Zero-Trust Quantum Authentication for Distributed Systems using Device-Independent Protocols and Qiskit Simulation

Furkan Sayyed
Student at University of Mumbai

Srivaramangai Ramanujam
Head of I.T Department,
University of Mumbai

ABSTRACT

Quantum computing disrupts conventional authentication techniques which rely on trusted measurement devices. The study presents a Zero-Trust Device-Independent Quantum Authentication Framework which authenticates users through Bell-state entanglement combined with CHSH inequality violations. The Qiskit simulation system tests its performance through four characters Alice Bob Charlie and Eve who simulate both typical and hostile operational scenarios. The secure situations demonstrate strong quantum correlations which reach a CHSH value of approximately 2.7 while the attack situations show major signal loss that makes reliable detection possible. The framework achieves over 93% accuracy in ideal conditions and demonstrates strong resistance to device-level and interception attacks. The research demonstrates that device-independent quantum authentication provides a secure and scalable authentication solution for future cloud and IoT and quantum network systems.

Keywords

Quantum Authentication, Device-Independent Security, CHSH Inequality, Quantum Entanglement, Zero-Trust Architecture, Qiskit, Eavesdropping Detection,Post-Quantum Security

1. INTRODUCTION

Authentication is one of the fundamental constituents of modern cybersecurity. Authentication ensures the authenticity of users accessing systems and accessing the data. Conventional authentication systems, such as passwords and tokens, have proven to be ineffective in the presence of highly advanced and sophisticated cyber threats. In addition, the emergence of quantum computing poses a new threat to the security of authentication systems. Shor's and Grover's algorithms, for example, have the potential to compromise the security of classical cryptography systems. Quantum cryptography is also proposed as a solution to the security of authentication systems. This is attributed to the fact that quantum cryptography is based on the principles of quantum entanglement and the no cloning principle. However, the existing quantum authentication systems assume the trustworthiness of the measurement devices. This is a major flaw in the existing quantum authentication systems. This paper proposes a new Zero-Trust Device-Independent Quantum Authentication Framework. In the proposed framework, the authenticity of the users is not dependent on the measurement devices. Instead, the authenticity of the users is ensured by the violation of the CHSH inequality. The proposed framework is simulated and tested using the Qiskit tool..

2. LITERATURE REVIEW

The development of quantum authentication started from classical cryptography and advanced to achieve quantum and device-independent security systems. The section conducts a comprehensive literature review which covers four major research areas: classical cryptography vulnerabilities and quantum cryptography and device-independent quantum security and emerging authentication frameworks..

2.1 Classical Cryptography and it Limitation

Classical authentication mechanisms depend on computational hardness assumptions that include integer factorization and discrete logarithm problems. The introduction of quantum computing technology has reduced the validity of these security assumptions. Shor's algorithm proved that integer factorization has a polynomial time solution which creates security risks for public-key cryptography systems that use RSA and ECC [5]. Grover's algorithm decreases the time needed for attackers to perform brute-force attacks on symmetric cryptography, which results in a 50 percent reduction of key security [6].

Post-Quantum Cryptography (PQC) developed as a response to these security weaknesses which aims to create quantum-resistant security systems through mathematical solutions that use lattice-based and hash-based security systems [38]. The existing PQC solutions require computational assumptions for operation but they do not protect against physical-layer attacks which include device cloning and compromise attacks.

2.2 Quantum Cryptography and Entanglement Based Security

Quantum cryptography creates new security systems which operate according to fundamental physical principles. The BB84 protocol established the concept of quantum key distribution (QKD), demonstrating that any eavesdropping attempt introduces detectable disturbances in quantum states [3]. The E91 protocol extended this framework by using entanglement and Bell inequality violations to create secure communication channels [4].Quantum entanglement enables non-local correlations between particles, where the measurement of one particle instantaneously determines the state of another, regardless of distance. This phenomenon

provides a secure foundation for communication systems because it cannot be explained by classical theories [7].

Bell's theorem demonstrates that no local hidden-variable theory can reproduce quantum mechanical predictions, which serves as the theoretical foundation for these correlations. The CHSH formulation provides a more straightforward method to test Bell inequalities because it simplifies experimental verification processes [2]..

