IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Beyond Ideal Randomness: A Comprehensive Study On Practical Quantum Random Number Generators For Cryptographic Security

[1]Kantepalli Akhil, [2]K. Kanagalakshmi
[1]MCA Student, [2] Associate Professor
[1]School of Science and Computer Studies,
[1]CMR University, Bengaluru, India

Abstract: Quantum cryptography is a development that is crucial in improving cybersecurity, because it is based on quantum mechanics concepts and can be used to produce genuine random numbers, which are important in a strong cryptography. The abstract summarizes the findings of 30 major researches, which discuss different quantum random number generators (QRNGs) and their use in securing digital communications.

The emergent distinction between QRNGs and classical pseudorandom number generators is noted in many studies pointing out the novel properties of quantum mechanics to generate indeed random numbers [1][2]. It is important to note that research highlights the need to have device-independent and semi-device-independent QRNG protocol that would offer security guarantees against adversarial tampering without requiring the security of the used devices [3][4].

Additionally, information that is known about entropy sources, approaches to extracting randomness, and the rigorous statistical justification [5][6] of high-quality RNG confirms that such RNG can be even more important in cryptography and information security. The enhanced method of public verification and combination of QRNGs and cloud services have bright prospects in a number of services in the finance and data privacy industry [7][8].

To sum up, quantum technologies will become even more diversified on an ongoing basis, and their implementation into cybersecurity systems can serve as an even stronger protection against new threats, which is why it is impossible to overestimate the role of quantum technologies in the security of the future of digital communications [9][10].

Index Terms: **Quantum Random Number Generator, Cryptographic Security, Quantum Key Distribution, Randomness Bias, QRNG Limitations.**

I Introduction

At a time when cyber security matters most, random number generation comes up as one of the pillars in cryptography and secure communications. High-quality randomness is very essential and is essential in providing key generating activities, where it is expected to be unpredictable and resilient against an attacker. Deterministic algorithms In some traditional random number generators (RNGs), which generate sequences that are deterministic (although upon inspection the generated sequence may be random), the sequence is always predictable since the algorithm used to generate the sequence depends on an initial seed. This predictability is a major threat especially in cryptographic uses where encryption procedure can only be secure in case the keys are not predictable [1][2].

This should be compared to quantum random number generators (QRNGs) in which the uncertainty inherent to quantum mechanics is utilized to provide real randomness. Vacuum fluctuations and photon detection are some examples of the phenomena used by quantum RNGs to generate an unpredictable outcome that is free of any biasness that is inherent in classical methods [3][4]. As opposed to pseudo-random number generators, whose mathematical functions can in many instances be duplicated then replicated using algorithmic creation, QRNG offers a security level that is necessary in an environment that is becoming ever more vulnerable to the potentialities of quantum computing [5][6].

The surrounding environment of this trend is the need to find more randomness, in particular, in the area of post-quantum cryptography (PQC) the role of QRNGs increases. Not only are these generators able to provide rates of secure random numbers generation high enough to be practically useful, but also are able to resist the pressure of a host of statistical tests, which makes these generators utterly important in establishing secured communications [7][8]. This paper is a synopsis of the nature and performance of QRNGs especially on how it will be implemented and the effects of operational imperfection to generated randomness, thus advancing greater insight to effecting cryptographic security.

II Literature Review

Evolution of Random Number Generators

Classic random number generators (RNGs) have long been based on deterministic algorithms which generate seemingly randomly generated sequences that turn out to be predictable given the initial state (or even the algorithm). Such pseudorandom number generators (PRNG) lack the actual randomness needed to apply to cryptography modes exploitable by an adversary (Quantum Randomness in Cryptography--A Survey, [19]). To eliminate this, the classical systems were developed to utilize the physical sources of entropy, e.g. thermal noise, which are however plagued by environmental biases and the problem of repeatability (Entropy and Randomness, [15]).

