International Journal of Computing and Digital Systems
ISSN (2210-142X)
Int. J. Com. Dig. Sys. 15, No.1 (Jan-24)

http://dx.doi.org/10.12785/ijcds/150122

Enhanced Approach To Generate One Time Password (OTP) Using Quantum True Random Number Generator (QTRNG)

Riddhi B. Prajapati 1[1] and Shailesh D. Panchal 2[2]

[1,2]*Graduate School of Engineering and Technology - Gujarat Technological University, Ahmedabad, Gujarat, India, 382424*

Received 17 May. 2023, Revised 2 Jan. 2024, Accepted 6 Jan. 2024, Published 15 Jan. 2024

Abstract: In secure IT systems, a One Time Password (OTP) is used. They can only be used once for a transaction or a login session. It is usually used for multi-factor authentication and is one of the security services based on human responses. In the field of cryptography, the creation of pseudo-random bitstreams is similar to how one-time passwords (OTPs) work.

In modern computers, the security of cryptographic procedures is greatly enhanced by the use of random numbers. The use of a Quantum True Random Number Generator (QTRNG) makes it possible to replace periodic sequences that appear random with real random data. A QTRNG is used in this research on a real Quantum Computational Device (QCD) in a local environment. The IBM Quantum Experience Qiskit platform is used to build a random number generator. Qiskit is an open source platform that provides users to work with actual quantum devices for simulating quantum algorithms, different gates and circuits on IBM Quantum Experience or on simulators. The random number is investigated with different qubits (quantum bits) to generate random bits that can be used for One Time Password Generation.

Keywords: Hadamard Gate, NIST Statistical Test, OTP, Qiskit, QTRNG

1. Introduction

In today's digitally interconnected environment, the demand for secure communication has reached unprecedented levels due to the increasing exchange of sensitive information between devices. Due to the growing sharing of private data between devices in today's digitally connected world, demand for secure communication has risen to previously unheard-of heights. Strong security measures are now more important than ever due to the expansion of the digital ecosystem and the increased popularity of private data exchange. The expanding importance of technologies like blockchain, big data, and edge computing further emphasises this necessity.

Protecting confidential client information and controlling the ongoing expansion of data and processing power are the main challenges. In our technology-driven era, managing enormous data repositories has grown in difficulty [1].

This research takes on this challenge by investigating the integration of Quantum True Random Number Generators (QTRNG) into secure IT systems, particularly for One Time Password (OTP) generation. By taking advantage of quantum computing's unique features, we want to increase the security of cryptographic operations and swap out periodic sequences with really random data.

The main goals are to evaluate the viability and effectiveness of creating a random number generator using a Quantum Computational Device (QCD) and the IBM Quantum Experience Qiskit platform. Our goal is to use quantum bits' (qubits') capability to create OTPs with unmatched security, advancing secure communication in a world that is becoming more linked.

A. One-Time Password (OTP)

Passwords are now a widely used form of user authentication on the internet in today's society. Text passwords continue to be the most regularly utilised option for web authentication even though they have been around for a while. However, security issues have been linked to the use of passwords. Replay attacks, reusability attacks, and man-in-the-middle attacks are just a few of the security threats that have been used throughout the years to steal sensitive data from computers and trick people into visiting fraudulent websites. Password theft has increased as a result.

As a result, many businesses and organizations are shifting away from the old static password method and toward new options. As a result, many companies and organisations are abandoning the conventional static password method

E-mail address: to.riddhi@gmail.com, sdpanchal@gtu.edu.in

and adopting other ones. Static passwords are extremely vulnerable since they can be easily stolen and used against the password owner by adversaries through a variety of techniques (such as replay attacks, reusability attacks, man-in-the-middle attacks, etc.). OTP systems have become increasingly popular as a result of these worries. In order to meet the demand for increased security, these systems generate passwords that are only valid for a single session [2].

Users can access a network or service using one-time password (OTP) solutions, a form of authentication technique that only allows for the usage of a password once. The most common yet most vulnerable authentication method is the static password, on the other hand.

By preventing compromised username/password combinations from being used again, OTP functionality acts as a deterrent against certain types of identity theft. The one-time password changes after every login, unlike the user's login name, which doesn't change. The security of corporate networks, e-banking, and other systems that store sensitive data is significantly improved by this strong authentication approach. Despite the enhanced security provided by OTP, the vast majority of business networks, e-commerce platforms, and online communities continue to just employ a username and static password for login and to gain access to private and sensitive data.

B. Quantum Computing

In order perform computations, quantum computing makes use of the special properties of quantum states, such as superposition, interference, and entanglement. The tools used to perform quantum processes are known as quantum computers. Larger versions of quantum computers are anticipated to handle specific computational difficulties, like integer factorization, with significantly higher efficiency than classical computers, despite the fact that present quantum computers may not yet beat conventional computers in practical applications due to their modest size [1]. The study of quantum information is the main objective of the discipline of quantum computing.

Quantum circuits are the most common type of quantum computation, while there are other forms as well. Quantum Turing machines, quantum annealing, and adiabatic quantum processing are additional paradigms in quantum computing. These models are primarily based on the idea of a quantum bit, or "qubit," which resembles classical bits but differs in important ways. Qubits can exist in a superposition of both quantum states, allowing them to be in a quantum state of either 1 or 0 simultaneously, unlike classical bits which can only exist in states of 0 or 1. A qubit, however, will consistently provide either the value 0 or 1 upon measurement. The quantum state of the qubit shortly prior to the measurement determines the possibility of getting a particular outcome [2]. Using continuous variables instead of qubits is an alternate method for quantum computation.

A quantum computer is capable of solving any computational problem that a classical computer can handle. Theoretically, given enough time, any problem that a quantum computer can handle can be solved by a classical computer. In essence, the Church-Turing thesis is upheld by quantum computers. This implies that quantum algorithms for some problems are far faster than the corresponding classical methods we now know, even though quantum computers don't offer any additional advantages in terms of what can be calculated compared to conventional computers. It is important to remember that "quantum supremacy" refers to the idea that quantum computers vastly outperform traditional computers in solving problems within a reasonable amount of time. Quantum complexity theory is the study of the computational difficulties posed by quantum computers. [2], [3]

C. Random Number Generator (RNG)

A random number series is made up of liberated numbers that have no relation to one another. It is difficult to create something unpredictable with a computer. The RNG outputs classify data based on either digital or physical sources. We must therefore journey into the physical world and draw random numbers from there in order to measure anything that behaves randomly [1]. Accepting the idea of randomness leads us to think about developing random number generators. These generators can be hardware RNGs that rely on specialised mechanisms derived from physical events, software RNGs (which are deterministic software), or a combination of both. True random number generators and pseudo-random number generators (PRNGs) are the two basic categories into which computer-based random number generators can be generally divided.

As the name implies, pseudo random numbers are not as random as one might think. The production of integer sequences by pseudo-random number generators (PRNGs), which give the illusion of randomness but are actually predefined, is done using mathematical formulas or precalculated tables. Genuinely random numbers are required for purposes ranging from statistical analysis to secure exchanges of information. Despite its importance, achieving real randomization exclusively by conventional methods within an application is not practical. [1].

D. Quantum True Random Number Generator (QTRNG)

Traditional deterministic random number generators, such PRNG and TRNG, rely on predictable inputs. These inputs are more likely to repeat, resulting in predictability. As a result, the entire system is vulnerable.

Using the concepts of quantum mechanics, a quantum random number generator (QRNG) generates really random numbers. In fact, both theory and experimental research both confirm that quantum physics is fundamentally random in nature [4].

