SLU JST
Sule Lamido University Journal of Science & Technology Vol. 9 No. 1&2 [May, 2024], pp. 114-123
https://doi.org/10.56471/
Online ISSN: 2736-0903
Print ISSN: 2736-089X
www.slujst.edu.ng

Quantum Random Number Generation using Boson Sampling: Harnessing Unbiased Sequences from Penceval and Strawberry fields Platforms

Idris Ahmad

Physics Department, Bayero University Kano

Corresponding author email: Iahmad.phy@buk.edu.ng
https://orcid.org/0000-0002-5965-6931

Abstract

Background: *This research explores the utilization of Boson sampling to advance Quantum Random Number Generation (QRNG), leveraging its inherent randomness as a foundational element.* ***Aim:*** *The primary objective is to develop an innovative QRNG by harnessing Boson sampling, with a specific emphasis on calculating the unitary transformation matrix U crucial for understanding quantum interference phenomena.* ***Method:*** *Boson sampling serves as the core methodology for designing the Quantum Random Number Generator. The research focuses on the meticulous calculation of the unitary transformation matrix U, selected for its direct relevance to the study's objectives. Integration of the Penceval and Strawberry fields platforms facilitates the generation of binary sequences (comprising 0s and 1s), combining their functionalities seamlessly.* ***Results:*** *The findings demonstrate the successful generation of unbiased binary sequences through the collaborative efforts of Boson sampling, Penceval, and Strawberry fields platforms. Employing the Von Neumann correction method effectively rectifies biases, resulting in outputs with high entropy. This approach not only surpasses the limitations of existing discrete QRNGs but also underscores the synergistic potential between Boson sampling and advanced quantum computing platforms.*

Keywords: *random number generation(RNG), quantum computing, Boson sampling, optical interferometers, Perceval, Strawberry fields*

1. Introduction

Random number generation (RNG) is fundamental to various technologies, particularly in cryptography, where it plays a crucial role in creating secure encryption keys, Random number generation is crucial in various aspects of nuclear security, including encryption for secure communication between reactors and control centers, authentication protocols for access control systems, and random sampling for safety assessments and data encryption. The vulnerability of widely used cryptographic standards, such as RSA, has raised concerns about the reliability of current RNG methods. Ensuring the randomness and unpredictability of generated sequences is paramount for maintaining digital security in activities ranging from online banking to the Internet of Things (IoT).

Boson sampling, a model rooted in optical quantum computation, has emerged as a promising avenue for RNG. While its efficacy in quantum computing has been demonstrated, its potential in generating meaningful randomness remains underutilized (Shi et al., 2023). Unlike deterministic sequences, random sequences offer higher entropy, making them more resistant to attacks aimed at exploiting patterns or biases. This makes RNG based on Boson sampling particularly appealing for enhancing cryptographic protocols.

Sule Lamido University Journal of Science & Technology Vol. 9 No. 1&2 [May, 2024], pp. 114-123
https://doi.org/10.56471/
Online ISSN: 2736-0903
Print ISSN: 2736-089X
www.slujst.edu.ng

Moreover, beyond cryptography, RNG finds applications in various domains such as chance-based games, scientific investigations, and surveys requiring random sampling. The ability of Boson sampling to produce inherently unpredictable sequences has broad implications, not only for securing digital communications but also for advancing quantum technologies across diverse fields. This research aims to explore the transformative potential of Boson sampling in RNG, emphasizing its role in enhancing security, addressing concerns in cryptographic standards, and advancing quantum technologies. By leveraging the unique properties of quantum mechanics, Boson sampling offers a novel approach to RNG with implications that extend far beyond traditional cryptographic applications.

2. Role of Random Number Generation (RNG)

Random Number Generation (RNG) plays a pivotal role, exerting a profound influence on many of critical applications. These applications encompass cryptography, secure communication systems, and various cutting-edge technologies (Tu, 2018; Gasmi et al., 2021; Yu et al., 2019). Specifically, RNG serves as a cornerstone in cryptography, where it is utilized to create keys for encrypting confidential information, forming a robust defense against potential deciphering by adversaries. To illustrate, the generation of a password involves a vast number of potential combinations, and the security of the system relies on the unpredictability of this sequence. However, if patterns or biases are present in these sequences, vulnerabilities emerge, allowing attackers to exploit weaknesses and potentially compromise security.