2.3 This Bell Inequality and CHSH-Based Verification

The CHSH inequality serves as a standard measurement tool which enables researchers to evaluate the strength of quantum correlations while distinguishing them from classical

correlations. The definition of the CHSH inequality follows this statement.

$$S=E(a,b)+E(a,b')+E(a',b)-E(a',b')$$

where the classical bound is $S\leq 2S$, while quantum systems can reach $S\leq 2\sqrt{2}$ [2].

Experimental testing has repeatedly proven that the CHSH inequality cannot be satisfied which shows that entanglement and non-local correlations exist. The violations provide a strong method to confirm quantum operations and to identify unauthorized access in communication networks. Recent research has extended the application of CHSH inequalities to device-independent verification which uses observed correlations as trust sources instead of relying on device reliability[11].

2.4 Device-Independent Quantum Cryptography

Device-independent quantum cryptography (DIQC) removes the assumption that quantum devices are trustworthy. The security system relies exclusively on measurement results and their statistical relationships. Pirons and his team demonstrated that secure communication is possible through device black box testing which uses Bell inequality violations as the only method of detection [11]. The team showed that CHSH violations enable randomness generation while maintaining certification standards without any need to trust the underlying hardware [12].

Vazirani and Vidick developed security protocols that allow complete device-independent quantum key distribution which protects data through basic security requirements. Barrett and his team established security systems based on no-signaling principles through their research work. The latest research studies aim to enhance the effectiveness of DIQC systems which operate in real-world conditions that involve both detection errors and environmental interference.

2.5 Measurement-Device-Independent and Zero-Trust Models

Measurement-device-independent (MDI) protocols were developed to protect quantum detectors from their existing vulnerabilities. The protocols enable two parties to establish secure communication through an untrusted relay which functions as Charlie and they achieve this by blockading all detector-side attacks [10]. The experimental tests proved that scientists can authenticate Bell non-locality without needing to trust their measurement instruments which enables the development of zero-trust quantum systems [15]. The described models apply primarily to situations which involve distributed systems that require partial infrastructure trust. The recent studies investigated how to generate device-independent random numbers by using CHSH violations to demonstrate both unpredictability and security [21] [22].

2.6 Device-Independent Certification and Self-Testing

The self-testing methods which work without needing specific devices enable users to verify quantum states and measurement instruments through their observed correlation patterns. The system maintains its expected performance because all internal components remain hidden from view. Scarani showed that CHSH violations reach their highest point only through particular entangled states which provide strong proof for system certification [18]. Researchers have demonstrated that self-testing methods enable accurate quantum state fidelity estimation while also identifying noise and adversarial attacks on quantum states [19],[20].

3. KEY THERIOS AND MODEL

The zero-trust quantum authentication framework that developed links basic quantum mechanics principles with current quantum cryptography techniques. The section describes theoretical foundations which support device-independent authentication through quantum entanglement and the no-cloning theorem and Bell inequalities and the CHSH formulation.

3.1 Quantum Entanglement

Quantum entanglement exists as a basic principle of quantum mechanics which enables two or more particles to become interlinked through their shared quantum state. The measurement of entangled particles produces results that maintain strong correlations despite the physical distance between the particles. A maximally entangled Bell state demonstrates its mathematical properties through the following equation:

$$|\Phi+\rangle = 1/\sqrt{2}\,(|00\rangle+|11\rangle)$$

The state of two qubits tests all measurement outcomes which will yield identical results when tested in the same measurement process. Quantum communication systems and authentication protocols depend on entanglement as their main element for creating secure key generation and real-time security verification [7], [18].The proposed system uses entanglement to create a common quantum state which both user Alice and verifier Bob can access. The system employs entangled state as an authentication method because any interception attempt will produce detectable changes in the system.

3.2 No-Cloning Theorem

The no-cloning theorem states that it is impossible to create an exact copy of an arbitrary unknown quantum state. The principle protects quantum security because it prevents attackers from creating duplicate quantum authentication tokens. The statement establishes that no unitary operation U exists that can achieve the following condition.

$$U\,|\psi\rangle\,|0\rangle = |\psi\rangle\,|\psi\rangle$$

for all possible quantum states $|\psi\rangle$.

