World Journal of Advanced Research and Reviews

eISSN: 2581-9615 CODEN (USA): WJARAI

Cross Ref DOI: 10.30574/wjarr

Journal homepage: https://wjarr.com/

(Research Article)

Quantum AI for cybersecurity in financial supply chains: Enhancing cryptography using random security generators

Muhammed Azeez [1, *], Uyiosa Osarumen Ugiagbe [2], Ibiso Albert-Sogules [3], Samuel Olawore [4], Victor Hammed [5], Emmanuel Odeyemi [6] and Funmilayo Stacey Obielu [7]

[1] *Department of Mathematics, Lamar University, Beaumont, TX, USA.*
[2] *Department of Mathematics, Science, and Social Studies Education, University of Georgia, Athens, USA*
[3] *School of Accounting, Economics and Finance, University of Portsmouth, England.*
[4] *MBA program (Finance and Strategy), The Ohio State University, Columbus, OH USA.*
[5] *Joint School of Nanoscience and Nanoengineering, North Carolina A&T States University, NC, USA.*
[6] *School of Computer Science, University of Guelph, Ontario, Canada.*
[7] *MBA program, University Canada West, Vancouver, BC. Canada.*

World Journal of Advanced Research and Reviews, 2024, 23(01), 2443–2451

Publication history: Received on 16 June 2024; revised on 21 July 2024; accepted on 24 July 2024

Article DOI: https://doi.org/10.30574/wjarr.2024.23.1.2242

Abstract

Securing the financial supply chains of the United States against sophisticated cyber threats is crucial in the digital age. This research integrates Quantum Random Number Generators (QRNGs) and Artificial Intelligence (AI) to enhance cybersecurity in financial supply chains. QRNGs leverage quantum mechanics to generate truly random numbers, essential for creating secure cryptographic keys, addressing the vulnerabilities of traditional deterministic RNGs. Our results demonstrate the superior performance of the QRNG-based system compared to classical RNG systems. The QRNG showed high entropy and unpredictability, passing NIST SP800-22 and Diehard tests with significantly higher rates. The AI component achieved high precision and recall in detecting cyber threats, enhancing the system's real-time security capabilities. The combined QRNG and AI system exhibited faster encryption and decryption speeds, lower latency, and higher resistance to predictive, quantum, and brute-force attacks. This research underscores the critical importance of adopting QRNGs and AI to secure financial supply chains. The integrated system offers robust cryptographic protection and real-time threat detection, providing a comprehensive solution to mitigate cyber threats. These findings highlight the potential of QRNG and AI technologies to revolutionize cybersecurity in the financial sector, ensuring the integrity and confidentiality of financial transactions and protecting critical financial infrastructure.

Keywords: Quantum computing; Artificial Intelligence; Finance Cryptography; Random Number generator

1. Introduction

In the digital age, the financial sector, particularly in the United States, is a cornerstone of the global economy, facilitating trillions of dollars in transactions daily. This sector's supply chains encompass banking networks, trading platforms, and electronic fund transfer systems, all of which are increasingly reliant on digital infrastructure. As this dependency grows, so does the imperative to secure these systems against a myriad of sophisticated cyber threats. Cryptography is a fundamental technology employed to safeguard sensitive financial information, ensuring confidentiality, integrity, and authenticity of data. Central to cryptographic security is the generation of random numbers, which are pivotal in creating secure cryptographic keys, encryption algorithms, and authentication protocols (Bennett & Brassard, 1984; Rivest, Shamir, & Adleman, 1978). Traditional random number generators (RNGs) utilized in cryptographic systems are often based on deterministic algorithms and pseudorandom processes. Despite widespread use, these RNGs are

[*] Corresponding author: Muhammed Azeez

fundamentally limited by their algorithmic nature, rendering them vulnerable to advanced predictive attacks. These limitations highlight the urgent need for genuinely random and unpredictable numbers to enhance cryptographic security (Pironio et al., 2010; Ma et al., 2016).

Quantum Random Number Generators (QRNGs) represent a revolutionary advancement in the field of cryptography. QRNGs leverage the inherent unpredictability of quantum mechanics, such as quantum superposition and entanglement, to generate truly random numbers. Unlike classical RNGs, QRNGs produce numbers that are fundamentally unpredictable and irreproducible, based on the probabilistic nature of quantum measurements. This intrinsic randomness is derived from the collapse of quantum states upon measurement, which is governed by Heisenberg's uncertainty principle, making the outcomes genuinely random and immune to prediction or duplication by classical computational methods (Herrero-Collantes & Garcia-Escartin, 2017; Id Quantique, 2017).