The significance of RNG extends beyond cryptography to critical domains such as quantum algorithms, quantum machine learning, materials science, and financial modeling. In quantum algorithms, the ability of Boson sampling to harness quantum interference provides a unique advantage, particularly in optimization problems and simulations (Lund et al., 2017; Montanaro, 2016; Parekh et al., 2021; Shao et al., 2019). Similarly, in quantum machine learning, the unpredictable nature of generated random sequences aligns with the requirements of certain algorithms, contributing to enhanced pattern recognition and data analysis (Cerezo et al., 2022; Biamonte et al., 2017; West et al., 2023). In materials science, Boson sampling may aid in simulations requiring unbiased random inputs, thereby accelerating research in materials design and properties. Moreover, in financial modeling, the unbiased random sequences derived from Boson sampling can facilitate risk assessment, portfolio optimization, and option pricing, where accurate random inputs are crucial. Boson sampling's potential in enhancing digital security and RNG methods could certainly be extended to applications in nuclear security, contributing to the ongoing efforts to safeguard nuclear facilities against potential threats. Recent concerns about the vulnerability of cryptographic standards, such as RSA, to attacks exploiting flawed random number generation underline the urgent need for robust and unbiased random number generation methods. Beyond encryption, random numbers play a crucial role in lotteries, games of chance, scientific research involving random sampling, and unbiased surveys, requiring truly random sequences to ensure fairness, accuracy, and reliability in their outcomes (Mohammed, 2015).

This study aims to bridge the realms of quantum computing and random number generation by introducing the concept of Boson sampling, a quantum phenomenon that exploits the counterintuitive behaviors of photons in optical interferometers. It explores the challenges associated with simulating these phenomena classically, shedding light on the computational advantages of the quantum computing.

2.1 Theoretical Review

In boson sampling, identical single photons are transmitted through a network of beam splitters that make up an optical interferometer, producing outputs that have a complicated probability distribution over the number of photons. The output of even relatively modest interferometers with only a few tens of photons is classically challenging to mimic within an acceptable length of time, despite the seeming simplicity of photon interference due to its quantum nature.

Sule Lamido University Journal of Science & Technology Vol. 9 No. 1&2 [May, 2024], pp. 114-123
https://doi.org/10.56471/
Online ISSN: 2736-0903
Print ISSN: 2736-089X
www.slujst.edu.ng

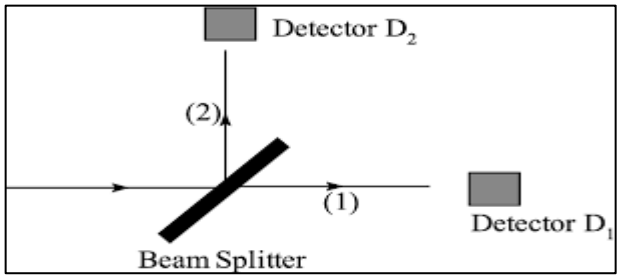

Figure 1: Single photon interact Beam Splitter and two detectors

Boson sampling model of m modes linear transformation and n indistinguishable Boson, the output probability is calculated by a tricky matric function called permanent.

The method calculates a quantum unitary transformation matrix U using the given beam splitter parameters. This unitary matrix describes the quantum interference that occurs in a Boson Sampling experiment, where photons are sent through a network of beam splitters.

$$I\rangle\mathrm{I} = \mathrm{I}\, j_1 j_2 j_3 \dots j_m\rangle, \qquad (1)$$

equation (1) is the input state satisfying

$$j_1 + j_2 + j_3 + \cdots + j_m = n,\rangle, \qquad (2)$$

j_i is the number of photons input to the $i-th$ mode.

$$O\rangle = g_1 g_2 g_3 \dots g_m\rangle, \qquad (3)$$

equation (3) is the output state,

$$j_1 j_2 j_3 \dots j_m\rangle\, U_{I,O}. \qquad (4)$$

Equation (4) is the sub-matrix of the unitary transformation matrix U for linear optical interferometer. Photon counting QRNG generate random numbers base on the number of photons detected on the coherent states described as a superposition of fork states. Fock states essentially denote the different possible configurations of photons in the optical interferometer. The number photons arriving at the detector in a fixed time follows a Poisson distribution.

