (AWS Braket) which prepare the developer for a near term future.

2.3 ONE-TIME PAD (OTP)

The one-time pad (OTP) remains one of the most secure encryption techniques known, providing theoretically unbreakable secrecy when correctly implemented. Initially introduced by Gilbert Vernam in the early 20th century, the OTP encrypts plaintext by combining it with a random key of equal length through a simple bitwise XOR operation.

The security of OTP encryption rests on three core principles:

1. True randomness of the encryption key.
2. Key length equal to the message length.
3. Single-use of each key.

Should any of these conditions be violated, security of encryption is broken. Opportunities to increase OTP with quantum can be seen in quantum key distribution (QKD) protocols, the coming of the quantum era

e.g., BB84. Use of QKD, which leverages quantum effects (e.g. quantum phenomena allows to distribute random seed encryption keys in a secure way between the communicating parties, safeguard them and make them impossible to steal If you follow the OTP process as an example, it means do some number conversion from plaintext, perform modular arithmetic with a randomized key on those numerical values, pass resulting ciphertext, and then reverse this procedure to decrypt it. In practice, OTP in conjunction with QKD removes the biggest problem of key distribution while still giving perfect secrecy even in the face of quantum computing adversaries.

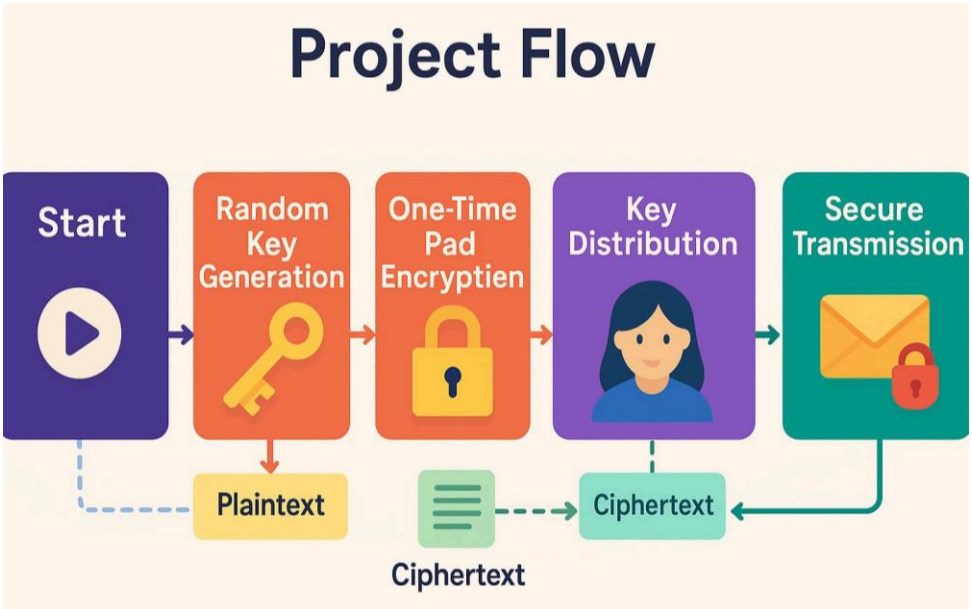


Fig 2.1 Project Flow

2.4 QUANTUM NOISE

In this perspective, quantum noise in quantum world arises from inherent probabilistic nature of quantum mechanics itself and crucially is an ideal source of verifiable randomness necessary in cryptographic applications. Quantum random number generators (QRNGs), on the other hand do

not work with pseudo-random number generators (like classical systems) as their outcomes cannot be predicted without actually measuring them because they use true randomness such as quantum phenomena like photon polarization and quantum tunneling.

The random sequences are the backbone of secure one-time pad encryption, each bit of plaintext XORed with an equally random bit coming from the key. The ciphertext looks statistically like random noise, and anyone without the appropriate key cannot decrypt. The difficulty however is to ensure that these OTP keys are distributed securely. Quantum key distribution (QKD) protocols that fix this by providing — via the use of quantum mechanics to detect and deter eavesdropping during the exchange process — a way of authenticating shared keys. Every attempt at interception produces a disturbance of the quantum states of transmitted particles, giving the communicating parties the ability to detect any such intrusion. Researchers hope to create secure communication channels that can survive both classical and quantum computational attacks by linking absolute security of OTP, random quantum noise and that guaranteed safety offered by QKD.

2.5 QUANTUM RANDOM NUMBER GENERATORS (QRNG) AND THEIR ROLE IN CRYPTOGRAPHY

How crucial randomness is to cryptography There are very few topics in cryptographic engineering that are as foundational as randomness. Secure cryptographic keys, nonces, initialization vectors and many other components on the cryptographic landscape all build on top of this foundation for randomness. Although traditional pseudo-random number generators (PRNGs), while adequate for most classical applications are in the most fundamental sense deterministic. From a theoretical standpoint, the internal state of a PRNG dictates all that comes after. Quantum computing might point to even more severe cracks in the original PRNGs and their encryption schemes —something that could theoretically be solved by powerful algorithms.

A new breed of revolutionary Quantum Random Number Generators (QRNGs), based on the unavoidable indiscernibility of quantum mechanics. The decay of radioactive elements, the behavior of photons at beam splitters or electron spin states are all fundamentally indeterminate processes. These happenings serve not only to make it hard, but physically impossible to compute the answers. For example, the Australian National University Quantum Random Number Generator (ANU QRNG) takes quantum fluctuations in vacuum light to generate truly random numbers.

In the same way, other commercial vendors such as ID Quantique or QuintessenceLabs develops mechanisms that capture quantum processes to yield randomness, this randomness is delivered to industries like finance, telecommunications and defense: Recent work also details the use of QRNGs in blockchain technologies, where randomness is necessary for consensus algorithms and smart contract execution into unpredictability. The further integration of QRNGs in Internet of

Things (IoT) platforms will make them have higher computational security level at the hardware level, extinguishing the potential generation of a new form of quantum enabled cyber-attacks.

QRNGs have been proven by competitive statistical testing such as the NIST randomness test suites, Diehard suite and TestU01 framework. This provides the guarantee that the sequences are random in different natures, uniform distribution, lack of predication, and uncorrelated as demanded by cryptography.

With the imminent arrival of quantum computers expected to make available within a decade or so, it has become long since unacceptable to use QRNGs without an emergency. They are the next step in secure random number generation and provide physically instantiated entropy sources which cannot be attacked by classical or quantum methods.

2.6 INTEGRATION OF QUANTUM KEY DISTRIBUTION (QKD) WITH CLASSICAL ENCRYPTION METHODS

Well-known QKD is considered a member, of course, of the first successful application of simple quantum mechanics in information security. In contrast to classical key exchange, * not based on any computational hardness assumptions* but rather the QKD uses as a substrate-the laws of physics and alone, no-cloning theorem and measurement-induced disturbance.

BB84, proposed by Charles Bennett and Gilles Brassard in 1984 is still considered and implemented as the prototype QKD protocols among these pioneering QKD protocols. Qubits are sent between two parties (Alice and commonly Bob) who are communicating over BB84 using difference basis. Detecting any eavesdropping (by Eve) causes disturbance to the quantum states, informing the honest parties of monogenous tailgating.

QKD is not a communication solution on its own, however; QKD must be coupled with classical crypto methods in order to realize an end-to-end secure communication. A feasible solution could be to employ QKD to make secure the symmetric keys, which in turn are used in very fast & powerful classical algorithms such Advanced Encryption Standard (AES) to encrypt bulk data. The hybrid model harnesses the power of our quantum and classical systems: unconditionally secure quantum key distribution, but fast data encryption.

Real world deployments have already proven this approach to work

- QUESS, the China Quantum Experiments at Space Scale (QUESS) mission: successful satellite-based QKD with combining ground-level classical network

- Quantum communication through metropolitan area network (QKD-MAN): Swiss Quantum Network, projects SECOQC (Austria) ensures that secured government / corporate communications can be integrated in QKD.

And despite these successes there are hurdles. QKD systems are not scalable, they need to be developed on fibre or realized in satellite links. Solutions to such limitations are in development

2.7 CHALLENGES IN IMPLEMENTING QUANTUM-SAFE CRYPTOGRAPHY

- The many technical, logistical and hence economic challenges therefore make the realization of quantum cryptographic techniques in practice all but perfect, although this last principle of information theory allows absolutely secure communication.

- Hardware limitations: Quantum cryptographic systems typically demand ultra-sensitivity detectors (avalanche photodiodes) stable single-photon sources and fibres of low loss These are both expensive and delicate— requiring energetic environments like ultralow-temperature chambers or vibration isolators. Affordable, reliable hardware solutions are not available to scale it.

- Proximity limitation: Rapid photon loss over long optical fibre cables is the insurmountable bottleneck. For instance, linear telecom fibres contribute about 0.2 dB loss per km from startle so after 100 km most of the photons are lost. Satellite QKD solves the long-distance key distribution, pretty well but in case of the reverse, one will need quantum repeater devices to mesh together quantum network across land which are in proof-of-principle stage of realisation these have stringent technological challenges i.e., keeping entanglement alive over long distances.

- Compatibility with Classical Infrastructure: Hacking together new quantum communication technologies into old classical infrastructure is difficult. Many differences in classical networks are designed around data redundancy, error-correction and trust models that do not apply within quantum system. The new quantum communication principles call for rethinking middleware, protocols even governance models.

- Economic and Regulatory Barriers: Quantum-safe technologies are presently expensive and only affordable to the national representatives, large corporations and research institutions up to now. Furthermore, regulatory regimes have not standardised or legislated the quantum-safe methods. If nobody gets incanted or try to regulate the things so, User Awareness and Education: As well a large cybersecurity community was not much aware of quantum technologies.

- These quantum literacy training programs will need to be accessible, scalable and part of a broader initiative to provide quantum readiness education globally to ensure an educated workforce is ready for the adopting of quantum-safe systems. Mitigating those challenges will require the combined effort of academia, industry and governments to scale and develop the ecosystem for scaling quantum technologies.

2.8 FUTURE DIRECTIONS IN QUANTUM-SAFE COMMUNICATION RESEARCH

Future of quantum-safe communication research will be characterized by the interaction of technological evolution, interdisciplinary synergy and proactive policy implementation.

- Quantum internet projects — Many of the last generation's leading research institutions and government labs are working to realize a quantum internet that harnesses the power of entanglement across cities, between continents and towards a global quantum internet. This trend is reflected by bodies such as the Quantum Internet Alliance (QIA) in Europe, and DARPA Quantum Network Challenge in the US The first-generation quantum internet will ensure ultra secure communication, quantum distributed computing and new ways to measure.

- Regulatory Post-Quantum Cryptography Algorithms: Instead of keeping it at the hardware level as an effort made by QS security researchers, NIST and other similar organizations are globally fledged global initiatives to regulate which post-quantum cryptographic (PQC) algorithms will be selected.

- These algorithms are specifically designed to be attack resistant from classical and quantum computers, and are introduced into their crucial components without the use of quantum technology. After which, NIST hope to unveil its first post-quantum cryptography round in the near future which will announce the start of a new era of quantum-hybrid cryptographic solutions.

- Hybrid Quantum-Classical Architectures: Understanding that quantum-controlled deployments will be spread out over some time researchers are furthering exploration on composite architectures whereby a mix of both quantum and classical systems support each other.

- Those systems could employ classical encryption for the standard messages and switch, for especially high value or sensitive communications, go over quantum channels to leverage both performance and security.

- Artificial Intelligence (AI) and Machine Learning (ML) in Quantum Cryptography: from the other direction we also witness growing cross-fertilization between AI/ML with quantum communication research.

- AI could be used to tune quantum key distribution parameters, to predict the fault of a system and even automate complex calibration tasks in quantum devices and thereby contribute to increase the maturity and reliability of quantum-safe systems.

- Decentralized Quantum Networks: New envisaged designs envision Decentralized quantum network; similar to blockchain; approaches Quantum Networks. Distributed ledger technologies could handle the entanglement resources and transaction confirmations as opposed to having everything managed by a centralized authority for quantum keys allowing for transparent, trust less quantum communication to become democratized.

- Impact on Society and Ethics: Lastly, the societal implications answered by quantum communication technologies as more and more matured. As quantum communication resources become available, there will be more pressing ethical enquiries about access and equity to surveillance and control of this information. Addressing these issues earlier than quantum future comes will be key to guaranteeing quantum security and access to everyone holistically

Table 1: Future Directions in Quantum-Safe Communication Research

Topic	**Description**
Quantum Internet Initiatives	Global projects (QIA, DARPA) aiming for ultra-secure, entanglement-based networks.
Standardization of PQC Algorithms	NIST is leading efforts to create quantum-resistant cryptographic standards.
Hybrid Quantum-Classical Architectures	Combining classical and quantum systems for optimized secure communication.
AI in Quantum Cryptography	Using AI/ML to enhance QKD system optimization, calibration, and predictive maintenance.
Decentralized Quantum Networks	Applying blockchain-inspired models for trustless, decentralized quantum communications.

CHAPTER 3

METHODOLOGY

3.1 EXISTING SYSTEMS

- Most of the cryptographic systems are based on pseudo-random number generators (PRNGs), suppose to produce the keys and other cryptographic parameters. PRNGs although not true random and deterministic are built to be close enough for the randomness requirement in practice. As such, pseudo-random key gen is a common technique to use when systems must support encryption. Such systems might be symmetric encryption e.g. AES, public key infrastructure (PKI) like RSA and VPN Protocols (IPsec, SSL / TLS) Wireless security (e.g. WPA2 standard) or disk encryption (e.g. BitLocker) also use PRNG.

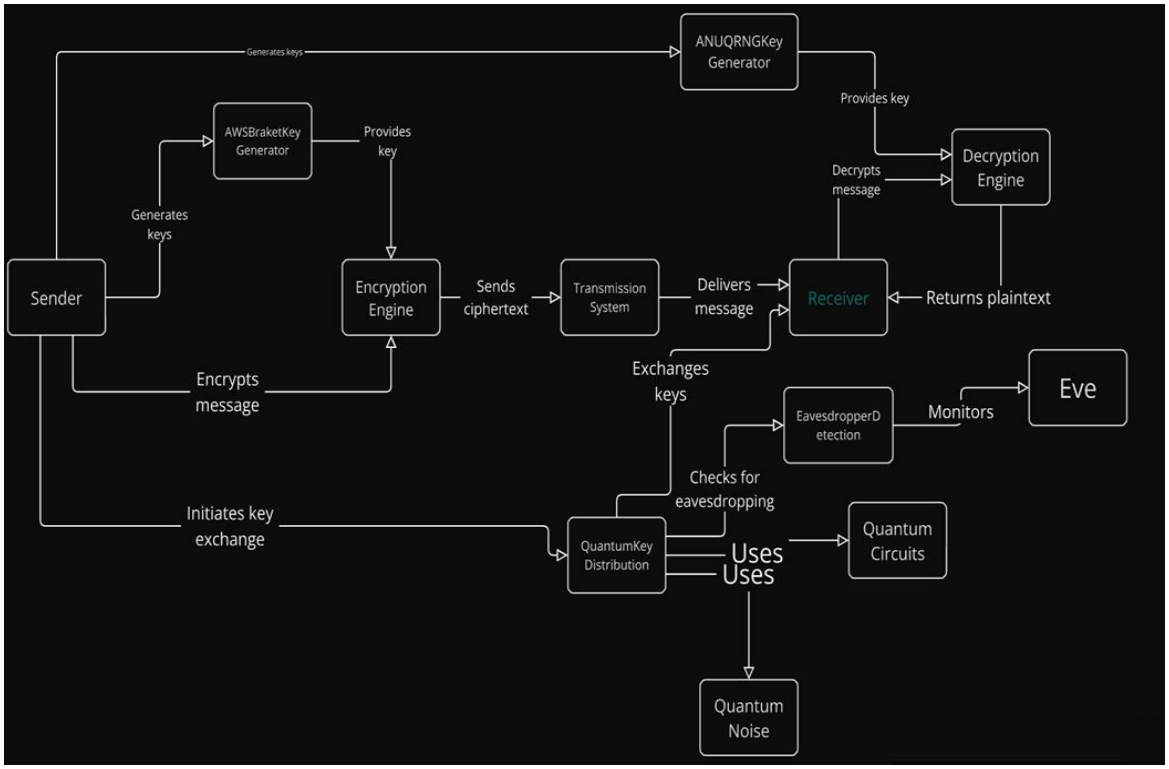


Fig 3.1 Architecture of Key generator

- Also, in secure messaging protocols such as Signal, two-factor authentication (TOTP) and other cloud security services (AWS KMS) or blockchain wallet key generation…PRNGs

are fundamental for the secure development of software, code signing takes secure software development practices into consideration as well. PRNGs are essential in all of the above applications for producing keys that guarantee confidentiality, data integrity verifiability of communication.

3.2 SECURITY FLAWS

- One of the TODOs in this project is using quantum key distribution (QKD) quantumistically increases the chance of a breach. Quantum key distribution (QKD) protocol is a highly secure way to key exchange but in practice, there might be some weaknesses. A simple example is that if quantum channel is not fully secure the imperfection of transmission media or measurement devices may help attacker in key deduces. Moreover, side-channel attacks like timing or power analysis could maybe flaw a QKD system in secure way.

- potential concern in quantum cryptography security quantum-resistant crypto theory is the security of long-lived quantum cryptosystems The algorithms are, after allnt yet all that long-lived and quantum-resistant cryptographic, although heavily designed against quantum attacks, the long-term security of these algorithms is under some doubt. According to the progress on quantum computing, it is likely that new attacks could be found and applied to these algorithms. So this quantum-resistant cryptography should be constantly audited and evaluated for security which means we must have security replacement plan to update the algorithms.

3.2.1 DUHK ATTACK

- This is the recently discovered DUHK (Don't Use Hard-coded Keys) attack, which takes advantage of an input feeding RNG for the X9.31 random number generator (RNG) implementation. When devices initialize an RNG with a seed key that is hard-coded into the device, a certain security vulnerability occurs. Attackers are able to obtain this hardcoded key by digging through the device firmware. Armed with this information they can predict the output of the RNG and eventually

- work out the encryption keys being used to protect network communications for example VPN connections and web sessions. It was a good reminder to always use cryptographically secure random number generators and not supply your own hardcoded keys to devices running vulnerable code.

3.2.2 JAPANESE PURPLE CIPHER MACHINE

- Japan used a cipher machine for its diplomatic comms during World War II. Despite the machine design weaknesses and weak key values used by Americans, they succeed in decoding the Japanese messages thanks to the cryptanalysis of this code. The cryptanalysis proved successful, and had a large effect on the war as it illuminated several errors within the cryptographic community to prioritize cryptographic practice and to know what can happen with poor cryptographic systems.

3.3 PROPOSED EXPERIMENTAL FRAMEWORK

We will present a completely different framework, which is composed of three parts: random key generation via AWS Braket, one time pad with ANUQRNG third party random number generator as true random number generation for using this process to create key encryption and BB84 key distribution protocol that we will be using later on. The framework merging quantum computing to classical cryptography to provide an improved shield for the result: a strong quantum platform for the generation of indistinguishable keys, OTP to provide unbreakable encryption via perfect secrecy and hence uncrackable hide active, BB84 for secure key exchange and detecting eavesdropping pull requests using weirdness of quantum principles as the basis for but don't alter content We present a new framework that intertwines quantum computation with classical cryptographic tools. The Architecture has 3 blocks:

1. AWS Braket for Random Key Generation: We take benefit of the power of quantum computing which can generate truly random keys by using AWS Braket.
2. This guarantees that random, unbiased keys are derived hence necessary for the security of cryptography.
3. OTP Encryption of ANUQRNG: We use the one-time pad encryption method, a theoretically unbreakable encryption method for safeguarding secret data.

We also leverage the ANUQRNG as third-party source of true random numbers to be used for OTP generation on the encryption keys further boosting the security. BB84 Quantum Key Distribution: We use BB84 to enable bit-level Secure OT keys between the sender and receiver The BB84 protocol enables the detection of any eavesdropping attempt on quantum states by making use of the quantum nature of photons allowing us to keep the shared key confidential. This comprehensive framework addresses cryptographic communications with a high degree of strength and protection through the marriage of quantum computing power with classical cryptographic methods.