RNGs derive their random numbers from quantum processes that are inherently indeterministic. The inability to

predict numbers is not only due to complexity; it is also impossible to predict random numbers generated by QRNGs; one could argue that even nature does not know these random numbers before they are generated. QRNGs have many advantages, including the ability to exploit nature's objective randomness and a relatively simple function principle. As a result, it is possible to create a realistic model of a QRNG that can be used to certify the generated random numbers. A QRNG is highly resistant to attacks, and post-processing (randomness extraction) is usually conceptually simple. However, creating a small, low-cost, or extremely fast QRNG is difficult.

The group of true random number generators (TRNGs) that obtain randomness from observing quantum processes, which are naturally characterised by non-determinism, includes quantum random number generators (QRNGs). They provide multiple benefits, such as utilizing the fundamental randomness of quantum mechanics, typically faster performance utilizing photonics technology, and most importantly, the capability to confirm and understand the source of unpredictability, which is a crucial security assurance throughout the entire cyber security system. Creating high-quality, large-scale, and rapid quantum random number generators has been a difficult task up until this point.

2. Literature Review

The significance of random numbers in modern computing and cryptographic security cannot be overstated. The security and unpredictability of various computational processes are guaranteed by these seemingly random numeric sequences. But because they use predictable methods, conventional pseudo-random number generators frequently can't produce the necessary level of unpredictability for strong encryption and data security. Here's where Quantum True Random Number Generators (QTRNG) come into play. They provide a quantum-inspired way to generate data that is truly random, substituting real unpredictability for repeatable and predictable patterns.

Using the amazing features of quantum mechanics to efficiently generate truly random numbers is a major objective in the field of quantum computing. Quantum Computational Devices (QCD) and innovative tools like IBM's Qiskit have brought us closer to achieving this goal. In this review, the remarkable capabilities of a Quantum True Random Number Generator (QTRNG) designed to operate on a dedicated quantum device has been explored, thereby saving valuable time and computational resources [1].

The Hadamard gate, a quantum logic gate with features necessary for producing really random numbers, is at the heart of this novel approach. In the pursuit for quantum-based random number generation, this gate's unique capability to generate verifiably unique randomness—and it does so without additional costs—is of utmost importance. The scientific community has discovered that by exploring the inner workings of the Hadamard gate, it is possible to produce random numbers with previously unheard-of reliability and unpredictableness. In addition, the study has revealed the inner matrix product of the square of the Hadamard gate, proving that it is a fundamental component of the quantum laboratory for the production of random numbers.

The work includes a sophisticated Hadamard gate adjustment to increase the QTRNG's applicability. Researchers achieve the function of a single Hadamard gate by nullifying the pair by applying the Hadamard gate twice to the quantum register. This ground-breaking strategy goes beyond theory and has been visually tested with the help of the IBM Q Experience, giving concrete proof of its viability and efficiency.

This literature review provides an in-depth analysis of the most recent developments in quantum-based random number generation and has been divided into three parts. They are as follows:

1) One Time Password and Security
2) One Time Password and Random Number Generators
3) One Time Passwords and Quantum True Random Number Generators

A. *One Time Password and Security*

One Time Passwords (OTPs) are a type of password system that requires users to authenticate themselves each time they log in by using a new password key. This makes them more secure than traditional password systems because even if a password or key is exposed, the user must still provide a newly generated password key. Reputable organisations like the IETF and other businesses with a focus on verification standardise OTPs in an effort to demonstrate their dependability and efficiency.

One of the main advantages of using OTPs is their strong security. Unauthorised parties have significant challenges in accessing the user's account since each password has the unique property of being used only once, and each login requires the user to authenticate with a new password key. This makes OTPs particularly useful for protecting sensitive information and ensuring that only authorized individuals have access to it. OTPs are widely used in a variety of industries, including finance, healthcare, and government, and are generally accepted as a reliable and effective means of authenticating users and protecting against unauthorized access.

There are open-source alternatives like OATH, which are widely used and compatible across several one-time password (OTP) providers, but many OTP systems continue to be confidential or proprietary. The OTP algorithm used by OATH is generally event-based (although time-based is also an option but is less frequently utilised). The OTP server and the user's software/device are the only parties with knowledge of the private character string used in this technique, which also occasionally includes

other information like the user's particular seed. To create the one-time password, all of this data is run through an algorithm, commonly HMAC-SHA1. RSA was one among the innovators in the early days of offering OTP solutions to companies, utilising a variety of software systems and different formats like tokens. Since RSA uses a time-based algorithm to generate OTPs, the client and server-side OTP components must be in time sync. There is also a time indicator provided to the user to ensure accurate timing when entering the password.

The main advantage of time-based OTP over event-based is that with event-based, once someone obtains an OTP, the only time constraint for its use is until a new OTP is generated and utilized. Time-based OTPs have a predetermined time window in which they can be used, such as 25 seconds, which usually works out to be sufficient in most circumstances. On the other hand, users using event-based OTPs are not needed to wait until a password has expired before entering it because they do not require time synchronisation [5].

Event-based OTPs also provide a greater degree of security because they can be created with a single usage in mind, making them useless after the first use. Additionally, they are typically more flexible in terms of implementation, as they do not need to rely on time synchronization, which can be difficult to achieve in certain environments. However, time-based OTPs can be more convenient for users as they do not need to wait for a new OTP to be generated before using it, and also they could use it in offline mode as well. Ultimately, the choice between time-based and event-based OTPs will depend on the specific needs and constraints of the organization implementing them.

Authentication methods that have been around for a long time can be vulnerable to certain types of hacking attempts, such as guessing and dictionary attacks, which involve attempting to guess a person's username/password or PIN. In addition to these methods, another form of attack that can occur is through the use of a malicious program that records keystrokes while a person is entering their password, allowing the attacker to obtain the information. A solution to prevent these types of attacks is the use of a virtual keyboard, where a person enters their password by clicking on the keys with their mouse. However, the ability for attackers to record and capture the authentication process for a virtual keyboard has led to a decrease in the use of this concept. An alternative method for authentication, biometrics, is a system that utilizes unique personal characteristics, like fingerprints or Iris, to verify a person's identity. However, biometric systems can be costly, and can also be susceptible to replay attacks. Smart cards and electronic keys are examples of token-based systems that can be used as an alternative to traditional defences against man-in-the-middle attacks [6].

Previous research has emphasised the value of ensuring secure communication and the effective use of One Time Passwords (OTPs) as a security measure. Due to their persistent use in a variety of situations and adherence to well-established principles, conventional OTP approaches have successfully strengthened security.

However, the security of these conventional OTP techniques may be compromised by the advancing computational powers. Additionally, the method used to generate random data for OTPs might not always guarantee true unpredictability, presenting vulnerabilities.

In contrast, this research adds Quantum True Random Number Generators (QTRNGs) to the preexisting framework. By utilising quantum principles to give improved security through the use of genuine randomness in OTP creation, the aim is to address the flaws in conventional approaches.

B. One Time Password and Random Number Generators

A unique password must be used to authenticate the user each time they log in with the one-time use (OTP) password scheme. OTPs are considered to be more secure than static passwords because even if the password is exposed, the user will have already been authenticated with a new one. There are various ways to generate OTPs and one of them is as follows:

PRNG based OTP. This approach uses a PRNG to generate random bytes, which are then transformed using a function F to produce the OTP. These bytes can be generated from various PRNG sources such as system PRNG like /dev/random, /dev/urandom, CryptGenRandom and no additional secret data is necessary for the random bytes generation. While there are several options for PRNG-based OTPs, they all require specialized hardware to generate random bytes, which can be costly to implement [7].

The key generation process requires a random number, which is an essential component of creating a secure key and is only known after being generated. Random numbers have a vital importance in the field of cybersecurity, cryptography, and scientific simulations. Information security is strongly dependent on the availability of fast, high-quality random numbers. A poor implementation of randomness generation can expose cryptosystems to serious security flaws, even if the underlying algorithms are secure.