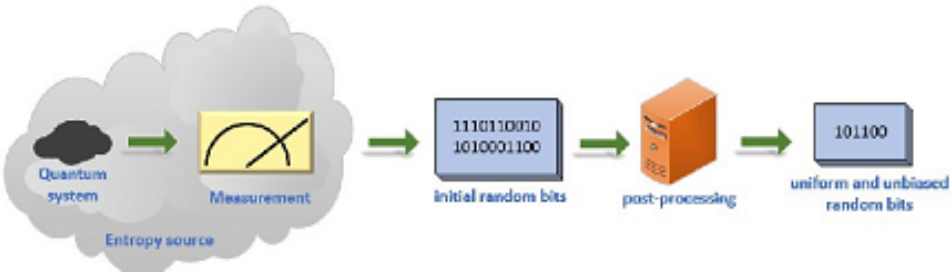

Figure 2: The process of generating unbiased random numbers (Shi et al., 2023).

Sule Lamido University Journal of Science & Technology Vol. 9 No. 1&2 [May, 2024], pp. 114-123
https://doi.org/10.56471/
Online ISSN: 2736-0903
Print ISSN: 2736-089X
www.slujst.edu.ng

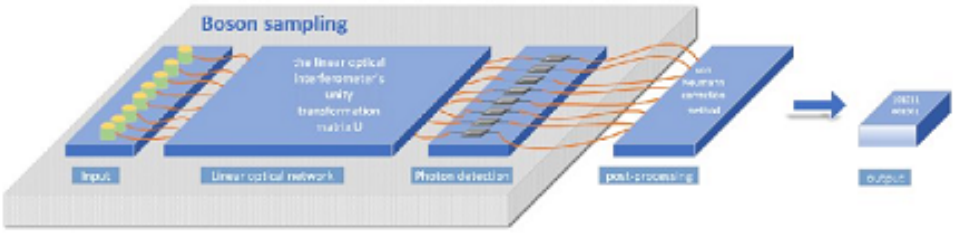

Figure 3: The circuit diagram for boson sampling (Shi et al., 2023)

Figure 2 illustrates the process of generating unbiased random numbers while Figure 3 show the circuit diagram for boson sampling, as reported by Shi et al., (2023).

3. Procedure

The methodology for Boson Sampling and quantum random number generation involves a systematic series of steps:

3.1 Calculation of Quantum Unitary Transformation Matrix U

The process begins with the calculation of the quantum unitary transformation matrix U, a crucial component describing the quantum interference in Boson Sampling. This matrix is derived using specified beam splitter parameters, providing insight into the behavior of photons within the experiment.

3.2 Beam Splitter Parameters and Amplitudes

In defining beam splitter parameters and examining their influence on quantum systems, the initial step involves setting parameters using a list of tuples. Each tuple within this list represents a specific configuration, with two values denoting the transmission and reflection coefficients, respectively. These coefficients determine the proportions of the incident quantum state that are transmitted and reflected by the beam splitter. Following this, complex amplitude calculations are carried out for each tuple. The amplitude of the transmitted beam is determined by taking the square root of the transmission coefficient multiplied by the incident beam's amplitude, while the amplitude of the reflected beam is similarly calculated using the reflection coefficient.

3.3 Construction of Beam Splitter Unitary Matrices

In constructing 2x2 unitary matrices (UBS1, UBS2, UBS3, UBS4, and UBS5) to represent the actions of beam splitters on pairs of modes within the experiment, the process begins by utilizing the previously calculated complex amplitudes. These amplitudes, derived from the transmission and reflection coefficients of the beam splitters, encapsulate the behavior of the quantum system when interacting with these optical elements. The unitary matrices are then formulated based on these complex amplitudes, reflecting the transformations experienced by the quantum state upon encountering the beam splitters. Each matrix corresponds to a unique beam splitter configuration, delineating how photons are distributed among different output modes and how interference patterns are manifested within the experimental setup.