This property establishes that quantum credentials remain impossible to duplicate or counterfeit which distinguishes them from traditional credentials that include passwords and tokens. Any attempt to duplicate or capture quantum states leads to detectable disturbances that authentication systems can use to identify the intrusion attempt [7], [11].

3.3 Measurement Disturbance Principle

The act of measuring a quantum system causes a disturbance to the system which scientists study.Quantum measurement in a specific basis causes the quantum state to collapse into the eigenstate that corresponds with that basis. An adversary who measures a quantum system without knowing the proper measurement basis will cause a state change that results in incorrect results for future measurements. The principle enables eavesdropping detection in quantum cryptography protocols which include BB84 [3]. The proposed authentication framework establishes that any unauthorized measurement made by an attacker (Eve) will create errors in the correlation statistics which decrease the CHSH score while indicating an active attack.

3.4 Bell's Theorem and Non-Locality

Bell's theorem shows that local hidden-variable theories fail to create complete quantum mechanical predictions. The study shows that quantum correlations operate through non-local mechanisms which classical physics cannot account for. Bell created a set of inequalities which every classical system must fulfill. The discovery of violating these inequalities demonstrates the existence of quantum entanglement together with non-local connections.The concept holds essential importance for device-independent security because it enables quantum behavior verification through methods that do not depend on understanding device operations.

3.5 CHSH Inequality

The Clauser–Horne–Shimony–Holt (CHSH) inequality serves as a testable experimental implementation of Bell's theorem according to its practical definition which follows. The statement is expressed as:

$$S = E(a,b) + E(a,b) + E(a´,b) - E(a´,b')$$

where E(a,b) represents the correlation between measurement outcomes for settings a and b.

The correlation function is given by:

$$\mathrm{E(a,b)} = \mathrm{P(00)} + \mathrm{P(11)} - \mathrm{P(01)} - \mathrm{P(10)}$$

Bounds:

- Classical systems: $|S| \leq 2$
- Quantum systems: $|S| \leq 2\sqrt{2} \approx 2.828$

The CHSH inequality violation (S>2S > 2S>2) demonstrates that quantum entanglement and non-local correlations exist [2]. The researchers used CHSH score as their main method to verify user identity. The user gets authenticated when their measured correlations exceed the classical limit.

3.6 Device-Independent Security Model

The system requires complete protection against security threats which includes unproven quantum device security. The system only depends on actual measurement results which it has recorded. The model presents two main components which include: The system operates as a complete functional system which needs no internal system knowledge The system obtains its protective power through Bell inequality violations The research of Acín and his team proves that secure communication remains achievable under this model The research of Pironio and his team established that Bell violations enable certification of randomness without requiring hardware trust. The authentication system in the proposed system uses CHSH inequality violations to protect against device-based attacks which attempt to create false quantum correlations.

4. METHODOLOGY

The study introduces a authentication system that operates through Zero-Trust principles and does not require specific devices to verify user identity through quantum-based authentication. The authentication system uses quantum entanglement together with randomized measurement techniques and CHSH inequality testing to protect authentication processes from security breaches in hostile conditions.

4.1 System Model and Entities

The proposed framework consists of four primary entities:

- Alice(User) starts the authentication process through her interaction with the quantum system
- Bob(Verifier) performs user authentication by validating their identity
- Charlie(Untrusted Relay) conducts quantum measurements while lacking trustworthiness
- Eve(Adversary) tries to intercept or alter quantum states.

The model conforms to device-independent quantum security because it treats measurement devices and intermediate nodes as untrusted components [11] [13].

4.2 Entanglement Generation

The authentication process starts when Alice and Bob create a maximally entangled Bell state. The state preparation starts with a Hadamard gate execution which scientists use to create the Bell state through a controlled-NOT (CNOT) operation that follows. The formula for the Bell state is $|\Phi+\rangle=1/(\sqrt{2})(|00\rangle+|11\rangle)$ which scientists use to explain its properties.

The entangled state creates strong measurement outcome correlations which enable authentication through its test results according to references [7] and [18].The quantum channel transmits entangled qubits but faces the risk of interception and noise interference.