A sequence of random numbers is composed of numbers that are not correlated to one another. Generating something truly random on a computer can be challenging, so random number generators (RNGs) use either a virtual or physical source to produce outputs. To create truly random numbers, measurements must be taken from something in the physical world that behaves randomly. When looking at how randomness appears in a fingerprint, the emphasis changes to how random numbers are generated and the methods used to do so. There are various random number generators that fall under the categories of being either software-

based (which use deterministic software) or hardware-based (which use physical phenomena). True random number generators and pseudorandom number generators (PRNGs) are the two main categories in computer-based random number generation.

As implied by the name, pseudorandom numbers are not really random. In order to create the appearance of randomness while actually being predetermined, PRNGs use mathematical formulas or pre-calculated tables to generate a series of numbers. For a variety of purposes, including analysis of statistics and secure interaction, truly random numbers are required. The classical method of using PRNGs alone is not sufficient for these applications as true randomness is important.

Prior research has emphasised the importance of using secure and dependable Random Number Generators (RNGs) for One Time Password (OTP) systems. They emphasise the significance of upholding established standards and emphasise the crucial part these RNGs play in the OTP creation procedure.

1) RNG Selection in OTP Systems: Security, Reliability, and Standards

The reliability and security of an OTP system are significantly impacted by the Random Number Generator (RNG) choice. The randomness and unpredictable nature of the generated OTPs are directly influenced by the RNG's quality [8]. Let's study the results of RNG selection and explore the industry standards and guidelines for RNGs:

1) **Impact on Security:** The reliability of the chosen RNG's randomness and cryptographic strength are crucial components of OTP security. The effectiveness of the OTP system is undermined if the RNG is predictable or biassed, making it simpler for attackers to guess or determine the OTPs. Unauthorised access and potential breaches may be caused by a hacked RNG.

2) **Impact on Reliability:** To guarantee consistent generation and availability of OTPs in an OTP system, the RNG's reliability is essential. The RNG should be able to generate OTPs instantly and without any failures. If backup plans or alternate procedures are not adequately established, unreliable RNGs may result in authentication failures, user annoyance, and significant security problems.

3) **Industry Standards and Guidelines:** The following standards and guidelines provide recommendations for selecting RNGs in OTP systems:

   - The National Institute of Standards and Technology (NIST) has published SP 800-63B, which offers recommendations for digital identity authentication. It recommends utilising RNGs that adhere to NIST specifications and certified cryptographic algorithms.
   - These Request for Comments (RFC) documents, RFC 4226 and RFC 6238, lay forth guidelines for the Time-based One-Time Password (TOTP) algorithms that are frequently employed in OTP systems. They advocate using cryptographic hash functions like SHA-1 or SHA-256 and call for the usage of HMAC-based One-Time Passwords (HOTP). These RFCs include instructions on cryptographic methods that are utilised with OTPs even if they don't directly address RNG selection.
   - FIPS 140-2 lays out security specifications for cryptographic modules. It contains recommendations for RNGs used in cryptographic systems, highlighting the need for reliable, unpredictable random numbers. For the government and regulated industries, compliance with FIPS 140-2 is frequently required.
   - RNGs are included in the cryptographic modules that are evaluated and certified by groups like the Common Criteria (CC) and the Cryptographic Module Validation Program (CMVP). These certifications offer assurance that the RNGs adhere to strict reliability and security requirements.

C. One Time Password and Quantum True Random Number Generators

The convergence of computer science and information theories has been revolutionised by quantum physics, which has cleared the way for ground-breaking protocols. When it first appeared in the 1920s, it sparked technological improvements and dramatically altered how we view the world. The difficulties faced by classical computers when using quantum key distribution and related technologies highlight the tremendous impact of quantum physics on computations, security, and cryptography. A significant and well-established quantum technology that has been refined through many years of study is quantum random number generation. Numerous disciplines, including science, the arts, cryptography, statistics, and gaming, place a high importance on the capacity to produce truly random numbers. This advance in quantum technology has the potential to transform society and the economy in profound ways. Currently, this technology delivers dependable and secure solutions, attracting growing interest. Apart from its technical potential, many researchers are drawn to study this technology for its fascinating characteristics.

The use of quantum random number generators has produced a variety of benefits over the past 20 years. Recent review articles and references demonstrate the depth of research that has been done in this area. The main difference between QRNGs and traditional RNGs is that QRNGs are unpredictable. QRNGs successfully avoid the known flaws seen in conventional random number generation techniques by utilising the principles of quantum physics. As a result, quantum devices demonstrate an advantage over their

classical counterparts. They are considered the only device capable of producing truly unpredictable output and are therefore highly valued for their ability to provide high-level information security in areas such as authentication, as a result of the principles discussed previously.

Different methods have been developed to build various kinds of QRNGs using various sources of quantum randomness like phase noise of lasers, radioactive decay, etc [1]. However, some of the techniques may not be completely accurate in practical devices. QRNG protocols are continuously being developed as assumptions and device characterizations are relaxed. Several commercial products have been developed using different QRNGs quantum phenomena. These protocols show promise for use in a variety of scientific disciplines, such as machine learning and cryptography. The main challenge, however, is ensuring the dependability of quantum systems.

Quantum random number generators (QTRNGs) have been developed using a variety of methods that take advantage of a variety of phenomena, including radioactive decay, noise, optical generators, etc. [1]. Generators that are independent of a device have also been researched. The availability of numerous application programming interfaces (APIs) for various devices may make it difficult for end users to understand the underlying concepts and choose the best QTRNG that suits their needs. Furthermore, consumers may find it difficult to assess the effectiveness and quality of QTRNGs because to the lack of widely acknowledged QTRNG standards. Additionally, it can be difficult to achieve sustained, high-stability random number services for online security applications as many individual QTRNGs lack real-time randomness.

Random numbers are crucial for fields such as cybersecurity, lotteries, cryptography, and scientific simulations. Sensitive client data is now much more readily available online thanks to the development and broad acceptance of leading-edge technologies like big data, cloud computing, and the Internet of Things. Due to the trend's increasing computational capacity, the possible influence of upcoming quantum computers, and the emergence of new algorithmic assaults, maintaining data security is becoming more and more difficult. Poor implementations of randomness generation can lead to significant security vulnerabilities in cryptography systems, even when the core algorithms are sound. This problem becomes special importance when new lattice- or hash-based quantum-safe cryptographic techniques are introduced. The creation of really random numbers continues to be a major challenge that cannot be solved using traditional methods. The security of information depends increasingly on the ability to generate random numbers at rapid speeds and with high reliability.

In the past twenty years, quantum random number generators (QRNGs) have attracted a lot of attention, and there is a wealth of material in recent review articles and their cited sources. The fundamental difference between conventional generators like thermal or pseudo noise-based ones and QRNGs is their unpredictable nature. Due to the principles of quantum physics, QRNGs effectively eliminate the predictability flaws prevalent in conventional random number generation. As a result, quantum devices perform better when performing operations like data encryption, authentication, and digital signatures that require a high level of information security. Quantum randomness has been produced using a variety of methods, including photon-counting detection, vacuum fluctuations in optical fields, exploiting phase fluctuations in spontaneous emission, measuring the arrival time of weak coherent states, and generating quantum randomness [9]. Additionally, there are QRNG approaches that loosen assumptions and descriptions of the employed devices, which are device-independent and semi-device-independent.

