Quantum Computing Approaches to Random Number Generation: A Digital Twin of Photon Beam Splitter Experiment using QuTiP

Rounak Biswas
Research Scholar
Visva-Bharati
Santiniketan-731235

Utpal Roy
Professor
Visva-Bharati
Santiniketan-731235

ABSTRACT

Quantum computing utilizes the inherent randomness characteristic of quantum mechanics, offering a promising framework for various applications, including random number generation (RNG), which is critical for cryptography and secure communication. This paper introduces a digital twin of a photon beam splitter experiment, simulated utilizing the QuTiP Python library, to model and analyse the probabilities of photon detection at varying beam splitter angles. By employing quantum principles such as superposition and entanglement, we illustrate how alterations in the angles of the beam splitter influence both the randomness and the convergence rate of the generated photon detection events. The resulting randomness, validated through rigorous statistical testing, emphasizes the potential of photon-based experiments to enhance RNG models. This investigation highlights the significance of quantum computing methodologies in the context of RNG and examines how digital twin simulations can improve the efficiency and security of quantum cryptographic systems. Furthermore, another motivation for this research is to explore diverse quantum methods for generating randomness, as the entire field of quantum computation is engaged in continually exploring efficient problem-solving strategies. The study carefully navigates this exploration to identify various means of integrating the intrinsic randomness of quantum systems with practical applications in the real world.

General Terms

Quantum Computing, Random Number Generation (RNG), Quantum Experiment, Quantum Simulation

Keywords

Quantum Random Number Generator (QRNG), Digital Twin, Photon Beam Splitter, QuTiP, Superposition, Entanglement, Statistical Testing, Quantum Cryptography

1. INTRODUCTION

Quantum mechanics, with its intrinsic randomness, has long been a cornerstone for advancing technologies in various fields, including computing, complex mathematical problem solving, cryptography, and secure communication**[1]**. The field of quantum computing takes this randomness a step further by leveraging quantum phenomena such as superposition, uncertainty, and entanglement to solve complex problems with unprecedented efficiency. One critical area of cryptography or network security is to use a trustworthy randomness source. We will use the classical machine to generate or produce good-quality randomness in digital electronics. Classical machines are deterministic, and determinism is unsuitable for generating random sequences**[2]**. In this domain, the inherent randomness of quantum computers or quantum mechanics plays a crucial role. Unlike classical RNG, which is deterministic and can be predicted or reverse-engineered, quantum-based RNGs utilizes the inherent uncertainty of quantum systems to produce truly random sequences, which is essential for cryptographic applications and enhancing data security.

This study focuses on photon-based random number generation using a digital twin model of a quantum experiment, wherein a photon beam splitter directs photons toward two detectors, simulating their probabilistic behaviour**[3]**. The experiment employs quantum principles to model how variations in the angle of the beam splitter affect photon detection probabilities. These variations lead to the generation of random numbers, which are tested for reliability using rigorous statistical methods**[4], [5]**.

In quantum mechanics, beam splitters are vital in experiments dealing with light and photons. When a photon light pulse passes through a beam splitter, it has a probabilistic chance of being either reflected or transmitted, resulting in detection by one of two detectors. This phenomenon is a crucial enabler for generating randomness in quantum systems. Previous studies have shown that the inherent randomness of quantum events like photon detection can be effectively connected to develop RNG models. However, the specific effect of beam splitter angles on the convergence and quality of randomness has yet to be fully explored.

This paper explores how varying the angle of the photon beam splitter influences the randomness and convergence rate of photon detection events. By simulating the behaviour of photons passing through a beam splitter with different angles, we categorize the results into two distinct types based on their convergence rates. Some angles result in rapid convergence to an equal probability distribution between the two detectors, while others show delayed convergence. These findings shed light on the dynamic behaviour of photons in quantum systems and their implications for optimizing RNG processes.