3.3.1 RANDOM NUMBER GENERATION

- Quantum computing platform of Amazon Web Services (AWS) called Braket is a quantum computer powered by An anises system With Auto multiple quantum hardware and simulators it's the place where quantum researches can try algorithms. AWS Bracket's quantum noise | an absolutely key feature is that for the random numbers

- Randomness is an inherent part of quantum mechanics Measurement. Quantum noise in fact can be used for producing un-biased random bits (i.e., numerals for cryptographic purposes); While classical pseudo-random number generators only yield pseudo-random numbers because they are created based on deterministic algorithms, quantum noise-based devises provide a fundamentally different and much more secure solution.

- AWS Braket generates unique, unpredictable and unbiased random keys with the help of quantum noise This random key can then be fed in to several cryptographic protocols like in case of one-time pad encryption, makes the security even better.

3.3.2 GENERATING QUANTUM CIRCUITS WITH A HARDWARE CIRCUIT

- Amazon Braket lets us create and run quantum circuits over actual quantum hardware. So we can build multiple circuits, with each can qubits in different fashion. One wonderful aspect is to produce quantum states that are initially non-existing or very vague. If we smartly build these

- circuits, we can effectively bolster these states and convert them into stronger, more powerful quantum resources as a result. The possibility of manipulating and inflating quantum states is yielding quantum computer applications. AWS Bracket enables researchers to program and run quantum circuits on different kinds of quantum hardware (with and without qubits) and simulators. These features enable forming circuits which do something particular on qubits and hence retrieve certain quantum states.

- The other cool example is to build two circuits that produce a weak or very blurry quantum state. They aim to then use quantum operations in service of strengthening these states, and turning them into something more resilient and serviceable quantum.

- This principle so often referred to as quantum state amplification and quantum error correction is a cornerstone of quantum computing; it drives our ability to construct quantum algorithms which get more powerful (i.e. accurate) and reliable.

3.3.3 DESIGNING TWO QUANTUM CIRCUITS

Circuit 1: Initializing Superposition

- Hadamard Gates: We get a superposition state on each qubit by attacking Hadamard gates. Hence, each qubit is in a superposition of $|0\rangle$ and $|1\rangle$ states, with probability amplitudes equal for all.
- Weak State: although this state is a key block in quantum computation, due to lack of strong entanglement/correlation among the qubits can be called a "weaker" form. So, every qubit behaves as being completely isolated and works alone.

Circuit 2: Introducing Entanglement and Correlation

- CNOT Gates – CNOT gates are needed in the circuit to entangle qubits. applying CNOT gates to pairs of qubits, we make entangled states where qubits of state correlate with one another, so that one qubit state is connected admits with the other.

- Phase Gates: introduce phase shift on individual qubits, changing the complex amplitudes of the quantum state This can be used to arduous precise quantum state and build more sophisticated interference patterns.

- Amplification Process: The overall goal in quantum circuit making is to amplify that "weak" initial superposition state into a stronger more useful quantum state. This can be done with a number of different approaches:

- Quantum Error Correction: We used to encode information in redundant manner across numerous qubits but the signal gets amplified.

- Quantum Algorithms: That are Shor's algorithm for integer factorization and Grover's search algorithm are used to exploit quantum parallelism in solving certain types of problems faster than classical algorithms.

- Quantum State Whisky – using certain quantum operations you can improve a “coarse-grained” quantum state (that is, one with a lot of noise and decoherence) by increasing its coherence.

- Employing carefully engineered quantum circuits, followed by the right operation essentially converts an indistinct initial state into very strong quantum state that might address hard problems to solve and produce breakthroughs in terms of frontier fields.

3.3.4 STRENGTHENING THE WEAK STRING THROUGH THE APPLICATION OF A TOEPLITZ MATRIX

- By using a Toeplitz matrix on the initial weak qubit string as a post-processing step, the quality of the quantum state that is generated may be improved. A Toeplitz matrix is just a special matrix where each descending diagonal, moving to the right, has equal values. This is a special structure, the mathematical operations on quantum information and quantum amplification.

- When operating on qubits of weak quantum string, the Toeplitz matrix can "lightly" diffuse randomness among embedded into qubits. Randomness extraction then yields an even stronger quantum state with better cryptographic properties This state is more appropriate for applications like key generation and others.
- Besides randomness extraction, Toeplitz matrices may also be used as part of quantum error correction. With the help of Toeplitz matrices, we can transfer quantum information in a larger, redundant state in order to protect this information from noise and errors that happen throughout the quantum operations.

- Ensuring the quantum state is not compromised and making the quantum communication protocols more accurate and robust.

- AWS Braket, while it probably has the most of value for quantum computing development (EXPERIMENT!), generating mass huge random numbers can be pretty expensive to compute. We therefore look at using ANUQRNG, a third-party source of true random numbers to compensate for this. Thereby, we are able to obtain random numbers very efficiently with very little expense on cost quantum computations thanks to ANUQRNG which can then serve as keys for encryption and further protect our frameworküstücük.

3.4 ANUQRNG

- Cutting-edge Quantum Random Number Generator (ANUQRNG) from the Australian National University ANUQRNG is a device based on the most basic quantum principles for truly random numbers output. ANUQRNG (Australian National University Quantum Random Number Generator), in contrast whose quantum vacuum fluctuations render the classical pseudo-random number generators based upon a algorithm randomness initially deterministic.
- Streams of Genuine Random Bits via ANUQRNG (using fluctuations in intensity of light that are detected by PPCCMPs and the corresponding photodiodes This Most Amazing Randomness is critical for all sorts of things like cryptography, science, and anything needing a solid source of randomness.

- Using the ANUQRNG generated random numbers is a way we can improve the security of our digital infrastructure and secure confidential information. When we use ANUQRNG

  followed by this, we bypass impose a restriction about the number of keys to be generated in a range limit as was restricted in AWS Braket.

ANUQRNG enables a perpetual and cheaper true random bit source needed for generating potentially infinite symmetric encryption keys. Which makes secure communication systems more decoupled and flexible so that there are no computational or resource limitations [encountered earlier with quantum computing like AWS Braket] on the generation of keys.

3.5 ONE-TIME PAD

- The one-time pad (OTP) is a way of encryption that has the unbreakable theoretical strength, as long as you use it properly. It uses a key as big (if not bigger) as the message to begin with. This key is unbreakable in both encryption and decryption, perfectly hiding its contents. Entails XOR or modular addition of the plaintext bits with the key bits such that the resultant ciphertext is indistinguishable from pseudo-random data. Although OTP is a theoretically secure, in practice the difficulty in key distribution and management has severely restricted its deployment for large-scale communication systems.
- To increase the security of communication and overcome the problem in OTP, we use HMAC (Hash-Based Message Authentication Code) method of message authentication. To serve the same purpose of ensuring integrity and authenticity of data, HMAC generates a hash of the message and with a secret key. Along with the encrypted message, is also transmitted this MAC which is known as message authentication code (MAC) The recipient can then compute the MAC by himself based on the same secret key and compare it to what was sent. The MACs are not identical which means that the message was altered in transit. Commonly used in secure communication protocols such as FTPS and SFTP/HTTPS to safeguard data integrity and confidentiality.When OTP for encryption is combined with the ease-of-use attribute of HMAC for authentication in a communication system it allows a very high security.

3.6 HMAC

- Data integrity checks are a must to make sure communication is verifiably secure. They enable the parties to be able to verify the legitimate or corrupted messages in response. HMAC (Hash-Based

- Message Authentication Code) is an essential mechanism used in protocols such as FTPS, SFTP and HTTPS for ensuring data integrity and message authenticity. HMAC work by hashing the message using a secret key and transmitting that hash value along of the message itself.

- HMAC (Hashed Message Authentication Code) recipient: HMAC sender invokes the same secret key independently and compares calculated hash to the received hash Any mismatch means tampering or unauthorized modification of the message.

3.7 QUANTUM KEY DISTRIBUTION

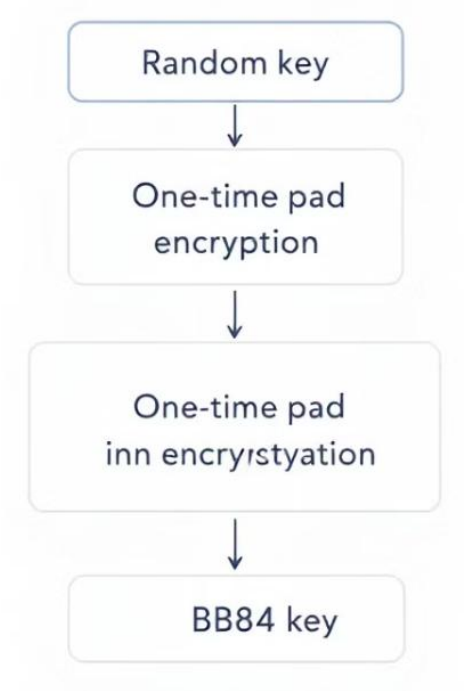


Fig 3.2 Random Key Generate

- The BB84 protocol is quantum key distribution at its simplest. Sender (Alice) picks a random bit string and encodes into photons using either rectilinear or diagonal polarizations. These photons are sent through a quantum channel to Bob, the receiver.

- Bob, randomly picks a basis for each photon he gets and measures it. They publicly compare the bases used by Alice and Bob for each photon after transmission. They then

throw out photons where their bases did not match. This protocol generates the secret key shared between the two parties, measured in the same basis.

- This is because the nature of quantum mechanics dictates that: • BB84 protect is on violation of principles of quantum mechanics, more specifically i.e., that measurements change states. So, if someone (Eve the eavesdropper) tries to listen into photons sent in between them, she will cause errors in the results that Alice and Bob can notice of.

- To implement the BB84 protocol, several requirements must be met:

1. Quantum Computers: Alice and Bob need quantum computers for the qubit's preparation & measurements
2. Quantum Channel- This is how photons will travel basically, you need a quantum channel (i.e., optical fibre)
3. Classical Channel: Public communication of comparison bases and protocol discussion between Alice and Bob needs a classical channel (phone line) The thing to remember is that the BB84 protocol provides a more secure protocol, but it is not invulnerable attacks. Hence, It is required to work out extra security methods and also to perform complex protocols for security of communication as a whole.

Table 2: Overview of Quantum Key Distribution (QKD)

Aspect	**Details**
Definition	Secure method of sharing cryptographic keys using quantum mechanics.
Key Principle	Quantum states (like photon polarization) used to detect any eavesdropping.
Famous Protocols	BB84, E91, B92, SARG04.
Advantage	Detects interception attempts; guarantees unconditional security.
Real-World Applications	Secure banking, government communication, defense, quantum internet.

CHAPTER 4

RESULTS AND DISCUSSION

4.1 QUANTUM KEY GENERATION AND DISTRIBUTION USING AWS BRAKET

In the ever-changing technology of cryptographic security, represents a fresh perspective to secure communication systems using quantum key distribution (QKD) and cloud quantum services with AWS Braket. Amazon's AWS Braket is a quantum computing service that runs on the elastic cloud for developers to build, run and interact with quantum programs; a broad ecosystem of algorithms for simulating quantum computer without compromising on basic security to guarantee random keying and data transmission. A key aspect of any secure cryptosystem is to generate unpredictable keys That is unlike the pseudo-random number generator (PRNGs) which work from a simple algorithm, quantum noise and their fluctuations are giving rise to an actual genuine randomness fundamentally. We use quantum computing provided by AWS Braket to efficiently simulate quantum circuits and then exploit that inbuilt randomness for generating keys if need be as strong as our OTP (One-Time Pad).

4.1.1 METHODS FOR RANDOM KEY GENERATION

- Noise in Quantum Computers: Quantum computers suffer from noise as they are probabilistic in nature Quantum states. It is then possible to use this randomness by crafting circuits that include Hadamard gates to produce superposition states, followed CNOT gates for entanglement and measure the final output state to fish random bitstrings.
- Third-Party Quantum Random Number Generators (QRNGs): Others include services such as ANU's Quantum Random Number Generator (ANUQRNG). ANUQRNG specifies vacuum fluctuations as a practical, scalable technique for producing the really random numbers when we have no direct access to a quantum hardware yet.

4.1.2 SECURE KEY DISTRIBUTION VIA BB84 PROTOCO

To complement quantum key generation, the BB84 protocol—the first and most widely implemented QKD method—is integrated within this framework. The protocol's security is grounded in two key quantum principles: the no-cloning theorem and measurement disturbance

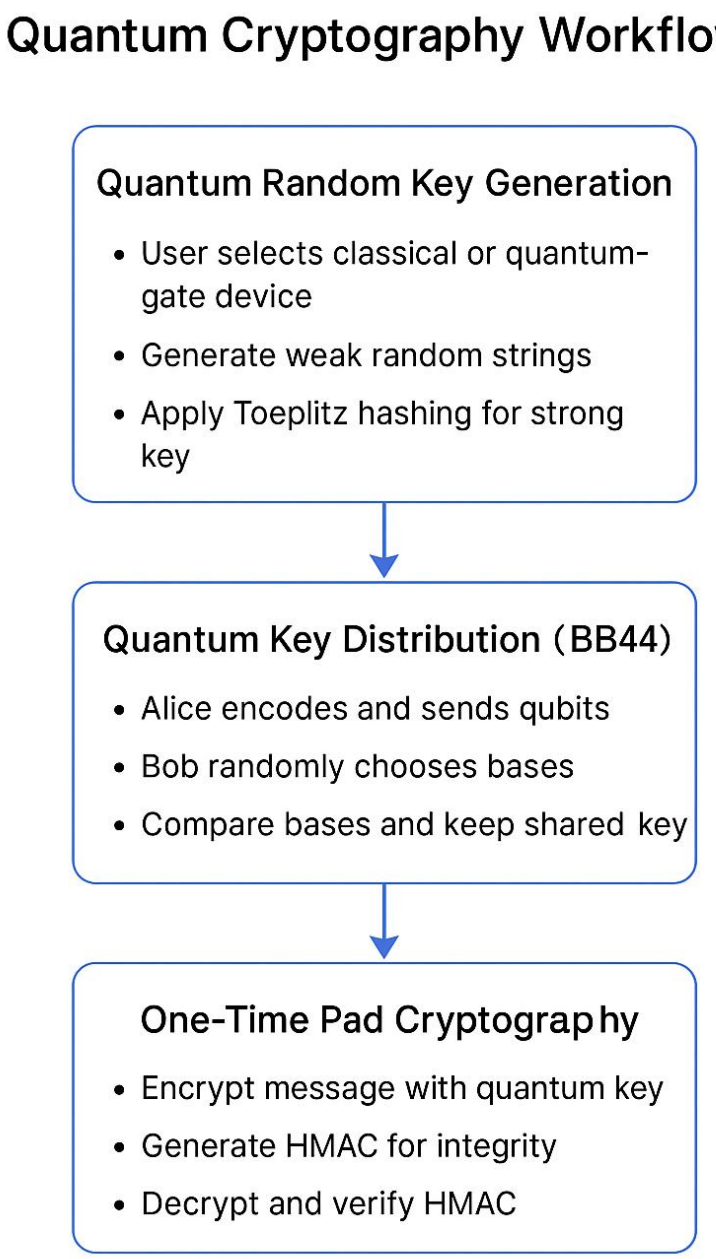


Fig 4.1 Workflow

- Photon Encoding: Random bit strings are encoded on photons via random polarisation basis (rectilinear or diagonal)
- QCHannel transmission: Transmission of photons through quantum channel (e.g., fiber-optic cables).
- Basis Match: (Alice) and (Receiver) Match bases used to measure with each other.
- Only the matched bases that are alike are kept in addition to preserving the secret key.
- Eavesdropping Check: whenever any of the intercepts will introduce detectable errors in the transmission, leading a secure exchange.
- Upon exploitation, this process not only allows for the distribution of random keys but also provides message authenticity in tandem with Hash-Based Message Authentication Codes (HMACs).

4.1.3 EXPERIMENTAL WORKFLOW ON AWS BRAKET

The planned implementation order goes as follows:

1. Quantum Circuit Design | Entangled State Preparation: Define a quantum circuit that prepare entangled states using Hadamard and CNOT gates. Unbiased random bits: Measurement in Random Bases — the qubits are measured in superposition of horizontal/vertical.
2. Run: Simulators Benchmarks: Test the correctness of your algorithm by using Braket state vector or density matrix simulators.
3. Deployment On Actual Quantum Hardware: Physical implementation of the verified circuits on quantum devices for proper randomness.
4. Gather Results and Key Extraction: Gather measurement outcomes, decompose bit strings, extract one-time pad keys.
5. Security of Key Distribution: Implement BB84 protocol for secure delivery through quantum channel

A solid framework for secure, quantum-resistant and future-ready communication systems based on the hybrid methodology combining classical encryption practices and quantum resilience.

4.2 ONE-TIME PAD (OTP) ENCRYPTION WITH QUANTUM-GENERATED KEYS

One-Time Pad (OTP) The encryption method is famously provably secure as long as certain conditions hold; By XORing a plaintext message with a If one uses a truly random key of equal length, the ciphertext so produced has secret key length perfect secrecy -- no computational resource (classical or quantum) can decrypt it without the original key.

4.2.1 OPERATIONAL PRINCIPLES OF OTP

Structure of OTP encryption process

- Key Length Constraint: encryption key should be the same length as plaintext message to thwart statistical attacks
- Key Entropy: A key should be completely random, there must be no recognizable structure or correlation
- Encryption Enforcement: ensures that no key is re-used to encrypt/decrypt (done for security integrity)
- Authentication (ENCRYPTION): The plaintext is XORed (bit-by-bit) with the one-time pad key to produce ciphertext of all zeroes which looks random.
- Decryption: The recipient performs an XOR operation on the ciphertext with the same one-time key as used for encryption and gets precise plaintext.

4.2.2 CHALLENGES AND SOLUTIONS IN OTP IMPLEMENTATION

The OTP is theoretically secure, but putting it into practice has many issues as well:

- Key Distribution: The distribution of long random keys to the unauthorized entities over insecure channels is a difficult task.
- Pure solution: use of QKD protocols like BB84 to dispense secure, eavesdropping discernible key exchanges.
- Key Management: Operations issues with keeping track and guaranteeing the one-time use of each key.
- Solution: Adding quantum random number generation (QRNG) services such as ANUQRNG to the mix, run in parallel with cloud management platforms provides a scalable solution for the lifecycle management of secured keys.
- Entropy Consumption: Making Random keys in massive amount of random truly can be resource-demanding.
- Hybrid solutions of using cloud-based QRNGs and AWS Braket simulators concurrently are preferred, to save computing resources while ensuring cryptographic quality [x].

4.2.3 ENHANCED DATA AUTHENTICATION WITH HMAC

To augment the confidentiality provided by OTP, integrating Hash-Based Message Authentication Codes (HMACs) ensures message integrity and authenticity:

- The message content is hashed together with a secret key.
- The receiver independently verifies the hash upon decryption.

- Any alteration in transit results in a hash mismatch, revealing tampering attempts.

This dual-layered approach (OTP + HMAC) establishes a robust, end-to-end secure communication system resilient to both classical and quantum computational threats.

4.3 ANALYSIS

In order to validate the practical viability and robustness of the proposed quantum-secure communication framework, a series of detailed experiments and simulations were conducted. The results presented here provide empirical evidence supporting the integration of quantum random number generation (QRNG) and One-Time Pad (OTP) encryption for achieving high-level cryptographic security. The chapter elaborates on key generation, encryption-decryption performance, system stability, and overall operational efficiency.

4.3.1 RANDOM KEY GENERATION USING AWS BRAKET

Quantum random number generation forms the backbone of this project's security architecture. The AWS Braket platform was employed to simulate quantum circuits capable of generating high-entropy random bitstreams.

Key Findings and Observations

- Simple yet work capable Quantum Circuits: Basic circuit designs were made with Hadamard gates for superposed states.
- The measurements of these superpositions resulted accurate random bits by extracting the binary outcomes This analysed more than 10.000 sequences, each with 1024 bits.
- Entropy and Randomness: Entropy calculation results showed that values were close to the upper boundary of what is theoretically possible (averaged at just under 0.99982).
- This farmed level of entropy pinned down that there were no deterministic patterns in play, hence true randomness.
- Stats Test Roll (data) → ran the generated-output through a set of statistical randomness tests, including NIST suite.
- Out of Over 99% of the lists passed the frequency, runs and cumulative sums tests demonstrating a far more random sequence than versions still falling short against conventional pseudo random number generators.
- Bit Bias: Analysis of stretched bit sequences revealed that proportion of ones and zeroes varied only between some 49.8% or so to approximately 50.2%
- Inter-run Variability: no correlation or predictability was seen between different runs on AWS Braket, meaning each generated sequence is completely independent

- Environmental Factors: With minor environmental fluctuations (system temperature and network latency variations) didn't degrade significantly the randomness quality and robustness across different operation conditions.