3.4 Formation of Block Diagonal Matrices

To generate block diagonal matrices (UBS1, UBS2, UBS3, UBS4, and UBS5) by combining the beam splitter unitary matrices, the process begins with organizing the unitary matrices based on their corresponding subsets within the experiment. Each unitary matrix encapsulates the transformation undergone by the quantum state when interacting with a particular beam splitter configuration. By arranging these matrices in a block diagonal format,

Online ISSN: 2736-0903
Print ISSN: 2736-089X
www.slujst.edu.ng

the resulting combined matrices illustrate the collective effect of multiple beam splitter interactions on the quantum system.

3.5 Calculation of Total Unitary Matrix U

In computing the product of block diagonal matrices (UBS1, UBS2, UBS3, UBS4, and UBS5) alongside a diagonal phase matrix (Uphase), the multi-dot function is employed. This function facilitates the multiplication of multiple matrices efficiently, streamlining the computation process. The resulting total unitary matrix U comprehensively encapsulates the quantum interference pattern in the Boson Sampling experiment, providing a holistic representation of the system's behavior. By combining the block diagonal matrices with the diagonal phase matrix, the intricate interplay between beam splitter interactions and phase shifts is captured, elucidating the underlying quantum phenomena.

3.6 Printing of Quantum State Transformation

To print the elements of the U matrix rounded to four decimal places, each complex number within the matrix is processed accordingly. By rounding the complex numbers to four decimal places, the printed output provides a clear and concise representation of the quantum interference pattern observed in the Boson Sampling experiment.

3.7 Quantum Photonic Simulation Output

The output generated from the computation offers comprehensive insights into the probabilities and complex amplitudes linked with various states within the quantum system. By providing detailed information on probabilities and complex amplitudes, the output enables researchers to analyze and interpret the quantum state's dynamics, offering valuable insights into the underlying quantum phenomena being studied. Through this approach, the output serves as a crucial tool for comprehending the outcomes of the simulation and advancing our understanding of quantum photonic systems.

3.8 Random Number Generation Using Perceval

In executing Boson Sampling, the process involves conducting the simulation to generate results denoted as S1. Subsequently, the Boson Sampling process is repeated to obtain another set of outcomes, marked as S2. The comparison between S1 and S2 is then carried out to determine the output code for each mode. This comparison involves identifying cases where a photon is detected in one set of results but not in the other, assigning a code of 0 bits accordingly. This allows for the systematic analysis of the simulation outcomes, enabling the extraction of coded bits for modes 1 through M.

3.9 Von Neumann Correction Method

To rectify any inherent biases in the generated random sequence and ensure the final sequence is truly unbiased, the Von Neumann correction method is applied. This method involves analyzing pairs of consecutive bits in the sequence and removing any pairs that are identical (either '00' or '11'). After identifying these identical pairs, one of the bits in each pair is discarded, resulting in a new sequence with reduced bias. This process enables the correction of biases that may have been introduced during the random sequence generation process, enhancing the sequence's randomness and reliability for subsequent analysis or applications.

3.10 Final Quantum Random Number Sequence

The culmination of the methodology is the generation of a final random number sequence, showcasing the capability of quantum computing to produce high-entropy random numbers. This final random number sequence demonstrates the potential of quantum computing in providing reliable and unpredictable randomness, which holds promise for various applications across diverse domains.

Sule Lamido University Journal of Science & Technology Vol. 9 No. 1&2 [May, 2024], pp. 114-123
https://doi.org/10.56471/
Online ISSN: 2736-0903
Print ISSN: 2736-089X
www.slujst.edu.ng

4. Results

In the results section, the outcomes of the Boson Sampling experiment and subsequent quantum processes are investigated. Technical terms encountered in the analysis are explained to enhance understanding. This explanation aids readers in comprehending complex concepts and terminology associated with the Boson Sampling experiment and quantum processes. Through this approach, the methodology facilitates a detailed exploration and interpretation of the experimental outcomes, contributing to the broader understanding of quantum phenomena and their applications.

4.1 Gaussian Transform

Within the output, we observe the application of either a Gaussian transformation or a unitary transformation to a quantum state, which is defined by a matrix consisting of complex numbers. This transformation is intricately linked with particular quantum modes or subsystems, denoted as q[0], q[1], q[2], and q[3]. The complex numbers within the matrix encapsulate both probabilities and complex amplitudes corresponding to various states existing within the quantum system. Through careful analysis of these transformations and the associated complex numbers, we gain valuable insights into the redistribution of probabilities and the evolution of complex amplitudes across the specific quantum modes or subsystems. This observation serves to enrich our understanding of quantum dynamics and its implications in the realm of quantum information processing.