To test the experiment, we use the QuTiP python package to build up a digital twin model of the experiment. The digital twin allows us to precisely simulate and control experimental parameters, offering insights into the practical application of quantum mechanics for RNG. In doing so, we advance our understanding of how quantum mechanics can be applied to real-world problems, particularly in the domain of quantum cryptography**[6]**.

2. RELATED STUDY

Quantum mechanics, with its inherent randomness, offers a fundamentally unpredictable source for generating random numbers, which are crucial for cryptographic protocols. While

traditional RNG methods rely on deterministic algorithms, making them vulnerable to prediction, QRNGs exploit quantum phenomena such as superposition and entanglement to ensure unpredictability[7].

Previous research has demonstrated various ways quantum mechanics can be integrated into RNG models. Studies such as explore the combination of artificial intelligence (AI) and cryptography to detect randomness in encrypted data streams, highlighting the need for robust encryption algorithms in securing digital communications[8]. Although these AI-based methods offer improvements in randomness detection, they still rely on classical mechanics and deterministic processes, which cannot fully replicate the unpredictability of quantum systems.

Digital twin technology, while historically applied in fields such as manufacturing and healthcare, has recently begun to play a role in quantum mechanics[9], [10]. Digital twins create virtual replicas of physical systems, allowing precise simulations that mirror real-world quantum experiments. Researchers like have utilized digital twins to simulate complex systems, including quantum optical devices, enabling the exploration of phenomena like photon detection and light interference[11]. Despite the progress in integrating digital twins into quantum research, there remain challenges in scaling these models for large-scale applications and optimizing their use for random number generation[12].

Our work addresses these challenges by applying digital twin simulations to quantum random number generation using photon beam splitters. Quantum mechanics-based randomness has also been explored in device-independent randomness generation, where quantum systems produce certified randomness without needing a detailed model of the generating device[13]. This approach demonstrates the potential for cryptographic security, as it leverages the fundamental properties of quantum systems to ensure randomness.

Studies such as[14] have examined the broader applications of quantum computing in cryptography, emphasizing its potential for secure communication protocols. However, the role of quantum random number generators in these systems is still under investigation.

By simulating the behaviour of quantum systems like photon beam splitters, researchers aim to optimize the generation of random numbers, ensuring that these sequences meet the rigorous statistical criteria required for cryptographic use. Our research builds on these foundations by using QuTiP[15], a quantum simulation library, to model photon detection probabilities and assess the impact of beam splitter angles on the randomness of detection events. In conclusion, the literature highlights the transformative impact of quantum computing on randomness generation and cryptographic security[16].

3. KEY TERMS

3.1 Quantum Computation

Quantum computation works on the principles of quantum mechanics, offering capabilities beyond classical computing. The fundamental unit of quantum information is the qubit, which, unlike classical bits, can exist in a superposition of states (both 0 and 1 simultaneously). This enables quantum computers to perform many calculations in parallel, vastly increasing their potential for complex problem-solving.

Entanglement, yet another important phenomenon which occurs within the domain of quantum; the two qubits are correlated so that the state of one affects the other, regardless of distance. It is interdependence that leads to many of the most powerful applications in quantum algorithms and secure communication.

Then the Quantum gates applicable to build up quantum circuit, like the way classical gates manipulate bits. Hadamard and CNOT gates from this class of quantum gates create superposition and entanglement, which forms the very basis of quantum calculations.

Other quantum algorithms exploit these principles to solve problems like the factors of big numbers and database search efficiently. In random number generation, for instance, quantum computers exploit the intrinsic randomness in the behaviour of photons in quantum mechanics to produce all random sequences demanded for security in cryptography.

3.2 Inherent Randomness

Inherent randomness refers to the fundamental unpredictability observed in various natural phenomena, where outcomes cannot be precisely determined in advance due to the probabilistic nature of underlying processes. Unlike deterministic systems governed by fixed rules and initial conditions, inherently random processes exhibit spontaneous fluctuations and variability that withstand precise prediction.