There was a paradigm shift when quantum random number generators (QRNGs) were invented, to take advantage of the underlying quantum indeterminacy to generate truly unpredictable outputs. Photons-based schemes became the early QRNG implementations where single photons found their at probabilistic paths at beam splitters resulting in binary outcome generation (Quantum Random Number Generation, [8]). Later advances put forward such techniques as homodyne and heterodyne detection that utilize the vacuum fluctuations and phase noise to achieve even faster speeds and even smaller designs (Quantum Generators of Random Numbers, [2]). More modern developments entail source-device-independent methods with rates up to 17 Gbps (Source-Device-Independent Heterodyne QRNG, [4]), squeezing operations and time-of-flight measurements in order to provide greater randomness extraction (Quantum Randomness Through Squeezing, [16]; Characterizing QRNG Efficiency, [30]).

Applications in Cryptography

Such cryptographic systems, which require keys with high entropy, have now become incomplete without QRNGs. Specifically, the protocols of Quantum Key Distribution (QKD) such as BB84 are based on the unpredictability of quantum states to ensure the protection against any eavesdropping; any subsequent attempt at intercepting or measuring quantum states creates disturbances that may be detected (Certified QRNG Based on Single-Photon Entanglement, [18]). Differential studies have shown the QRNG to be usable as an addition to a QKD network, both over optical fibre and satellite channels, which represent its practical cryptographic application (Optical Fibre-Based QRNG, [17]).

QRNGs are also used in public infrastructures of randomness in addition to secure key generation. Examples are cloud platforms where quantum sources are incorporated to provide strong random seeds applicable to a wide range of security services, e.g., the quantum cloud project of Alibaba (Quantum Random Number Cloud Platform, [13]). The goal of these directions is to provide provably-trustworthy randomness to select applications like secure transaction, lotteries and publicly-verifiable randomness beacons (QRNGs with Entanglements to Make them Publicly Testable, [23]).

Security Evaluation

Although QRNGs in theory guarantee perfect randomness, real-world based QRNGs are vulnerable to corruption and external factors. The mismatch of detector efficiency or custom blinding attacks, are only some of the device-level vulnerabilities that are a security threat (Source-Independent QRNG Against Detector Attacks, [20]). Subtly, environmental noise may also pose some biases to effect the quality of randomness unless proper calibration is done (Practical Security of Continuous-Variable QRNG, [3]; Security Improvement for Source-Independent QRNG, [25]).

As a means to protect against them, statistically strict validation schemes have been constructed. Commonly used standard test suites are NIST SP 800-22 and Dieharder, which are used to test the statistical uniformity and independence of the generated sequences (Advanced Statistical Testing of QRNGs, [28]). These tests have been confirmed to be passed by many of the current QRNG models even though long-term stability is under research (Testing Behavioral Stability of QRNGs, [29]). Certification proposals, such as proposals of formal standards on the ETSI and ISO projects, attempt to set an international standard, but these protocols are currently in infant stages (Novel Certification for QRNGs, [11]).

Research Gaps

Although there is a significant progress, research on QRNGs has important gaps that need to be filled in before it can become mainstream. Top of these reasons is the fact that there is no universal standard or certification procedures of QRNG hardware that make embedding in regulated security systems a difficult task (Security of Private Randomness Generation, [26]). Moreover, the majority of the current QRNGs are not device-independent, i.e., they have the degree of security of trusting both the manufacturer and the integrity of the device (Device-Independent QRNG, [12]; Quantum RNG with Untrusted Sources [21]).

There is also the issue of scalability and real time performance. During this dynamically changing process of cryptographic systems to manage the enormous data transmission flows, the throughput of QRNGs would have to evolve in ways which does not compromise the statistical quality (Improved Real-Time Post-Processing for QRNGs, [10]). New post-processing algorithms and hybrid schemes: quantum randomness mixed with classical sources of entropy promise to correct these problems (Machine Learning Cryptanalysis on QRNGs, [22]). Nevertheless, the following studies should focus on creating sound, fast, bias-free QRNGs that can fit harmoniously into world-cryptographic infrastructures.