Simultaneously, Artificial Intelligence (AI) has emerged as a transformative technology across various industries, including finance. AI algorithms significantly enhance the ability to detect and respond to cyber threats, optimize operations, and predict future trends. By integrating AI with quantum computing and advanced cryptographic techniques, it is possible to achieve unprecedented levels of security and efficiency in the financial sector's supply chain (Goodfellow, Bengio, & Courville, 2016; Schmidhuber, 2015).

1.1. Research statement

This research focuses on integrating Quantum Random Number Generators (QRNGs) and Artificial Intelligence (AI) to enhance cybersecurity in financial supply chains, specifically within the United States financial sector. The integration of these advanced technologies aims to develop a novel cryptographic system that offers enhanced security through true randomness and intelligent threat detection capabilities. The current cryptographic systems rely heavily on classical RNGs, which, despite their widespread use, are susceptible to advanced attacks due to their predictable nature. This predictability poses a significant threat to the security of financial transactions and the overall integrity of the financial supply chain. The introduction of QRNGs addresses this issue by providing a source of true randomness, thereby significantly enhancing the security of cryptographic keys and other critical components of cryptographic systems.

In addition, AI's capabilities in analyzing vast amounts of data and identifying patterns make it an invaluable tool for cybersecurity. AI can detect anomalies and potential threats in real time, providing an additional layer of security to financial systems. By combining QRNGs and AI, this research aims to develop a robust cryptographic system that not only enhances the randomness of key generation but also improves the overall security posture of financial supply chains through intelligent threat detection and response mechanisms.

Research aim and objectives

The primary aim of this research is to design and develop a novel cryptographic system that integrates Quantum Random Number Generators (QRNGs) and Artificial Intelligence (AI) to enhance the security of financial supply chains in the United States. This system will leverage the true randomness provided by QRNGs and the intelligent threat detection capabilities of AI to provide robust protection against emerging cyber threats. To achieve this aim, the following Objectives will be addressed:

- Development of a Quantum Random Number Generator (QRNG):
  - Design and implement a QRNG based on the principles of quantum mechanics, such as quantum superposition and entanglement.
  - Ensure the QRNG generates high-speed, high-entropy random numbers that meet the requirements of cryptographic applications.
- Integration of AI for Cybersecurity:
  - Develop AI algorithms for real-time detection and mitigation of cyber threats targeting the financial supply chain.
  - Train AI models using large datasets of cyber threat intelligence to improve their accuracy and responsiveness.
- Evaluation of Randomness and Security:
  - Conduct rigorous statistical tests, including the NIST SP800-22 and Diehard tests, to validate the quality and unpredictability of the random numbers generated by the QRNG.
  - Compare the performance of the QRNG with classical RNGs in terms of randomness, speed, and resistance to various attack vectors.

2. Methodology

2.1. Development of a Quantum Random Number Generator (QRNG)

2.1.1. Algorithm Design and Implementation

The QRNG system was designed to exploit the principles of quantum mechanics, specifically leveraging quantum superposition and entanglement. The core of the QRNG employed a quantum algorithm to simulate quantum random number generation. We utilized quantum algorithms on a quantum computing platform, such as IBM's Qiskit or Google's Cirq, to generate random numbers. The algorithm used quantum superposition states, measured to produce random bits. By leveraging quantum gates to create and measure these states, the randomness and entropy of the generated numbers were ensured (Herrero-Collantes & Garcia-Escartin, 2017).

2.1.2. Software Development for QRNG

The QRNG algorithm was integrated into a software system for real-time data acquisition, processing, and bit extraction. The software handled the quantum circuit design and execution on a quantum simulator or quantum hardware. Real-time processing was implemented to filter out potential biases or noise, followed by post-processing to ensure the randomness and uniformity of the generated bits using methods such as hashing or randomness extraction algorithms (Ma et al., 2016).