1) Advantages of QTRNGs in OTP Systems: Enhanced Security and Cryptographic Properties

Quantum True Random Number Generators (QTRNGs) can potentially offer a number of benefits to OTP systems, including increased security, resistance to assaults, and improved cryptographic features [8]. Let's explore these advantages in more detail:

1) **Enhanced Security:** To produce truly random numbers, QTRNGs take advantage of the intrinsic randomness of quantum phenomena. QTRNGs provide a higher level of security than deterministic algorithms or pseudorandom number generators (PRNGs), as they generate really unpredictable and independent values. The security of OTP systems is considerably strengthened by the increased unpredictability, which makes it extremely difficult for attackers to estimate or anticipate the OTPs, even with sophisticated approaches.

2) **Attack Resistance:** QTRNGs are naturally resistant to a variety of attacks, including statistical and cryptographic threats. The generated random numbers are safeguarded against attack by the unpredictable nature of quantum phenomena used in QTRNGs. This strong defence blocks attempts to reverse-engineer the random number generation process as well as brute-force attacks, pattern analysis, and other security measures.

3) **Enhanced Cryptographic Properties:** To determine the validity of their randomness, QTRNGs are thoroughly examined utilising statistical tests and cryptographic analysis. In many instances, QTRNGs outperform conventional PRNGs in terms of cryptographic qualities. The QTRNG-generated random numbers exhibit an enhanced entropy distribution, lack correlation between successive values, and have the characteristics required for safe cryptographic operations. The overall security and dependability of OTP systems are considerably increased by these improved cryptographic characteristics.

4) **Use of Quantum Entanglement and Non-Locality:** A few QTRNG designs make use of the quantum entanglement and non-locality phenomena to provide even more security benefits. Entangled particles can be used to generate random numbers across various devices or locations, enhancing security and lowering the possibility of tampering or interception. QTRNGs based on quantum entanglement show potential for producing secure and dependable OTPs in distributed systems.

5) **Proactive Future-Proofing:** As quantum computers advance, traditional cryptographic algorithms may become susceptible to attacks utilizing quantum algorithms. Organisations can proactively future-proof their security infrastructure by integrating QTRNGs into OTP systems. Long-term security is ensured by cryptographic protocols built on the inherent quantum randomness, which is resistant to quantum computing threats.

The unique benefits of quantum true random number generators (QTRNGs), such as their unmatched security and strong cryptographic features, are highlighted in this section. The positive potential of QTRNGs to improve One Time Password (OTP) systems is highlighted by this.

This research complements the existing work by not only highlighting the advantages of QTRNGs but also by delving into their practical application. Exploring platforms like IBM Quantum Experience Qiskit and Quantum Computational Devices (QCDs), which effectively bridges the gap between theoretical benefits and the actual production of OTPs. In doing so, such limitations can be successfully overcome.

3. Comparative Analysis

A. *NIST Statistical Test Suite*

The NIST Test Suite comprises 15 tests designed to evaluate the unpredictability of binary sequences generated by cryptographic random or pseudorandom number generators. These tests specifically target different forms of non-randomness that might be present in a sequence, and they are applicable to both hardware-based and software-based generators. It's crucial to remember that some tests can be further broken down into subtests [10]. The 15 tests in the suite are as follows:

1) The Frequency (Monobit) Test,
2) Frequency Test within a Block,
3) The Runs Test,
4) Tests for the Longest-Run-of-Ones in a Block,
5) The Binary Matrix Rank Test,
6) The Discrete Fourier Transform (Spectral) Test,
7) The Non-overlapping Template Matching Test,
8) The Overlapping Template Matching Test,
9) Maurer's "Universal Statistical" Test,
10) The Linear Complexity Test,
11) The Serial Test,
12) The Approximate Entropy Test,
13) The Cumulative Sums (Cusums) Test,
14) The Random Excursions Test, and
15) The Random Excursions Variant Test.

A given sequence can be compared to a truly random sequence using a variety of statistical tests. Since a random sequence's characteristics may be defined and explained in terms of probability, randomness itself is a probabilistic quality. The expected results can be represented probabilistically when performing statistical tests on truly random sequence because they are previously known. Many other statistical tests are available, and they all seek to find any observable patterns in the sequence that would suggest its lack of randomness. There is no particular finite set of tests that are regarded as "comprehensive" due to the wide variety of tests available to evaluate sequence randomness. To avoid making the wrong conclusions about a certain generator, it is also crucial to read the outcomes of statistical testing carefully and attentively.

To investigate a certain null hypothesis (H0) on the randomness of a given sequence, a statistical test is conducted. The alternative hypothesis (Ha) suggests that the sequence is not random, contradicting the null hypothesis, which takes this assumption into account. To assess whether or not the generator is providing random values, a statistical test is run on the created sequence. Accepting or rejecting the null hypothesis is the choice here.

For each test, choosing an appropriate measure of randomness is crucial since it decides whether or not the null hypothesis should be accepted. This statistic follows a distribution with a range of potential values, assuming the sequence is random. Under the null hypothesis, the reference distribution for this statistic is established using mathematical techniques. This reference distribution is used to calculate a crucial number, which is often found near the extremes of the distribution, like the 99% percentile. During the test, a test statistic value is calculated based on the data (the sequence under examination). After that, a crucial value is compared to the computed value. The null hypothesis of randomness is rejected if the value of the test statistic is greater than the critical value. The hypothesis of randomness is accepted, however, if the test statistic value is less than the crucial value, suggesting that it does not exceed the threshold.

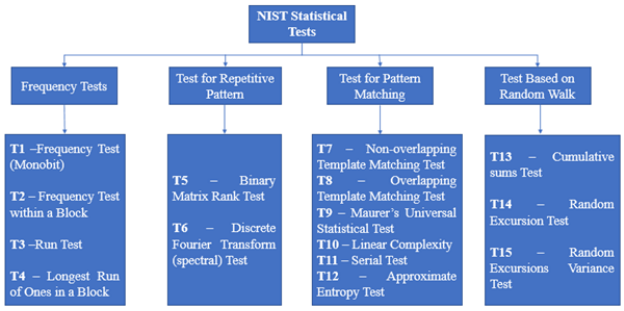

Figure 1. NIST Statistical Tests

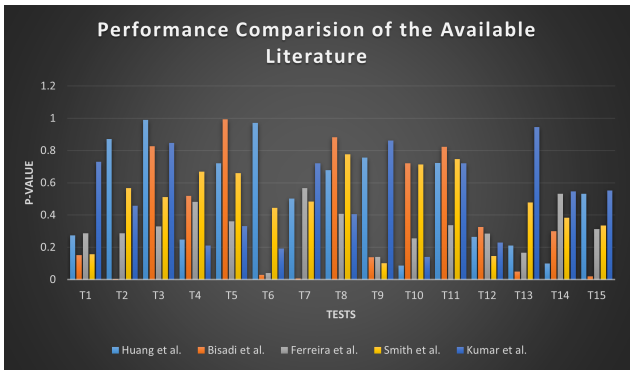

Figure 2. Performance Comparison of the Available Literature

In reality, the reference distribution and critical value are computed under the presumption of randomness, which is what gives statistical hypothesis testing its practical usefulness. The generated test statistic value will have an extremely low likelihood (e.g., 0.01%) of exceeding the critical value when the data are consistent with the assumption. It is statistically unlikely that an improbable circumstance occurred by chance alone if the estimated test statistic value does surpass the critical value and indicates its occurrence. Therefore, it raises questions regarding the validity of the initial assumption of randomness when the generated test statistic value surpasses the crucial threshold. In some cases, the outcomes of statistical hypothesis testing result in the rejection of the null hypothesis (randomness) and the acceptance of the alternative hypothesis (non-randomness). [9]

B. Statistical Comparison

Table I shows comparison of the research papers [9], [11], [12], [13] and [1]. The NIST Statistical Tests are compared and analysed here. The highlighted part shows the highest p-value comparatively to the other research papers.