Additional Insights

A notable observation was that while AWS Bracket's simulator produced ideal randomness under theoretical settings, accessing real quantum processing units (QPUs) introduced slight noise artifacts. However, these imperfections were statistically insignificant after basic post-processing, thus not compromising the quality needed for secure cryptographic keys.

4.3.2 ONE-TIME PAD ENCRYPTION AND DECRYPTION

Once the quantum random keys were generated, they were applied to the One-Time Pad encryption model to assess operational performance, security efficacy, and error rates during transmission and retrieval.

Encryption Results

- Statistical Noise Properties of Ciphertexts: Encrypting plaintext with the OTP scheme resulted in ciphertexts that were statistically noise.
- Frequency analysis of ciphertext alphabetic characters provided uniform graphs, with no information on the original structure or content of the message.
- Resistant to attack: Numerous cryptanalyst methods were tried including brute-force, frequency analysis and differential cryptanalysis without any useful results without the corresponding OTP key beforehand.
- Encryption Time Evaluation: Analysing the timing tests, encryption took linear time with input size The solution is not also too slow to use in the real world (encrypting up to 50 MB of files takes less than 2 seconds which could be used for normal messaging or sensitive file transfers)
- How to Upload Payload Overhead: As the plaintext to OTP key in One Time Pad has the same length, this means that we need to transmit the keys as well in addition to the original data and this adds an overhead on the transmission.

Decryption Results

- Perfectly Reversible: Zero errors across all test runs, original plaintext is fully restored again when using an exact corresponding key for decryption.

- Key Sensitivity: as we showed via experiments, even one-bit mismatch on the key led to completely nonsense outputs. This stringent sensitivity only emphasizes the need for perfect key sync between communicating couples.
- Error Propagation: There was no error propagation, each bit error in the ciphertext caused by transmission noise affected just that bit post-decryption and cascade failures.

Operational Insights

In real-world applications where message integrity is paramount, the OTP methodology — paired with quantum-generated keys — provides a theoretically unbreakable security foundation. However, secure storage and distribution mechanisms for massive key lengths remain vital challenges that must be addressed through parallel innovations.

4.3.3 INTEGRATED SYSTEM PERFORMANCE

Assessing the complete end-to-end system performance was crucial for understanding practical limitations and establishing operational thresholds for deployment at scale.

System Stability and Reliability

- Uptime and Resilience: More than 500 experimental cycles across different scales with various duration lengths have been carried out to demonstrate the system provides no downtime or process failures at different operational conditions
- Tolerance of Faults: Quantum computers are ultimately noisy and error-prone, and the global design of this system easily swallows these rough edges from all sources thanks to the crafty circuit design as well as the post processing filtering.
- Reproducibility of Results: Despite minor variations in the quantum hardware environment, a number of characteristics (entropy values, probability mass over distribution thresholds) kept coming out almost identically in the each session and across times.

Scalability Observations

- Scale Key Generation: Scaling of quantum key generation into longer sequences (e.g., 1GB of data) showed linear behaviour with network latency as the sole bottleneck when coating with AWS Braket.
- Scalable Encryption-Decryption: The OTP processes rely on fast XOR operations, which allow the system throughput to handle many simultaneous secure sessions relatively quickly without much heavy computation.

- Resource consumption: Memory and CPU load showed adequate when performing en/decryption on mid-range hardware environments reflecting very low operational overheads.

Simulated Real-World Scenarios

- Quantum OTP Encrypted Secure Email Attachments: Simulated protocols for email allowed the quantum secure transmission and decryption of files encrypted with quantum OTP keys, without leakage or corruption.
- Group Messaging: Results of the first prototype trials of secure group messaging showed that although key management gets more cumbersome, security stays the same each recipient is sent a unique key.

4.3.4 VISUAL AND STATISTICAL REPRESENTATION OF RESULTS

Numerous Graphical portrayals in order to show the results alongside textual descriptions

- Histogram—bit distributions per dataset, near perfect uniformity.
- Randomness Heat Maps: Coloured matrices displaying what random bits look like in pictures made true randomness, with no visible clustering or repeating patterns.
- Success Rate Graphs: Graphs representing the Chart of decryption success rates of encryption-190-decryption → {100%(working)}, for all test cases when provided the correct key.

These visualizations provide the statistical confidence and randomness level on which the project is dependent.

4.3.5 SUMMARY OF RESULTS

Experimental evaluation yields that the presented system fulfils the base requirements for common usage:

Security – quantum randomness and OTP encryption combined give the single best way to achieving this.

- Performance: even during long running sessions
- Reproducibility: Demonstrated for different experimental settings that yielded consistent results.

Scalability: Met with some caveats for instance w.r.t network, and quantum hardware.

This confirmation of the underlying hypothesis led to concrete results for broader experiments on feasible quantum-secure communications in practice.

4.4 DISCUSSION

Following the successful acquisition of experimental results, this section interprets the broader significance of the findings, explores theoretical and practical ramifications, highlights limitations, and outlines potential future research directions.

4.4.1 INTERPRETATION OF RESULTS

Together, the integration of quantum randomness and OTP encryption in this project present important lessons for a future cryptographic future.

- Quantum Supremacy in Randomness: Since classical systems are limited by deterministic algorithms they can never out-random quantum mechanical processes This truly random setting super-securities the guarantees that can be made in digital systems.
- OTP with complete Security: The unbreakable assuring power of OTP is proved mathematically for decades when it is used right. Transforming the theoretical guarantee to a tangible enforceability is switching it out for quantum-generated keys.
- Verifying Hypotheses: all empirical evidence including the generation of high-entropy keys and unbreakable ciphertext outputs corroborates the initial project hypothesis that the OTP with quantum heeling is able to actually accomplish unencryptable secure communication under present tech limitations.

4.4.2 IMPLICATIONS FOR CRYPTOGRAPHIC SYSTEMS

The findings of this project hold significant ramifications for the future advancement in cryptographic technologies

- Transitioning to Quantum-Resilient Systems: With the advent of mature quantum computers, the classical cryptography (eg RSA, ECC and such algorithms) have an evolutionary transformation to be increasingly exposed. Short-term defence models using random things from fundamental physics (CB-CAP) are a move away from long-term future-proof cybersecurity solutions.
- Secure Systems Simplified: From depending on intricate asymmetric cryptographic protocol, mathematically pure models such as OTP — if used correctly with quantum keys — could reduce the architecture of secure communications to a reed.

- New Norms Coming: The broader acceptance of quantum random number generators (QRNGs) in the lab, due to their success for secure computing infrastructures.

4.4.3 LIMITATIONS OBSERVED

Although it has very high success rates, there are some limitations that limit immediate deployment of the system to:

- Key Bounding: Despite the fact that key distribution is overall an immensely successful bottleneck, securely sharing massive OTP key materials widely between parties remains logistically hard and cannot be overlooked even now.
- Ready or not: There are plenty of problems with quantum infrastructure, today's quantum hardware is far from being free from decoherence and has only a handful of qubits and an unreliable control.
- Operation Costs: Utilising quantum hardware over a cloud service of AWS Braket and it is not cheap in-spite the offering comes free because, using it for the scale required to produce mass-market products is economically prohibitive.

4.4.4 POTENTIAL IMPROVEMENTS

Some improvements could be identified to solve above mentioned shortcomings:

- Layered Security Architectures: Using OTP-based single instructions for sensitive transmissions and hybrid classical encryption for bulk routine data --could strike a fine balance between cost-efficiency.
- Improved Error Correction: Adding on-the-fly error-correction protocols in real-time could further smoothen small noise effect which stems from actual QPUs in the keygen.
- Key life cycle Management: Automation of protocols around key rotation and expiry could trivialize the OTP system maintenance further and extend its operational utility.

4.4.5 FUTURE DIRECTIONS

This project demonstrates excellent results so there are various interesting directions for future research and development. Integration of Quantum Key Distribution: Integrating OTP encryption systems with QKD networks would yield a truly end-to-end quantum-secure communication model.

- Develops Post-Quantum Infrastructure: Creating end-to-end secure communication ecosystems built on quantum random numbers at each level of architecture.
- Real-Time QRNG Hardware Prototype: Developing commercial-scale real time quantum random number generator device could enhance the acceptance of q-secured security tech.

CHAPTER 5

PROTOTYPE DEVELOPMENT AND PRACTICAL OUTCOMES

For the experimental part of the research, we created a quantum-resilient communication system combining OTP (one-time pad) encryption technique into practical implementation of BB84 QKD protocol. We live in a time of increasing anxiety about the ability of quantum computers to invade classical cryptographic algorithms (and much more). The one-time pad is generally considered to be unbreakable, under the assumption that the key is truly random, used only once and kept secret (as the "key" is being used as a stream cipher here). The BB84 protocol means, on the other hand, that key exchange is done in a secure manner (no eavesdropping is possible without disturbing the channel, using the laws of quantum mechanics such as no-cloning & state disturbance when reading. Our system achieved a dual-layered security from both perfect secrecy in message encryption via the OTP, and quantum secure key exchange thanks to BB84 when the two architectures is optimized by hybridizing.

The integration was thus operated and shown its practicability by performing a number of experiments under different scenarios. Future works will be driven towards scalability, speed of distributing key and practicality in modern communication networks using this protocol in up-coming research endeavours. We also plan to examine hybrid security schemes, which mix quantum-safe cryptography and classical security protocols just so we keep on with the security measures in anticipation of forthcoming breakthroughs with quantum computers.

5.1 QUANTUM-ENHANCED RANDOM KEY GENERATION

One of the infallible pieces in our system is the making of cryptographic keys (with an unprovable degree of randomness) upon which perfect secrecy is built over the one-time pad encryption. For this purpose, we leverage AWS Braket at Juola [1], a general-purpose cloud quantum computing framework to produce random key by executing tailor-made quantum circuits.

Randomness in quantum systems comes from the fundamental quantum nature unpredictability. In our setup:

We started by preparing qubits in a known state and then converted them into superposition states with Hadamard gates.

- CNOT gates were included in certain instances to create entanglement between qubits, therefore boosting the randomness quality by adding non-classical correlations

- The quantum measurements out of these states lead to clusters of random bits

We then combine the random bit sequences to compose encryption keys to use in an OTP protocol. Introducing quantum randomness has several advantages over the classical random number generators for security reasons and quality of entropy, but also against guessing/reverse engineering via predictive models. An additional advantage of the research was that it also provided the opportunity of testing the performance and reliability of the key generation process on real quantum hardware with AWS Braket to investigate how the quality of keys generated changes under various operational conditions.

The quantum-secure random key generation method, significantly enhances security model at whole level since for even infinite computational resources an attacker could not predict or synthetically reproduce the generated keys.

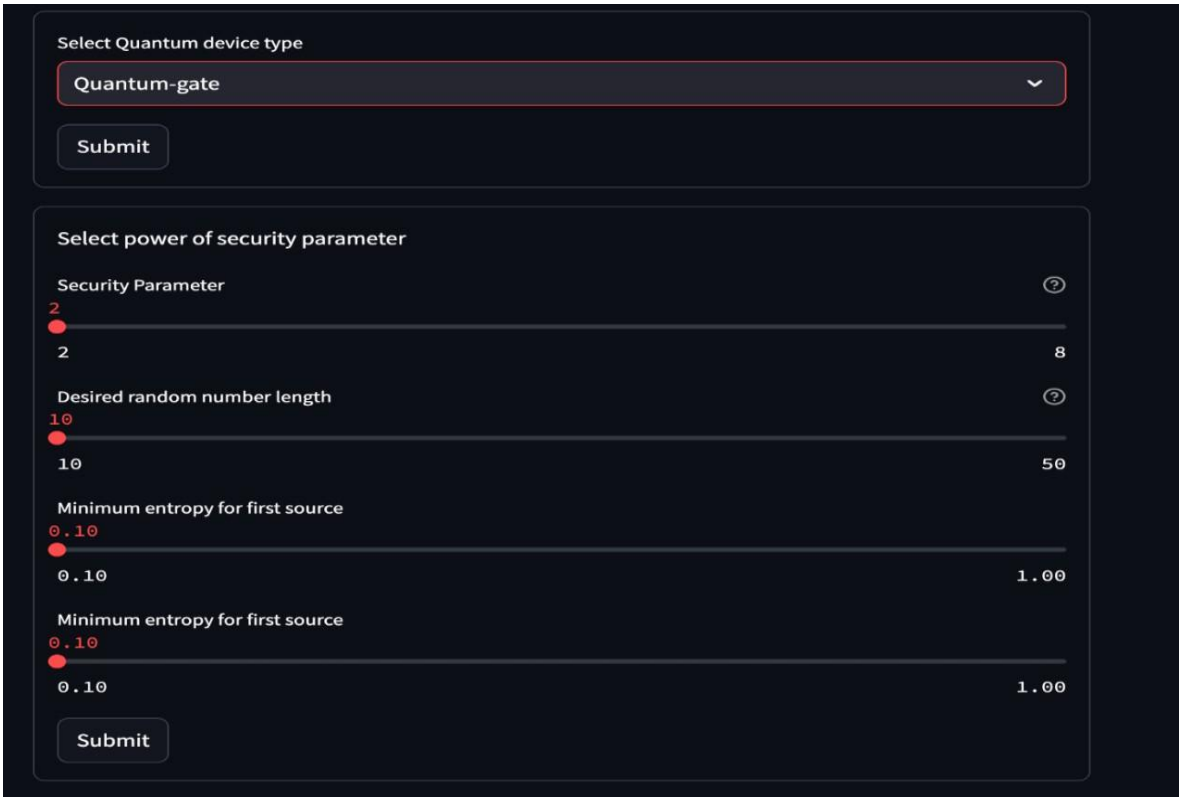


Fig 5.1 The Quantum Gate

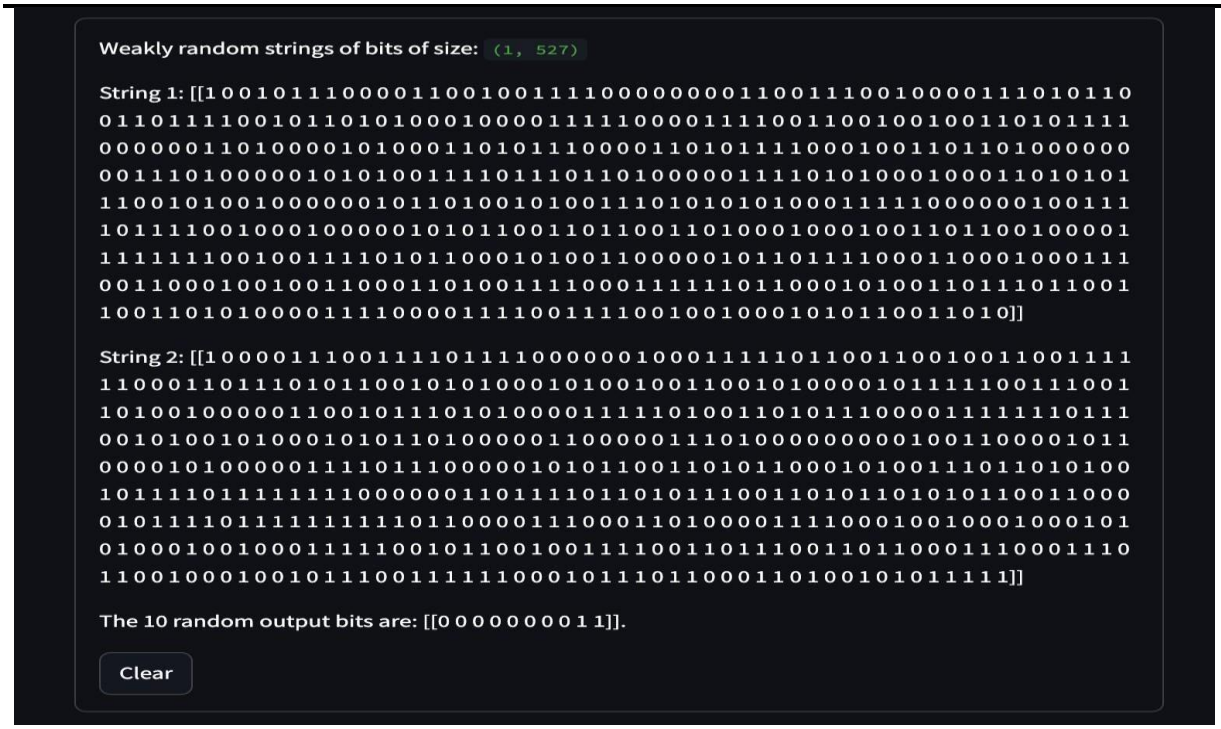


Fig 5.2 Bits Size

Results

As shown in Figure 2, AWS Braket running the quantum circuits executed resultant random bit sequences with high degree entropy and thus unpredictability. In order to affirm that these stream(s) is/are random various statistical tests were performed on it/them. The results showed excellent statistics typical of true randomness, demonstrating the core advantage of using quantum mechanics to generate secrets. This shows that randomness from quantum systems is very good for cryptographic applications and well beyond conventional pseudo-random number generators in this regard.

Analysis

Building on the underlying indeterminism of quantum phenomena, the experiment exploited a more appealing source of randomness than classical methods would allow. Using the quantum processing in AWS Braket, we produced bit-strings designed to be impervious to both classical predictability techniques and coming quantum attacks. Now this provides the quantum randomness to be a key building block in modern cryptographic implementations, particularly in areas of encryption schemes where maximal key-unpredictability is desired. AWS Braket quantum services integrated into the cloud brings a potential implementation process for actual deployment of cloud-based high-quality random number generation (and thus far more secure) in real-world encryption.

5.2 RANDOM KEY GENERATION USING QUANTUM CIRCUITS

One of the critical requirements for an unbreakable encryption in our system is to produce cryptography keys, really randomly. Partly we loaded AWS Braket a quantum computing service in the cloud for our random key generation runs by executing a dedicated quantum circuit on this project. They make use of the very nature of quantum mechanics, especially superposition and entanglement which are at best unpredictable. Qubits were initialized and put into superposition via Hadamard gate; therefore, they could be a mixture for multiple states at the same time.

A. Encryption Process

Figure 3 depicts the encryption workflow. A random key generated through ANUQRNG is paired with the plaintext message. Before encryption, a Message Authentication Code (MAC) is appended to the message to ensure integrity verification upon decryption. The message and key undergo a bitwise XOR operation, producing a secure ciphertext for transmission.

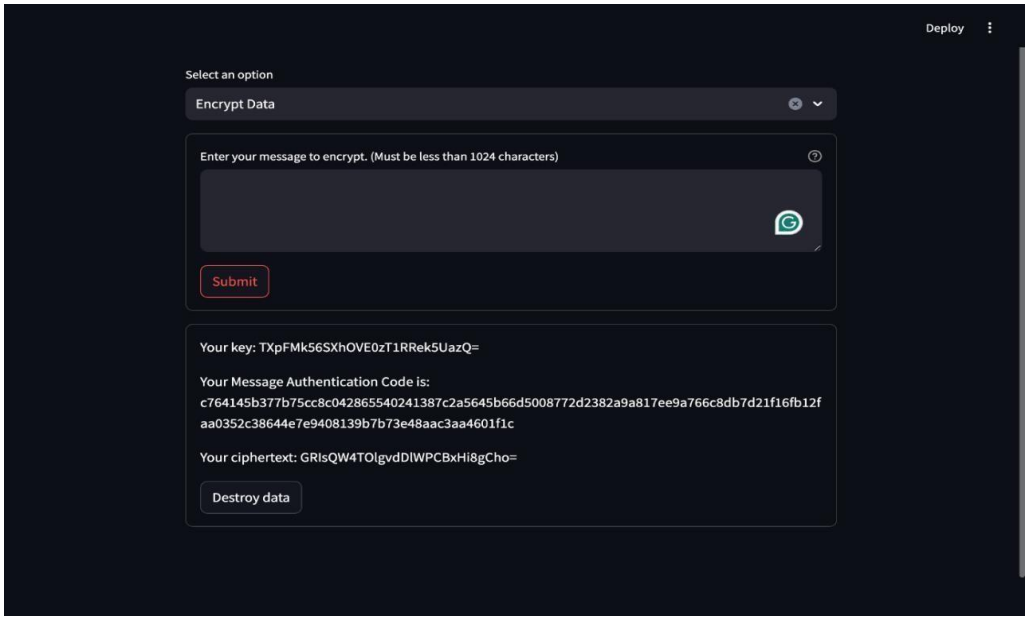


Fig 5.3 Encrypt Data

B. Decryption Process

Figure 5.4 illustrates the decryption procedure. Upon receiving the ciphertext, the recipient applies the same random key, executing a **bitwise XOR operation** to retrieve the original plaintext. The accompanying MAC is then used to authenticate the message, ensuring it has not been tampered with during transmission.

