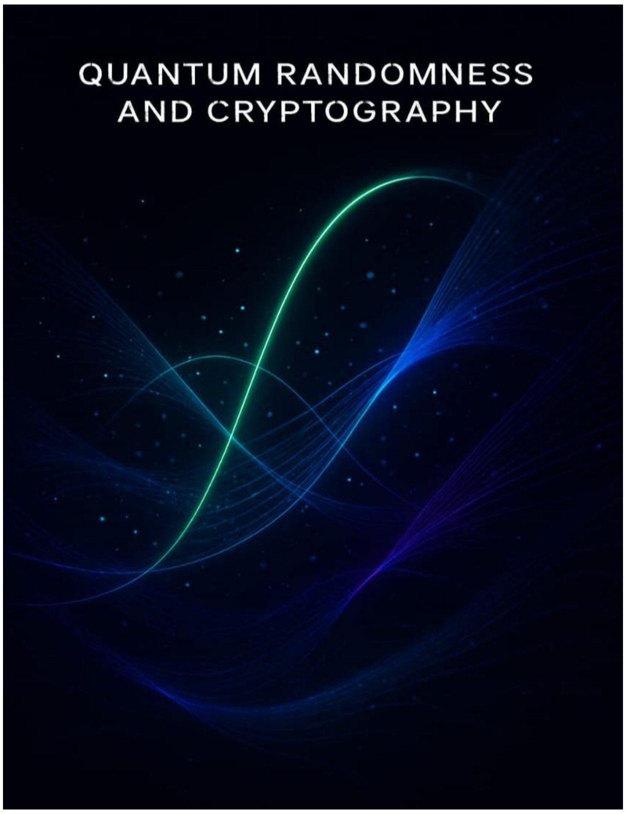

Randomness in Quantum Cryptography: A False Sense of Security?

A report on the implications of Pseudorandom Number Generators (PRNGs) vs Quantum Random Number Generators (QRNGs) in cryptographic protocols and quantum experiments.

ABSTRACT

An independent study exploring the role of random number generators in quantum cryptography and foundational quantum experiments, with a focus on the risks and implications of using pseudo randomness in protocols requiring true unpredictability.

Biswajyoti Nath
Department of Computer Science
Barak Valley Engineering College
Sribhumi, Assam, India
July 2025

Abstract

Randomness plays a pivotal role in quantum cryptography and several quantum experiments, particularly in Bell Tests and quantum key distribution (QKD) protocols. However, the source of this randomness is generally overlooked or ignored. While Pseudo Random Number Generators (PRNGs) are commonly used in cryptographic systems due to their efficiency factor, they are fundamentally deterministic and can, in principle, be predicted or manipulated. In Contrast, Quantum Random Number Generators (QRNGs) harness real quantum uncertainty to produce true randomness.

This report explores the implication of using PRNGs over QRNGs in quantum protocols and experiments, highlighting potential security issues and loopholes. This report emphasizes the importance of true randomness in ensuring validity and security of quantum-based technologies and argues that QRNGs may be necessary in contexts where unpredictability is not just desirable but critical.

Table of Contents

1. Introduction

Randomness plays a fundamental role in both modern cryptography and quantum physics. In classical cryptographic systems, random numbers are essential for encryption, key generation, and secure communications. In the context of quantum physics, randomness is not merely a useful tool but a central feature of quantum mechanics itself, manifesting in phenomena like quantum superposition and entanglement.

However, not all randomness is created equal. In many systems, Pseudorandom Number Generators (PRNGs) are used to produce sequences of numbers that appear random but are ultimately generated through deterministic algorithms. While sufficient for many everyday applications, PRNGs rely on initial seeds and computational processes, making them, in principle, predictable. In contrast, Quantum Random Number Generators (QRNGs) leverage intrinsic quantum phenomena to produce true, irreducible randomness, free from deterministic origins.

This distinction becomes crucial in specific contexts—particularly in quantum cryptography and foundational experiments like Bell tests. In such cases, the integrity of an experiment or protocol can hinge on the unpredictability of random numbers. For instance, Bell tests demand truly random choices of measurement settings to avoid loopholes that could undermine the test’s conclusions about nonlocality. Similarly, the security of certain quantum cryptographic protocols depends on the generation of truly unpredictable keys.