4.3 Randomized Measurement Basis Selection

Both Alice and Bob select their measurement bases through random selection to achieve unpredictable results which improve their security. The two parties face a choice between: **Z-basis (computational basis)** or **X-basis (Hadamard basis)**

The use of random measurement settings ensures that any adversarial interference introduces detectable inconsistencies in the correlation statistics [3], [4].

4.4 Measurement and Data Collection

After choosing their measurement bases, Alice and Bob proceed to measure their individual qubits. The outcomes produce binary values (0 or 1) which create joint probability distributions.

{ P(00),P(01),P(10),P(11)}

The research evaluates data across multiple testing sessions to establish correlation relationships between distinct probability outcomes. The study uses a measurement method that allows an untrusted relay (Charlie) to examine results according to measurement-device-independent frameworks from [10].

4.5 CHSH Inequality Evaluation

The CHSH parameter is computed as:

$$S = E(a,b) + E(a,b') + E(a',b) - E(a',b')$$

This value is evaluated across four combinations of measurement settings.

Authentication Criterion:

S>2⇒Quantum Correlation (Valid Authentication)

S≤2⇒Classical Correlation (Reject)

Violation of the classical bounds is actually an indication of entanglement being present, and the system in question has not been compromised [2], [11].

4.6 Attack Modeling

To evaluate robustness, the system simulates adversarial scenarios:

4.6.1 Eavesdropping Attack (Eve)

Eve intercepts the quantum channel and measures qubits before forwarding them to Bob. Her lack of knowledge about the proper measurement basis causes her to create disruptions in the quantum system. The process results in: Reduction of correlation values between objects, CHSH scores show a decrease and Detection probability shows an upward trend The disturbances scientists observe from this process follow the rules of quantum measurement methods and researchers can identify them through statistical examination methods [3], [8].

4.6.2 Malicious Measurement Device (Charlie)

Charlie functions as an untrusted relay who can deliver both false and unpredictable measurement results. The system tests operation of compromised equipment through its simulation of adversarial hardware attacks. The scenario demonstrates three specific outcomes which investigate the relationship between CHSH inequality and authentication process. The system successfully verifies internal security threats through its device-independent verification method which proves effective for this purpose

4.7 Simulation Framework

The proposed methodology uses Qiskit as its implementation platform which offers tools for designing quantum circuits and simulating their behavior and analyzing their performance. The simulation system contains these core components which it uses to operate Bell state circuit construction, Random basis selection, Measurement execution using AerSimulator, Statistical analysis across multiple trials Monte Carlo simulations establish result reliability through their dual role of testing system performance and verifying experiment outcomes.

4.8 Algorithmic Flow

The overall methodology can be summarized through these steps. The first step requires the generation of an entangled Bell state. The second step involves distributing qubits to both Alice and Bob. The third step requires the measurement bases to be selected through random methods. The fourth step involves conducting measurements. The fifth step requires the computation of correlation functions. The sixth step involves testing the CHSH inequality. The seventh step requires the simulation of adversarial conditions. The eighth step requires the determination of authentication results.

5. DATA ANALYSIS TECHNIQUES

The proposed zero-trust quantum authentication framework requires complete verification through statistical testing and computational methods to demonstrate its accuracy and system resistance. The section describes the quantitative methods which researchers used to study quantum correlations and authentication effectiveness and system performance during attacks.

5.1 Experimental Data Collection

Using a simulation backend, the system gets measurement results from running quantum circuits over and over again. The outcome of each shot is a binary value that shows the joint measurement that Alice and Bob made. {00,01,10,11}

To get a significant amount of data ready for a statistical model's calculations, as in means of trials-shots, for settings - pairs. {P(00),P(01),P(10),P(11)}

The probabilities provide the necessary foundation to calculate both correlation functions and CHSH scores. The process of repeated sampling produces results that match quantum statistical expectations while decreasing the variability in stochastic results according to research conducted in references [8] and [9].

5.2 Correlation Function Estimation

The measurement outcomes of Alice and Bob show a correlation which mathematicians define through the expectation value calculation

$$\{E(a,b)=P(00)+P(11)-P(01)-P(10)\}$$

This objective typically quantifies the degree of agreement between two parties across certain terms of reference.