In the domain of physics, inherent randomness manifests in several fundamental phenomena. One prominent example is the decay of radioactive isotopes, such as uranium or carbon-14. The timing of individual decay events cannot be predicted with certainty, as they occur randomly and independently of external influences. This randomness is intrinsic to the quantum nature of particles and their interactions, leading to a probabilistic distribution of decay times.

3.3 Digital Twin

Digital twins represent virtual counterparts of physical objects, processes, or systems, facilitating real-time monitoring, analysis, and optimization. By uniting data from sensors, simulations, and other inputs, they construct precise digital replicas mirroring the behaviour and attributes of their real-world counterparts.

Quantum digital twins extend the concept of digital twins into quantum mechanics, where they simulate quantum systems and phenomena with high fidelity. These virtual replicas leverage quantum computing techniques to model the behaviour of quantum particles, such as photons, electrons, and qubits, in complex quantum systems.

4. SIMULATION FRAMEWORK

The primary objective of this work is to develop a deterministic-free random number generation model by taking advantage of a quantum mechanical process known for its inherent randomness. The selected experiment involves the interaction of single-photon light sources with a beam splitter, followed by detection by two light detectors. It is well-established that these detectors exhibit a 50/50 probability of capturing the photon light pulses from the beam splitter, providing a reliable source of inherent randomness.

To simulate this quantum experiment and generate random strings of zeros and ones, we utilize the QuTiP package provided by the Python language. The simulation process involves the following steps:

1. Initialize Parameters:
   - Define the number of modes for the quantum system.
   - Set the angle of the beam splitter.

2. Define Operators:
   - Create annihilation and creation operators for each mode.
   - Calculate the beam splitter Hamiltonian based on the specified angle.

3. Initial State:
   - Prepare the initial quantum state with a single photon in mode 0.

4. Evolution:
   - Define the time steps for the evolution of the quantum state.
   - Apply the beam splitter Hamiltonian to evolve the state over time.

5. Measurement:
   - Calculate the probabilities of detecting photons in each mode based on the evolved quantum state.
   - Generate random outcomes for each time step based on the calculated probabilities.

Textbox a: Pseudo Code of the Model Using QuTiP

1. Initialize Parameters:

```
num_modes = modes
theta = angle
```

2. Define *Operators*:

```
for each mode:
    Create annihilation and
creation operators (a)

    Calculate Beam Splitter
Hamiltonian (H_bs)
```

3. Initial State:

```
    Prepare initial quantum state
(psi0) with single photon in mode
0
```

4. Evolution:

```
    Define time steps (times) for
evolution
    Evolve state through H_bs
using mesolve
```

5. Measurement:

```
    Calculate probabilities of
detecting photons (p1, p2)
    for each time step:
```

Generate random outcome based on p1 and p2 probabilities

Textbox b: Steps for Simulation Using Digital Twin of Photon Beam Splitter Experiment