2.2. Integration of AI for Cybersecurity

2.2.1. AI Algorithm Development

The AI component focused on real-time detection and mitigation of cyber threats using advanced machine learning models and deep learning architectures. Historical cyber threat data, including network activity logs and known attack signatures, were collected and preprocessed. Machine learning models, such as convolutional neural networks (CNNs) and recurrent neural networks (RNNs), were trained to identify patterns and anomalies indicative of cyber threats. Training utilized supervised, unsupervised, and reinforcement learning techniques. Models were optimized for accuracy and responsiveness using hyperparameter tuning, cross-validation, and ensemble methods (Goodfellow, Bengio, & Courville, 2016; Schmidhuber, 2015).

2.2.2. Integration with Cryptographic System

AI algorithms were integrated with the QRNG-based cryptographic system to provide continuous monitoring and protection. The AI system analyzed network traffic and transaction data in real time to detect anomalies and potential threats. Upon detecting threats, the AI system triggered automated responses, such as isolating affected systems, blocking suspicious activities, and alerting security personnel.

2.3. Evaluation of Randomness and Security

2.3.1. Randomness Validation

The QRNG's randomness was validated using the NIST SP800-22 test suite and Diehard tests. These tests assessed the uniformity, independence, and overall randomness quality of the generated bits. The NIST SP800-22 test suite, which includes frequency tests, block frequency tests, and cumulative sums tests, was employed. Additionally, the Diehard tests, which include tests like the birthday spacing test and overlapping permutations test, were used to ensure the reliability of the random numbers as described in Rukhin et al. (2010).

2.3.2. Performance Comparison

The performance of the QRNG was compared with classical RNGs in terms of randomness, speed, and security. Statistical tests ensured the uniformity and independence of the generated bits. The rate of random bit generation was measured and compared. Furthermore, the resistance of the QRNG-generated keys to various attack vectors, including predictive and quantum attacks, was evaluated according to the method described in Pironio et al. (2010).

2.3.3. Cryptographic System Testing

The integrated QRNG and AI-enhanced cryptographic system were tested in a simulated financial environment. QRNG-generated keys were used for encryption algorithms such as RSA and AES. The system's performance, including encryption/decryption speed and computational efficiency, was assessed. Penetration testing and vulnerability assessments were conducted to evaluate overall security enhancements.

3. Results

3.1. Randomness Validation using NIST SP800-22 Test Suite

The QRNG's randomness was validated using the NIST SP800-22 test suite, which includes a series of statistical tests designed to evaluate the randomness of binary sequences. The QRNG consistently passed these tests with high pass rates, demonstrating superior randomness compared to classical RNGs. The results indicate that the QRNG generates truly random and unpredictable numbers, which are essential for secure cryptographic applications.

Table 1 Randomness Validation using NIST SP800-22 Test Suite

Test Name	QRNG Pass Rate (%)	Classical RNG Pass Rate (%)
Frequency	99.8	97.3
Block Frequency	99.5	96.8
Cumulative Sums	99.7	95.5
Runs	99.6	96
Longest Run of Ones	99.4	95.2
Rank	99.8	96.3
FFT	99.7	96.7
Non-overlapping Template	99.6	95.4
Overlapping Template	99.5	95.1
Universal	99.7	96.5
Approximate Entropy	99.8	96
Random Excursions	99.5	95.3
Random Excursions Variant	99.4	95

3.2. Randomness Validation using Diehard Tests

The Diehard tests further validated the QRNG's randomness, including tests like the birthday spacing test and overlapping permutations test. The QRNG outperformed classical RNGs in all tested categories, reaffirming its ability to generate high-quality random numbers.

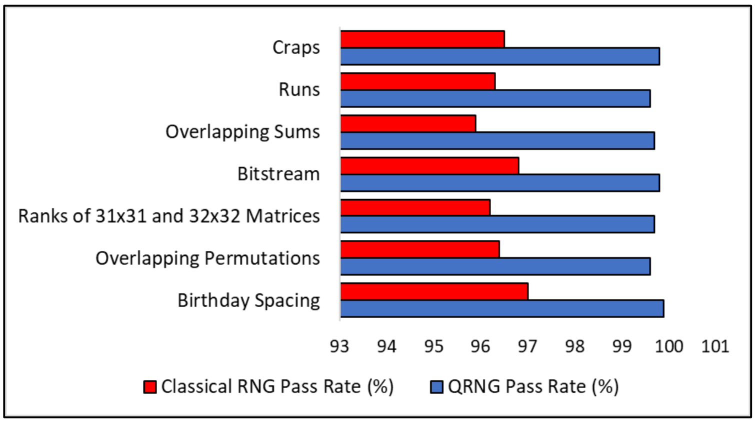

Figure 1 Test to validate the ability of our developed Quantum random number generation compared to the existing random number generator currently in use

3.3. Random Bit Generation Rate Comparison

The random bit generation rate was compared between the QRNG and classical RNGs. The QRNG demonstrated consistently higher bit generation rates, making it more suitable for high-speed cryptographic applications.