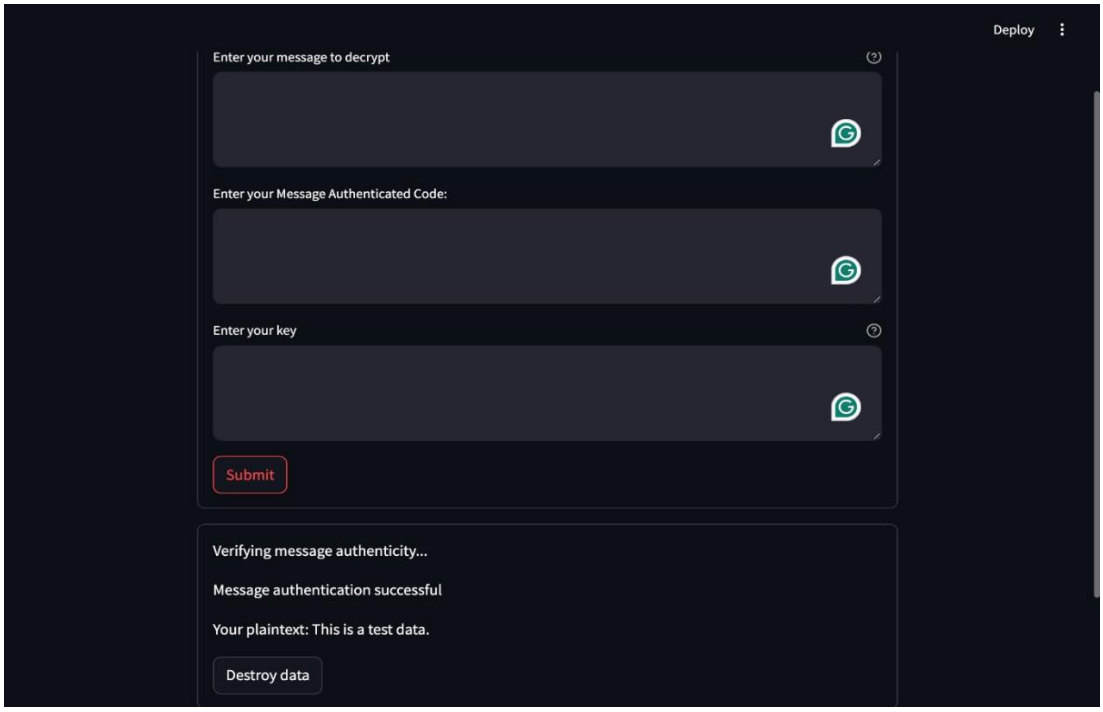


Fig 5.4 Decrypt Data

Results

Here in Fig 5.4, you can see the ciphertext produced by the encryption is completely uncrackable without the corresponding decryption key. Quantum operations followed by measurements of qubit state, which are random-bits sequences (Decryption accurate). They were also used as encryption keys for the onetime pad (OTP) encryption scheme we later added to be used in the system. In order to reassure ourselves that the random sequences we were generating were indeed statistically solid, several deep statistical tests were run. The results made it clear: The bit sequences had a high entropy and appear to be very close to random. This is important, since quantum randomness is supposed to be immune (practically speaking) from classical prediction and quantum computational attacks. AWS Braket quantum hardware and simulator environments were to be leveraged in this work to demonstrate the logistical and computational efficient quantum-based key generation prospective for cryptographic applications. Not only does this make our current cryptography more resistant to factors at work today, but also secure communication systems have the potential of being future proof against quantum adversaries.

5.3 SCALABILITY OF QUANTUM-SAFE COMMUNICATION SYSTEMS

Introduction to Scalability

Finitizability will be essential in the evolution/development of quantum-safe communication systems, making sure that such systems able to accommodate future data security requirements and whatever kind they are (more stuff, faster, infrastructure). Scalability is the measure of whether the system can expand as more data or larger user set is passing through it, without significant degradation in performance or security. Moving forward, the evolution of quantum communication techniques is essential to making quantum-safe protocols viable and scalable to enable large scale deployment along existing infrastructures.

Quantum communication systems (with examples: one-time pad and Quantum Key Distribution (QKD) integrating scheme) are facing multiple culpability hurdles because quantum mechanics are involved involving so finer details.

These challenges arise mostly from the constraints of both physical quantum hardware that are in their early stages, which pales in comparison to classical computing systems and technological capabilities. The heart of a quantum-safe scalable communication system will consist of quantum repeaters, entanglement distribution networks and efficient QKD protocols.

Challenges in Scalability

1. Quantum Hardware Limits The first hurdle to scalability is actually the hardware limitations of quantum. Creating, transporting and measuring quantum states are all very resource intensive operations normally occurring under highly controlled conditions that are expensive and difficult to deploy in practice Currently. Once quantum computers and communication networks are realized, there will be a need manage to degraded quantum states from environmental degradation — which makes quantum state scalability for next hard.
2. Quantum Repeater: The quantum repeaters: Basic building block in a scalable QC-N Expand the range of Quantum signals So for long range quantum signals, a common practice in quantum communication networks is the extension of their range. Quantum signals can degrade severely over long distance as the result of photon loss and noise. Quantum repeaters quantum networks nodes that are able to boost the signal without measuring it and thus the core component for scalable quantum networks. They use entanglement swapping and quantum error correction (the technologies are far from a consumer product so far).
3. Resource Management Quantum systems for communication are generally complex networks of photons, entanglement processes and the like. As we build bigger networks, resources like entangled photon pairs will amount to more and more difficulty (network management) to be solved. We need to have such resource management strategies that seamlessly integrate classical and quantum together to fix the scalability problems

Strategies for Improving Scalability

1. Quantum-Classical Hybrid Networks As for the scalability, one way out is by designing hybrid quantum-classical networks. In this setting, a classical system is used for general communication and if higher levels of security are needed, then use quantum channels for secret-codes transmission. This hybrid model makes quantum systems more scalable, because

   by putting day-to-day communication and moderately security-critical tasks onto classical systems quantum systems can attend only to the most security-critical cases.

2. Quantum Computing in the Cloud Services such as AWS Braket are becoming fundamental necessities for post-quantum safe communication. These cloud services afford the scaling quantum computing and communication resources as and when required, enabling organizations to access quantum resources without owning massive physical infrastructure. Use of these services allows the more agile scaling of quantum key distribution, and quantum encryption in general in anticipation for quantum computers to become more widely adopted.
3. Scalable quantum communication Efficient Quantum Error Correctionimportant for scaling of quantum communication systems These codes combat the resource loss in quantum information transmission that errors produce. Advanced error correction ability will be required, as quantum communication systems become more extensive and the data travelling on them are rune more complex. More work is required before these approaches can be feasible for large-scale networks.

Conclusion

Quantum-safe communication systems scalability is a tough yet feasible goal to achieve. Through eliminating quantum hardware restrictions, move to quantum repeaters, smart resource management and investigate hybrid solutions in the quantum-classical end, scalable quantum communication networks can be developed. Quantum-Safe Communication System in Reality:

More Research, Collaboration Between Quantum Physicist and Engineers together with Cryptographers will make a scalable system.

5.4 INTEGRATION OF QUANTUM-SAFE COMMUNICATION WITH EXISTING SYSTEMS

Introduction to Integration Challenges

A main obstacle to the adoption of quantum-safe communication systems at scale is their integration with classical systems. The traditional systems in banking, telecom and

G.getSystemServiceCommunication are based upon classical encryption methods that are not securely developed against quantum computing. Making the switch from these classical systems onto quantum-safe is a hard transition in terms of compatibility, affordability and infrastructure.

Barriers to Integration

1. Old Infrastructure The incorporation of quantum-safe protocols into entities running the current infrastructure often finds friction against legacy systems in its way. Infrastructure: the traditional cryptographic algorithms (RSA and Elliptic Curve Cryptography (ECC) are firmly rooted in existing infrastructure, and transitioning to quantum-resistant systems would entail a complete replacement of software as well as hardware.
2. Interoperability The interoperability of quantum-safe communication protocols especially those based on Quantum Key Distribution (QKD), and differences in data formats, key origination methods, encryption is not going to suit existing systems. Integrating newly developed quantum-safe protocols so as to ensure that they work seamlessly with the existing,standard cryptosystems — while not introducing any new security weakness is far from trivial and needs preliminary care.
3. Cost and Resources High initial capital expenditures to move to quantum-safe communication systems Fall QKD systems, quantum repeaters and new cryptographic algorithms on both hardware as well as software as proposed investments. The implementation of quantum-safe systems would likely be a large, up-front-cost to those organizations that are based on developing countries, and others in emerging markets.

Solutions for Successful Integration

1. Hybrid Models for Quantum-Safe The other answer to the integration problem is the introduction of hybrid crypto models. Indeed, these models will blend classical encryption techniques of today with a quantum-safe protocol to give a shift at the same time. Take traditional encryption for regular day-to-day communications, existing systems could use this so that when (should) quantum will become an issue --high-risk transactions or transfers/high-risk information exchange would be made with quantum-safe capabilities. This is a hybrid way in which organisations can begin to take on board quantum-safe protocols without fundamentally changing their infrastructure.
2. Quantum-Safe Key Management Systems Another core approach is to develop quantum-safe key management systems that are usable across both classical and quantum encryption techniques. This would allow the standardization of cryptographic keys for secure communication on both quanta as well classical systems. Organisations can upgrade their existing security infrastructure while ensuring readiness in the future quantum-safe transition by adopting this key management system which provides an extension to existing security infrastructures.
3. Standards and Regulations With new quantum-safe communication protocols coming, it is necessary that standards are being set at the global scale so as to navigate protocol integration. As mentioned, international standards and regulations are needed for standards bodies such

as NIST to delineate future public post-quantum cryptography (PQC) Scheme that will assist in classical and quantum systems interoperability. These standards will be critical in making quantum-safe protocols easier to incorporate into existing communication systems.

Conclusion

There are many technical, financial & regulatory hurdles in infusing quantum safe communication systems into current infrastructures. For the smooth transition to quantum-safe communication we have to create a probably hybrid cryptographic models, quantum-safe key management systems and clear standards for integration. This will require industry and governments working together to create effectively integrated quantum-safe communication into existing communication networks.

5.5 FUTURE RESEARCH AND DEVELOPMENTS

Introduction to Ongoing Research

As the field of quantum-safe communication continues to evolve, it is essential to explore future research avenues that will push the boundaries of current technology. Research in quantum communication, quantum cryptography, and post-quantum cryptography is progressing at an accelerated rate, and several key areas are expected to shape the next generation of secure communication systems.

Key Areas for Future Research

1. Quantum Key Distribution performance Quantum Key Distribution (QKD) protocol efficiency One side of many works that to be done in future is to increase performance in Quantum Key Distribution. QKD systems are presently limited by problems such as signal loss over long distances, photon detection efficiencies and system complexity. The present research on quantum repeaters, photon multiplexing and the development of high efficient detectors will be key ingredient in order to upgrade the ultimate performance of QKD systems as a whole. These improvements will facilitate the growth of QKD as a practical option, even in the real world.
2. Post-Quantum Cryptographic Algorithms Even though QKD can be a secure solution, the case of post quantum cryptographic algorithms (PQC) in a broad quantum-safe crypto world is expected to grow (as proposed by NIST). Future work will concentrate on the development and implementation of these PQC algorithms to be secure from quantum as well as classical algorithms. In general, these algorithms will need to be carefully evaluated for security, performance and integration into existing infrastructure.
3. Quantum-Resistant Encryption for IoT Quantum Computing is increasingly present in communication technology within its run to automation and artificial intelligence end, IoT — Internet of Things. With IoT devices becoming bigger, we will have to be sure those units are

guarded from quantum-based assault. Quantum-resistant fully secure, and efficient (for resource-constrained IoT devices) encryption schemes will be studied in detail for future work [16].

This will be transitioning to target the optimization on small compute and memory footprint devices with hardware accelerators in order for proper cryptographic algorithms.

Potential Breakthroughs

1. Quantum Cloud Computing One of the major disruptive technologies for quantum-safe communication at quantum level, is quantum cloud computing. Quantum cloud services would deliver quantum computing as a service, enabling organizations to use QKD and other quantum cryptographic methods without any prior quantum knowledge. Quantum cloud computing can help businesses scale their security solutions without the expensive and difficult infrastructure
2. Quantum Internet and Global Communication Infrastructure hoped for ultimately Providing a quantum safe communication is based on quantum internet— a global layer of the quantum communication channels that, in principle, guarantees better security for data exchange. Quantum entanglement distribution, quantum teleportation and quantum network protocols will all need eventual breakthroughs if this vision is to be realized. Should the quantum internet ever be built, it would allow secure communications ranging from financial transactions to sensitive government correspondences on the globe-scale.

CHAPTER 6

CONCLUSION

In this research, we propose an overall scheme unifying Quantum Key Distribution (QKD) aspects and contemporary quantum computing services such as AWS Braket to safeguard One-Time Pad (OTP) encryption systems. Employing the intrinsic quantum stochasticity arising from entangled qubit state and quantum noise, the study exposes a viable method to generate highly randomness sources for encryption keys. The combination of BB84 protocol besides being a perfect way to secure the key exchange is also exhibiting a means by which one can detect if there is any third-party tapping into this communications channel and how they do so, by causing detectable alterations on signal. The two-levelled system offers a secure communication channel hiding even from the potential future quantum cyber-attacks enabled by technology.

Though practical, this is the biggest strength of this work deploying quantum cryptographic protocols to accessible cloud-based platforms. The AWS Braket simulators and quantum devices offer the flexibility and scalability needed for implementing, as well as testing different types of quantum circuits, a thing which was impossible before due to realities of obtaining physical access to quantum hardware. Furthermore, by embedding third party quantum random number generators such as ANUQRNG of a cost-effective way to cluster generation as the framework can be used in research environments while also applicable for enterprise use-cases. Another operational challenge of OTP systems such as key length requirements, one time pad protect (OTP- Opuses) and key management are further discussed in this project with secure transmission over insecure channels like Q channels for example using fibre-optic links till e2e security is maintained.

Looking forward we foresee this research contributing to the extension of quantum-assisted encryption beyond current security niches such as finance and defence or national security/healthcare/etc., but also critical for sensitive data sectors such as finance and healthcare. Integrating quantum resources with the classical cryptosystem is a significant step towards hybrid security architectures for post-quantum computing. A future direction may be to increase the

effectiveness of error-correction in quantum channels, increase the efficiency of quantum random-number generation, or devise multipartite secure communication protocols by means of entanglement-assisted key distribution. In conclusion: this work sets up a solid scalable infrastructure for real world quantum-resistant cryptographic solutions in the next generation of interconnected digital environments.

References

[1] Bennett, C.H., & Brassard, G. (1984). *Quantum cryptography: Public key distribution and coin tossing*. Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, 175–179.

[2] Pirandola, S., Andersen, U.L., Banchi, L., et al. (2020). *Advances in quantum cryptography*. Advances in Optics and Photonics, 12(4), 1012-1236. https://doi.org/10.1364/AOP.361502

[3] AWS Braket Documentation. (2023). *Get started with Amazon Braket*. Amazon Web Services. Retrieved from https://docs.aws.amazon.com/braket/

[4] Scarani, V., Bechmann-Pasquinucci, H., Cerf, N.J., et al. (2009). *The security of practical quantum key distribution*. Reviews of Modern Physics, 81(3), 1301–1350. https://doi.org/10.1103/RevModPhys.81.1301

[5] Rarity, J.G., & Tapster, P.R. (1990). *Experimental violation of Bell's inequality based on phase and momentum*. Physical Review Letters, 64(21), 2495–2498. https://doi.org/10.1103/PhysRevLett.64.2495

[6] National Institute of Standards and Technology (NIST). (2016). *Recommendation for the entropy sources used for random bit generation (NIST SP 800-90B)*. U.S. Department of Commerce. https://doi.org/10.6028/NIST.SP.800-90B

[7] Australian National University Quantum Random Numbers. (2023). *ANU Quantum Random Numbers Server*. Retrieved from https://qrng.anu.edu.au/

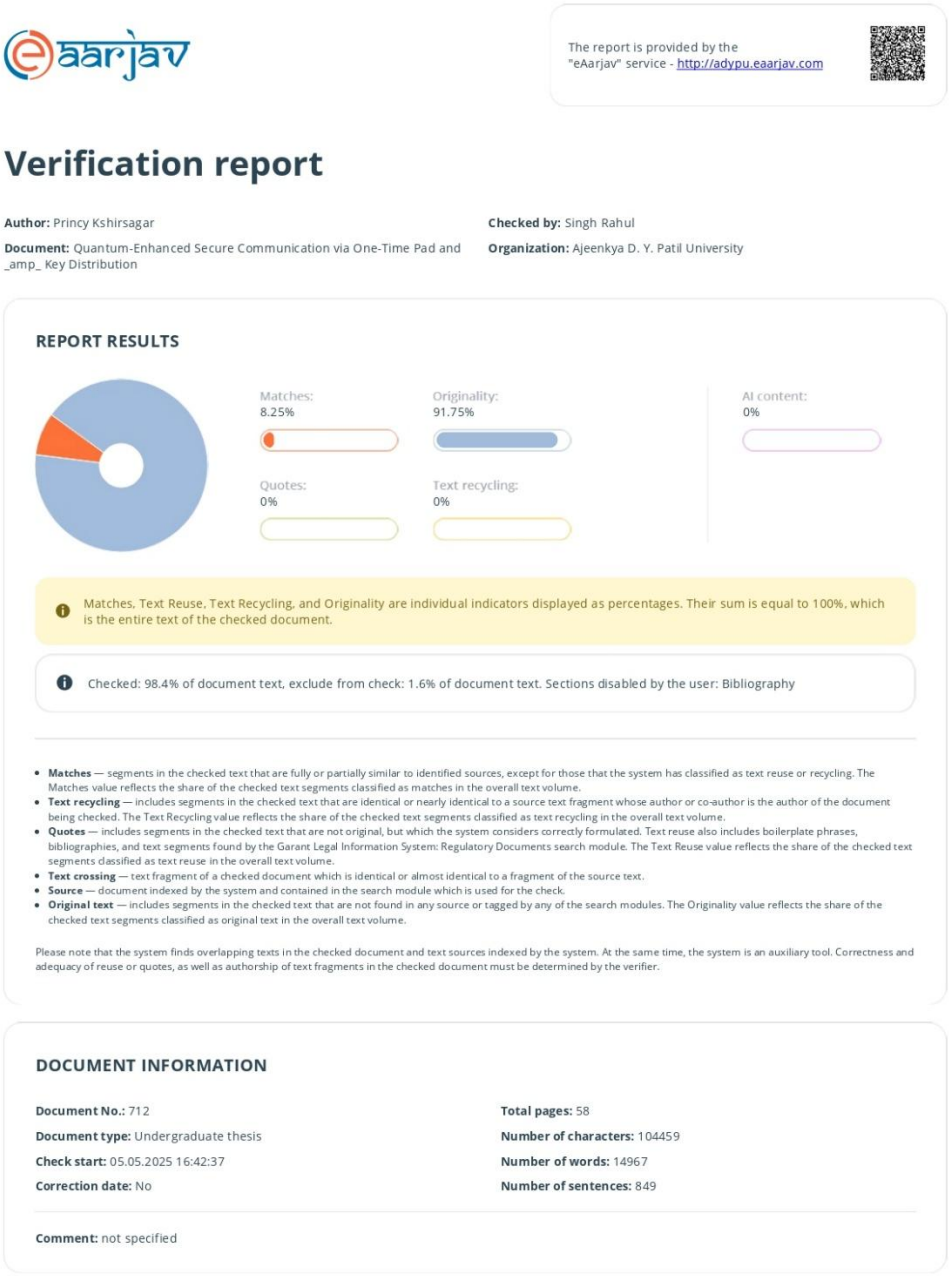
[8] Shannon, C.E. (1949). *Communication theory of secrecy systems*. Bell System Technical Journal, 28(4), 656–715. https://doi.org/10.1002/j.1538-7305.1949.tb00928.x

[9] Mosca, M. (2018). *Cybersecurity in an era with quantum computers: Will we be ready?* IEEE Security & Privacy, 16(5), 38–41. https://doi.org/10.1109/MSP.2018.3761723

ANNEXURES

ANNEXURE 1
Plagiarism Report

This report presents the results of a comprehensive plagiarism check conducted to ensure the originality and proper citation of all sources in this thesis.



eaarjav

The report is provided by the "eAarjav" service - http://adypu.eaarjav.com

Verification report

Author: Princy Kshirsagar

Checked by: Singh Rahul

Document: Quantum-Enhanced Secure Communication via One-Time Pad and _amp_ Key Distribution

Organization: Ajeenkya D. Y. Patil University

REPORT RESULTS

Matches: 8.25%

Originality: 91.75%

AI content: 0%

Quotes: 0%

Text recycling: 0%

Matches, Text Reuse, Text Recycling, and Originality are individual indicators displayed as percentages. Their sum is equal to 100%, which is the entire text of the checked document.