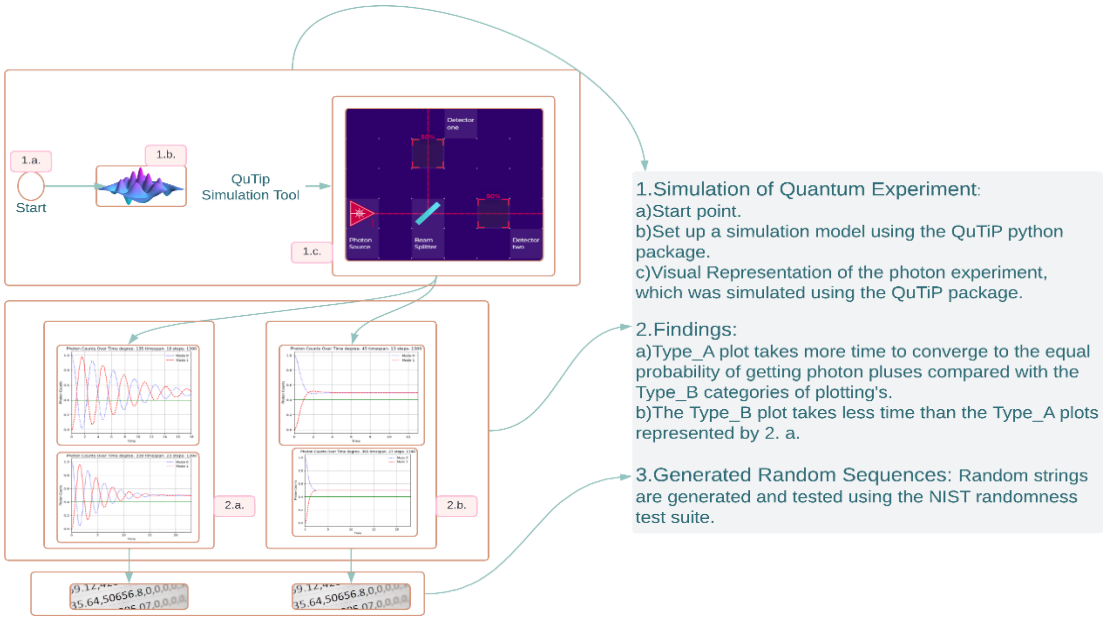

Figure 1: Graphical Abstract of The Simulated Framework

5. PLOTS AND RESULTS

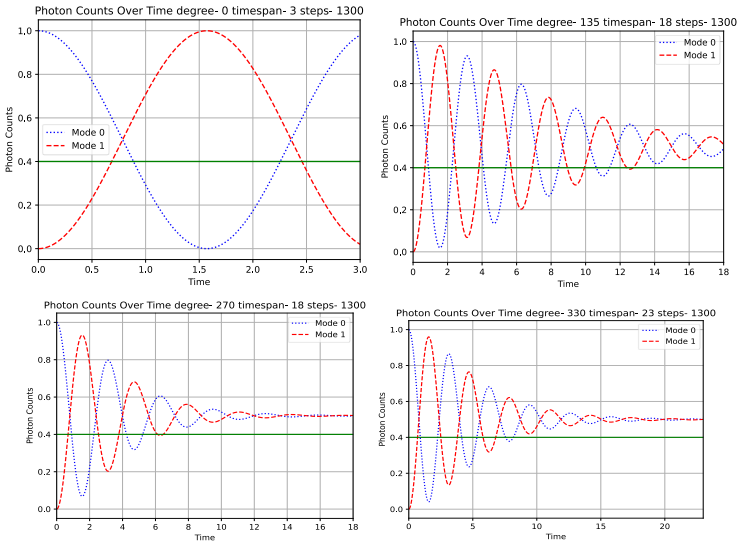

Figure 2: Photon counts over time plot (type_A)

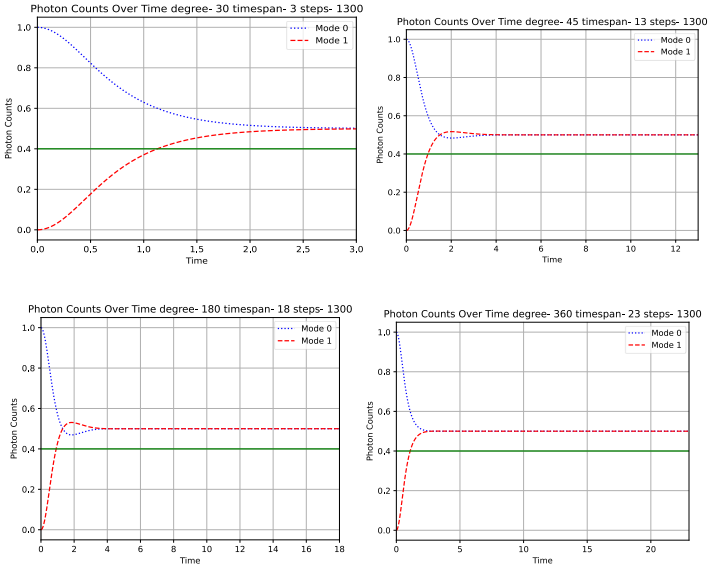

Figure 3: Photon counts over time plot (type_B)