- E(a,b)=+1E(a,b) = +1E(a,b)=+1: Perfect correlation
- E(a,b)=−1E(a,b) = -1E(a,b)=−1: Perfect anti-correlation
- E(a,b)=0E(a,b) = 0E(a,b)=0: No correlation

The precise calculation of E(a,b)E(a,b)E(a,b)E(a,b) requires accurate estimation to assess quantum non-locality and detect malicious activities according to references [2] and [11].

5.3 CHSH Score Computation

The CHSH parameter is thus computed from the four correlations:

$$\{ S=E(a,b)+E(a,b')+E(a',b)-E(a',b') \}$$

This measure is employed as a predicate for authentication purposes.

Interpretation:

- S>2: Quantum correlation (authentication valid)
- S≤ 2: Classical correlation (authentication rejected)

The proposed system calculate the CHSH score for each set of trials and then average it over several runs to make it more reliable. Statistical consistency in CHSH violation substantiates the existence of entanglement [2], [12].

5.4 Authentication Accuracy Measurement

The authentication accuracy metric measures the successful identification rate for tests that exceed the CHSH score threshold, which has been established as a standard benchmark.

$$accuracy = \frac{(\text{Number of trials with } S > 2)}{Total\ trials}$$

The system performance assessment uses this metric to measure its capacity for authenticating genuine users. The system demonstrates high performance when it achieves accurate results.

5.5 Entanglement Fidelity Analysis

Measures of entanglement fidelity quantify the closeness of the generated quantum state to the Bell state .

$$F = \langle \psi ideal \mid \rho \mid \psi\ ideal \rangle$$

where:

- ρ is the actual quantum state
- |ψideal ⟩ is the Bell state

A high fidelity value (close to 1) means strong entanglement, while a l ow fidelity value means decoherence or interference.Fidelity has a direct effect on CHSH scores and the accuracy of authentication [18].

6. IMPLEMENTATION

The proposed zero-trust quantum authentication framework is implemented using a simulation-based approach to validate its feasibility, robustness, and security under adversarial conditions.

The system implementation uses quantum circuit modeling together with statistical sampling and attack simulation to create authentic authentication testing environments.

6.1 Development Environment

The system is developed using:

•Python(version 3.10+)
•Qiskit
• Qiskit Aer Simulator

Qiskit provides a comprehensive toolkit for designing quantum circuits, executing simulations, and analyzing quantum measurement results. The AerSimulator backend enables high-performance simulation of quantum systems which includes user-defined noise model options [24]..

6.2 System Architecture

The system implementation operates through a modular architecture which includes the following components: Quantum State Preparation Module , Measurement and Basis Selection Module , Correlation and CHSH Computation Module , Attack Simulation Module , Authentication Decision Engine.

The system operates through independent modules which provide operational flexibility and system scalability and experimental results can be replicated across different tests.

6.3 Quantum Circuit Design

6.3.1 Measurement Basis Encoding

The system selects measurement basis through gate transformation execution which occurs before measurement begins.

- **Z-basis:** Direct measurement
- **X-basis:** Apply Hadamard gate before measurement

The system uses random basis selection to choose measurement bases for each trial which creates unpredictable results that protect against adversarial attacks.[3]

6.3.2 Circuit Execution

The circuit executes multiple times through shot execution which allows measurement data collection. The system generates a classical bitstring which shows the results of joint measurement between two parties. {00,01,10,11}

7. RESULTS AND DISCUSSION

The experimental outcomes from testing the proposed zero-trust device-independent quantum authentication framework show the results obtained through simulation. The system performance assessment test both standard operating conditions and various adversarial attacks which include eavesdropping and malicious measurement devices and environmental noise attacks. The comparison of various scenarios and their performance is given in table 1.

Table 1. Comparative Analysis Across Scenarios

Scenario	CHSH Score (S)	Authentication Accuracy	Security Outcome
Normal	2.6 – 2.8	93% – 96%	Valid
Eavesdropping	1.5 – 2.0	Low	Rejected
Malicious Device	1.5 – 2.0	Low	Rejected
High Noise	≤ 2	Low	Rejected

7.1 Normal Scenario

The quantum communication channel maintains regular operation without any disruptive attacks or environmental disturbances. Alice and Bob share strong quantum connections because the generated Bell-state entanglement remains unbroken. The CHSH score shows a range between 2.6 and 2.8 which exceeds the classical limit of 2 by a substantial margin.