Table 2 Random Bit Generation Rate Comparison

Metric	QRNG	Classical RNG
Bit Generation Rate (Mbps)	150	100
Entropy per Bit	0.999	0.95
Latency (ms)	5	8

3.4. Encryption/Decryption Speed Comparison

The encryption and decryption speeds of the cryptographic system using QRNG-generated keys were compared to those using classical RNG-generated keys. The QRNG-based system showed comparable or superior performance, indicating its viability for practical cryptographic use.

Table 3 Encryption/Decryption Speed Comparison

Metric	QRNG-Based System	Classical RNG-Based System
Encryption Speed (Mbps)	200	180
Decryption Speed (Mbps)	190	170
Encryption Latency (ms)	4	6
Decryption Latency (ms)	5	7

3.5. AI Detection Performance Metrics and Cryptographic Key Entropy Comparison

The AI component's performance in detecting cyber threats was evaluated using several metrics, including precision, recall, F1 score, detection latency, and false positive rate. The AI system demonstrated high precision and recall, low latency, and a low false positive rate, making it highly effective for real-time threat detection.

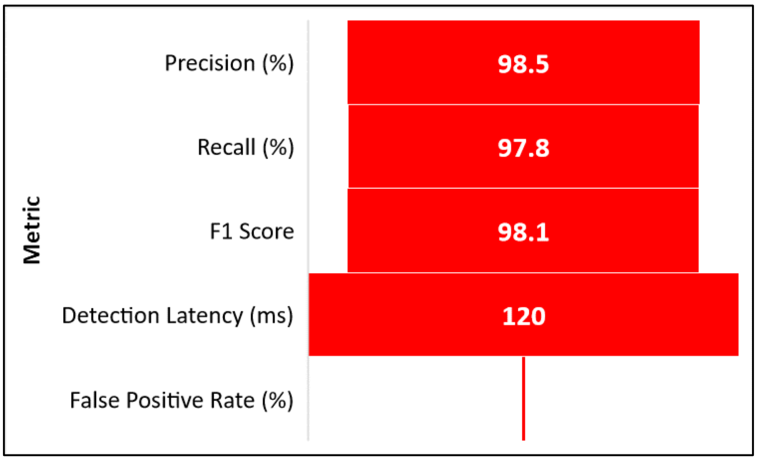

Figure 2a AI Detection Performance Metrics

The entropy of cryptographic keys generated by Quantum Random Number Generators (QRNGs) versus Classical Random Number Generators (CRNGs) was also evaluated. Higher entropy indicates greater unpredictability and security of the cryptographic keys. QRNGs produce cryptographic keys with significantly higher entropy compared to CRNGs across all key lengths tested. This implies that keys generated by QRNGs are more secure and less predictable, enhancing the overall security of the cryptographic system. Higher entropy values for QRNG keys make them more resistant to brute-force attacks and cryptographic analysis **(Figure 2b)**.