This report investigates the differences between PRNGs and QRNGs in these sensitive quantum applications. It examines the risks associated with relying on pseudo randomness in situations where true randomness is critical, explores existing experimental evidence and protocols, and argues for the careful consideration of random number sources in the design of quantum experiments and cryptographic systems.

2. Background and Theoretical Concepts

2.1 Pseudorandom Number Generators (PRNGs):

Pseudorandom Number Generators (PRNGs) are algorithms designed to produce sequences of numbers that mimic randomness. However, despite their widespread use in many fields—including simulations, computer science, and cryptography—PRNGs are fundamentally deterministic.

A PRNG operates by taking an initial input called a seed—a fixed, finite value—and using a deterministic mathematical formula to generate a long sequence of numbers that appears random. The same seed will always produce the exact same sequence. While these sequences often pass many statistical tests for randomness, they are not truly random in the strict sense, as they are entirely determined by the seed and the algorithm.

In many practical applications, PRNGs are sufficient because they are fast, efficient, and easily reproducible. They are widely implemented in software libraries, and modern PRNGs can produce sequences that are difficult to distinguish from true random numbers without significant computational effort.

However, in sensitive applications like cryptography and quantum experiments, this predictability can be problematic. If an attacker can learn the seed or reverse-engineer the PRNG's algorithm, they may be able to reproduce the entire random sequence, compromising the security or validity of the system.

Some well-known PRNG algorithms include:

- Linear Congruential Generators (LCGs)
- Mersenne Twister
- Xorshift

Cryptographically Secure PRNGs (CSPRNGs), such as those based on block ciphers or hash functions (though still ultimately deterministic)

Even Cryptographically Secure PRNGs, despite offering better protection against predictability in everyday systems, they remain fundamentally different from sources of true randomness, such as Quantum Random Number Generators (QRNGs).

2.2 Quantum Random Number Generators (QRNGs)

Quantum Random Number Generators (QRNGs) are devices that produce random numbers by exploiting the inherent unpredictability of quantum phenomena. Unlike PRNGs, which rely on deterministic algorithms, QRNGs generate randomness from physical processes that, according to quantum mechanics, are fundamentally indeterministic.

At the heart of a QRNG is a quantum system whose outcomes cannot be predicted, even in principle. A common approach involves measuring a quantum property such as the path of a single photon through a beam splitter. When a photon encounters a 50:50 beam splitter, quantum mechanics dictates that it has an equal probability of being transmitted or reflected—but the exact result is fundamentally random. This binary outcome can be converted into a random bit (0 or 1).

Other quantum processes used in QRNGs include:

- Quantum vacuum fluctuations
- Photon arrival times
- Quantum phase noise

These quantum effects yield genuine randomness because they are not governed by hidden deterministic variables, according to standard interpretations of quantum mechanics.

QRNGs are particularly valuable in applications where unpredictability is crucial, such as:
Quantum key distribution (QKD)
Bell test experiments
Randomness certification protocols

Unlike PRNGs, QRNGs are not algorithmically reproducible. However, practical QRNG devices require careful design to avoid introducing unwanted classical noise or biases that could compromise randomness quality. Certified QRNGs often include randomness extractors to remove any imperfections from the raw quantum data.

As technology advances, QRNGs are becoming more accessible, with commercial devices now available. Nevertheless, QRNGs tend to be more complex and costly compared to PRNGs, making them less common outside high-security or scientific applications.

3. The Problem of Randomness in Quantum Cryptography and Experiments

In both quantum cryptography and foundational quantum experiments, the quality and origin of randomness are not merely technical details—they can directly impact the validity, security, and trustworthiness of results.

3.1 Quantum Cryptography and Randomness

Quantum cryptography, particularly protocols like Quantum Key Distribution (QKD), relies on random numbers to generate secure cryptographic keys. If the random numbers used to create encryption keys are predictable, an attacker could potentially reconstruct those keys and compromise the system.

While cryptographically secure pseudorandom number generators (CSPRNGs) may provide strong protection against practical attacks in many conventional cryptographic systems, their use in quantum protocols introduces theoretical vulnerabilities. Any deterministic process can, in principle, be reverse-engineered under certain conditions, undermining the unconditional security promised by quantum cryptographic protocols.

True randomness, as provided by QRNGs, ensures that even an adversary with unlimited computational resources cannot predict the generated keys. This is crucial in quantum cryptography, where security guarantees depend on the assumption of truly random key generation.