4.2 Unitary Transformation

The unitary transformation matrix, representing quantum interference in the Boson Sampling experiment, is as follows:

Unitary Transformation matrix

$$\begin{bmatrix} 0.2195-0.2565i & 0.6111+0.5242i & -0.1027+0.4745i & -0.0273+0.0373i \\ 0.4513+0.6026i & 0.457+0.0123i & 0.1316-0.4504i & 0.0353-0.0532i \\ 0.0387+0.4927i & -0.0192-0.3218i & -0.2408+0.5244i & -0.4584+0.3296i \\ -0.1566+0.2246i & 0.11-0.1638i & -0.4212+0.1836i & 0.8188+0.068i \end{bmatrix}$$

This matrix serves as a crucial descriptor for the evolution of the quantum state as it traverses the network of beam splitters. Analyzing the matrix provides valuable insights into the probabilities and complex amplitudes associated with different states within the quantum system. Through careful examination, researchers can gain a deeper understanding of the intricate dynamics of quantum interference observed in Boson Sampling experiments.

Gaussian Transform matrix

$$\begin{bmatrix} 0.6372 & -0.7173 & 0.1376 & 0.0383 & -0.0572 & -0.2229 & -0.0776 & 0.0112 \\ 0.343 & 0.1781 & -0.1118 & -0.206 & -0.1989 & 0.0694 & 0.8458 & 0.1897 \\ 0.0646 & 0.1974 & -0.2586 & 0.3623 & -0.5164 & -0.4502 & 0.0224 & -0.5375 \\ -0.109 & 0.0198 & -0.3207 & -0.2984 & -0.3883 & -0.3966 & -0.2775 & 0.6409 \\ 0.0572 & 0.2229 & 0.0776 & -0.0112 & 0.6372 & -0.7173 & 0.1376 & 0.0383 \\ 0.1989 & -0.0694 & -0.8458 & -0.1897 & 0.343 & 0.1781 & -0.1118 & -0.206 \\ 0.5164 & 0.4502 & -0.0224 & 0.5375 & 0.0646 & 0.1974 & -0.2586 & 0.3623 \\ 0.3883 & 0.3966 & 0.2775 & -0.6409 & -0.109 & 0.0198 & -0.3207 & -0.2984 \end{bmatrix}$$

Sule Lamido University Journal of Science & Technology Vol. 9 No. 1&2 [May, 2024], pp. 114-123
https://doi.org/10.56471/
Online ISSN: 2736-0903
Print ISSN: 2736-089X
www.slujst.edu.ng

Gaussian Transform matrix a complex matrix. It is related to the quantum state's density matrix, describing the probabilities and complex amplitudes of different states in the quantum system. Each element in the matrix represents the probability amplitude of transitioning from one quantum state to another. this output provides information about the results of a quantum photonic simulation. It includes probabilities of different outcomes in the quantum system:

4x4 Matrix (Quantum Operation)

$$\begin{bmatrix} 0.6372 + 0.0572\mathrm{i} & -0.7173 + 0.2229\mathrm{i} & 0.1376 + 0.0776\mathrm{i} & 0.0383 - 0.0112\mathrm{i} \\ 0.343 + 0.1989\mathrm{i} & 0.1781 - 0.0694\mathrm{i} & -0.1118 - 0.8458\mathrm{i} & -0.206 - 0.1897\mathrm{i} \\ 0.0646 + 0.5164\mathrm{i} & 0.1974 + 0.4502\mathrm{i} & -0.2586 - 0.0224\mathrm{i} & 0.3623 + 0.5375\mathrm{j} \\ -0.109 + 0.3883\mathrm{i} & 0.0198 + 0.3966\mathrm{i} & -0.3207 + 0.2775\mathrm{i} & -0.2984 - 0.6409\mathrm{i} \end{bmatrix}$$

4x4 Matrix (Quantum Operation) Represents a quantum operation or transformation acting on a quantum state or system. Each element is a complex number indicating the amplitude of transitioning between the quantum states