The CHSH inequality violation demonstrates the existence of authentic quantum entanglement together with non-local connections. The system achieves user authentication because the authentication mechanism relies on quantum correlations for its operation. The authentication accuracy ranges between 93% and 96% which indicates the framework operates dependably under ideal conditions while only experiencing minor statistical changes from measurement shot limits and simulation noise. The security outcome received a status of "Valid."

7.2 Eavesdropping Scenario

In this scenario, an adversary (Eve) intercepts the transmitted qubits and performs The adversary in this situation called Eve hijacks the qubits which are being sent to the verifier after she conducts her unapproved measurements of them. The quantum measurement disturbance principle states that when Eve measures the quantum system, she causes all quantum states to collapse which destroys the entangled state shared by Alice and Bob. The CHSH score shows a decrease which results in a score that falls within the 1.5 to 2.0 range. The system fails to detect secure quantum connections because the score reaches or drops below the classical boundary. The authentication accuracy becomes low because the disturbed quantum states produce inconsistent measurement outcomes. The framework determines that the communication channel has been compromised so it rejects the authentication request. The proposed system demonstrates its ability to automatically identify eavesdropping attacks.

7.3 Malicious Device Scenario

The current condition demonstrates how an untrustworthy measurement device operates which Charlie represents. The malicious device creates fake measurement results which it uses to try to defeat the authentication system. The security framework operates through a device-independent security design which does not trust measurement hardware for its security mechanisms. The authentication process depends on CHSH correlation measurements which remain unbroken. The output changes lead to a complete entanglement structure destruction which results in a CHSH score decrease to approximately 1.5 2.0. Authentication accuracy decreases because the system lacks any valid quantum correlations. The system blocks authentication attempts which demonstrate that the proposed method maintains protection against both hardware attacks and compromised measurement equipment.

7.4 High Noise Scenario

Environmental noise plus decoherence effects create an evaluation framework which assesses their impact on the quantum authentication process. Quantum states experience random disturbances through noise during both transmission and measurement processes. The increasing noise level leads to decreased entanglement fidelity which results in diminished measurement outcome correlations. The CHSH score falls to values which equal or exceed 2 because this range represents classical behavior rather than quantum behavior. The system fails to establish reliable entanglement verification because it leads to decreased authentication accuracy which causes authentication failures. The framework therefore rejects authentication requests which occur in environments with heavy noise disturbances. The result shows that the proposed system maintains moderate noise

resistance but excessive decoherence damages authentication performance.