Table 1 Test Data & NIST Test Suite Result for Beam Splitter 135 Degree 15 Timespan 1300 Steps (type_A)

Type of Test	P-Value	Conclusion	Column1
1. frequency_rounak_visvabharati_testtypeone	0.067173616	testone_ran_pass	
2. frequencyblock_rounak_visvabharati_testtypeone	9.89E-39	testone_ran_fail	
3. run_test_rounak_visvabharati_testtypeone	5.10E-28	testone_ran_fail	
4. longest_ones_block_rounak_visvabharati_testtypeone	5.08E-08	testone_ran_fail	
5. binary_matrix_rank_rounak_visvabharati_testtypeone	0.039104616	testone_ran_pass	
6. discrete_fourier_trans_rounak_visvabharati_testtypeone	0.001465531	testone_ran_fail	
7. non-overlapping_templ_rounak_visvabharati_testtypeone	2.36E-12	testone_ran_fail	
8. overlapping_template_rounak_visvabharati_testtypeone	0.295708275	testone_ran_pass	
9. maurers_univer_statis_rounak_visvabharati_testtypeone	-1	testone_ran_fail	
10.linear_complexity_rounak_visvabharati_testtypeone	0.919688854	testone_ran_pass	
11. serial_rounak_visvabharati_testtypeone	0	testone_ran_fail	
	0	testone_ran_fail	
12. approximate_entropy_rounak_visvabharati_testtypeone	0.154215379	testone_ran_pass	
13. cumul_sums_forward_rounak_visvabharati_testtypeone	0.080263409	testone_ran_pass	
14. cumul_sums_reverse_rounak_visvabharati_testtypeone	0.003788618	testone_ran_fail	
15. ran_excursions_rounak_visvabharati_testtypeone			
State	Chi Squared	P-Value	Conclusion
-4	127.5714286	7.80E-26	testone_ran_fail
-3	40.888	9.88E-08	testone_ran_fail
-2	34.46666667	1.92E-06	testone_ran_fail
-1	3.8	0.578555291	testone_ran_pass
1	5	0.415880187	testone_ran_pass
2	7.355555556	0.195511394	testone_ran_pass
3	18.2416	0.002658367	testone_ran_fail
4	28.40408163	3.03E-05	testone_ran_fail
16. ran_excursions_variant_rounak_visvabharati_testtypeone			
State	COUNTS	P-Value	Conclusion
-9	6	0.93886499	testone_ran_pass
-8	6	0.934925312	testone_ran_pass
-7	5	1	testone_ran_pass
-6	5	1	testone_ran_pass
-5	5	1	testone_ran_pass
-4	6	0.904861129	testone_ran_pass
-3	7	0.777297411	testone_ran_pass
-2	6	0.855132141	testone_ran_pass
-1	5	1	testone_ran_pass
1	4	0.751829634	testone_ran_pass
2	5	1	testone_ran_pass
3	6	0.887537084	testone_ran_pass
4	5	1	testone_ran_pass
5	5	1	testone_ran_pass
6	5	1	testone_ran_pass
7	5	1	testone_ran_pass
8	6	0.934925312	testone_ran_pass
9	7	0.878088367	testone_ran_pass