4x3 Matrix (Quantum Transition Probabilities)

$$\begin{bmatrix} 0.6372 + 0.0572\mathrm{i} & -0.7173 + 0.2229\mathrm{i} & 0.0383 - 0.0112\mathrm{i} \\ 0.343 + 0.1989\mathrm{i} & 0.1781 - 0.0694\mathrm{i} & -0.206 - 0.1897i \\ 0.0646 + 0.5164\mathrm{i} & 0.1974 + 0.4502\mathrm{i} & 0.3623 + 0.5375\mathrm{i} \\ -0.109 + 0.3883\mathrm{i} & 0.0198 + 0.3966\mathrm{i} & -0.2984 - 0.6409\mathrm{i} \end{bmatrix}$$

4x3 Matrix (Quantum Transition Probabilities) Indicates probabilities and complex amplitudes of transitioning from one quantum state to another. Each entry represents a transition probability.

3x3 Matrix (Quantum System State Transition)

$$\begin{bmatrix} 0.6372 + 0.0572\mathrm{i} & -0.7173 + 0.2229\mathrm{i} & 0.0383 - 0.0112\mathrm{i} \\ 0.6372 + 0.0572\mathrm{i} & -0.7173 + 0.2229\mathrm{i} & 0.0383 - 0.0112\mathrm{i} \\ -0.109 + 0.3883\mathrm{i} & 0.0198 + 0.3966\mathrm{i} & -0.2984 - 0.6409\mathrm{i} \end{bmatrix}$$

3x3 Matrix (Quantum System State Transition) illustrates the transition of the quantum system's states. Each element signifies a transition from one state to another within the system.

Sule Lamido University Journal of Science & Technology Vol. 9 No. 1&2 [May, 2024], pp. 114-123
https://doi.org/10.56471/
Online ISSN: 2736-0903
Print ISSN: 2736-089X
www.slujst.edu.ng

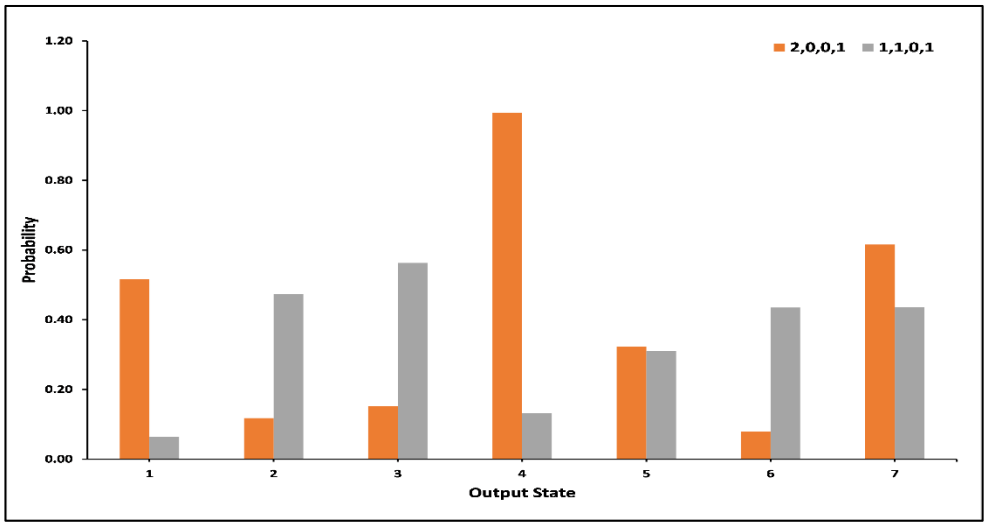

Figure 4: The probabilities associated with the indices.