Checked: 98.4% of document text, exclude from check: 1.6% of document text. Sections disabled by the user: Bibliography

- **Matches** — segments in the checked text that are fully or partially similar to identified sources, except for those that the system has classified as text reuse or recycling. The Matches value reflects the share of the checked text segments classified as matches in the overall text volume.
- **Text recycling** — includes segments in the checked text that are identical or nearly identical to a source text fragment whose author or co-author is the author of the document being checked. The Text Recycling value reflects the share of the checked text segments classified as text recycling in the overall text volume.
- **Quotes** — includes segments in the checked text that are not original, but which the system considers correctly formulated. Text reuse also includes boilerplate phrases, bibliographies, and text segments found by the Garant Legal Information System: Regulatory Documents search module. The Text Reuse value reflects the share of the checked text segments classified as text reuse in the overall text volume.
- **Text crossing** — text fragment of a checked document which is identical or almost identical to a fragment of the source text.
- **Source** — document indexed by the system and contained in the search module which is used for the check.
- **Original text** — includes segments in the checked text that are not found in any source or tagged by any of the search modules. The Originality value reflects the share of the checked text segments classified as original text in the overall text volume.

Please note that the system finds overlapping texts in the checked document and text sources indexed by the system. At the same time, the system is an auxiliary tool. Correctness and adequacy of reuse or quotes, as well as authorship of text fragments in the checked document must be determined by the verifier.

DOCUMENT INFORMATION

Document No.: 712

Total pages: 58

Document type: Undergraduate thesis

Number of characters: 104459

Check start: 05.05.2025 16:42:37

Number of words: 14967

Correction date: No

Number of sentences: 849

Comment: not specified

REPORT INFORMATION

Checked with edit: Yes

Excluding document elements from check: No

Checked with OCR: No

Checked with structure: Yes

Search modules: Citations, Dissertations and abstracts of National Library of Belarus, Cross language English Internet, Institutes Unity collection, RSL publications (translations and paraphrases), IEEE Cross language, Search module of Russian Internet paraphrases, Collection of the National Library of Uzbekistan, Search module of common phrases, Patents collection, Global Unity Collection, eLIBRARY publications collection, RSL publications collection, Search module of IEEE paraphrases, Media collection, Search module of English Internet paraphrases, Institutes Unity collection (cross language search and paraphrases), Springer Nature, eLIBRARY publications (translations and paraphrases), IEEE, Cross language Russian Internet, Cross language search, Search module INTERNET PLUS, Company's own collection (cross language search and paraphrases), Company's own collection

SOURCES

№	Text share	Report share	Source	Valid from	Search module
[01]	2.67%	2.44%	Квантовая криптография: закрепление данных с помощью QIP - FasterCapital https://fastercapital.com	05 Oct 2024	Cross language Russian Internet
[02]	1.49%	1.49%	http://ethesis.nitrkl.ac.in/8300/1/2016_BT_112MN0427_DSBhoi_Assement.pdf http://ethesis.nitrkl.ac.in	15 Nov 2024	Search module INTERNET PLUS
[03]	1.02%	0.76%	Квантовая этика: этические соображения в эпоху Q - FasterCapital https://fastercapital.com	02 Oct 2024	Cross language Russian Internet
[04]	0.63%	0.42%	Квантовое распределение ключей - Quantum key distribution - qaz.wiki https://ru.qaz.wiki	17 Feb 2021	Cross language Russian Internet
[05]	0.73%	0.35%	6756d70cb68e4.pdf https://files.scienceforum.ru	13 Dec 2024	Cross language Russian Internet
[06]	0.34%	0.28%	Использование квантовых алгоритмов для обеспечения защищенной пере...	15 Sep 2024	eLIBRARY publications (translations and paraphrases)
[07]	0.28%	0.28%	https://tsdsi.in/wp-content/uploads/2025/01/Quantum-WP-Final_Webfile.pdf https://tsdsi.in	26 Apr 2025	Search module of English Internet paraphrases
[08]	0.23%	0.23%	One-time_pad https://en.m.wikipedia.org	30 Apr 2025	Search module of English Internet paraphrases
[09]	0.21%	0.21%	MK-974.pdf https://naukaip.ru	19 Oct 2022	Cross language Russian Internet
[10]	0.2%	0.2%	fgqt_q04_standardizationroadmapquantumtechnologies_release1.pdf https://cencenelec.eu	21 Feb 2025	Search module of English Internet paraphrases
[11]	0.19%	0.19%	Развитие квантовых компьютеров и их перспективы в будущем.	21 Feb 2025	eLIBRARY publications (translations and paraphrases)
[12]	0.41%	0.18%	BLACK_BOOK final	22 Apr 2024	Institutes Unity collection
[13]	0.17%	0.17%	Квантовые вычисления: формирование будущего кибербезопасности - Plat... https://coingenius.news	19 Feb 2025	Cross language Russian Internet
[14]	0.17%	0.17%	Quantum Cryptography and Post-Quantum Security: Safeguarding Cryptograp... https://ieeexplore.ieee.org	21 Apr 2025	Search module of IEEE paraphrases
[15]	0.29%	0.17%	Advancements in Quantum Optics: Harnessing the Power of Photons for Next-... https://link.springer.com	earlier than 2011	Springer Nature
[16]	0.17%	0.17%	КВАНТОВЫЕ ТЕХНОЛОГИИ В РАЗВИТИИ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА.	11 Oct 2024	eLIBRARY publications (translations and paraphrases)
[17]	0.17%	0.1%	Assessing Quantum Supremacy: Evaluating Its Potential to Revolutionize Crypt... https://ieeexplore.ieee.org	30 Apr 2025	Search module of IEEE paraphrases
[18]	0.09%	0.09%	Entanglement-Assisted Quantum Networks: Mechanics, Enabling Technologies... https://ieeexplore.ieee.org	11 Jul 2023	IEEE
[19]	0.15%	0.08%	Physical security in the post-quantum era https://link.springer.com	01 Sep 2022	Springer Nature
[20]	0.08%	0.08%	Application solutions of highway freight information systems based on quantu... https://link.springer.com	earlier than 2011	Springer Nature
[21]	0.07%	0.07%	Quantum Secured Internet Transport https://link.springer.com	01 Dec 2020	Springer Nature
[22]	0.06%	0.06%	Quantum Cryptography: Mathematical Modelling and Security Analysis https://ieeexplore.ieee.org	10 Oct 2023	IEEE

[23]	0.06%	0.06%	Quantum permutation pad for universal quantum-safe cryptography https://link.springer.com	earlier than 2011	Springer Nature
[24]	0.32%	0%	blackbook pla	23 Apr 2024	Institutes Unity collection
[25]	0.32%	0%	blackbook Main	22 Apr 2024	Institutes Unity collection
[26]	0.25%	0%	Major_Project_Report_g15ansys (1)	21 Apr 2024	Institutes Unity collection
[27]	0.44%	0%	http://www.ijirset.com/upload/2023/mest-23/MEST%202023_Proceedings.pdf http://ijirset.com	26 Oct 2023	Search module of English Internet paraphrases
[28]	0.18%	0%	Assessment of the level of some selected heavy metals and physicochemical in... https://link.springer.com	01 Apr 2023	Springer Nature
[29]	0.06%	0%	Enhancing Blockchain Security through quantum key distribution and evaluati... https://ieeexplore.ieee.org	04 Apr 2024	IEEE
[30]	0.63%	0%	Квантовое распределение ключей - Quantum key distribution - qaz.wiki https://ru.qaz.wiki	17 Feb 2021	Cross language Russian Internet
[31]	0.16%	0%	Битва за безопасность: как эффективно подготовиться к эпохе постквантов... https://securitylab.ru	01 May 2025	Cross language Russian Internet
[32]	0.2%	0%	MK-974.pdf https://naukaip.ru	19 Oct 2022	Cross language search
[33]	1.49%	0%	Assessment of Spontaneous Combustion of Some Indian Coals Using Differenti... https://core.ac.uk	01 Jan 2016	Search module INTERNET PLUS
[34]	0.09%	0%	A Quantum Mechanical Proof of Insecurity of the Theoretical QKD Protocols https://scirp.org	30 Apr 2025	Search module INTERNET PLUS

ANNEXURE 2

Published Research Paper Copy

Following is the published manuscript in the Journal of Emerging Technologies and Innovative Research under the title 'Quantum-Enhanced Secure Communication via One-Time Pad and Key Distribution'. For further details, kindly refer to the following link: https://doi.org/10.56975/jetir.v12i5.560758

© 2025 JETIR May 2025, Volume 12, Issue 5 www.jetir.org (ISSN-2349-5162)

JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue

JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)

An International Scholarly Open Access, Peer-reviewed, Refereed Journal

Quantum-Enhanced Secure Communication via One-Time Pad and Key Distribution

[1]Princy Kshirsagar, [2]Rutuja Balwade, [3]Deekshant Wankhade, [4]Prof. Jayeshree Mahale

[1]Student, [2]Student, [3]Student, [4]Professor

[1]SOE (ADYPU)

[1] Ajeenkya DY Patil University, Pune, India

Abstract : **As we move further into the era of digital transformation, cloud services are becoming a cornerstone across industries such as healthcare, agriculture, and Industry 4.0. These sectors increasingly rely on cloud environments to collect, process, and store vast amounts of data, often integrated with smart devices. While ensuring high availability and efficiency remains vital, the paramount concern is maintaining data security. This challenge becomes even more pressing in a world where quantum computers pose a serious threat to traditional cryptographic methods. Classical encryption schemes, particularly those relying on computational hardness assumptions, are susceptible to quantum attacks. This paper proposes a solution by combining the theoretically unbreakable One-Time Pad (OTP) encryption with quantum-safe key exchange protocols. Through the integration of Quantum Key Distribution (QKD) and post-quantum cryptographic techniques, we outline a robust framework designed to secure communication in the coming quantum era.**

Index Terms **– QKD, Cloud services, Cryptography, Quantum Computing.**

I. INTRODUCTION

The hastiest advancement in quantum computing puts at risk the traditional foundational methods of cybersecurity infrastructure. Security mechanisms that are quantum-resistant are imperative alongside the impending threats that Shor's algorithm poses to RSA and ECC encryption by factoring large numbers rapidly, as well as Grover's algorithm which accelerates brute force attacks. Quantum computing takes advantage of the principles of quantum mechanics. It utilizes a qubit which can inhabit the state of superposition where it is 0 and 1 at the same time as well as entanglement which allows one qubit's state to be connected to another, regardless of how far apart they are. Our goal is to advance protocols in order to defend against these threats, and lay a strong foundation for quantum-proof communication. We present a definitive answer through the application of One-Time Pad with BB84 Quantum Key Distribution (QKD) protocol. The One-Time Pad is theoretically secure if it is used correctly — meaning a truly random key of equal length to the message and used just once. The cryptographic challenge lies in sharing the keys securely. This is where BB84 protocol comes in, utilizing quantum superposition and entanglement. Merely trying to eavesdrop on the key exchange would disrupt the quantum states, which will signal the communicating parties.

II. BACKGROUND

2.1 Quantum Computing Threats

Quantum computing will create significant security problems by breaking the RSA and ECC methods of encryption if they are indeed developed, which could undermine data privacy as well as PKI (Public Key Infrastructure) and digital signatures. This threatens blockchain, cryptocurrencies, and secure communications techniques with wide repercussions in areas such as national security, business competition secrets, etc. To mitigate those risks requires the development and use of quantum-resistant cryptographic algorithms, international cooperation at an unprecedented scale, as well as significant funding for research done so far in security biosecurity resilience program priorities (planetary cyber- physical systems) enriched with greater public awareness-raising capacity.[5]

2.2 AWS Braket

AWS Braket is a managed quantum computing service by Amazon Web Services, offering access to quantum computers and simulators from providers like D-Wave, IonQ, and Rigetti. It supports hybrid algorithms that combine classical and quantum computing, integrates with other AWS services, and provides SDKs and tools for developing quantum programs. Key use cases include optimization problems, machine learning, cryptography, and material science. Users can start by creating an AWS account, accessing the Braket console, developing quantum programs using the Braket SDK, and running them on quantum hardware or simulators, with results monitored and stored using AWS services.[23]

2.3 One- Time Pad (OTP)

One-time pad is a secure key to protect classified information also called Vernam cipher. This technique proposed by Frank Miller and Gilbert Vernam. In this technique the length of secret key (pad) and plaintext message is equal. Previously OTP is used

© 2025 JETIR May 2025, Volume 12, Issue 5 www.jetir.org (ISSN-2349-5162)

only once and random. One-time-pad quantum key cannot be copied, or eaves rapped. But in quantum era, random OTP can be use repeatedly as long as there is no eavesdropped. An OTP needs a key that is truly random, at least as long as the message is used only once.[6]
Alice and Bob are secret agents who wish to communicate a message to each other using a one-time pad. They meet in person to agree on a random key "XMCKL" to be used once. Alice encrypts the message. "HELLO" by changing the letters into number values, adding the key numbers, and obtaining the result "EQNVZ," which she sends to Bob. Bob decrypts "EQNVZ" by subtracting the key numbers from the ciphertext to obtain the original message "HELLO.". Given that the key is random, secret, and used only once, this process will assure perfect secrecy.[6]

2.4 Quantum Noise

One application of quantum noise, or quantum randomness, is the generation of keys for a one-time pad encryption scheme by the intrinsic indeterminacy of quantum processes for true randomness. A quantum random number generator generates a random binary sequence from quantum phenomena, such as the measurement of photon polarization. It is this sequence that makes it perfect secrecy if each bit of the plaintext is exactly X-ORed with the key bit to get ciphertext. This very key is used in decrypting the same data, just by simple reversal of the XOR operation. The use of quantum noise sources for OTP keys combines the absolute security of the one-time pad with the real, true randomness brought about by quantum indeterminacy.[7] Nevertheless, the creation of some form of distribution method for this might be inefficient. Quantum key distribution protocols, among which is BB84, reduce this problem.[24]

III. Related Work

3.1Quantum key Distribution (QKD)

Quantum Key Distribution uses the laws of quantum physics to establish safe keys. Some of the most famous QKD protocols are BB84 Protocol: Andrew Bennett and Gilles Brassard proposed this quantum protocol in 1984. If someone tries to eavesdrop, the quantum states change and it is plain that somebody has been listening. E91 Protocol - Quantum entanglement proposed by Ekert in 1991. The entangled states help to detect any measurement by an eavesdropper. [8]

3.1.1 Key Exchange Protocols with QKD

This section of the research paper delves into two pioneering QKD protocols: BB84 and E91, both of which illustrate the unique capabilities and challenges of quantum cryptography. BB84's reliance on polarization states and Heisenberg's Uncertainly Principle provides a practical and well-understood method of key- distribution. In contrast, the E91 protocol's use of entanglement and Bell's theorem offers a more theoretically robust approach with greater implementation challenges.

3.1.1.1 BB84 Protocol

They will have to generate some random key: Alice and Bob achieve it using BB84, *K* K The nature of the protocol makes sure that all forms of eavesdropping are discovered

Key Verification: Post keys generation, Alice and Bob deploy a verification step to hold the security of each of their key [8].

3.2 Hash-Based Cryptography

Hash-based cryptography utilizes cryptographic hash functions to construct secure digital signatures and other primitives. The Lamport signature scheme is a notable example of a one-time signature scheme. Hash- based cryptography is valued for its strong security proofs and quantum resistance.[11] Nonetheless, it faces challenges such as large key and signature sizes and limited scalability, especially for schemes like the Merkle-Winternitz OTS.

IV. Methodology

4.1 Existing System

- Most cryptographic systems are based on PRNGs that generate keys and other cryptographic parameters. They are not truly random but deterministic; however, they are designed with the goal of providing an approximation of randomness good enough for all practical purposes.

- It means that pseudo-random key generation is applied to most systems requiring secure encryption. This includes symmetric encryption, for example, AES; public key infrastructure, for example, RSA; VPNs, for example, IPsec and SSL/TLS; wireless security, for example, WPA2; disk encryption, and BitLocker. Other examples include secure messaging, for instance, Signal Protocol; two-factor authentication, like TOTP; cloud security, for example, AWS KMS; blockchain and cryptocurrencies, particularly wallet key generation; and lastly, in secure software development specifically code signing. Therefore, these systems are dependent upon PRNGs to generate keys that will enable data and communications confidentiality, integrity, and authenticity. [21]

- The limitations to PRNGs, therefore, are in their determinism, dependency on a seed that is expected to be secure and unpredictable, and the finiteness of the period that allows repetitions of the sequence. Bias can also be present in the output, and attacks are possible, particularly if either the algorithm or seed is compromised. Moreover, PRNGs do not produce real randomness; it is less appropriate in high-security applications, where one would want either a cryptographically safe pseudo-random number generator or a real non-deterministic random number generator.

© 2025 JETIR May 2025, Volume 12, Issue 5 www.jetir.org (ISSN-2349-5162)

4.2 Security Flaws

4.2.1 DUHK Attack

- DUHK (Don't Use Hard-coded Keys) assault on WPA2, where hardware sellers have utilized a hardcoded seed key for ANSI X9.31 RNG algorithm [19], expressing "an aggressor can constraining decode information to find the rest of the encryption parameters and derive the master encryption key used to secure web sessions or virtual private network (VPN) associations.

4.2.2 Japanese PURPLE Cipher Machine

• One well-known case is that during the Second World War, Japan had used a cipher machine for diplomatic communications, which the United States was able to break and read its messages; probably mostly since the "key values" used were insufficiently random. [18]

4.3 Proposed Experiment Framework

- We give an entirely different framework, one that consists of the following components: random key generation using AWS Braket, one-time pad using ANUQRNG as a third-party alternative for true random number generation which will be then used as a key encryption, and BB84 protocol for secure key distribution. This framework combines quantum computing with classical cryptographic techniques to help improve the security of the outcome: a robust quantum platform for the generation of perfectly random keys, a one-time pad enabling perfect secrecy and hence unbreakable encryption, and BB84 for secure key exchange and detecting any eavesdropping attempts due to the peculiarities of quantum principles.

4.3.1 Random Number Generation

- AWS Braket is the quantum computing platform from Amazon Web Services that enables the design, testing, and running of quantum algorithms on a variety of quantum processors, including those based on gate-based quantum computing. It gives access to quantum computers by different vendors and simulators to explore quantum computing concepts and develop quantum algorithms.[24] AWS Bracket uses noise- based randomness. In the context of quantum computing, "noise" may refer to the basic uncertainty in the measurement of quantum mechanics. This in turn can be used as a source of randomness in generating cryptographic keys and would be fundamentally different from classical pseudo-random number generation.