III Proposed Methodology

Literature-Based Theoretical Review

In order to study the situation with quantum random number generators (QRNGs) deeply, a systematic literature review was carried out within the framework of this research. Academic writings were retrieved in the well-known databases including IEEE Xplore, SpringerLink, and arXiv. The criteria used to select these articles and preprints included the consideration of peer-reviewed studies and high-impact preprints that either provided their experimental results to compare with the ones pertinent to QRNGs or provided them theoretically.

Thematic analysis was done to identify and merge important patterns in the literature. Observed were recurring problems such as output sequence bias, throughput constraints and device trust requirements amongst various implementations of the QRNG. This had assisted in defining a constant list of research gaps that are vital to the practice of QRNG deployment.

Conceptual Analysis

Block diagrams and conceptual schematics were used in order to explain the functional principles of QRNGs. Basic models of QRNG most often have a source of photons feeding its particles into a beamsplitter. Photons follow divergent paths depending on the innate quantum ambiguities, and the readings are sensed to come up with random outputs in the form of binary components. This involves tapping naturally into quantum superposition and wavefunction collapse in order to guarantee unpredictability.

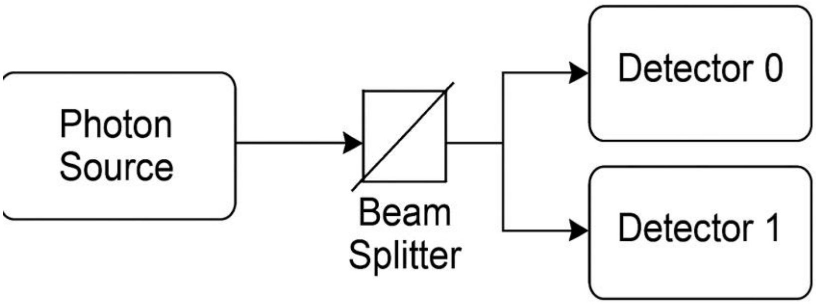

Fig.1: Basic QRNG Architecture

A diagram with a photon source introducing a beam splitter and two detectors (0 or 1) with labels to show that randomness is due to the path that is taken.

This visualization will help to understand how phenomena involving quantum mechanics is transformed into a measurable random result and where may the possible biases occur because of the hardware flaws or the environment interactions.

Algorithmic Reasoning and Simulation

To support the theoretical study, a theoretical Python simulation was performed by the means of qiskit and numpy libraries. This is a simulation of the probabilistic behavior of photons at a beam splitter that create bit streams as would output a QRNG.

Simple statistical solutions were carried out on the output:

Using the matplotlib to draw a histogram that will help to see how widespread both 0s and 1s are so that there was no serious imbalance.

The randomness property was ensured by calculation of Shannon entropy which showed values close to the ideal entropy of 1 in the binary sequences

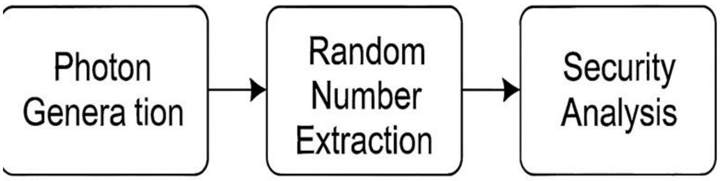

Fig.2: Block Diagram of QRNG Components

histogram bar graph with about the same number of occurrences of 0s and 1s, which visually confirms close to uniformity.

The simulation confirmed literature results through demonstration of the potential of detecting small biases in a statistical results by studying entropy and frequency early in a simulation run.