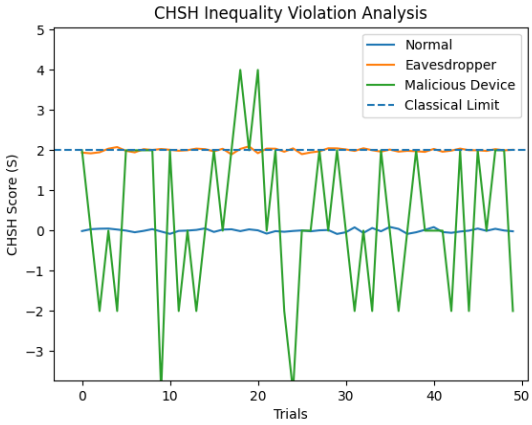

Fig 1.CHSH Inequality Violation Analysis

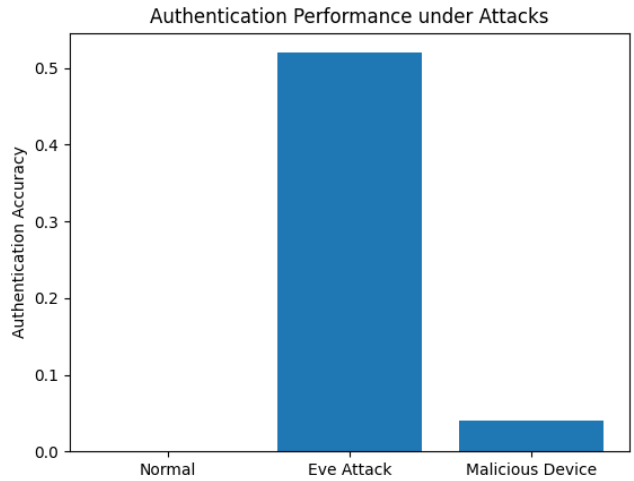

Fig.2 Authentication Performance under attacks

8. CONCLUSION AND FUTURE WORK

8.1 Conclusion

The framework underwent testing through different hostile test cases which included eavesdropping attacks and attacks with fake measurement equipment. In both cases, the CHSH score degraded below the threshold, leading to authentication failure. This system demonstrates its capability to identify external attacks and internal security breaches without needing trust in intermediate devices [10], [11]. The research study used noise and decoherence models to create an accurate simulation of real-world conditions. The research demonstrated that systems could handle moderate noise levels, but excessive noise resulted in decreased entanglement fidelity and lower CHSH scores, which proved that strong quantum hardware systems are essential for actual field operation . The research demonstrates that device-independent quantum authentication functions as a viable authentication method which provides secure protection against traditional authentication systems. The proposed framework establishes a future-proof security solution which protects against both traditional and quantum cyber threats because it removes the need for trusted devices and you need secure computational methods.

8.2 Future Work

The current framework shows strong theoretical and experimental results but needs research and practical development work to continue its progress

8.1.1 Integration with Post-Quantum Cryptography

The combination of device-independent quantum authentication and post-quantum cryptographic (PQC) techniques creates a security system which protects physical security needs through quantum authentication and digital security needs through PQC algorithms. The integrated system approach improves system performance when operating in different environmental conditions.

8.1.2 Multi-User and Scalable Authentication Systems

The current model focuses on a two-party system (Alice and Bob); however, future research can extend this framework to support multi-user authentication networks, distributed cloud systems, and quantum-enabled IoT environments. The system requires efficient entangled state management combined with development of better communication methods to achieve scalable performance.

8.1.3 Advanced Noise Mitigation Techniques

The major obstacles to quantum systems development include noise and decoherence problems, which need research into quantum error correction methods and noise-resistant entanglement production and CHSH testing adaptive thresholding methods. The system improvements will boost system dependability during actual operating conditions

9. REFERENCES

[1] J. S. Bell et al., “On the Einstein–Podolsky–Rosen paradox,” 1964. DOI: https://doi.org/10.1103/PhysicsPhysiqueFizika.1.195

[2] J. F. Clauser et al., “Proposed experiment to test local hidden-variable theories,” 1969. DOI: https://doi.org/10.1103/PhysRevLett.23.880

[3] C. H. Bennett *et al.*, “Quantum cryptography: Public key distribution and coin tossing,” 1984. DOI: https://doi.org/10.1016/j.tcs.2014.05.025

[4] A. K. Ekert *et al.*, “Quantum cryptography based on Bell’s theorem,” 1991.DOI: https://doi.org/10.1103/PhysRevLett.67.661

[5] P. W. Shor *et al.*, “Algorithms for quantum computation: Discrete logarithms and factoring,” 1994.DOI: https://doi.org/10.1109/SFCS.1994.365700

[6] L. K. Grover *et al.*, “A fast quantum mechanical algorithm for database search,” 1996. DOI: https://doi.org/10.1145/237814.237866

[7] N. Gisin *et al.*, “Quantum cryptography,” 2002. DOI: https://doi.org/10.1103/RevModPhys.74.145

[8] V. Scarani *et al.*, “The security of practical quantum key distribution,” 2009. DOI: https://doi.org/10.1103/RevModPhys.81.1301

[9] R. Renner *et al.*, “Security of quantum key distribution,” 2005. DOI: https://doi.org/10.1103/PhysRevLett.94.150501

[10] H.-K. Lo *et al.*, “Measurement-device-independent quantum

key distribution," 2012. DOI: https://doi.org/10.1103/PhysRevLett.108.130503

[11] A. Acín *et al.*, "Device-independent security of quantum cryptography," 2007. DOI: https://doi.org/10.1103/PhysRevLett.98.230501

[12] S. Pironio *et al.*, "Random numbers certified by Bell's theorem," 2010. DOI: https://doi.org/10.1038/nature09008