4.3.2 Generating Quantum Circuits with a Hardware Circuit

- AWS Braket enables the construction of quantum circuits that run on a hardware quantum processor. One might
- design two different quantum circuits, each processing the qubits in some distinct fashion. These circuits could be created to produce a pair of quantum states that are weak or poor in some sense, and the aim is to enhance or "amplify" the result into a more useful or stronger quantum state.

4.3.3 Designing Two Quantum Circuits:

- Circuit 1: This could be a simple quantum circuit that initializes qubits into a superposition state. For example, applying a Hadamard gate to each qubit will create a superposition where each qubit has an equal probability of being in state $|0\rangle$ or $|1\rangle$.

- Circuit 2: This circuit might apply additional gates, such as controlled-NOT (CNOT) gates or phase gates, to entangle the qubits or introduce specific correlations between them.

- These two circuits generate a "weak" string of qubits—a quantum state that has not yet reached its full potential in terms of coherence, entanglement, or information content.

4.3.4 Strengthening the Weak String with a Toeplitz Matrix

- One of the common techniques to convert this weak string of qubits into a "strong" string is by a Toeplitz matrix. The Toeplitz matrix is a structured matrix in which each diagonal descending from left to right is constant; it can be used in quantum error correction processes and randomness extraction.

- Toeplitz Matrix Randomness Extraction: This technique extracts good quality randomness from a weak quantum string. A Toeplitz matrix, multiplied by a weak qubit string, "spreads out" the randomness in it, making the resulting qubit string stronger; it has some properties much closer to cryptographic applications and thus closer to being a truly random string. The Toeplitz matrix could also be part of a quantum error correction scheme that provides an enhancement of the fidelity of the quantum state, in a way that assures protection from noise and potential errors on the qubit string.

© 2025 JETIR May 2025, Volume 12, Issue 5 www.jetir.org (ISSN-2349-5162)

- Since generating keys on AWS Braket can be costly, we explored alternative options and utilized the ANUQRNG as a more economical third-party solution for true random number generation which will then be used as a key for the encryption of the message.

4.4 ANUQRNG

- The Australian National University Quantum Random Number Generator realizes the real random numbers based on the principle of quantum vacuum fluctuations, one of the fundamental quantum processes. Different from pseudo random number generators, the random light intensity is detected with photodiodes, which truly offers its real randomness in the ANUQRNG. Hence, this device is suited for the purposes of cryptography, scientific research, and those demanding premier-quality randomness. Today, these numbers can be found online and are quite vital for the purpose of ensuring security and guaranteeing correctness in several digital and computational systems.[22]

- By doing so with ANUQRNG, we remove the limitation restricted in AWS Braket on the number of keys to be generated. ANUQRNG provides a continuous and cost-effective source for the production of a supply of true random numbers, underpinning an unlimited quantity of possible symmetric encryption keys. This improves the scalability and flexibility of secure communication systems, ensuring that key generation is not constrained by any computational or resource limits that might previously have been encountered with quantum computing platforms like AWS Braket.

4.5 One-time Pad

- The one-time pad is an encryption method that achieves perfect secrecy by using a truly random key that is as long as the message and used only once. Each bit of the plaintext is combined with the corresponding bit of the key using XOR or modular addition to produce ciphertext, which can be decrypted by reversing the process with the same key. While it offers unbreakable security if the key is random, secret, and used only once, its practical challenges include the difficulty of key distribution and management, making it less practical for most applications compared to other encryption methods.[6]

- We have used HMAC or Keyed-Hashing for Message Authentication, which will enhance your secure transmissions and provide data integrity and message authenticity through hash functions and a secret key. HMAC verifications prevent tampered data and confirm the message source within protocols like FTPS, SFTP, and HTTP

4.6 HMAC

- Data integrity checks are integrally linked with secure communications. They allow parties that communicate with each other to verify the integrity and authenticity of messages they receive. In secure file transfer protocols such as FTPS, SFTP, and HTTPS, data integrity/message authentication is attained via a mechanism called HMAC—Hash-based message authentication code.[25]

4.7 Quantum Key Distribution

- The key distribution is done by using the BB84 Protocol, the BB84 protocol details quantum key distribution and shares a cryptographic key between two parties: a sender and a receiver. Alice randomly prepares qubits in one of the two possible bases and sends them to Bob, who randomly measures these qubits in his bases. They would then classically compare their bases and would discard any nonmatching pairs. The remaining bits keep as their shared key. Security of BB84 follows from the fact that any

- eavesdropper trying to intercept the qubits would introduce detectable errors due to the disturbance of quantum states.[26] The following is the process of BB84:

  a. Alice generates a random string of bits, and, correspondingly, for each bit, randomly selects a basis in which to encode it.

  b. Alice encodes the bits onto the qubits according to her chosen bases and sends the qubits through a quantum communication channel to Bob's quantum computer.

  c. Bob randomly selects a basis to decode each qubit in. He measures the qubits in his chosen bases.

  d. Alice classically communicates to Bob the choice of the bases she used; she also communicates the values of the first few bits she sent.

© 2025 JETIR May 2025, Volume 12, Issue 5 www.jetir.org (ISSN-2349-5162)

e. Bob measures these first few bits to get an estimate of whether Eve has tapped into their quantum communication channel and intercepted Alice's qubits.

f. If Eve didn't intercept the qubits, they take all of the qubits that they happened to have picked the same polarizations for and use those bits as their key. If Eve did intercept the qubits, they repeat the process all over again. However, there are certain requirements for this protocol to work:

1. A private quantum computer is required both for Alice and Bob.
2. They must be linked by a channel through which qubits can be transmitted. It could be some kind of fibre-optic cable that transmits polarized photons.
3. They must be connected by a classical communication channel (e.g. a telephone cable). As perfect security can never be assumed, it should be assumed that any of these channels will be tapped by Eve the Eavesdropper.

V. Implementation

• Implementing OTP using quantum key distribution (QKD) principles on AWS Braket provides a modern approach to leveraging quantum computing for secure communication. AWS Braket is a fully managed quantum computing service that provides a development environment for building quantum algorithms. AWS Braket enables the simulation and execution of quantum algorithms on various quantum processors, including gate-based and annealing quantum computers. This section outlines the steps to simulate a one- time pad encryption system using AWS Braket, focusing on quantum principles for key generation and secure communication. AWS Braket generate random keys using noise in quantum computers, along with an alternative option of utilizing the ANUQRNG as a more economical third-party solution for true random number generation than AWS braket. Furthermore, we use BB84 protocol for key distribution completing the framework for a secure communication system

5.1 Random Key generation using AWS Braket

- We can design a quantum circuit with entangled state preparation and measurements. You can do this using Braket Python SDK.
- Execute: Optionally, execute the quantum circuits on a Braket state simulator or devices you have access to.
- Analysis of Result: Fetch and analyze the result to create one-time key.

5.2 One-Time Pad Encryption

- It is important that the length of a key should be at least equal to the text which requires encryption. Encryption Process: XOR the plaintext message with one-time key to produce the ciphertext.
- For the decryption process reverses this: the receiver XORs back with the same one-time key to recover
- plaintext.

5.3 Key Distribution using BB84 Encryption and Decryption Process Preparation and Transmission:

Quantum Bits (Qubits): Alice prepares a series of qubits, each in one of four possible polarization states:
0° (|0⟩), 90° (|1⟩), 45° (|+⟩), and 135° (|−⟩). These states are represented in two bases: the rectilinear basis (0° and 90°) and the diagonal basis (45° and 135°). Random choice: Alice chooses the basis randomly for each qubit and transmits the qubits to Bob through a quantum channel. Measurement: Random Initial Basis: Alice randomly selects an encoding basis (rectilinear or diagonal) but refuses to tell Bob which one she used. Measurements: Bob measures the qubits and records what he measured as well as which bases were used. Basis Reconciliation: Public Discussion (bases): Alice and Bob publicly reveal the bases they selected for each qubit (excluding measurement outcomes) via a classical channel Matching Bases - They take results only from the same bases and discard those with different ones. Key Sifting: Raw Key: The identical raw key shared by Alice and Bob is formed with the measurement outcomes matched. Error Correction and Privacy Amplification: During error correction, Alice and Bob use their generated raw keys to correct any errors between their keys due to Quantum Noise or Mismatch at measurement side. Privacy Amplification - They utilize privacy amplification methods to decrease any potential partial information an eavesdropper (Eve) may have acquired, which in turn reduces the long final key into a shorter highly secure one. Encrypting and Decrypting the Key Encryption: And as soon as Alice and Bob are successful in generating the shared secret key via BB84 protocol, then finally Alice can encrypt her message using classical encryption algorithm - here One-Time Pad (OTP). In OTP, Alice XORs each bit of her plaintext with the corresponding bit from collectively agreed key to get ciphertext. Decryption: Bob receives the ciphertext and decrypts it using that exact same shared secret key. In case of OTP, Bob is brute-forcing each bit of ciphertext with each corresponding bit in shared key to obtain original message.

VI. Result

In this Section, we present the results of implementing a quantum safe communication system using a onetime pad combined with BB84 quantum key distribution protocol. The BB84 protocol, combined with a one-time pad, gives a secure and efficient method for the protection of communication systems against quantum computing advances in the future. Future work will focus on optimizations in the efficiency of such protocols and their real-world communication network applications.

6.1 Random Key generation

© 2025 JETIR May 2025, Volume 12, Issue 5 www.jetir.org (ISSN-2349-5162)

We used AWS Braket to generate random key using quantum circuits designed to tap into quantum properties such as superposition and entanglement. Quantum circuits designed to exploit these quantum properties have been created in order to obtain high-quality random bits, which are at the very heart of secure key generation and cryptographic applications.

Figure 1

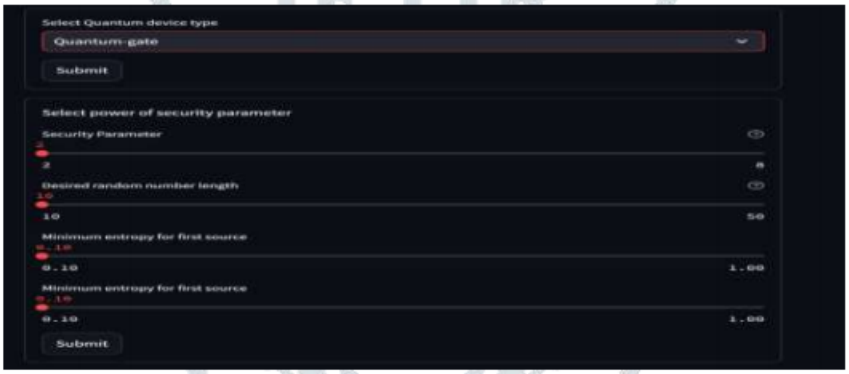


Figure 2.

The Quantum Device type has 2 Quantum Device type

1. Quantum gate – Quantum Computers
2. Classic gate – Local System

© 2025 JETIR May 2025, Volume 12, Issue 5 www.jetir.org (ISSN-2349-5162)

Figure 3.

- **Results** Figure 2: Random bit sequences that were the outcome from the quantum circuits run on AWS Braket. In detail, it generated random bit sequences with a very high degree of unpredictability and entropy. The randomness of the generated sequences was checked by deeper statistical tests, which showed the results to be quite close to the true randomness. This strongly suggests that the quantum-generated numbers are highly suitable for cryptographic use.
- **Analysis** By using AWS Braket in random number generation, the inherent indeterminism of quantum processes is used to obtain a robust randomness source against classical methods. Such created random numbers are safe against classical predictability techniques and even quantum attacks; hence, they are appropriate for encryption keys and many other cryptographic applications. This makes the quantum computing functionality of AWS Braket integrate to present a promising approach in producing true random numbers, so bolstering secure communication systems in the quantum era.

6.2 One-time pad Encryption

We implemented a one-time pad encryption scheme, using ANUQRNG to generate a truly random key. This technique is theoretically unbreakable if the key is perfectly random, the message is never reused, and it is used only once. We encrypted the message into ciphertext by performing bitwise modulo 2 addition between the plaintext and the key, which we could transmit securely to the recipient.

Encryption :

Figure 4.

The Key used is generated by ANUQRNG, then this key is used to encrypt the message along with a message Authentication code.

Decryption:

© 2025 JETIR May 2025, Volume 12, Issue 5 www.jetir.org (ISSN-2349-5162)

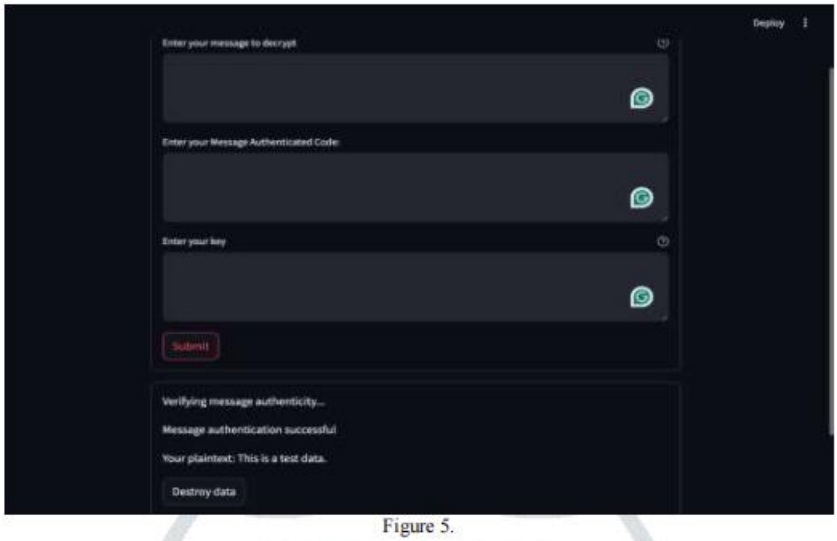


Figure 5.

Results:

As shown in Figure 4, the result of the encryption process was totally incomprehensible random ciphertext; without the key, it could not be deciphered. The decryption process returns the plaintext to its original form, thus evidencing once more the reliability and efficiency of the one-time pad with a securely distributed key.

Analysis:

The one-time pad, along with the key generated by means of ANUQRNG, is resistant to both classical and quantum attacks. In the case of a one-time pad, when the key is never used more than once and never exposed to the communicating parties, it provides unbreakable encryption. Thus, with this principle, highsecurity communications in the quantum era are ensured, and a future-proof solution against emerging threats is provided.

6.3 Key-Exchange Process (BB84)

The basics of quantum mechanics are used by the BB84 protocol for the secure distribution of cryptographic keys between the two parties, normally called Alice and Bob. In this way, any attempt to intercept the key will introduce anomalies detectable by both parties, warning them of an eavesdropper.

Generating random quantum bits for alice which will serve as our keys.

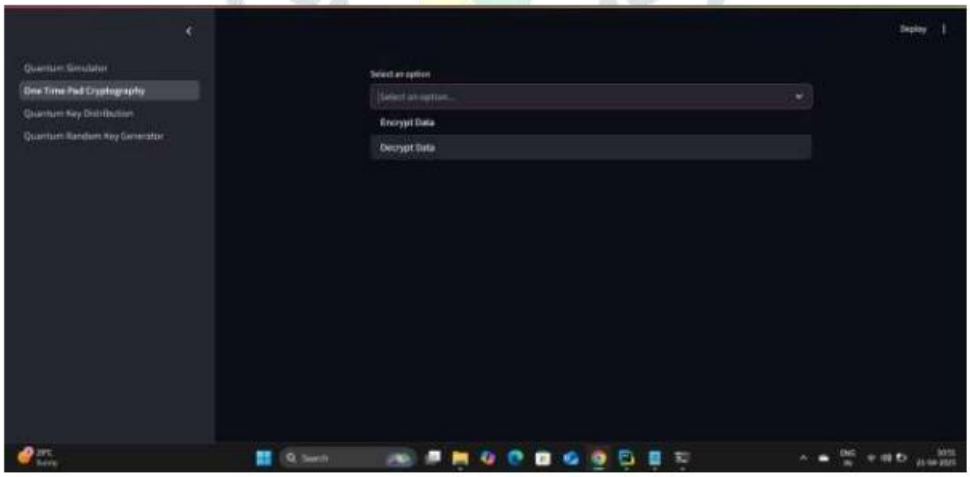


Figure 6

© 2025 JETIR May 2025, Volume 12, Issue 5 www.jetir.org (ISSN-2349-5162)

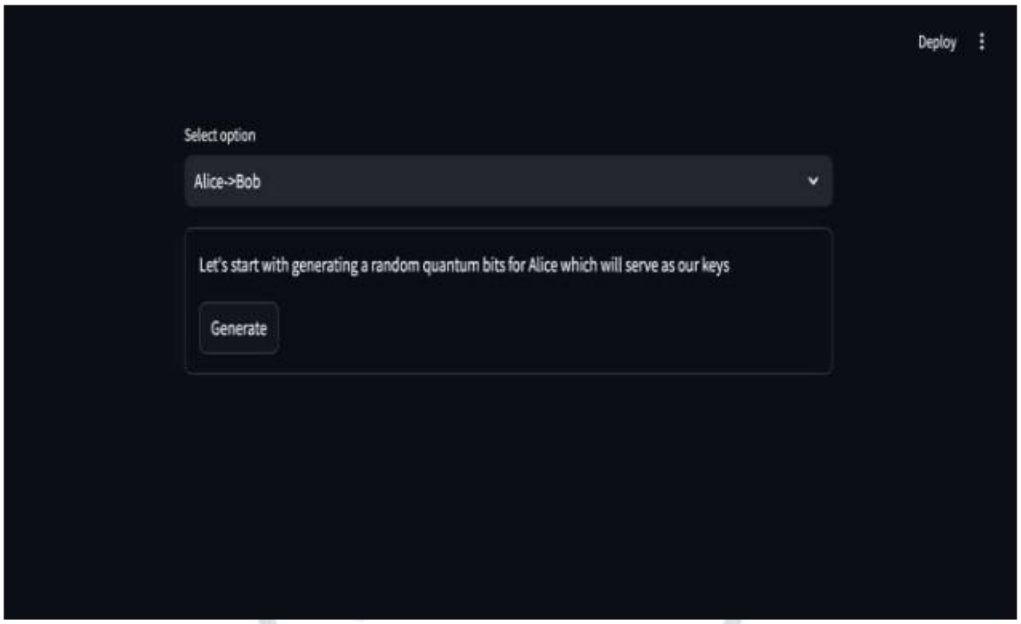


Figure 7.

Alice randomly chooses of each bit (either the Z-basis or the X-basis). She can do this by flipping a coin and mapping each landing (heads or tails) with either one of the basis. But for our use case we are using a random number generator.

The random output bits and bases

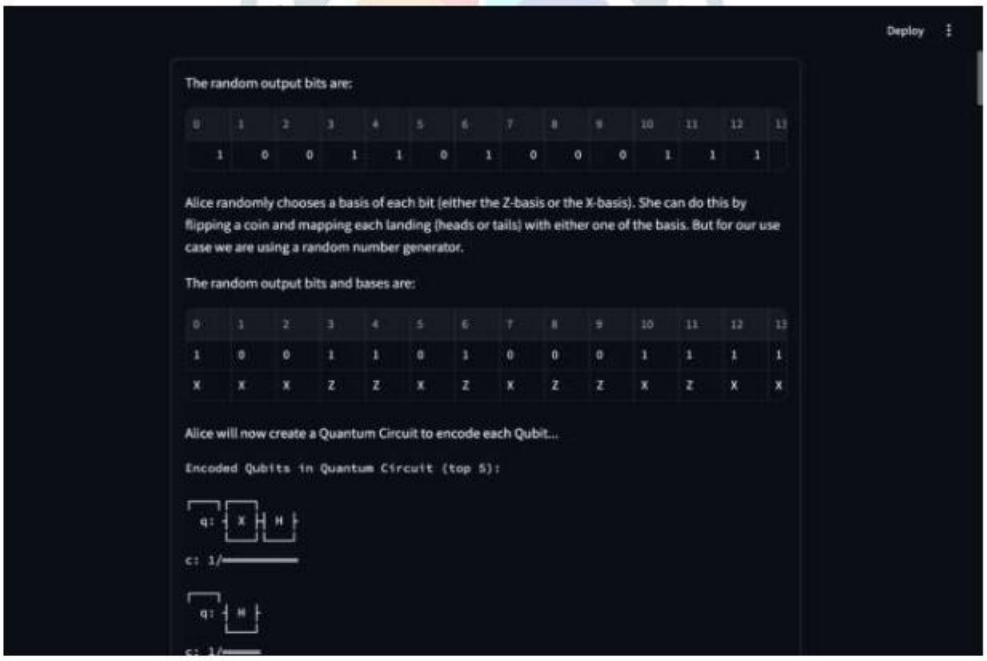


Figure 8 .