Methodological Limitations

It is important to mention that the work is more theoretical in nature and simulation based and does not make use of communications with physical hardware QRNGs in a laboratory setting. Although the scope of the paper manages to triangulate between experimental papers and the theoretical modeling of its concepts so that the research is well-grounded, it would be reinforced by a practical device testing activity in the future

V Discussion

Technical Challenges in QRNGs

Bias in Generated Sequences

The key difficulty in implementing QRNGs is no bias, that is, leaning towards a particular result. To give an example: because of tiny flaws in a beam splitter or differences in the effectiveness of detectors, a QRNG can give a small bias, say 54% 0s compared to 46% 1s. Minor departures in an even spread may, even on the scale of millions of bits, reveal minor patterns that attackers may use. These problems have been outlined in the studies, and they advise constant calibration and real-time statistical tests to overcome these hazards (Practical Security Analysis of QRNGs, [3]; Advanced Statistical Testing, [28]).

Entropy vs. True Quantum Randomness

Although QRNGs claim to exploit randomness on the basis of quantum physics, operational implementations of QRNGs nonetheless need entropy extraction algorithm to process raw results. As an example photon emission rates can vary or the detector can have dark counts which will cause classical noise. The aim of post-processing, typically through a cryptographic hash functions or randomness extractors, is to extract pure randomness. It however adds complexity to the design and even a limitation of performance (Improved Real-Time Post-Processing, [10]).

Cost and Hardware Requirements

The QRNGs especially those based on entanglement or squeezing are still expensive, and a controlled laboratory environment is necessary. Off-the-shelf QRNG modules, like the one by ID Quantique, are small yet are expensive investments, which make their wide scale use on consumer hardware economically unviable. Eventually, increased manufacturing processes mean the price will reduce, but currently QRNGs find a major usage in the high-assurance area of banking and government communication.

5.2 Integration with Cryptographic Systems

Supporting Quantum Key Distribution (QKD)

QRNGs play an essential role in QKD protocols, e.g., BB84, in which the randomness of key generation is directly connected to security. In case of predictability of the random numbers put in use of encoding quantum states, the very core warranty of QKD is exposed to flimsiness. Combinations of high-speed QRNGs with a QKD system have been shown to achieve secure key rates over hundreds of kilometers of optical fiber, attesting to QRNGs key position in actual quantum-safe networks (Source-Device-Independent QRNG at 17 Gbps, [4]).

Integration Limitations with Existing Internet Infrastructure

Nevertheless, a method of incorporating QRNG-based security into traditional internet protocols is challenging. The modern cryptography process in networks has been based on deterministic handshake protocols and central certificate authorities. Key negotiation with quantum randomness embedded would involve either redesigns of protocols or a hybrid system taking a combination of both classical and quantum strategies. Furthermore, a majority of existing hardware does not have quantum entropy interface which necessitates middleware.

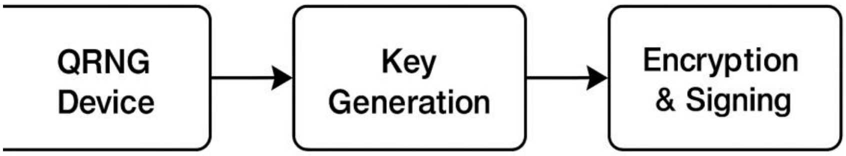

Fig.3: QRNG Integration in Cryptographic Systems

Security Implications

Consequences of Biased QRNGs

Using QRNGs with bias or insecurely tested cryptographic strength compromises cryptography. In case of an attacker being able to model or predict the output tendencies even partially he or she can considerably diminish an effective key space, turning an imagined 256-bit security into something that can be brute-forced. Weaker seeding of classical PRNGs are just one of historical examples of cryptographic failures with the important lessons learned to be applied to QRNGs when engineering rigor is not up to the mark.

Exploitation of Non-Uniform Randomness

There is even a threat of using more advanced statistical or machine learning algorithm to find delicate patterns in important streams of defective QRNGs (Machine Learning Cryptanalysis of QRNGs, [22]). This is particularly troubling in certain products such as multi-session VPN tunnels or blockchain systems in which randomness reuse may exacerbate security issues. Therefore the implementations of QRNG should involve sustained randomness health checking and fail-safe fall-back to safe(r) states upon the detection of anomalies.