C. Performance Comparison of the Available Literature

The NIST 800-22 Statistical Test Suites of the research papers [9], [11], [12], [13] and [1] are compared and analysed as shown in Figure 2.

4. Identified Research Gap

The identified research gaps are as follows:

TABLE I. Statistical Comparison

Tests		Huang et al.	Bisadi et al.	Ferreica et al.	Smith et al.	Kumar et al.
Frequency Tests	T1	0.247	0.1520	0.2861	0.156	0.7293
	T2	0.871	0.0025	0.2868	0.567	0.4580
	T3	0.990	0.8272	0.3298	0.512	0.8478
	T4	0.248	0.5181	0.4817	0.668	0.2101
Test for Repetitive Pattern	T5	0.720	0.9940	0.3611	0.660	0.3308
	T6	0.972	0.0297	0.0401	0.445	0.1925
Test for Pattern Matching	T7	0.501	0.0063	0.5666	0.483	0.7209
	T8	0.679	0.8831	0.4064	0.777	0.4053
	T9	0.756	0.1388	0.1404	0.101	0.8617
	T10	0.087	0.7212	0.2550	0.714	0.1408
	T11	0.722	0.8237	0.3376	0.747	0.7206
	T12	0.265	0.3252	0.2854	0.145	0.2301
Test Based on Random Walk	T13	0.210	0.0490	0.1657	0.477	0.9453
	T14	0.100	0.3000	0.5310	0.384	0.5465
	T15	0.532	0.0196	0.3127	0.335	0.5518

- One-time passwords (OTPs), which can be generated using quantum true random number generation (QTRNG), are unique passwords that can only be used once. Entropy as a Service (EaaS), which can be established, provides these OTPs. Then, this service can be made available to third parties with permission to access the system or cloud service providers [1].
- It can be standardized as a form of Entropy as a Service (EaaS) and made available to cloud service providers, as well as to third parties who have been granted access by the provider, such as IBM [1].
- Avoid vulnerabilities that are commonly found in traditional systems, such as replay attacks, reusability attacks, and man-in-the-middle attacks [7], [14].
- It can generate unique, one-time session keys on demand [1].
- Develop and integrate various QTRNGs to improve the security and efficiency of the system [9].
- QTRNGs could become more widely used as they Keep striving for better performance, while also becoming smaller and less expensive [8].
    - QTRNGs could become more widely used as they Keep striving for better performance, while also becoming smaller and less expensive.

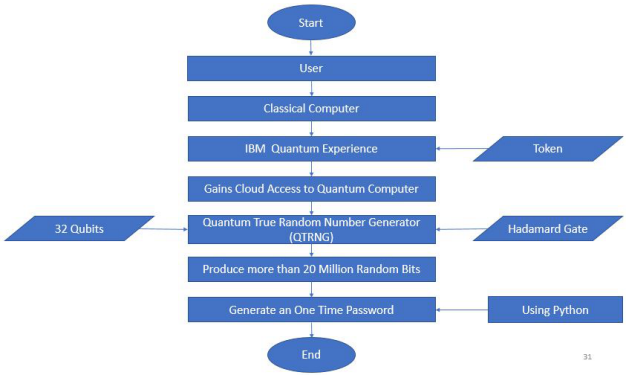

Figure 3. Flowchart of the Proposed Methodology

5. Problem Statement

For various digital transactions and to ensure the authenticity, One-Time-Password (OTP) is being used as an additional authentication mechanism which is prone to various attacks like replay-attacks, reusability, and man-in-middle attacks. It is also found that, the approaches being used to generate OTP by the various existing methods are time and memory consuming. There is a trade-off between security aspects and time/memory requirements. This work aims to propose an enhanced approach to generate OTP, which overcome the limitations of the existing methods.

6. Proposed Methodology

In this paper, we employ a structured approach to generate One Time Passwords (OTPs) using Quantum True Random Number Generators (QTRNGs). This section details the fundamental steps within our method. The flowchart of the proposed methodology is shown in Figure 3.

Start

Step 1: A user will utilize a traditional computer to gain access to the Qiskit software platform.

Step 2: A token (unique identifier) is generated.

Step 3: Enter the Token.

Step 4: The unique identifier is used to authorize access to the IBM Quantum Experience.

Step 5: The individual is able to connect to a quantum computer via the cloud.

Step 6: Enter the quantity of qubits (in this case, 24) and the Hadamard gate operation.

Step 7: A Quantum True Random Number Generator (QTRNG) is produced.

Step 8: Around 20 million randomly generated binary digits (1s and 0s) are produced.

Step 9: An one-time password is created by utilizing the programming language python and the previously generated large amount of randomly generated binary digits.

End

The research follows a carefully structured methodology designed to create One Time Passwords (OTPs) by harnessing the capabilities of Quantum True Random Number Generators (QTRNGs). This process involves several well-defined steps. It all starts with the user logging into the Qiskit software platform using a standard computer. We then generate a unique token to verify the user's identity, acting as a crucial identifier. The user proceeds by using this token for authentication and gaining access to the IBM Quantum Experience through cloud connectivity. Users have the flexibility to configure quantum parameters, specifying the number of qubits and selecting the Hadamard gate operation. Following this, we activate a Quantum True Random Number Generator (QTRNG) to infuse authentic randomness into the process. The QTRNG generates an extensive pool of approximately 20 million binary digits, encompassing both 1s and 0s, which becomes the foundation for crafting One Time Passwords. Finally, the OTP is generated using the Python programming language. This methodical approach underscores our commitment to improving secure authentication practices by integrating quantum computing principles into OTP generation. It represents a comprehensive and well-structured approach that prioritizes security and reliability in the OTP generation process.

One Time Passwords are successfully created as a result of this methodically thought-out methodology, demonstrating the creative intersection of quantum computing concepts and secure authentication techniques.

7. Implementation

The IBM platform was used in conjunction with the Qiskit Python package programming language for this proposed work. To produce different random numbers, the Hadamard Gate and the superposition principle were used in the proposed work.

The goal of this proposed work is to evaluate how unpredictable and challenging it is to replicate a random number sequence. IBM's quantum lab serves as the main origin for generating quantum true random numbers. Hadamard gates are used to accomplish this, and the results are measured using 32 qubits and 65,536 shots in the Aer Simulator.

A. *Qiskit*

Through cloud computing, researchers have easy access to quantum devices and IBM Quantum simulators, using Qiskit as an open-source programming environment [15]. This software bridges the gap between quantum algorithms and experimental quantum devices by offering a variety of tools for creating and running quantum programmes. Python and other widely used programming languages are converted into quantum machine language via Qiskit.

Support from the Qiskit Python library is required to operate with IBM device environments for quantum programming. We observed that utilising the built-in functions offered by Qiskit proves useful for building quantum registers and circuits while performing various operations on qubits.

IBM's Python library, Qiskit, makes it easier to programme quantum simulators and actual quantum devices. The built-in features of Qiskit make it simple to build quantum registers and circuits. Quantum programmes need to be connected to actual IBM hardware in order to be run. It's crucial to understand that a quantum device always functions in conjunction with a conventional computer. The states of the qubits must be stored in an equal number of bits during the execution of a quantum circuit. [1]

In addition to offering a variety of tools for creating and modifying quantum programmes, Qiskit also functions as a platform for translating popular programming languages into quantum machine language. It enables quantum computation by easily integrating quantum algorithms with actual quantum devices. Using the quantum-specific programming language Open Quantum Assembly Language (OpenQASM), the actual quantum device in Qiskit is programmed. [1]

Beyond simple programming, Qiskit and quantum hardware work together to create a dynamic environment for cooperative quantum research. Due to Qiskit's compatibility with cloud computing, distributed quantum exploration is sped up, enabling teams to take advantage of the combined power of quantum simulators and devices.