3.2 Bell Tests and Randomness Loopholes

In Bell test experiments, randomness plays an even more foundational role. These experiments are designed to test the nature of reality itself—specifically, whether quantum correlations can be explained by local hidden variable theories or whether they require genuine quantum nonlocality.

A critical assumption in such experiments is the freedom-of-choice or measurement independence assumption. This requires that the choice of measurement settings (for example, the angle of a polarizer) is independent of any hidden variables that might influence the outcomes of the experiment. If the random number generators used to select measurement settings are predictable or correlated with the system being measured, this loophole can be exploited to simulate quantum-like results using entirely classical mechanisms. This would invalidate the experiment's ability to rule out local hidden variable theories.

Several advanced Bell tests in recent years have explicitly addressed this loophole by using QRNGs or even human-generated randomness to ensure genuine unpredictability in the choice of measurement settings.

3.3 Summary of the Problem

In both quantum cryptography and Bell tests, the source of randomness is not a trivial implementation detail—it is central to the integrity and conclusions of the entire process. Using PRNGs in these sensitive scenarios risks introducing vulnerabilities or loopholes that could fundamentally undermine the experiment’s goals or security guarantees.

As quantum technologies advance, it becomes increasingly important to carefully assess whether PRNGs are appropriate in specific applications, or whether QRNGs should be considered essential despite their practical challenges.

4. Case Studies and Examples

To better illustrate the practical importance of the distinction between pseudorandom and quantum random number generators, this section examines specific cases from quantum experiments and protocols where the choice of randomness source played a critical role.

4.1 The 2015 Loophole-Free Bell Test Experiments

One of the most famous examples of QRNG usage is found in the 2015 “loophole-free” Bell tests conducted by several independent research teams, including groups led by Ronald Hanson (Delft University of Technology), Anton Zeilinger (University of Vienna), and others.

These experiments aimed to simultaneously close two major loopholes in Bell tests:

The detection loophole (inefficient detectors missing events).

The freedom-of-choice loophole (measurement settings not chosen independently).

To address the freedom-of-choice loophole, these experiments used QRNGs to select measurement settings at each detector location. The QRNGs ensured that the choices were fundamentally unpredictable and uncorrelated with any hidden variables in the experiment.

Additionally, these choices were made within time windows sufficiently short to prevent any communication between the two detector stations, further strengthening the nonlocality claims.

Without the use of QRNGs in these experiments, the results could have been questioned, as a deterministic PRNG could not guarantee the same independence of choices.

4.2 Quantum Key Distribution (QKD) Systems

In practical Quantum Key Distribution (QKD) systems, QRNGs are increasingly being adopted to generate secure cryptographic keys.

For example, the commercial QKD systems developed by companies like ID Quantique and Toshiba incorporate QRNGs to ensure that the keys generated during the key exchange process are truly random. These systems typically exploit quantum optical processes, such as photon arrival times or phase noise, to produce randomness.

Using QRNGs eliminates the risk of predictability that arises with PRNGs. In QKD, even a tiny vulnerability due to predictable randomness can undermine the entire security guarantee, making QRNGs an essential component for achieving true unconditional security.

4.3 The “Big Bell Test” (Human Randomness Experiment)

An interesting alternative case is the Big Bell Test (2018), an international collaborative experiment involving over 100,000 volunteers worldwide who provided random inputs through an online platform to help close the freedom-of-choice loophole in Bell tests.

Although not a QRNG-based study, this experiment highlighted the importance of independent, unpredictable randomness. It demonstrated that even unconventional sources of randomness—when free from hidden deterministic mechanisms—can help in closing loopholes in fundamental tests of quantum mechanics.

This case underscores that the origin of randomness, whether quantum or otherwise, is critical for such experiments.

4.4 Summary of Examples

These case studies collectively demonstrate that in high-stakes quantum applications—whether foundational experiments or cryptographic protocols—the source of randomness cannot be an afterthought. QRNGs (and other fundamentally independent randomness sources) have become an essential tool in ensuring security, integrity, and scientific validity.

5. Discussion

The distinction between pseudorandom and quantum random number generators is not merely theoretical; it has significant practical and philosophical implications for both quantum cryptography and foundational experiments.