Test Data:
000000000000000100000010000000000000010001100000000000000100000100100010010000000001010
001011001011111101011010100110111111101111111111111111111111111111111111111111111111111
111111111111111111111101111111111101111101111101111111101111110101001010100101100100
100110001000010010000101010000000000000100000000000000000000000000000000000000000000
000000000000000000000000000000001110100011000000000000100010100001100001011101010000
111001001001111111101011101101111111110111101101011111111111111011111101111111111111
111111110111011111111111111111111110011011011111111111111110000100000001110110100000
010101000110010000110001000100010010000000110000000000000000000001010000000010001100
100010000000100010011010111110100000010010000000000101110001000001100100010010000001
000111000111111111101100101111100111111101011101110001101111110111111011100110111
101111001010100100011011001010000111011110010100111100111100110011010011100111000
100000011010010010010100110100000000110000000101100000000001110100000011000000000011
100100000011000011010110001110000000111001100001100110010010001010010100011110111111
001111001110100000111011111111110001100001111000011000010110110111110100111010111100
0001100110111111100000111011111111100110010110001001100111101111011000000011000000001
1110111010001101000111111001000000000011010001100101000100100000000011000

Table 2: Test Data & NIST Test Suite Result for Beam Splitter 360 Degree 18 Timespan 1300 Steps (type_B)

Type of Test	P-Value	Conclusion	Conclusion
1. frequency_rounak_visvabharati_testType2	0.04043901	test2_ran_pass	
2. frequencyblock_rounak_visvabharati_testType2	0.368482932	test2_ran_pass	
3. run_test_rounak_visvabharati_testType2	0.086814556	test2_ran_pass	
4. longest_ones_block_rounak_visvabharati_testType2	0.806728839	test2_ran_pass	
5. binary_matrix_rank_rounak_visvabharati_testType2	0.693720141	test2_ran_pass	
6. discrete_fourier_trans_rounak_visvabharati_testType2	0.566530538	test2_ran_pass	
7. non-overlapping_templ_rounak_visvabharati_testType2	0.068364769	test2_ran_pass	
8. overlapping_template_rounak_visvabharati_testType2	0.886588558	test2_ran_pass	
9. maurers_univer_statis_rounak_visvabharati_testType2	-1	test1_ran_fail	
10.linear_complexity_rounak_visvabharati_testType2	0.919688854	test2_ran_pass	
11. serial_rounak_visvabharati_testType2	0.978588151	test2_ran_pass	
	0.900823599	test2_ran_pass	
12. approximate_entropy_rounak_visvabharati_testType2	0.481417971	test2_ran_pass	
13. cumul_sums_forward_rounak_visvabharati_testType2	0.080878019	test2_ran_pass	
14. cumul_sums_reverse_rounak_visvabharati_testType2	0.075546268	test2_ran_pass	
15. ran_excursions_rounak_visvabharati_testType2			
State	Chi Squared	P-Value	Conclusion
-4	16.85714286	0.004778852	test1_ran_fail
-3	11.66	0.039755555	test2_ran_pass
-2	8.444444444	0.13338289	test2_ran_pass
-1	6	0.306218918	test2_ran_pass
1	2	0.849145036	test2_ran_pass
2	1.333333333	0.931464617	test2_ran_pass
3	0.8	0.977033344	test2_ran_pass
4	0.571428571	0.989273997	test2_ran_pass
16. ran_excursions_variant_rounak_visvabharati_testType2			
State	COUNTS	P-Value	Conclusion
-9	10	0.606905427	test2_ran_pass
-8	7	0.784191229	test2_ran_pass
-7	5	0.921886184	test2_ran_pass
-6	2	0.83117041	test2_ran_pass
-5	1	0.72367361	test2_ran_pass
-4	2	0.789268026	test2_ran_pass
-3	3	0.874367061	test2_ran_pass
-2	4	1	test2_ran_pass
-1	4	1	test2_ran_pass
1	2	0.479500122	test2_ran_pass

Test Data:

10001110000001110000000011001000101001110000111100101110000101000101101000100011100100

6. RESULT DISCUSSION

The execution of the `*twin_Photon_Beam_Splt*` function with varying parameters yielded interesting results, leading to the categorization of generated plots into two distinct types: Type A and Type B.