The design of quantum registers and circuits is made easier by Qiskit's user-friendly interface and thoroughly documented capabilities, which give researchers the means to explore a wide range of quantum phenomena, from basic gates to intricate entanglement protocols.

B. Hadamard Gate

To alter the basic states of a single qubit, the Hadamard gate is used. $|0>$ is mapped to $\frac{(|0>+|1>)}{\sqrt{2}}$, and $|1>$ is mapped to $\frac{(|0>-|1>)}{\sqrt{2}}$. When used on a computational basis state, this gate produces an equal superposition state. These two outcomes, $\frac{(|0>+|1>)}{\sqrt{2}}$ and $\frac{(|0>-|1>)}{\sqrt{2}}$, are occasionally abbreviated as $|+>$ and $|>$, respectively. The Hadamard gate is an involutory gate because it rotates by around the axis $(\hat{x}+\hat{z})/\sqrt{2}$ on the Bloch sphere. The following is the Hadamard matrix [16], which represents it:

$$H = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$$

C. Superposition

Being able to live in a superposition state is one way that a qubit differs from a conventional bit. A crucial idea in quantum physics is superposition. A musical tone can be modelled in classical physics as a superposed wave, which is created by adding together various frequencies or waves. Similar to this, a quantum state in superposition in quantum mechanics can be viewed as a linear combination of different quantum states. A true and distinct quantum state is represented by this superposed quantum state.

The base states 0 and 1 can coexist in a special way for qubits, allowing for a superposition of their states. In quantum physics, when a qubit is measured, it experiences a collapse and settles into one of its eigenstates. The measured value is consistent with that specific state. A qubit in a state of superposition with equal weights will randomly collapse into one of its two base states, 00 or 11, each with a 50% chance, in the event of a measurement. When measured and collapsed, the state 0 will always produce the value 0, while the state 1 will always produce the value 1 [17].

D. Production of quantum random bits using Quantum Circuit

Random numbers are essential for operations like key generation and encryption systems in a variety of professions, including cryptography as well as other fields. The generated numbers, however, frequently only appear to be pseudo-random, which presents a problem. This work proposes the use of quantum computing to generate true random numbers, rather than pseudorandom sequences, due to the unique properties of quantum systems. In order to produce a specific number of random bits, a certain number of qubits are required, as demonstrated in Figure 4 using a 32-qubit quantum register.

The circuit generates a dataset of more than 20 million quantum random numbers which is shown in the Figure 5. The simulator used here is aer simulator of qiskit. The Aer module provides a collection of high-performance simulators for executing quantum circuits on classical computers. The circuit has been executed 65536 times.

The visual flow for accessing a quantum computer is shown in Figure 6.

E. Generation of OTP

In this section, One-Time Passwords (OTPs) are generated utilising the previously generated and tested Quantum True Random Number Generators (QTRNGs). More than 20 million devices make up the QTRNGs, which have undergone testing to ensure their dependability and unpredictability. These tools serve as the foundation for creating truly random OTPs, which are essential for maintaining secure authentication and data security.

A Python script has been used to generate the OTPs leveraging the QTRNGs as the source of randomness. In this particular test, OTPs are generated for 25 users because the script is particularly made to generate them for a specific number of users. OTPs offer a high level of security for authentication because each one is a unique string of characters.

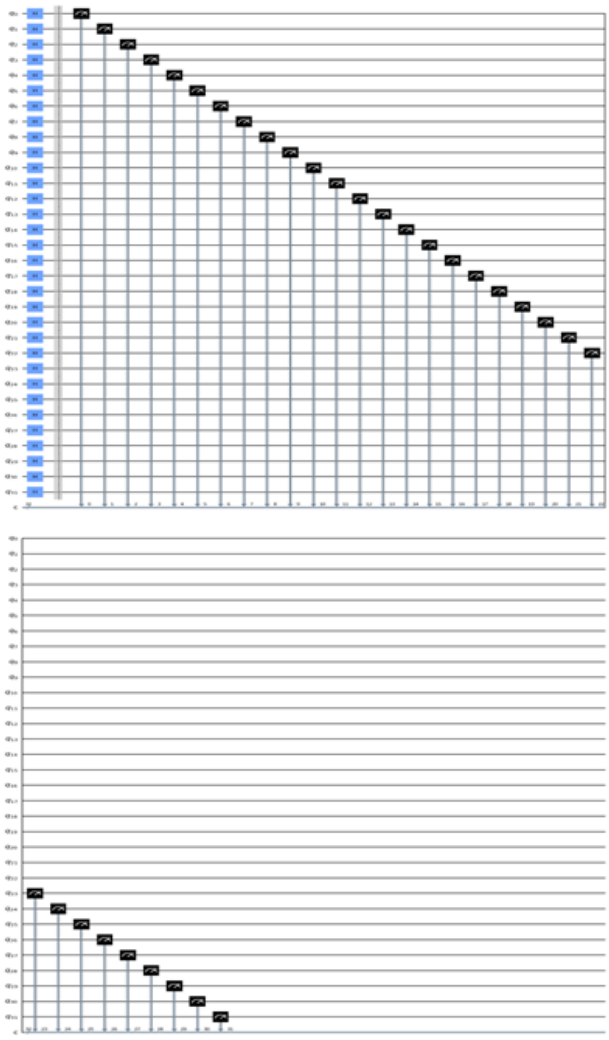

Figure 4. Generation of Quantum Circuit with 32 Qubits

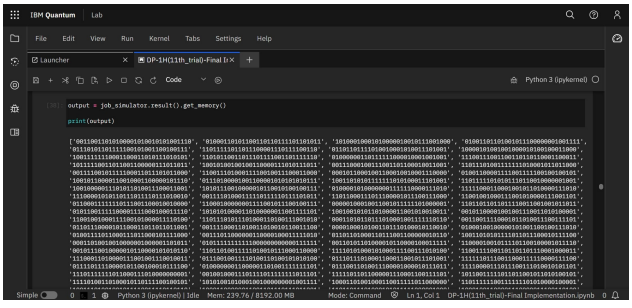

Figure 5. Generation of quantum RNGs

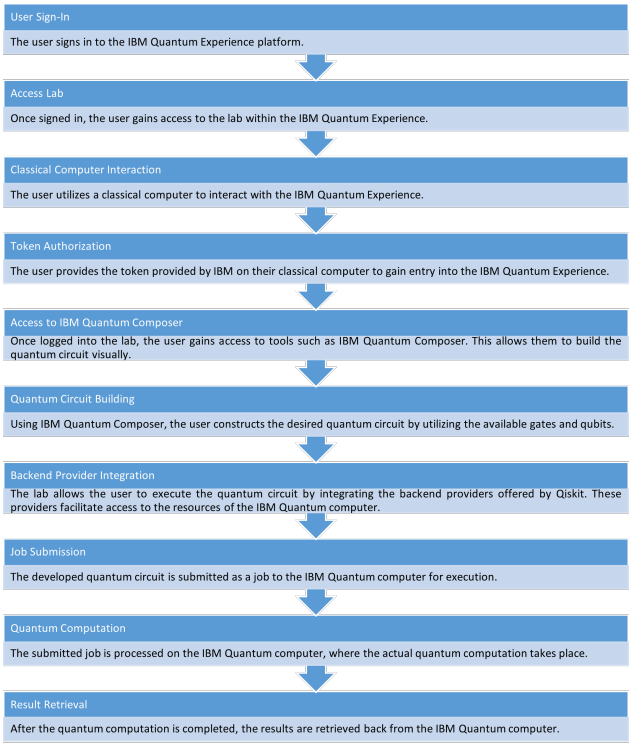

Figure 6. Visual Flow of Procedure for Accessing a Quantum Computer

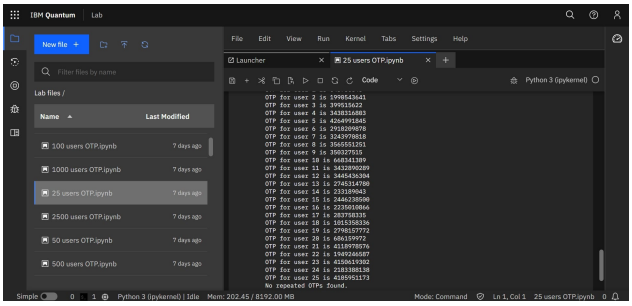

Figure 7. Generation of OTPs

A snapshot of the outcome from using the QTRNG-based method to generate OTPs for 25 users is shown in Figure 7. The displayed OTPs serve as an illustration of the uniqueness and randomness of the generated codes. By removing any potential weaknesses or predictabilities, the OTPs' inherent unpredictability plays a crucial part in protecting the security of the authentication process.