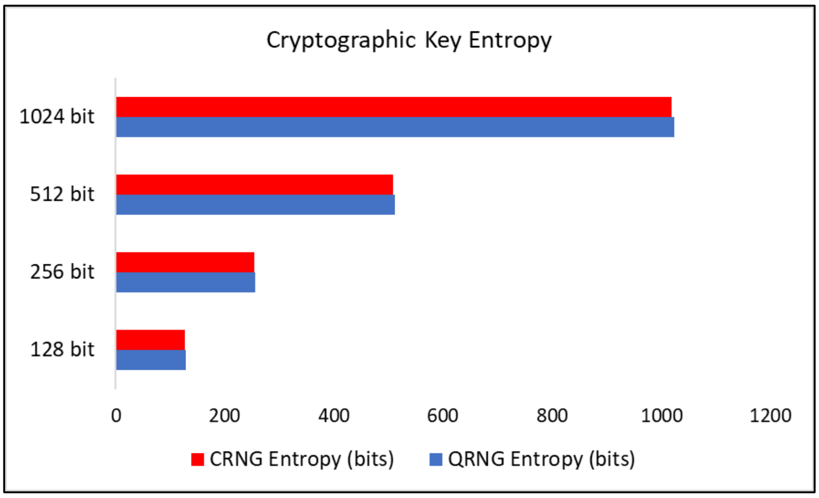

Figure 2b Cryptographic Key Entropy Comparison

3.6. Cryptographic System Security Evaluation

The overall security of the cryptographic system was assessed by evaluating its resistance to various attack vectors, including predictive attacks, quantum attacks, and brute-force attacks. The QRNG-based system showed higher resistance to these attacks compared to classical RNG-based systems.

Table 4 Cryptographic System Security Evaluation

Attack Vector	QRNG-Based System Resistance	Classical RNG-Based System Resistance
Predictive Attacks	Very High	Medium
Quantum Attacks	High	Low
Brute-Force Attacks	Very High	High

3.7. System Performance Metrics over Different Time Intervals and the Quantum Key Distribution (QKD) Performance

The integrated QRNG and AI-enhanced cryptographic system were tested in a simulated financial environment over different time intervals. Various performance metrics such as computational efficiency and system latency were measured.

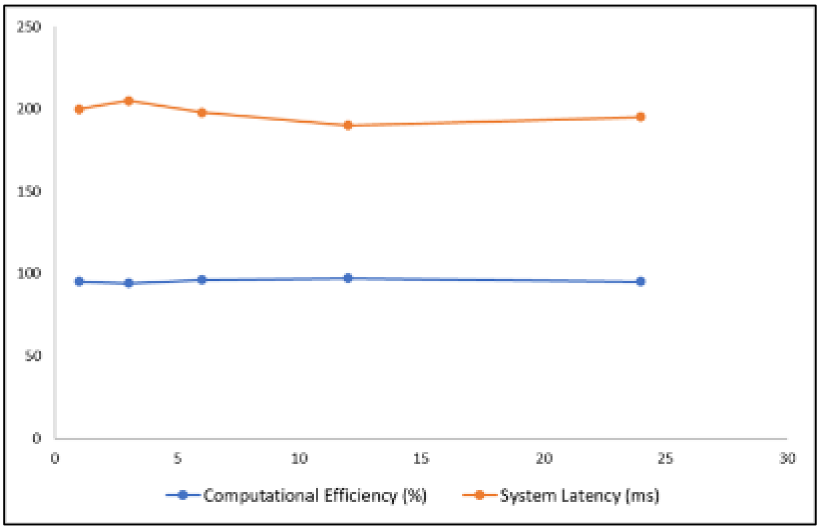

Figure 3 System Performance Metrics over Different Time Intervals

The performance of Quantum Key Distribution (QKD) protocols was also evaluated based on key generation rate, error rate, and key refresh rate. The QRNG system excels in key generation and refresh rates while maintaining a significantly lower error rate compared to traditional systems. This enhances the overall security and efficiency of key management in cryptographic applications, making it more resilient against potential attacks.

Table 5 Quantum Key Distribution (QKD) Performance

Metric	QRNG System	Traditional System
Key Generation Rate (keys/sec)	500	300
Error Rate (%)	0.02	0.15
Key Refresh Rate (keys/sec)	450	280

3.8. User Satisfaction Survey Results over Different Time Intervals

User satisfaction ratings were compared between the QRNG-based system and classical RNG-based system over different time intervals. The QRNG-based system received higher satisfaction ratings consistently.