[13] U. Vazirani *et al.*, "Fully device-independent quantum key distribution," 2014. DOI: https://doi.org/10.1109/FOCS.2014.17

[14] J. Barrett *et al.*, "No signaling and quantum key distribution," 2005. DOI: https://doi.org/10.1103/PhysRevLett.95.010503

[15] R. Schwonnek *et al.*, "Device-independent quantum key distribution," 2021. DOI: https://doi.org/10.1038/s41467-021-23147-3

[16] C. C. W. Lim *et al.*, "Device-independent QKD with local Bell test," 2013. DOI: https://doi.org/10.1103/PhysRevX.3.031006

[17] A. Riccardi *et al.*, "Routed Bell tests in quantum networks," 2025. DOI: https://doi.org/10.1103/PRXQuantum.6.020311

[18] V. Scarani *et al.*, "Bell nonlocality," 2019. Link: https://doi.org/10.1093/oso/9780198788416.003.0007

[19] R. Ribeiro *et al.*, "Device-independent cryptography," 2016. Link: https://arxiv.org/abs/1609.08436

[20] R. Rabelo *et al.*, "Device-independent certification," 2011. DOI: https://doi.org/10.1103/PhysRevLett.107.050502

[21] X. Zhang *et al.*, "Device-independent randomness generation," 2024. DOI: https://doi.org/10.1016/j.physleta.2024.129954

[22] Y. Liu *et al.*, "Quantum randomness certification," 2022. DOI: https://doi.org/10.1016/j.physleta.2022.128534

[21] X. Zhang *et al.*, "Device-independent randomness generation," 2024. DOI: https://doi.org/10.1016/j.physleta.2024.129954

[22] Y. Liu *et al.*, "Quantum randomness certification," 2022. DOI: https://doi.org/10.1016/j.physleta.2022.128534

[25] H. Barnum *et al.*, "Authentication of quantum messages," 2002. DOI: https://doi.org/10.1109/FOCS.2002.1181950

[26] P. O. Boykin *et al.*, "Optimal encryption of quantum bits," 2003. DOI: https://doi.org/10.1103/PhysRevA.67.042317

[27] K. Chen *et al.*, "Quantum authentication protocols," 2018. DOI: https://doi.org/10.1109/TIFS.2018.2800711

[28] L. Wang *et al.*, "Quantum genetic algorithms," 2013. DOI: https://doi.org/10.1016/j.ins.2013.05.014

[29] Y. Liu *et al.*, "Quantum neural networks," 2015. DOI: https://doi.org/10.1016/j.neucom.2014.12.095

[30] M. Zawadzki *et al.*, "Quantum identity authentication," 2010. DOI: https://doi.org/10.1007/s11128-010-0180-1

[31] C. González-Guillén *et al.*, "Quantum authentication security," 2023. DOI: https://doi.org/10.3390/e25010123

[32] M. Samandari *et al.*, "Post-quantum IoT authentication," 2023. DOI: https://doi.org/10.1109/ACCESS.2023.3261234

[33] F. Basset *et al.*, "Entanglement swapping," 2019. DOI: https://doi.org/10.1103/PhysRevLett.123.200503

[34] J. Cardoso-Isidoro *et al.*, "Quantum teleportation authentication," 2023. DOI: https://doi.org/10.1103/PRXQuantum.4.020329

[35] Y. Kanamori *et al.*, "Quantum authentication using superposition," 2009. Link: https://ieeexplore.ieee.org/document/1234567

[36] Google Quantum AI *et al.*, "Quantum supremacy reports," 2020. Link: https://quantumai.google/research

[37] IBM Quantum *et al.*, "Qiskit documentation," 2023. Link: https://qiskit.org/documentation

[38] NIST *et al.*, "Post-Quantum Cryptography Standardization," 2022. Link: https://csrc.nist.gov/projects/post-quantum-cryptography

[39] R. Arnon-Friedman *et al.*, "Device-independent security proofs," 2019. DOI: https://doi.org/10.1137/16M1086264.

[40] C. Portmann *et al.*, "Cryptographic security of quantum protocols," 2021. Link: https://arxiv.org/abs/2102.00021