5.1 When Are QRNGs Necessary?

From the cases discussed, it is clear that QRNGs are essential in situations where unpredictability must be guaranteed at the physical level:

In loophole-free Bell tests, QRNGs help ensure that measurement settings are chosen in a way that cannot be influenced by hidden variables.

In quantum key distribution (QKD), QRNGs remove the risk of cryptographic keys being predictable by attackers with knowledge of the algorithm or the seed, thus preserving the unconditional security that quantum cryptography promises.

In such scenarios, PRNGs—even those that are cryptographically secure—are fundamentally insufficient, because their randomness is ultimately derived from deterministic processes, no matter how complex.

5.2 Trade-offs Between PRNGs and QRNGs

Despite their advantages, QRNGs also present some challenges:

- Cost: QRNG hardware is more expensive than software-based PRNGs.
- Speed: While QRNG speeds have improved, they may still lag behind the fastest PRNGs in some applications.
- Complexity: QRNGs require specialized quantum hardware, making them harder to integrate in every system.
- Reliability: QRNGs can sometimes be sensitive to environmental noise or require careful calibration.

In many practical applications, such as simulations, games, or non-critical cryptographic tasks, PRNGs are likely to remain the default choice due to their simplicity and efficiency.

However, in scientific experiments or high-security systems, where even minimal predictability can lead to serious consequences, QRNGs provide a necessary safeguard.

5.3 Broader Implications

The question of randomness also raises deeper philosophical issues about determinism, predictability, and the nature of physical laws. Quantum mechanics uniquely allows for truly random processes, unlike classical physics. The use of QRNGs in experiments reflects this fundamental shift in how randomness is understood in modern science.

Furthermore, as quantum technologies become more integrated into everyday systems—such as quantum-safe encryption—questions around the proper source of randomness will become even more important.

5.4 Personal Reflection

This report emerged from an observation that, despite the critical role of randomness in quantum systems, its source is often overlooked or assumed without scrutiny. As quantum technologies develop, it is important for researchers and engineers to carefully consider whether PRNGs are suitable for their specific applications, or whether QRNGs are necessary

6. Conclusion

Randomness is a fundamental component of both quantum cryptography and foundational quantum experiments. However, this report has shown that not all sources of randomness are equivalent. While pseudorandom number generators (PRNGs) are widely used in many systems due to their efficiency and ease of implementation, they remain deterministic at their core and therefore potentially predictable.

In contrast, quantum random number generators (QRNGs) produce randomness derived from inherently unpredictable quantum processes. In applications where unpredictability is not just desirable but essential—such as loophole-free Bell tests and quantum key distribution protocols—QRNGs offer a level of security and experimental integrity that PRNGs cannot match.

The case studies examined in this report, including recent Bell test experiments and commercial quantum cryptography systems, demonstrate the growing importance of QRNGs in both research and technology. These examples highlight that randomness should not be treated as a simple technical detail but as a crucial design element that can impact the security, validity, and outcomes of quantum technologies.

As quantum technologies advance and become more widely adopted, the question of randomness will only grow in significance. Careful consideration of the source of randomness will remain essential for ensuring both scientific rigor and security in quantum systems.

7. Acknowledgements

The author would like to thank Prof. Gilles Brassard for his reply to a personal inquiry regarding the role of random number generators in quantum cryptography. His response provided valuable perspective and partially inspired the writing of this report. All opinions, interpretations, and conclusions expressed here are solely those of the author.

8. Bibliography

1. J. S. Bell, Speakable and Unspeakable in Quantum Mechanics, Cambridge University Press, 1987.
2. R. Hanson et al., "Loophole-free Bell inequality violation using electron spins separated by 1.3 kilometres", Nature 526, 682–686 (2015).
3. Zeilinger et al., "Significant-Loophole-Free Test of Bell’s Theorem with Entangled Photons", Physical Review Letters 115, 250401 (2015).
4. S. Pironio et al., "Random numbers certified by Bell’s theorem", Nature 464, 1021–1024 (2010).
5. ID Quantique, Quantis Quantum Random Number Generator, Technical Datasheet.
6. Wikipedia contributors, “Quantum random number generator,” Wikipedia, The Free Encyclopedia.
7. M. Herrero-Collantes and J. C. Garcia-Escartin, “Quantum random number generators,” Rev. Mod. Phys. 89, 015004 (2017).

License Notice