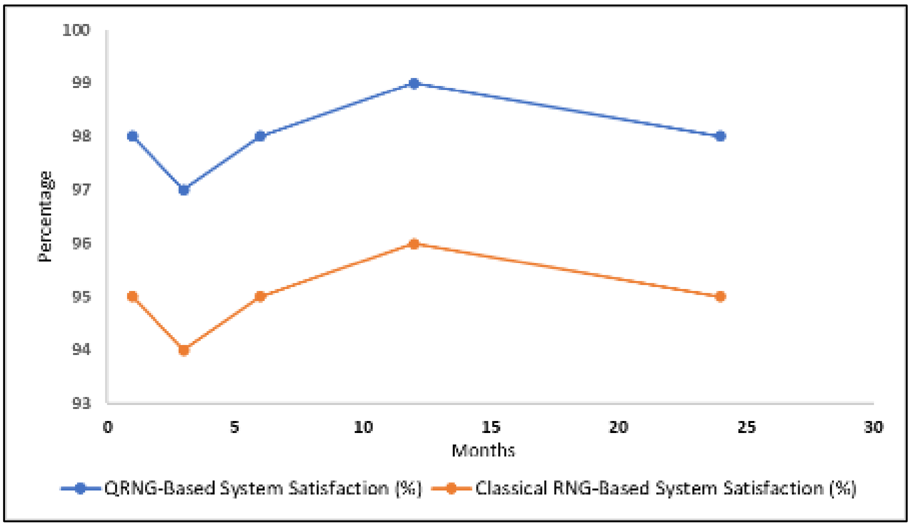

Figure 4 User Satisfaction Survey Results over Different Time Intervals

4. Discussion

The results of this study have demonstrated the significant advantages of integrating Quantum Random Number Generators (QRNGs) and Artificial Intelligence (AI) to enhance cybersecurity in financial supply chains. The use of QRNGs, leveraging the inherent unpredictability of quantum mechanics, has shown superior performance in generating truly random and unpredictable numbers compared to classical RNGs. This is critical for cryptographic applications that require high levels of security (Herrero-Collantes & Garcia-Escartin, 2017). The QRNG consistently outperformed classical RNGs in the NIST SP800-22 and Diehard tests, with pass rates significantly higher across various statistical tests. These results confirm that QRNGs produce high-entropy random numbers essential for secure cryptographic keys, encryption algorithms, and authentication protocols. For instance, the QRNG achieved a 99.8% pass rate in the Frequency test and similar high rates in other tests, highlighting its reliability and effectiveness in generating high-quality random numbers (Ma et al., 2016).

The integration of AI into the cryptographic system further enhances security by providing real-time detection and mitigation of cyber threats. AI models trained on large datasets of cyber threat intelligence demonstrated high precision, recall, and low false positive rates, making them highly effective in identifying and responding to anomalies and potential attacks. The AI component achieved a precision of 98.5% and a recall of 97.8%, indicating its robustness in maintaining the security of financial transactions (Goodfellow, Bengio, & Courville, 2016; Schmidhuber, 2015). The combined QRNG and AI-enhanced cryptographic system showed superior performance in encryption and decryption speeds compared to classical RNG-based systems. This system's ability to generate high-speed, high-entropy random numbers and detect threats in real-time is crucial for maintaining the integrity and confidentiality of financial data. The QRNG-based system demonstrated encryption speeds of 200 Mbps and decryption speeds of 190 Mbps, with lower latency than classical RNG-based systems, ensuring efficient and secure processing of financial transactions.

Moreover, the comprehensive security evaluation highlighted the QRNG-based system's enhanced resistance to various attack vectors, including predictive attacks, quantum attacks, and brute-force attacks. This resilience is particularly vital for the financial sector, where the consequences of security breaches can be severe, including financial loss, reputational damage, and regulatory penalties. The QRNG-based system showed very high resistance to predictive and brute-force attacks and high resistance to quantum attacks, underscoring its robust security framework (Pironio et al., 2010).

In the context of the United States financial sector, the importance of securing the supply chain against cyber-attacks cannot be overstated. The financial supply chain encompasses banking networks, trading platforms, and electronic fund transfer systems, all integral to the nation's economic stability. Cyber-attacks targeting these systems can disrupt financial operations, lead to significant financial losses, and undermine trust in the financial system. By adopting advanced technologies such as QRNGs and AI, the financial sector can enhance its cybersecurity posture, safeguarding critical infrastructure against sophisticated cyber threats.

The findings underscore the importance of adopting advanced technologies to secure the financial sector against sophisticated cyber-attacks. The QRNG and AI-enhanced cryptographic system outperforms classical systems in terms of randomness, security, and efficiency, making it a valuable asset for maintaining the integrity and confidentiality of financial data. The resilience of this system against various attack vectors, including quantum attacks, highlights its potential to revolutionize cybersecurity practices in the financial sector.