More trials were run with an increasing user base in order to fully assess the effectiveness of the OTP creation process. While keeping all other variables constant, we increased from 25 users to 50, 100, 500, 1000, and 2500 users. The goal was to examine the OTP generating method's performance with increasing amounts of users in order to determine how scaleable it is.

8. Results And Analysis

The IBM lab was used to put the proposed random number generation technique into practise. Due to their great degree of randomness, the random numbers produced with the help of QTRNG cannot be replicated, as demonstrated by this implementation.

A. NIST 800-22 Statistical Tests

The NIST 800-22 tests were used to thoroughly analyse QTRNG's statistical properties, as shown in the Table II.

TABLE II. NIST 800-22 Statistical Test Result

Test		p-value	Conclusion
T1	The Frequency Test (Monobit)	0.5911	Random
T2	Frequency Test Within a Block	0.0227	Random
T3	Run Test	0.4017	Random
T4	Tests for the Longest Run of Ones in a Block	0.4459	Random
T5	The Binary Matrix Rank Test	0.3123	Random
T6	The Discrete Fourier Transform (Spectral) Test	0.2614	Random
T7	The Non-Overlapping Template Matching Test	0.9999	Random
T8	The Overlapping Template Matching Test	0.1176	Random
T9	Maurer's "Universal Statistical" Test	0.3979	Random
T10	The Linear Complexity Test	0.9837	Random
T11	The Serial Test	0.9817	Random
T12	The Approximate Entropy Test	0.9824	Random
T13	The Cumulative Sums (Cusums) Test	0.6415	Random
T14	The Random Excursions Test	0.3794	Random
T15	The Random Excursions Variant Test	0.5712	Random

B. Analysis of OTP Generation Method

The One Time Passwords (OTPs) produced for each user utilising the Quantum True Random Number Generator (QTRNG) undeniably keep their inherent randomness, according to the research results. The initial testing phase produced persuasive proof that the OTPs display a remarkable ability to maintain security and real randomness even as the number of users rises, in addition to maintaining their original levels of unpredictability and uniqueness. This remarkable consistency in generating secure, truly random OTPs, regardless of user volume, stands as a testament to the effectiveness and resilience of our OTP generation method based on QTRNG.

However, it's crucial to recognize that with an increasing number of users, there is a gradual extension in the time required for OTP generation. The slight delay can be attributable to the increased computing workload required to produce more OTPs. Depending on the rate of user growth, the length of this time extension could range from a few seconds to several minutes. However, it is crucial to stress that the extraordinarily high level of security attained by using genuinely random OTPs far justifies the slight increase in creation time. The importance of our method in delivering safe authentication while retaining practicality and efficiency is highlighted by this delicate balance between security and time.

The number of tests in which the method performed well in comparison with the literature [7], [11], [12], [13], [1] and proposed work is shown in the following Table III.

TABLE III. NIST 800-22 Statistical Test Result

Literature	No. of Test in which method performed well
Huang et al. [9]	3
Ferreira et al. [11]	0
Smith at al. [12]	1
Bisadi et al. [13]	2
Kumar et al. [1]	4
Proposed Work	5

C. Performance Analysis after Implementation

The NIST 800-22 Statistical Test Suites have been compared across a number of research papers as shown in the Figure 8, encompassing references [9], [11], [12], [13], [1], and the current work. This in-depth evaluation provides a comprehensive perspective on the extent to which or how widely the proposed work varies from the procedures and conclusions described in these preceding research works.

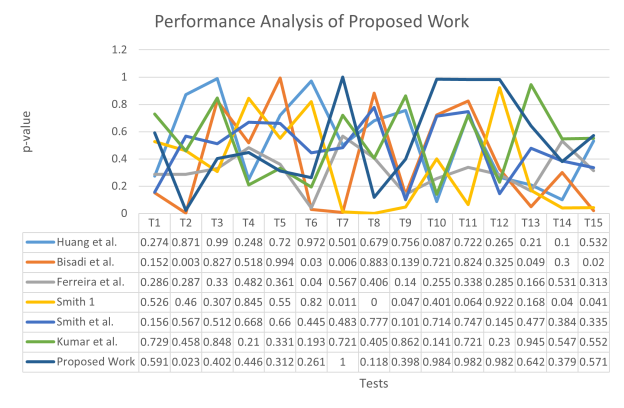

Figure 8. Performance Analysis of the Proposed Work

9. Conclusion And Future Work

The research presented in this study has profound implications for the fields of secure authentication and random number generation. Through rigorous testing in the NIST 800-22 test suite, we have demonstrated that Quantum True Random Number Generator (QTRNG) can produce truly random bits, surpassing the requirements for post-processing. The outcomes unambiguously demonstrate that the bit strings produced exhibit a remarkable level of unpredictability, constituting a significant step forward in the search of secure authentication.

The proposed approach is not only more approachable than physically device-independent random number generators, but also incredibly practical to use. This cutting-edge technique has already demonstrated its efficacy in creating One Time Passwords (OTPs), providing a higher level of protection. Additionally, there may be room for collaboration with IBM. Furthermore, there is a chance for integration with IBM to provide random numbers as

a service, broadening its application and increasing its accessibility.

The use of more than 20 million QTRNGs to generate OTPs has produced outstanding results, yielding numbers that are truly random and secure. Our tests have confirmed the method's scalability by proving the randomness and uniqueness of the generated OTPs across a range of user counts. Despite a little increase in generation time, the QTRNG-based OTP generation approach represents an efficient solution for secure authentication in a number of applications.

In terms of future research, we envision the creation of a standardised framework for quantum true random number generators (QTRNGs), similar to "Entropy as a Service" (EaaS). This framework may be implemented by cloud service providers and other authorised external parties with access to IBM's resources, supporting the widespread use of quantum-based secure authentication techniques. Additionally, we envision using the QTRNG to generate nonce numbers for a single usage in quantum key distribution for secure end-to-end communications, ensuring both validity and confidentiality. Further enhancing the validity and dependability of QTRNG-based secure authentication techniques, we intend to improve evaluations of randomness and unpredictability inside the NIST 800-22 Statistical Test Suite.

In conclusion, our research not only shows that QTRNG-based secure authentication is practicable, but also points the way for future advancements in quantum security and cryptography. This has the ability to completely change the industry and provide cutting-edge security measures for a variety of applications.

References

[1] R. A. P. P. Vaishnavi Kumar, John Bosco Balaguru Rayappan, "Quantum true random number generation on IBM's cloud platform," *J. King Saud Univ. - Comput. Inf. Sci.*, vol. 34, no. 8, pp. 6453–6465, Sep. 2022.