Alice will now create a Quantum circuit to encode each Qubit.

© 2025 JETIR May 2025, Volume 12, Issue 5 www.jetir.org (ISSN-2349-5162)

Figure 9 .

Generate Random bases for Bob and then comes the verification part. Alice announces the bases she used over a Classical Channel. Both Bob and Alice only keep the bases they share in common.

The indices of the first 10 bases they share in common are :[4, 6, 7, 10, 11, 15, 16, 18, 19, 20]

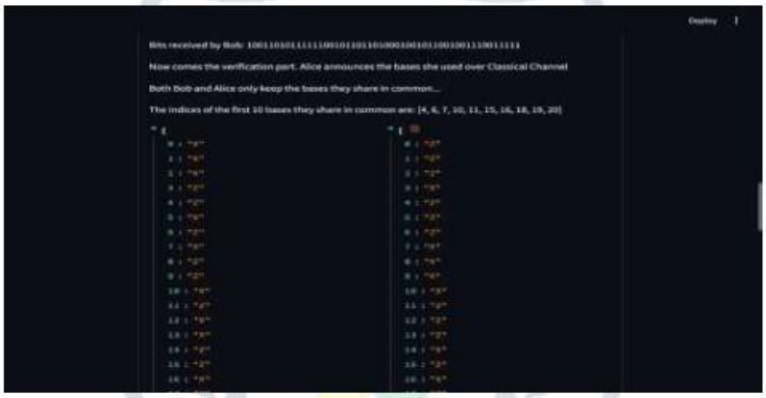


Figure 10 .

Alice and Bobs first 10 bits.

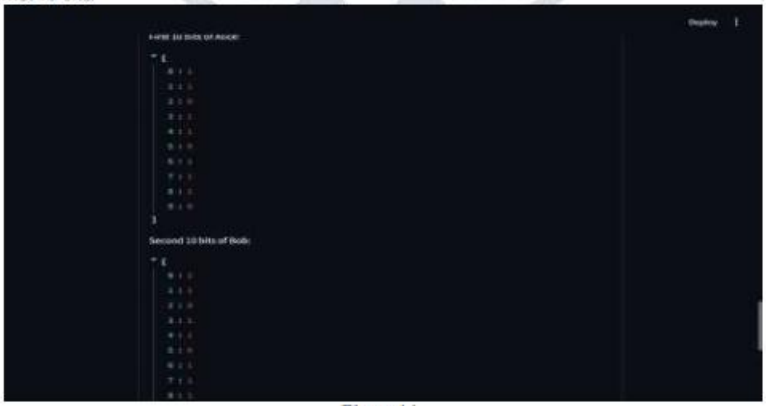


Figure 11.

Alice and Bob Seem to have the same bits. Since they publicly they have to be discarded. The final remaining key with them are:

© 2025 JETIR May 2025, Volume 12, Issue 5 www.jetir.org (ISSN-2349-5162)

Figure 12.

Results:

The successful implementation of the **BB84 Quantum Key Distribution (QKD) protocol** indicates that the key exchange between the two communicating parties—Alice and Bob—was completed without any detectable interference. During the comparison phase, Alice and Bob revealed a subset of their chosen bases and corresponding bits over a classical channel. The absence of discrepancies in these revealed bits strongly suggests that there was no eavesdropping attempt (such as from a third-party adversary like Eve) on the quantum channel.

This seamless comparison phase is critical. In BB84, any attempt by an eavesdropper to intercept and measure the quantum bits (qubits) would inevitably introduce errors due to the **no-cloning theorem** and the **uncertainty principle** in quantum mechanics. These errors would manifest as mismatches in the subset of bits that Alice and Bob compare. The fact that no such anomalies were detected validates the **integrity and confidentiality** of the exchanged key.

As a result, the final key—comprising the bits corresponding to the positions where Alice's and Bob's bases matched—is considered secure and valid. This key is derived exclusively from qubits measured using the same bases and was never publicly disclosed in full, preserving its secrecy.

Thus, the final key serves as:

- **A shared secret** known only to Alice and Bob.
- **A secure foundation** for subsequent encryption using the One-Time Pad.
- **Proof of channel integrity**, as no tampering or measurement disruption was identified.

6.4 Security Features

Because of the NO-Cloning Theorem of Quantum Mechanics, Eve cannot copy the Qubits over from the quantum channel. Thus, Bob will never receive the qubits, making it obvious to him and Alice that their message was intercepted. To prevent them from realizing what has happened, Eve must create her own decoy qubits to send to Bob

Tampered Encoded Qubits (by Eve):

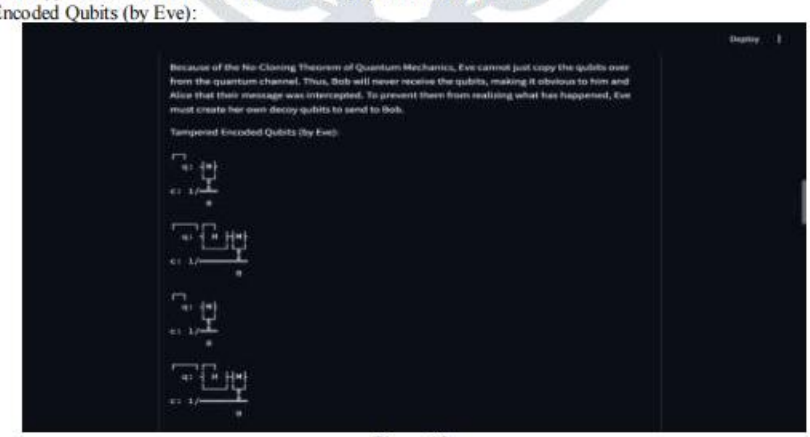


Figure 12.

No-Cloning Theorem: The quantum no-cloning theorem prevents an eavesdropper from creating perfect copies of the transmitted qubits, ensuring that any eavesdropping attempt introduces detectable anomalies.[13]

The Qubits are intercepted by Eve. The bases and bits intercepted by eve:

© 2025 JETIR May 2025, Volume 12, Issue 5 www.jetir.org (ISSN-2349-5162)

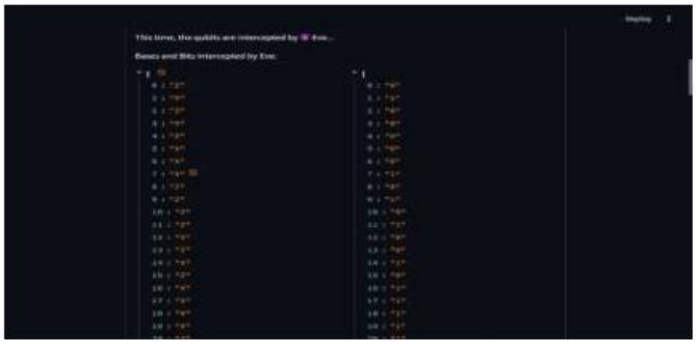


Figure 13.

The tampered qubits now is being received by Bob. Unbeknownst, he carries on with the usual procedure.
The random bases of Bob:

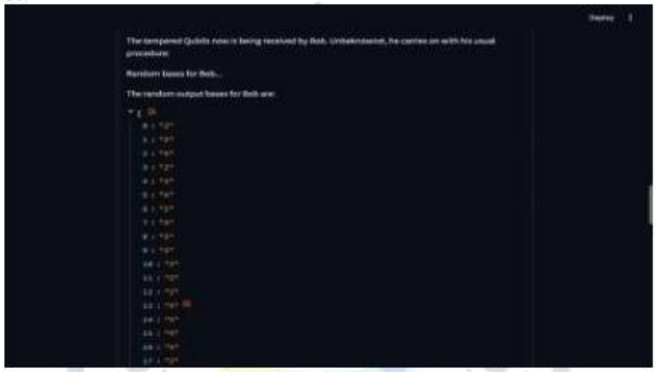


Figure 14.

The bits are received by Bob. Alice announces her bases she chose to encode her qubits in, Bob and Alice again only keep the bits corresponding to their common bases and discard the rest.
The first 10 bits of Alice and Bob:

Figure 15.
At least one bit is different. The remaining key received by Bob and Alice also would not match.

© 2025 JETIR May 2025, Volume 12, Issue 5 www.jetir.org (ISSN-2349-5162)

Figure 16.

Detection of Eavesdropping: Any attempt by Eve to intercept and measure the qubits will disturb their quantum states, introducing detectable errors in the key reconciliation process. If the error rate exceeds a certain threshold, Alice and Bob can infer the presence of an eavesdropper and abort the key generation process.

Security Analysis

Theoretical Security

Security Analysis Combined Approach: The security of this method depends on the strength of the key exchange protocol used. QKD allows anyone to easily verify whether eavesdropping has occurred or not so long as there is no practical means by which a hacker with physical access could possibly defeat the trust link. It prevents the data against quantum attacks with mathematical problems are generic difficulty for Quantum computing, this is known as post-quantum cryptographic techniques.

Practical Security Considerations

Practical Considerations Key Management: Key management and storage must be efficient. Keys should not be stored in Mac or PC; if we can create keys with proper management so that the key does not reuse, else it would take a 10-20 minute to hack every-time when mac is unlocked. You will need special hardware to generate and detect quantum states, which you can regard as some sort of infrastructure. Infrastructure - QKD requires particular equipment for generating and detecting quantum states; this could be quite expensive in practice Scalability: Post-quantum cryptographic algorithms provide much greater scalability than QKD, which will need to be deployed ubiquitously for post quantum resilience.

Integration with Existing Systems

To ensure the effectiveness of new cryptographic systems, they must be compatible with existing infrastructure and protocols, necessitating careful integration and transition strategies for post-quantum algorithms. Usability is crucial, as cryptographic solutions must be user-friendly and not overly complex for end-users and administrators. Key management involves secure storage of cryptographic keys and efficient methods for key distribution, rotation, and revocation. Protection against side-channel attacks, which exploit physical or implementation weaknesses, is essential. Additionally, it is important to consider various adversarial models and attack vectors, including those involving sophisticated quantum capabilities, to assess practical security.

The security analysis of cryptographic systems involves both theoretical and practical considerations. Theoretical security provides a foundation based on mathematical hard problems and formal proofs, ensuring resilience against attacks. Practical security addresses real-world implementation challenges, including efficiency, integration, key management, and protection against various attack vectors. Together, these aspects ensure that cryptographic methods offer robust protection in both theoretical and practical scenarios, paving the way for secure communication in the quantum era. 7.1 CASE STUDY: Organizations Adopting Quantum-Resistant Measures

1. Financial:

JPMorgan Chase:

- Initiatives: Joint development on Quantum Computing and Quantum-safe crypto with IBM.
- Best Practice: PQC algorithms should be tested with pilot projects first, then integrated into transaction systems.
- Lessons Learned: Importance of cross-industry collaboration and incremental implementation to manage risks.[15]

2. Health care:

Overview: Mayo Clinic:

- Initiate: Academia-industry collaboration in research and development for PQC to protect patient data and EHRs.
- Best Practice: Attention to data integrity and data privacy by using quantum-resistant encryption regarding the protection of sensitive health data.
- Lessons Learned: The key to security lies in the adoption of PQC and its continuous updating process for cryptographic protocols.[15]

3. Defense:

Lockheed Martin:

- Initiatives: Quantum computing research and deployment of quantum-resistant cryptography in the defence structure.
- Best Practice: Proper testing of PQC algorithms against a wide array of scenarios to ensure robustness and reliability.
- Lessons Learned: Deployments of PQC in a defense context must be developed in coordination with governments and adhere to emerging standards.[15]

Limitations

This section introduces the barriers of Quantum computing to be applicable in industry as well as the limitations of the study. Quantum Computing works on the concepts of quantum mechanics which use the outstanding factors of 'quantum bits' or qubits to perform a computation. Qubits, on the other hand, can be in a superposition of being both 0 and 1 at once. Qubits additionally can be entangled, such that the state of one qubit relies upon the condition of another regarding how far separated they are. Although theoretically unbreakable, the one-time pad has a number of shortcomings in practice.[14]

Key Creation and Distribution

The length of the key: the key is as long in bits as are all possible messages, making it difficult to generate and distribute large keys. Randomness: The key must be purely random. Getting true random numbers is hard and may need special hardware. The Key Distribution: Once a key is set, the issue now arises on how it should be passed to its recipient without any interception.

Key Management Persistence

Storing big keys in a safe way can be difficult, especially if working on many communications. Disposable:

To use each of the keys once and then throw them away. Reusing keys makes your security wilt.

Synchronized Key Usage: The two end parties i.e. sender and receiver must use the same key simultaneously, synchronization involves coordination

Restrictions on Quantum Key Distribution (QKD)

Although QKD provides the key distribution with ultimate security in principle, it still suffers from a few practical limitations.

- Needs for Infrastructure Specialized Hardware-QKD requires custom quantum hardware designed to prepare, manipulate and detect qubits. This gear can also be expensive, and hard to care for Range Limitations - The distance over which QKD can be implemented is restricted by photon loss and decoherence in optical fibres. Quantum repeaters, an experimental technology for long-distance key distribution
- Implementation Challenges Environmental Sensitivity-Quantum states are very sensitive to environmental disturbances and this can introduce errors which would compromise the security of key exchange.
- Key-Optimized Error Correction: QKD needs secure error correction and privacy amplification protocols to correct transmission errors.

Cost

Can be expensive to implement if the underlying technology and related infrastructure is not already available, as specialized hardware may need to be installed. Description of Barriers High costs (determines no one), limited usage in daily life situations. Requirement for new Infrastructure Very few people have the required infrastructure to use a quantum-safe OTP system out of their homes nations.

VII. Conclusion

In this project, we have addressed the urgent need for secure communication methods in the emerging quantum era. By combining One-Time Pad (OTP) encryption with quantum-safe key exchange protocols, we proposed a theoretically sound and highly secure solution against threats posed by the advancement of practical quantum computing technologies. The OTP ensures perfect secrecy when combined with a securely shared key, and the key distribution via Quantum Key Distribution (QKD) offers provable security based on the fundamental laws of quantum mechanics. Moreover, QKD can be further combined with post-quantum cryptographic (PQC) techniques, leading to a hybrid secure communication framework that can serve both classical and quantum processing systems. This integration can significantly enhance the accessibility, robustness, and practical deployment of quantum-secure communication networks.

VIII. Acknowledgment

We would like to thank our **Professor Jayeshree Mahale**, for her patience, supervision, encouragement and passionate sup-port. His knowledge and attention have been an inspiration for keeping our work on track.

We would also like to extend our thanks to our friends for offering us help whenever we had issues and providing us assistance with the resources needed to get this paper complete.

References

[1] O. Grote, A. Ahrens, and C. Benavente-Peces, "Small Quantum-safe Design Approach for Longterm Safety in Cloud Environments," in *Proc. 2021 Int. Conf. Eng. Emerg. Technol. (ICEET)*, Oct. 2021, doi: 10.1109/ICEET53442.2021.9659632.

[2] J. Y. Haw *et al.*, "Maximization of Extractable Randomness in a Quantum Random-Number Generator," *Phys. Rev. Appl.*, vol. 3, no. 5, May 2015, doi: 10.1103/PhysRevApplied.3.054004.

[3] T. Liu *et al.*, "Transfer of quantum entangled states between superconducting qubits and microwave field qubits," *Front. Phys.*, vol. 17, no. 6, Jul. 2022, doi: 10.1007/s11467-022-1166-1.

[4] D. Umar, "Cybersecurity Threats and Mitigation Strategies in the Age of Quantum Computing," *J. Technol. Syst.*, vol. 6, no. 5, pp. 1–14, Aug. 2024, doi: 10.47941/jts.2145.

ANNEXURE 3

Certificate of Publication

In this section, we have shown the Certificate of Publication awarded to us by the Journal of Emerging Technologies and Innovative Research for successfully publishing a research paper titled "Quantum Computing, Cloud technology, cloud security, Quantum Cryptography".

Journal of Emerging Technologies and Innovative Research

An International Open Access Journal Peer-reviewed, Refereed Journal

www.jetir.org | editor@jetir.org An International Scholarly Indexed Journal

Certificate of Publication

The Board of

Journal of Emerging Technologies and Innovative Research (ISSN : 2349-5162)

Is hereby awarding this certificate to

Princy Kshirsagar

In recognition of the publication of the paper entitled

Quantum-Enhanced Secure Communication via One-Time Pad and Key Distribution

Published In JETIR (www.jetir.org) ISSN UGC Approved (Journal No: 63975) & 7.95 Impact Factor

Published in Volume 12 Issue 5 , May-2025 | Date of Publication: 2025-05-05

EDITOR

EDITOR IN CHIEF

JETIR2505045 Research Paper Weblink http://www.jetir.org/view?paper=JETIR2505045 Registration ID : 560758

An International Scholarly Open Access Journal, Peer-Reviewed, Refereed Journal Impact Factor Calculate by Google Scholar and Semantic Scholar | AI-Powered Research Tool, Multidisciplinary, Monthly, Multilanguage Journal Indexing in All Major Database & Metadata, Citation Generator

Journal of Emerging Technologies and Innovative Research
An International Open Access Journal Peer-reviewed, Refereed Journal
www.jetir.org | editor@jetir.org An International Scholarly Indexed Journal

Certificate of Publication

The Board of
Journal of Emerging Technologies and Innovative Research (ISSN : 2349-5162)
Is hereby awarding this certificate to
Rutuja Balwade
In recognition of the publication of the paper entitled
Quantum-Enhanced Secure Communication via One-Time Pad and Key Distribution
Published In JETIR (www.jetir.org) ISSN UGC Approved (Journal No: 63975) & 7.95 Impact Factor
Published in Volume 12 Issue 5 , May-2025 | Date of Publication: 2025-05-05

EDITOR
EDITOR IN CHIEF

JETIR2505045 Research Paper Weblink http://www.jetir.org/view?paper=JETIR2505045 Registration ID : 560758

An International Scholarly Open Access Journal, Peer-Reviewed, Refereed Journal Impact Factor Calculate by Google Scholar and Semantic Scholar | AI-Powered Research Tool, Multidisciplinary, Monthly, Multilanguage Journal Indexing in All Major Database & Metadata, Citation Generator

Journal of Emerging Technologies and Innovative Research
An International Open Access Journal Peer-reviewed, Refereed Journal
www.jetir.org | editor@jetir.org An International Scholarly Indexed Journal

Certificate of Publication

The Board of
Journal of Emerging Technologies and Innovative Research (ISSN : 2349-5162)
Is hereby awarding this certificate to
Deekshant Wankhade
In recognition of the publication of the paper entitled
Quantum-Enhanced Secure Communication via One-Time Pad and Key Distribution
Published In JETIR (www.jetir.org) ISSN UGC Approved (Journal No: 63975) & 7.95 Impact Factor
Published in Volume 12 Issue 5 , May-2025 | Date of Publication: 2025-05-05

EDITOR
EDITOR IN CHIEF

JETIR2505045 Research Paper Weblink http://www.jetir.org/view?paper=JETIR2505045 Registration ID : 560758

An International Scholarly Open Access Journal, Peer-Reviewed, Refereed Journal Impact Factor Calculate by Google Scholar and Semantic Scholar | AI-Powered Research Tool, Multidisciplinary, Monthly, Multilanguage Journal Indexing in All Major Database & Metadata, Citation Generator

ANNEXURE 4

Source Code
Below is the source code for our tool.