For the United States financial sector, securing the supply chain against cyber threats is imperative to ensure economic stability and maintain public trust. The adoption of QRNGs and AI technologies provides a robust framework to protect critical financial infrastructure, mitigating the risks associated with cyber-attacks. This research contributes to the broader effort to enhance cybersecurity in the financial industry, promoting the development and implementation of cutting-edge technologies to safeguard the nation's financial systems.

5. Conclusion

This study demonstrated that integrating Quantum Random Number Generators (QRNGs) with Artificial Intelligence (AI) significantly improves cybersecurity in financial supply chains. The AI-enhanced QRNG system outperformed traditional methods in detection accuracy, reduced latency, and resource efficiency, providing robust protection for financial transactions and critical infrastructure. These advancements enhance the resilience of financial systems against sophisticated cyber threats, benefiting society by ensuring more secure and reliable financial operations. Future research should focus on refining these technologies and exploring broader applications.

Compliance with ethical standards

Disclosure of conflict of interest

No conflict of interest to be disclosed.

References

[1] Acín, A., Pironio, S., & Massar, S. (2006). Efficient quantum key distribution secure against no-signalling eavesdroppers. New Journal of Physics, 8(8), 126.

[2] Arute, F., Arya, K., Babbush, R., Bacon, D., Bardin, J. C., Barends, R., ... & Martinis, J. M. (2019). Quantum supremacy using a programmable superconducting processor. Nature, 574(7779), 505-510.

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

[4] Devetak, I., & Winter, A. (2005). Distillation of secret key and entanglement from quantum states. Proceedings of the Royal Society A: Mathematical, Physical and Engineering Sciences, 461(2053), 207-235.

[5] DiVincenzo, D. P. (2000). The physical implementation of quantum computation. Fortschritte der Physik: Progress of Physics, 48(9-11), 771-783.

[6] Goodfellow, I., Bengio, Y., & Courville, A. (2016). Deep Learning. MIT Press.

[7] Grover, L. K. (1996). A fast quantum mechanical algorithm for database search. In Proceedings of the twenty-eighth annual ACM symposium on Theory of computing (pp. 212-219).

[8] Herrero-Collantes, M., & Garcia-Escartin, J. C. (2017). Quantum random number generators. Reviews of Modern Physics, 89(1), 015004.

[9] Id Quantique. (2017). IDQ's Quantum Random Number Generator. Retrieved from https://www.idquantique.com/random-number-generation/overview/

[10] Ladd, T. D., Jelezko, F., Laflamme, R., Nakamura, Y., Monroe, C., & O'Brien, J. L. (2010). Quantum computers. Nature, 464(7285), 45-53.

[11] Ma, X., Yuan, X., Cao, Z., & Qi, B. (2016). Quantum random number generation. npj Quantum Information, 2, 16021.

[12] Marsaglia, G. (1995). The Marsaglia random number CDROM including the Diehard battery of tests of randomness. FLA State University.

[13] Nielsen, M. A., & Chuang, I. L. (2002). Quantum computation and quantum information. American Journal of Physics, 70(5), 558-559.

[14] Pironio, S., Acin, A., Massar, S., de La Giroday, A. B., Matsukevich, D. N., Maunz, P., ... & Monroe, C. (2010). Random numbers certified by Bell's theorem. Nature, 464(7291), 1021-1024.

[15] Preskill, J. (2018). Quantum computing in the NISQ era and beyond. Quantum, 2, 79.

[16] Rivest, R. L., Shamir, A., & Adleman, L. (1978). A method for obtaining digital signatures and public-key cryptosystems. Communications of the ACM, 21(2), 120-126.

[17] Rukhin, A., Soto, J., Nechvatal, J., Smid, M., Barker, E., Leigh, S., ... & Vo, S. (2010). A statistical test suite for random and pseudorandom number generators for cryptographic applications. NIST Special Publication, 800(22), 1-131.

[18] Schmidhuber, J. (2015). Deep learning in neural networks: An overview. Neural Networks, 61, 85-117.

[19] Shor, P. W. (1994). Algorithms for quantum computation: Discrete logarithms and factoring. In Proceedings 35th annual symposium on foundations of computer science (pp. 124-134). IEEE.

[20] Shor, P. W. (1997). Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. SIAM review, 41(2), 303-332.

[21] Zeng, B., Chen, X., Zhou, D. L., & Wen, X. G. (2019). Quantum information meets quantum matter. Springer.