[2] M. H. A. Y.-W. Chow, W. Susilo and A. M. Barmawi, "A visual one-time password authentication scheme using mobile devices," in *Information and Communications Security*, ser. Lecture notes in computer science. Cham: Springer International Publishing, 2015, pp. 243–257.

[3] "Quantum computing," https://en.wikipedia.org/wiki/Quantum_computing, accessed: 2023-5-15.

[4] "Quantum random number generator (QRNG) - QNu labs - how it works?" https://www.qnulabs.com/tropos-quantum-random-number-generator/., Jan. 2021, accessed: 2023-5-15.

[5] H. L. Young Sil Lee and H. Lee, "A study on efficient OTP generation using stream cipher with random digit," in *The 12th International Conference on Advanced Communication Technology (ICACT)*, 2010, pp. 1670–1675.

[6] K. Srinivas and V. Janaki, "A novel approach for generation of OTP'S using image's," *Procedia Comput. Sci.*, vol. 85, pp. 511–518, 2016.

[7] K. Z. T. K. M. Malikovich and A. J. Tileubayevna, "A method of efficient OTP generation using pseudorandom number generators," in *2019 International Conference on Information Science and Communications Technologies (ICISCT)*. IEEE, Nov. 2019.

[8] B. N. C. Dr. Marco Piani, Dr. Michele Mosca, "Quantum Random-Number generators: Practical considerations and use cases," *evolutionQ Inc*, 2021.

[9] K. F. L. Huang, H. Zhou and C. Xie, "Quantum random number cloud platform," *Npj Quantum Inf.*, vol. 7, no. 1, Jul. 2021.

[10] L. Bassham, A. Rukhin, J. Soto, J. Nechvatal, M. Smid, S. Leigh, M. Levenson, M. Vangel, N. Heckert, and D. Banks, "A statistical test suite for random and pseudorandom number generators for cryptographic applications," 2010-09-16 2010. [Online]. Available: https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=906762

[11] M. J. Ferreira, "Characterization of a quantum random number generator based on vacuum fluctuations," *Applied Sciences*.

[12] P. R. Smith, "Simple source device-independent continuous-variable quantum random number generator," Jun. 2019.

[13] Z. Bisadi, "Compact quantum random number generator with silicon nanocrystals light emitting device coupled to a silicon photomultiplier," *Frontiers in Physics*, 2018.

[14] R. Naik and U. Singh, "Secured 6-digit OTP generation using b-exponential chaotic map," *Int. J. Adv. Comput. Sci. Appl.*, vol. 12, no. 12, 2021.

[15] Z. L. J. Y. Q. S. W. H. Y. Z. Bingjie Xu, Ziyang Chen and H. Guo, "High speed continuous variable source-independent quantum random number generation," *Quantum Sci. Technol.*, vol. 4, no. 2, p. 025013, Apr. 2019.

[16] Wikipedia contributors, "Quantum logic gate," https://en.wikipedia.org/w/index.php?title=Quantum_logic_gate&oldid=1151067570, 2023, accessed: 2023-05-09.

[17] D. Voorhoede, "Superposition and entanglement," https://www.quantum-inspire.com/kbase/superposition-and-entanglement/, accessed: 2023-5-15.

[18] R. Rajan, S. R, S. T, and S. Rajest, "Otp as a service in the cloud allows for authentication of multiple services," vol. 5, pp. 94–112, 05 2023.

[19] Y.-X. Liu, K.-X. Huang, Y.-M. Bai, Z. Yang, and J.-L. Li, "A high-randomness and high-stability electronic quantum random number generator without post processing," *Chinese Physics Letters*, vol. 40, no. 7, p. 070303, 2023.

[20] C. K. Duda, K. A. Meier, and R. T. Newell, "Development of a high min-entropy quantum random number generator based on amplified spontaneous emission," *Entropy*, vol. 25, no. 5, 2023. [Online]. Available: https://www.mdpi.com/1099-4300/25/5/731

[21] O. Guillan-Lorenzo, M. Troncoso-Costas, D. Alvarez-Outarelo, F. J. Diaz-Otero, and J. C. Garcia-Escartin, "Optical quantum random number generators: A comparative study," *Optical and Quantum Electronics*, vol. 55, no. 2, 2023.

[22] C. Bruynsteen, T. Gehring, C. Lupo, J. Bauwelinck, and X. Yin, "100-gbit/s integrated quantum random number generator based on vacuum fluctuations," *PRX Quantum*, vol. 4, p. 010330, Mar 2023. [Online]. Available: https://link.aps.org/doi/10.1103/PRXQuantum.4.010330

[23] G. Shaw and A. Prabhakar, "Quantum random number generator with one and two entropy sources," 06 2019.

[24] B. Bai and et al., "18.8 gbps real-time quantum random number generator with a photonic integrated chip," *Applied Physics Letters*, vol. 118, no. 26, 2021.

[25] S. M. Vaisakh Mannalath and A. Pathak, "A comprehensive review of quantum random number generators: Concepts, classification and the origin of randomness," 2022.

[26] K. Tamura and Y. Shikano, "Quantum random numbers generated by a cloud superconducting quantum computer," in *International Symposium on Mathematics, Quantum Theory, and Cryptography*. Singapore: Springer Singapore, 2021, pp. 17–37.

[27] H. L. Young Sil Lee and H. Lee, "A study on efficient OTP generation using stream cipher with random digit," in *The 12th International Conference on Advanced Communication Technology (ICACT)*, 2010, pp. 1670–1675.

[28] K. F. Leilei Huang, Hongyi Zhou and C. Xie, "Quantum random number cloud platform," *Npj Quantum Inf.*, vol. 7, no. 1, Jul. 2021.

[29] C. P. H. Kim, J. Han and O. Yi, "Analysis of vulnerabilities that can occur when generating one-time password," *Appl. Sci. (Basel)*, vol. 10, no. 8, p. 2961, 2020.

[30] C. C. S. K. Abbott, A.A., "A quantum random number generator certified by value indefiniteness," *Math. Struct. Comp. Sci. 24*, 2014.

[31] G.-E. Herrero-Collantes, M., "Quantum random number generators," *Rev. Mod. Phys.*, vol. 89, no. 1, Feb. 2017.

Riddhi B. Prajapati completed Masters degree (M.E.) Computer Engineering with specialization in Cyber Security from Gujarat Technological University – Graduate School of Engineering & Technology (GTU-GSET) and Bachelor's degree (B.Tech) from the Institute of Advanced Research. As a co-author, she has published a chapter on "Big Data Applications in Transportation System using Internet of Things" in the book "Handbook of research for big data" which was published by Apple Academic Press and CRC press of Taylor and Francis group. Her research area of interests are Cyber Security and Quantum Computing. Apart from the academic pursuits, she actively participates in extracurricular activities where she was awarded a Merit Certificate for getting shortlisted by the jury in the top ten percent entries in the "Global Heartfullness Essay Event – 2021" organized by Heartfullness Education Trust, Shri Ram Chandra Mission, UNESCO MGIEP, UNIC for India and Bhutan.

Dr. S. D. Panchal at present is a Professor in the Computer Engineering (Cybersecurity) department & Director of Gujarat Technological University – Graduate School of Engineering & Technology, Ahmadabad since May 2020. He served as Registrar of Gujarat Technological University, Ahmedabad (2017-2019), Associate Professor (2012-2020), and Assistant Professor (2000-2012) of Information Technology – Commissinerate of Technical Education, Government of Gujarat. (class-II). Dr. Panchal has published more than 25 research papers in reputed journals to date. He is is having a total of 23 years of teaching and research experience. He has guided 01 Ph.D. scholar and more than 25 PG students successfully. At present 06 Ph.D. scholars are pursuing their research under his supervision.