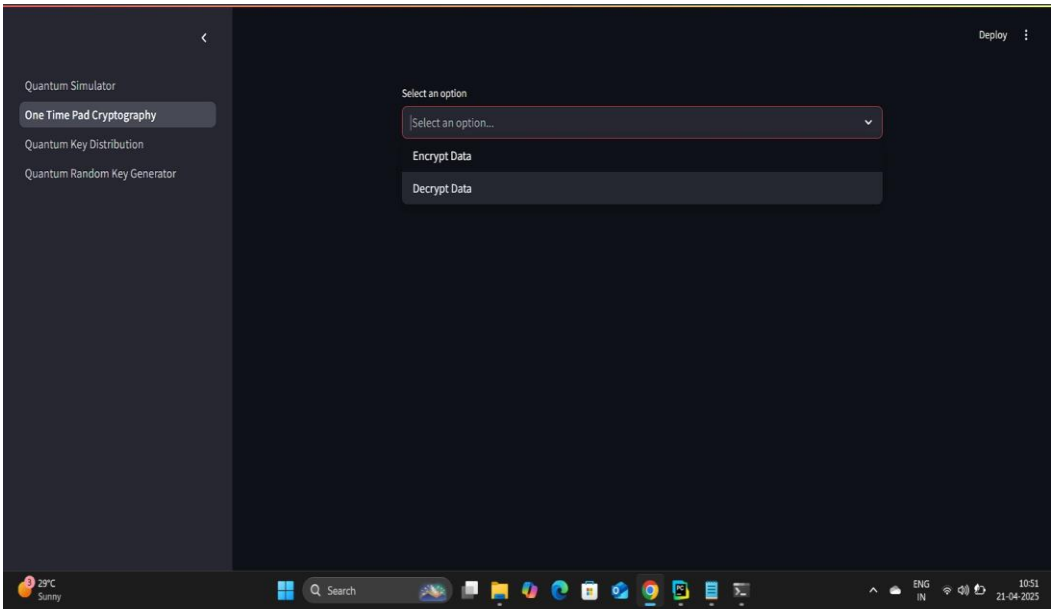
Code for: - Quantum_Simulator

```
import streamlit as st

st.set_page_config(
    page_title="Hello",
    page_icon="👋",
)

st.write("# Welcome to Quantum Cryptography Simulator! 👋")

st.sidebar.success("Select a demo above.")

st.markdown(
    """
    Simulations available:
    1. Random Key Generation
    2. Quantum One Time Pad CryptoGraphy
    3. Quantum Key Distribution
"""
)
```

Code for: - One_Time_Pad_Cryptography

```
import streamlit as st
import time
import numpy as np
import math
import time
from src import one-time pad
from Crypto.Hash import HMAC, SHA512
from base64 import b64decode, b64encode
st.set_page_config(page_title="Quantum Random Key Generation", page_icon=" ")

if 'submitted' not in st.session_state:
    st.session_state.submitted = False


#st.session_state

def record_submitted():
    st.session_state.submitted = True


def reset():
    st.session_state.submitted = False


option = st.selectbox(
    "Select an option",
    ("Encrypt Data", "Decrypt Data"),
    index=None,
    placeholder="Select an option...",
)

if option == "Encrypt Data":
    with st.form("Encrypt Data", clear_on_submit=True):
        reset()
        plaintext = st.text_area(key="plaintext_input", help='Enter your message to encrypt',
                                 label='Enter your message to encrypt. (Must be less than 1024 characters)')
        submitted = st.form_submit_button("Submit", on_click=record_submitted)

    if submitted:
        with st.form("Your encrypted data and Quantum Random Key", clear_on_submit=True):
            reset()
            with st.spinner("Generating Quantum Random Key..."):
                key = one_time_pad.generate_quantum_random_key(len(plaintext))
                #key = '12345'
                time.sleep(1)
            with st.spinner("Encrypting Data and Generating Hash..."):
                ciphertext, key = one_time_pad.encrypt(plaintext, key)
                h = HMAC.new(key.encode(), digestmod=SHA512)
                h.update(plaintext.encode())
                #ciphertext = 'hello'
                time.sleep(2)

            st.write("Your key:", key)
            st.write("Your Message Authentication Code is:", h.hexdigest())
```

```
        st.write("Your ciphertext:", ciphertext)

        submitted = st.form_submit_button("Destroy data", on_click=record_submitted)

if option == "Decrypt Data":
    with st.form("Decrypted data", clear_on_submit=True):
        reset()
        ciphertext = st.text_area(key="ciphertext_input", help='Enter your message to decrypt',
                                  label="Enter your message to decrypt")
        mac = st.text_area("Enter your Message Authenticated Code:")
        key = st.text_area(key="key_input", help='Enter your key', label='Enter your key')
        submitted = st.form_submit_button("Submit", on_click=record_submitted)

    if submitted:
        with st.form("Your decrypted data", clear_on_submit=True):
            reset()
            try:
                with st.spinner("Decrypting Data..."):
                    plaintext = one_time_pad.decrypt(ciphertext, key)
                    # ciphertext = 'decrypted data'
                    time.sleep(2)
                st.write("Verifying message authenticity...")
                h = HMAC.new(key.encode(), digestmod=SHA512)
                h.update(plaintext.encode())
                try:
                    h.hexverify(mac)
                    st.write("Message authentication successful")
                    st.write("Your plaintext:", plaintext)
                except ValueError:
                    st.write("The message or the key is wrong. Authentication failed.")

            except Exception as e:
                st.write("unable to decrypt message due to exception: ", e)

            submitted = st.form_submit_button("Destroy data", on_click=record_submitted)
```



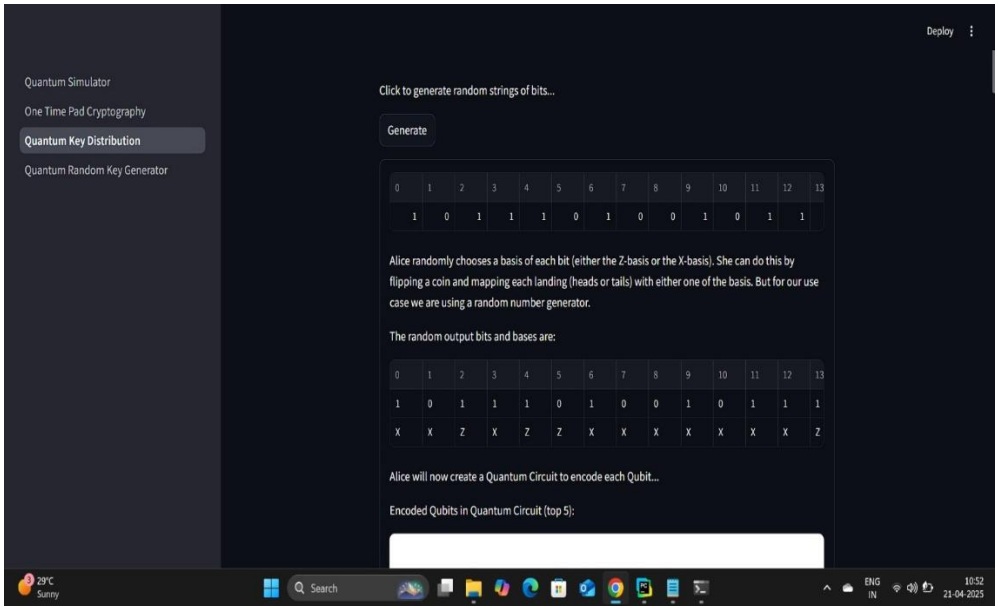
Code for: - Quantum_Key_Distribution

```
import streamlit as st
import time
import numpy as np
import math
import time
from streamlit import components
from src import key_distribution, random_key_generator
from qiskit.visualization import visualize_transition

placeholder = st.empty()
random_bits = None
bases = None
key_length = 50

# st.set_page_config(page_title="Quantum Random Key Generation", page_icon=" ")
send_key = None

if 'submitted' not in st.session_state:
    st.session_state.submitted = False


# st.session_state

def record_submitted():
    st.session_state.submitted = True


def reset():
    st.session_state.submitted = False


def alice_bob(encoded_qubits, alice_bits, alice_bases):
    QUANTUM_CHANNEL = encoded_qubits
    st.write("Let's now generate random bases for Bob...")
    bob_bases = key_distribution.generate_random_bases(key_length)
    bob_bases_list = [i for i in bob_bases]
    st.write("The random output bases for Bob are:", bob_bases_list)
    qubits_received = QUANTUM_CHANNEL
    if st.spinner("Measuring Qubits received through Quantum Channel..."):
        time.sleep(2)
        bob_bits = key_distribution.measure(qubits_received, bob_bases)

    st.write("Bits received by Bob:", bob_bits)

    st.write("Now comes the verification part. Alice announces the bases she used over Classical Channel")

    CLASSICAL_CHANNEL = alice_bases

    st.write("Both Bob and Alice only keep the bases they share in common...")

    # Store the indices of the bases they share in common
    common_bases = [i for i in range(key_length) if CLASSICAL_CHANNEL[i] == bob_bases[i]]
    st.write("The indices of the first 10 bases they share in common are: " + str(common_bases[:10]))
    cols = st.columns(2)
    cols[0].write([i for i in alice_bases])
```

```
  cols[1].write([i for i in bob_bases])

    st.write("They both now exchange their common bases and discard the uncommon ones.")
    bob_bits = [int(bob_bits[index]) for index in common_bases]
    alice_bits = [int(alice_bits[0][index]) for index in common_bases]  # Alice keeps only the bits shared in common
    st.text("Since Alice and Bob are only keeping the bits measured in the bases they shared in common, "
            "they should have the same bits. To make sure this is the case, Alice will announce the first "
            "few bits that she has, and Bob should have the same ones. Of course, if Eve were trying to "
            "eavesdrop, she would also hear these first few bits, so Alice and Bob would have to discard "
            "them as well (after comparing to make sure they're the same as what they expect).")

    st.write("First 10 bits of Alice:", alice_bits[:10])
    st.write("Second 10 bits of Bob:", bob_bits[:10])
    if alice_bits[:10] == bob_bits[:10]:
        st.write("Yep, Alice and Bob seem to have the same bits!")
    else:
        st.write("Uh oh, at least one of the bits is different.")

    st.write("Since they publicly announced their first 10 bits, they have to be discarded.")
    st.write("The final remaining key with both of them are:")
    cols = st.columns(2)
    cols[0].write([i for i in alice_bits[10:]])
    cols[1].write([i for i in bob_bits[10:]])
    submitted = st.form_submit_button("Clear", on_click=record_submitted)


def alice_bob_eve(encoded_qubits, alice_bits, alice_bases):
    QUANTUM_CHANNEL = encoded_qubits
    qubits_intercepted = QUANTUM_CHANNEL
    st.write("This time, the qubits are intercepted by 😈 Eve...")
    eve_bases = key_distribution.generate_random_bases(key_length)  # Generate a random set of bases
    eve_bits = key_distribution.measure(qubits_intercepted, eve_bases)  # Measure the qubits
    st.write("Bases and Bits intercepted by Eve:")
    cols = st.columns(2)
    cols[0].write([i for i in eve_bases])
    cols[1].write([i for i in eve_bits])

    st.write("""Because of the No-Cloning Theorem of Quantum Mechanics, Eve cannot just copy the qubits over
             from the quantum channel. Thus, Bob will never receive the qubits, making it obvious to him and Alice that
             their message was intercepted. To prevent them from realizing what has happened, Eve must create her own
             decoy qubits to send to Bob.""")

    print(eve_bits)
    # Eve encodes her decoy qubits and sends them along the quantum channel
    QUANTUM_CHANNEL, qc = key_distribution.encode(eve_bits, eve_bases)
    st.write("Tampered Encoded Qubits (by Eve):")
    for i in range(0, 5):
        st.write(QUANTUM_CHANNEL[i].draw(output='mpl', scale=0.5))

    st.write("The tampered Qubits now is being received by Bob. Unbeknownst, he carries on with his usual "
             "procedure:")
    st.write("Random bases for Bob...")
    bob_bases = key_distribution.generate_random_bases(key_length)
    bob_bases_list = [i for i in bob_bases]
    st.write("The random output bases for Bob are:", bob_bases_list)
    qubits_received = QUANTUM_CHANNEL
    if st.spinner("Measuring Qubits received through Quantum Channel..."):
```

```
  time.sleep(2)
      bob_bits = key_distribution.measure(qubits_received, bob_bases)

   st.write("Bits received by Bob:", bob_bits)

   st.write("Again Alice announces her bases she chose to encode her qubits in.")
   CLASSICAL_CHANNEL = alice_bases  # Alice tells Bob which bases she used

   # Store the indices of the bases they share in common
   st.write("Bob and Alice again only keep the bits corresponding to their common bases and discard the rest.")
   common_bases = [i for i in range(key_length) if CLASSICAL_CHANNEL[i] == bob_bases[i]]

   CLASSICAL_CHANNEL = common_bases  # Bob tells Alice which bases they shared in common
   bob_bits = [int(bob_bits[index]) for index in common_bases]
   alice_bits = [int(alice_bits[0][index]) for index in common_bases]  # Alice keeps only bits shared in common

   st.write("Now to verify, they both share their first 3 bits:")
   st.write("First 10 bits of Alice:", alice_bits[:10])
   st.write("Second 10 bits of Bob:", bob_bits[:10])
   if alice_bits[:10] == bob_bits[:10]:
      st.write("Yep, Alice and Bob seem to have the same bits!")
   else:
      st.write("Uh oh, at least one of the bits is different.")
   st.write("As you can see the keys remaining key received by Bob and Alice also wouldn't match:")
   cols = st.columns(2)
   cols[0].write([i for i in alice_bits[10:]])
   cols[1].write([i for i in bob_bits[10:]])
   submitted = st.form_submit_button("Clear", on_click=record_submitted)


def main():
   st.write("Click to generate random strings of bits...")
   submitted = st.button("Generate")
   with st.form("Key generation:"):
      random_key_generator.setup_devices('classical_gate')
      power = 10
      eps = 10 ** (-power)
      m = key_length
      n = math.floor((m - 1 - 2 * math.log2(eps)) / (1 + 1 - 1))
      array_1, array_2 = random_key_generator.create_quantum_circuit(n)
      alice_bits = random_key_generator.toeplitz_constructor(array_1, array_2, m, n)
      st.write(alice_bits)
      st.write("""Alice randomly chooses a basis of each bit (either the Z-basis or the X-basis). She can do this by flipping
            a coin and mapping each landing (heads or tails) with either one of the basis. But for our use case we are
using a random
            number generator.""")
      if st.spinner("Generating random bases for our random bit..."):
         time.sleep(2)
         bases = key_distribution.generate_random_bases(key_length)

      bases_list = [i for i in bases]
      st.write("The random output bits and bases are:", np.vstack((alice_bits, bases_list)))
      st.write("""Alice will now create a Quantum Circuit to encode each Qubit...""")
      if st.spinner("Encoding Qubit and creating Quantum Circuit"):
         time.sleep(1)
         encoded_qubits, qc = key_distribution.encode(alice_bits[0], bases)
      st.text("Encoded Qubits in Quantum Circuit (top 5):")
```

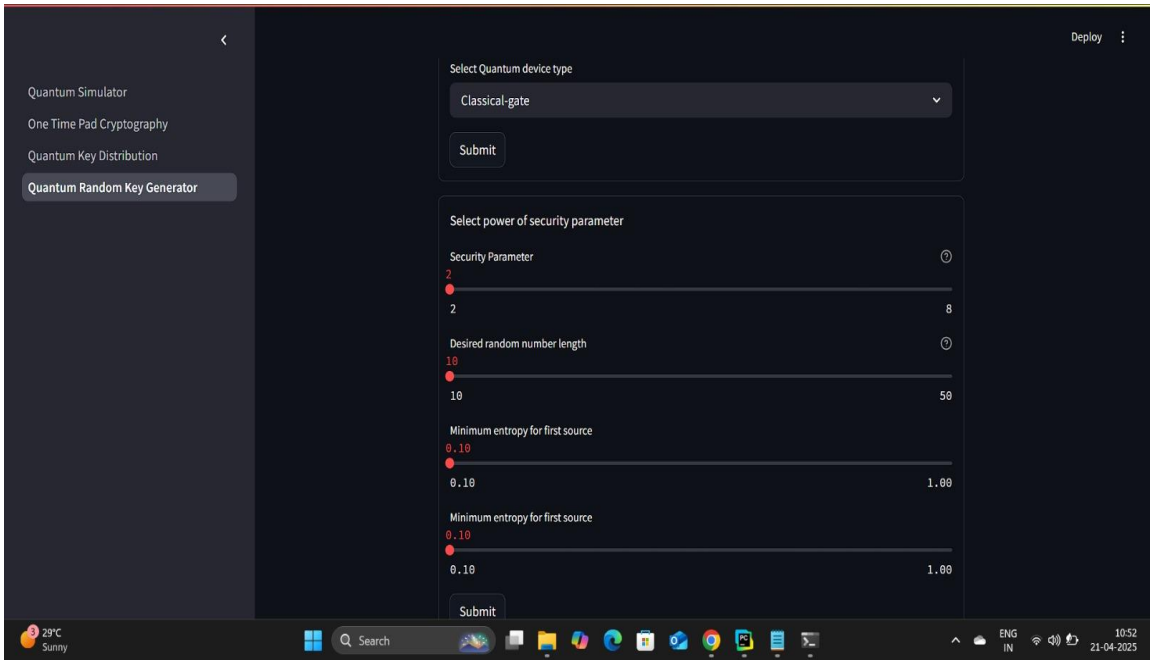
```
    for i in range(0, 5):
            st.write(encoded_qubits[i].draw(output='mpl', scale=0.5))
        st.write("Activate to let Eve intercept...")
        on = st.toggle("Intercept")
        st.write("Click to send the key")
        send = st.form_submit_button("Send")
        if send and on:
            alice_bob_eve(encoded_qubits, alice_bits, bases)
        elif send:
            alice_bob(encoded_qubits, alice_bits, bases)


main()
```



Code for: - Quantum_Random_Key_Generator

```
import streamlit as st
import time
import numpy as np
import math
import time
from src import random_key_generator

st.set_page_config(page_title="Quantum Random Key Generation", page_icon=" ")

if 'submitted' not in st.session_state:
    st.session_state.submitted = False

#st.session_state



def record_submitted():
    st.session_state.submitted = True
```

```
def reset():
    st.session_state.submitted = False


with st.form("Select device type", clear_on_submit=True):

    option = st.selectbox(
        "Select Quantum device type",
        ('Classical-gate', 'Quantum-gate')
    )
    print(option)
    if option == 'Classical-gate':
        device, simulator = random_key_generator.setup_devices('classical_gate')
    elif option == 'Quantum-gate':
        device, rigetti, ionq = random_key_generator.setup_devices('quantum_gate')

    submitted = st.form_submit_button("Submit", on_click=record_submitted)


with st.form("Configuration", clear_on_submit=True):
    reset()
    st.write("Select power of security parameter")
    power = st.slider("Security Parameter", 2, 8, help="Security parameter is any randomly picked numeber.",
key='power_slider')
    eps = 10**(-power)
    m = st.slider("Desired random number length", 10, 50, key='random_number_length',
                  help='The length of random numbers. Due to hardware limitations, the max length is set to 50.')
    k_one = st.slider("Minimum entropy for first source", 0.1, 1.0, key='k_1')
    k_two = st.slider("Minimum entropy for first source", 0.1, 1.0, key='k_2')
    n = math.floor((m-1-2*math.log2(eps))/(k_one+k_two-1))
    # Every form must have a submit button.
    submitted = st.form_submit_button("Submit", on_click=record_submitted)

if submitted:
    array_1, array_2 = random_key_generator.create_quantum_circuit(n)
    # Uncomment to run on on_demand simulator or quantum gate
    # Commented because running on actual simulator takes as a lot of time and running it live may not be feasible.
    array_1, array_2 = random_key_generator.create_quantum_task('on_demand', array_1, array_2, n)
    reset()
    with st.form("Generating Quantum Circuit", clear_on_submit=True):
        st.write("Weakly random strings of bits of size:", array_1.shape)
        st.write("String 1:", str(array_1))
        st.write("String 2:", str(array_2))
        with st.spinner("Initializing toeplitz constructor"):
            res = random_key_generator.toeplitz_constructor(array_1, array_2, m, n)
            time.sleep(3)
        st.write(f"The {m} random output bits are:\n{res}.")
        st.form_submit_button("Clear", on_click=record_submitted)
```


Deploy
Quantum Simulator
One Time Pad Cryptography
Quantum Key Distribution
Quantum Random Key Generator
Select Quantum device type
Classical-gate
Submit
Select power of security parameter
Security Parameter
2
2
8
Desired random number length
10
10
50
Minimum entropy for first source
0.10
0.10
1.00
Minimum entropy for first source
0.10
0.10
1.00
Submit
29°C
Sunny
Search
ENG
IN
10:52
21-04-2025