Type_A Plots (Figure 2): Type A plots illustrate scenarios where the detectors initially exhibit a 50/50 probability of detecting photon light pulses from the beam splitter. Alternatively, they may achieve this desired probability after a considerable time interval. For instance, plots corresponding to angles 0, 1, 35, 270, and 330 exemplify such behaviour. In these cases, the prolonged duration required to reach equilibrium may indicate complex interactions within the quantum system, resulting in delayed convergence to the desired outcome.

Type_B Plots (Figure 3): In contrast, Type B plots showcase parameter configurations where the detectors rapidly achieve the desired 50/50 probability. This quick convergence suggests a more efficient and predictable behaviour of the quantum system under specific parameter settings. Angles like 30, 45, 180, and 360 produce similar plot patterns and behave similarly in the random number generation process.

NIST Results (Table 1 & Table 2): To further investigate the randomness of the generated binary strings, representative samples from both Type_A and Type_B plots underwent rigorous testing using the NIST randomness test suite. This suite comprises 16 statistical tests designed to assess the quality of random sequences. A remarkable observation emerged after scrutinizing the NIST test results: the binary strings generated from Type B plots consistently passed all tests within the NIST suite. This robust performance across a comprehensive range of statistical measures underscores the inherent randomness

and reliability of the numbers generated under Type B configurations.

The significance of this finding cannot be overstated, particularly in the cryptographic applications and secure communication protocols. The ability to produce random numbers that withstand rigorous statistical scrutiny ensures the integrity and unpredictability required for safeguarding sensitive information and data privacy.

The difference between Type A and Type B plots highlights the subtle dynamics of quantum systems under various conditions, which helps deepen the understanding of quantum behaviour and guides future experiments and simulations for practical use of quantum phenomena.

In summary, the illustration between Type A and Type B plots, coupled with the validation of Type B plots through the NIST randomness test suite, underscores the importance of parameter selection and experimental design in achieving desired randomness characteristics in simulated quantum experiments. These findings floor the way for developing more robust and reliable random number generation techniques with broad applications across various domains.

7. CONCLUSION

In conclusion, the study proposes an innovative approach to address the short-comings of classical random number generation by utilizing the inherent unpredictability of quantum mechanics. Through this research, introduce a deterministic free random number generation model implanted in quantum properties, ensuring the generation of random numbers devoid of deterministic biases. This work advances random number generation and paves the way for leveraging quantum mechanical simulations to gather insights into various quantum phenomena, thereby contributing to a broader comprehension and utilization of quantum mechanics across diverse domains.

Executing the `*twin_Photon_Beam_Splt*` function with varying parameters yields intriguing results, categorizing generated plots into two distinct types: Type_A and Type_B. Type A plots illustrate scenarios where detectors initially exhibit a 50/50 probability of detecting photon light pulses from the beam splitter. Type_B plots showcase configurations where detectors rapidly achieve the desired 50/50 probability. Further investigation into the randomness of the generated binary strings using the NIST randomness test suite reveals that strings generated from Type_B plots consistently pass all tests, underscoring their inherent randomness and reliability.

In nutshell, this study highlights the importance of parameter selection and experimental design in achieving desired randomness characteristics in simulated quantum experiments. These findings also help in developing more robust and reliable random number generation techniques with broad applications across simulation, secure key generation, leader election, forecasting and model where any kind of randomness is required.

Future work could further optimize the quantum-inspired random number generation model and explore its applicability in real-world cryptographic systems. Additionally, investigating the scalability and efficiency of the proposed approach in large-scale applications would be a valuable avenue for future research.

8. REFERENCES

[1] M. N. Bera, A. Acín, M. Kuś, M. W. Mitchell, and M. Lewenstein, “Randomness in quantum mechanics: philosophy, physics and technology,” *Rep. Prog. Phys.*, vol. 80, no. 12, p. 124001, Nov. 2017, doi: 10.1088/1361-6633/aa8731.

[2] G. F. Dear, “Determinism in classical physics,” *Br. J. Philos. Sci.*, vol. 11, no. 44, pp. 289–304, Feb. 1961, doi: 10.1093/bjps/XI.44.289.