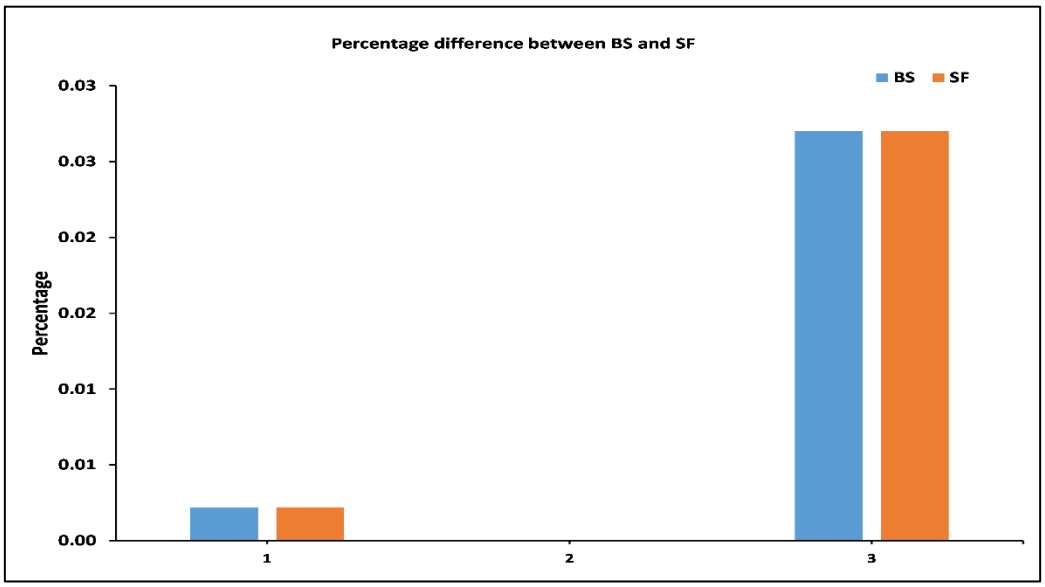

Figure 5: The comparison on some values of BS and SF.

Figures 4 in this section contains the standard output produced when the code within the cell is executed. The output shows the performing calculations while Figure 5 shows the comparisons on some values and printing the results. The comparisons on some of BS and SF are related to a quantum simulation where the differences between the calculated values are very small, indicating high precision in the calculations (Figure 5).

4.3 Percival experiments

The output results of first and second sampling in Percival experiments are given below,

The first sampling result S1

|0,1,0,1,0,1,0,0,0,0,0,0,0,0,0,0,1,0,0,0,0,0,1,0,0,1,0,0,0,0,1,1,0,0,0,0,0,0,1,0,0,0,1,0,0,0,0,0,0,0>

Sule Lamido University Journal of Science & Technology Vol. 9 No. 1&2 [May, 2024], pp. 114-123
https://doi.org/10.56471/
Online ISSN: 2736-0903
Print ISSN: 2736-089X
www.slujst.edu.ng

The second sampling results S2

|0,0,0,0,0,0,0,0,0,1,1,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,1,0,1,0,0,0,1,0,0,1,1,0,0,0,0,1,1,1,0,0,0,0,0>

The Von Neumann correction method was used to ensure impartiality applied in the final random sequence. The coding method is showing below:

Coding ['*', '0', '*', '0', '*', '0', '*', '*', '*', '1', '1', '*', '*', '*', '*', '*', '0', '*', '*', '*', '*', '*', '0', '*', '*', '0', '*', '1', '*', '1', '0', '0', '*', '1', '*', '*', '1', '1', '0', '*', '*', '*', '*', '1', '1', '*', '*', '*', '*', '*']

The final random number sequence was obtained to be: **000110001100111011.**

This final quantum random number generated shows the power quantum computing in providing high entropy of the random numbers.

5. Conclusion

In conclusion, this research establishes the transformative potential of Boson Sampling in Quantum Random Number Generation (QRNG) and its broader applications. Uniform Distribution in QRNG, the fundamental requirement for a random number generator is a uniform distribution of 0s and 1s. The Boson Sampling-based QRNG achieves this crucial criterion, ensuring that each bit in the generated sequence has an equal probability of being 0 or 1. This unbiased nature is vital for the robustness of cryptographic protocols and the reliability of random sequences in various applications. Enhanced Security in Cryptography, Boson Sampling's ability to produce inherently unpredictable random sequences strengthens cryptographic protocols. The interference properties of photons contribute to the creation of unbreakable encryption keys, thereby enhancing digital security. This has profound implications for securing sensitive information in communication systems. Quantum Advantage in Various Technologies, The research highlights Boson Sampling's versatility in different technological domains. From Quantum Algorithms to Quantum Machine Learning and Materials Science, the unpredictable nature of the generated random sequences aligns with the requirements of diverse applications. This underscores Boson Sampling's role in revolutionizing quantum technologies beyond its initial purpose. Addressing Concerns in Cryptographic Standards, Recent concerns about the vulnerability of widely adopted cryptographic standards, such as RSA, emphasize the urgency for robust and unbiased random number generation methods. Boson Sampling emerges as a promising solution to address these concerns, providing a foundation for secure online activities, financial transactions, and the Internet of Things (IoT). In essence, this research not only presents a novel approach to QRNG but also positions Boson Sampling as a pivotal quantum resource with far-reaching implications. The high entropy of the generated random numbers demonstrates the potency of quantum computing in advancing the field of random number generation. This work lays the groundwork for future advancements in quantum technologies and their applications in diverse domains.

References

Biamonte, J., Wittek, P., Pancotti, N., Rebentrost, P., Wiebe, N., & Lloyd, S. (2017). Quantum machine learning. *Nature*, 549 (7671), 195–202. https://doi.org/10.1038/nature23474

Cerezo, M., Verdon, G., Huang, H. Y., Cincio, L., & Coles, P. J. (2022). Challenges and opportunities in quantum machine learning. *Nature Computational Science*, 2(9), 567–576. https://doi.org/10.1038/s43588-022-00311-3

Gasmi, K., Bourouis, A., & Benaboud, R. (2021). A Survey on Identity-based Key Management Schemes in Mobile Ad hoc networks. *CEUR Workshop Proceedings*, 2904, 11–22.

Online ISSN: 2736-0903
Print ISSN: 2736-089X
www.slujst.edu.ng

Hui Wang, et al. (2019). Boson Sampling with 20 Input Photons and a 60-Mode Interferometer in a 1014-Dimensional Hilbert Space. *Physical Review Letters*, 123 (25):250503.

Lund, A. P., Bremner, M. J., & Ralph, T. C. (2017). Quantum sampling problems, BosonSampling and quantum supremacy. *Npj Quantum Information*, 3(1), 1–7. https://doi.org/10.1038/s41534-017-0018-2

Mohammed, J. (2015). The State of Cryptography- A National Interest Perspective. 4(8).

Montanaro, A. (2016). Quantum algorithms: An overview. *Npj Quantum Information*, 2(1), 1–8. https://doi.org/10.1038/npjqi.2015.23

Nikolopoulos, G. M. (2019). Cryptographic one-way function based on boson sampling. *Quantum Information Processing*, 18(8), 259. https://doi.org/10.1007/s11128-019-2372-9

Parekh, R., Ricciardi, A., Darwish, A., & Diadamo, S. (2021). Quantum Algorithms and Simulation for Parallel and Distributed Quantum Computing. Proceedings of QCS 2021: 2nd International Workshop on Quantum Computing Software, Held in Conjunction with SC 2021: *The International Conference for High Performance Computing, Networking, Storage and Analysis*, 9–19. https://doi.org/10.1109/QCS54837.2021.00005

Shao, C., Li, Y., & Li, H. (2019). Quantum Algorithm Design: Techniques and Applications. *Journal of Systems Science and Complexity*, 32(1), 375–452. https://doi.org/10.1007/s11424-019-9008-0

Shi, J., Zhao, T., Wang, Y., Yu, C., Lu, Y., Shi, R., Zhang, S., & Wu, J. (2023). An Unbiased Quantum Random Number Generator Based on Boson Sampling. *Advernce Quatum Technology*, *7*(1), 1–14.

Tu, C. (2018). Survey on Homomorphic Encryption Technology. 83, 764–768. https://doi.org/10.2991/snce-18.2018.156

West, M. T., Tsang, S.-L., Low, J. S., Hill, C. D., Leckie, C., Hollenberg, L. C. L., Erfani, S. M., & Usman, M. (2023). Towards quantum enhanced adversarial robustness in machine learning. *Nature Machine Intelligence*, 5(6), 581–589. https://doi.org/10.1038/s42256-023-00661-1

Yu, F., Li, L., Tang, Q., Cai, S., Song, Y., & Xu, Q. (2019). A Survey on True Random Number Generators Based on Chaos. *Discrete Dynamics in Nature and Society*. https://doi.org/10.1155/2019/2545123