[3] P. Grangier, G. Roger, and A. Aspect, “Experimental Evidence for a Photon Anticorrelation Effect on a Beam Splitter: A New Light on Single-Photon Interferences,” *Europhys. Lett.*, vol. 1, no. 4, p. 173, Feb. 1986, doi: 10.1209/0295-5075/1/4/004.

[4] L. E. Bassham *et al.*, “A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications,” *NIST*, Sep. 2010, Accessed: Mar. 29, 2024. [Online]. Available: https://www.nist.gov/publications/statistical-test-suite-random-and-pseudorandom-number-generators-cryptographic

[5] M. Sýs and Z. Říha, “Faster Randomness Testing with the NIST Statistical Test Suite,” in *Security, Privacy, and Applied Cryptography Engineering*, R. S. Chakraborty, V. Matyas, and P. Schaumont, Eds., Cham: Springer International Publishing, 2014, pp. 272–284. doi: 10.1007/978-3-319-12060-7_18.

[6] “Advances in quantum cryptography.” Accessed: Sep. 14, 2024. [Online]. Available: https://opg.optica.org/aop/fulltext.cfm?uri=aop-12-4-1012&id=444736

[7] A. Acín and L. Masanes, “Certified randomness in quantum physics,” *Nature*, vol. 540, no. 7632, pp. 213–219, Dec. 2016, doi: 10.1038/nature20119.

[8] J. Blackledge and N. Mosola, “Applications of Artificial Intelligence to Cryptography,” *Trans. Eng. Comput. Sci.*, vol. 8, no. 3, Art. no. 3, Jun. 2020, doi: 10.14738/tmlai.83.8219.

[9] B. R. Barricelli, E. Casiraghi, and D. Fogli, “A Survey on Digital Twin: Definitions, Characteristics, Applications, and Design Implications,” *IEEE Access*, vol. 7, pp. 167653–167671, 2019, doi: 10.1109/ACCESS.2019.2953499.

[10] M. Enders and N. Hoßbach, *Dimensions of Digital Twin Applications - A Literature Review*. 2019.

[11] H. Jiang, S. Qin, J. Fu, J. Zhang, and G. Ding, “How to model and implement connections between physical and virtual models for digital twin application,” *J. Manuf. Syst.*, vol. 58, pp. 36–51, Jan. 2021, doi: 10.1016/j.jmsy.2020.05.012.

[12] K. Jayakumar, K. Sivakami, P. Logamurthy, P. Sathiyamurthi, and N. Chandrasekaran, “Development of a Cryptographic Model Using Digits Classification for Cyber Security Applications,” *J. Cybersecurity Inf. Manag.*, no. Issue 2, pp. 287–299, Jan. 2024, doi: 10.54216/JCIM.140220.

[13] D. Aggarwal, K. B. R, R. Ghatikar, S. Chennuri, and A. Banerjee, “Generation of 1 GB full entropy random numbers with the enhanced-NRBG method,” *Phys. Scr.*, vol. 98, no. 12, p. 125112, Nov. 2023, doi: 10.1088/1402-4896/ad0811.

[14] C. S. Calude and K. Svozil, “Quantum Randomness and Value Indefiniteness,” *Adv. Sci. Lett.*, vol. 1, no. 2, pp.

165–168, Dec. 2008, doi: 10.1166/asl.2008.016.

[15] J. R. Johansson, P. D. Nation, and F. Nori, "QuTiP: An open-source Python framework for the dynamics of open quantum systems," *Comput. Phys. Commun.*, vol. 183, no. 8, pp. 1760–1772, Aug. 2012, doi: 10.1016/j.cpc.2012.02.021.

[16] D. E. Eastlake 3rd, S. Crocker, and J. I. Schiller, "Randomness Requirements for Security," Internet Engineering Task Force, Request for Comments RFC 4086, Jun. 2005. doi: 10.17487/RFC4086.