Future Potentials

Toward Trustless QRNG Architectures

New work is considering using the output of QRNGs as inputs to blockchain-based public randomness beacons, which offer audit and decentralized verification. This might permit participants to test the purity of the random sequence autonomously without having to rely upon only one hardware source and is an intriguing path towards a genuinely trustless QRNG frameworks (Quantum Random Number Cloud Platforms, [13]).

Standardization and Certification

The discipline also looks forward to establishment of international standards on quantum sources of entropy as entities like ETSI ISG-QKD and NIST continue to work on randomness certification. A standardized testing procedure would speed up the process since it would help the industries set specific standards to implement within the financial schemes, safe communications methods, and identity management processes that involve the use of QRNGs.

VI Limitations

Although the study has covered a lot of thematic coverage of the theoretical contribution of Quantum Random Number Generators (QRNGs) and how it can contribute to privacy enhancement of cryptography security, there are a number of limitations that must be noted to provide a context of the study.

To begin with, the analysis is simulation and theoretic in nature, with no physical QRNG hardware experimentation. In this way, knowledge about anomalies at the device level, including those attributed to thermal drift, detector inefficiencies or effects of real-time noise, is also deduced by secondary sources (with empirical confirmation being absent).

Secondly, despite the fact that in this work most of the materials used are extracted research articles published in funds, it is not true that all the cited works were that of peer-reviewed journals. Others have arXiv preprints or other technical reports as their basis, and are not necessarily a result of formal validation. This brings in the element of over-dependence on initial discoveries that may change as peer review occurs. Also, the conceptual and algorithmic models used in this research paper presuppose the basic architectures of QRNGs with simplified Matters; models of ideal beam splitters and photon detectors that do not have mechanical or optical flaws. In the real world, devices tend to have complicated dynamics and hidden dependencies that do not come out clearly in these models.

Last, other issues related to broader system integration were mentioned, where within the overarching potential issues we found latency due to entropy extraction or regulatory complexities in the deployment of quantum hardware into current infrastructures, but did not quantitatively investigated. Incorporating them into the work in research in the future, especially including practical testing of devices, and the use of hybrid systems would be much more applicable to the conclusions made here.

VII Conclusion

The paradigm shift in the quest to secure cryptography systems is the use of quantum random number generators (QRNGs). The sources can be based on quantum mechanics, which provides a fundamentally different source of randomness compared with classical pseudorandom generators, which are based on deterministic procedures susceptible to analysis and therefore to exploitation. With the ever improving quantum computing capabilities, there may be a threat to traditional cryptographic assumptions, QRNGs are even more important as the foundation of new generation security architectures.

This paper points out that although the theoretical basis of QRNGs offer unmatched possibilities of randomness, there are significant challenges associated with practical implementations of a QRNG that one cannot just ignore. Of them, the risks of making presumption of perfect randomness in practice implementations stand the first. Behind-the-scenes bias that might be present due to hardware flaws, throughput requirements that enable adoption in real-life high-speed networks, and the need to trace the honesty of QRNG hardware manufacturers all highlight that some of the most reproducible biases in the use of quantum randomness in cryptography emerge in surprisingly subtle and covert ways.

The main objective of the paper is to define three main areas of concern bias, trust, and speed that have been found as the key concerns that affect the reliability and security of QRNG systems through a thorough literature-based analysis. The statistical uniformity required to produce secure keys is endangered because of bias; issues of trust are introduced by the lack of transparency of hardware designs, proprietary or otherwise; and performance challenges are posed as QRNGs struggle to fit into the fast and data-intensive contemporary encryption workflow.

Considering the future, it surely needs to be mentioned that future studies must go beyond explanatory modeling and hypothetical demonstrations so that they can adopt practical experiments with devices as well as in vivo entropy verification and stringent certification systems. Laying the groundwork in terms of standardization of performance measures and developing globally recognized testing methodologies not only serves to help build trust in QRNG deployments, but also ensures that said deployments become applicable in key staff, financial applications and future quantum networking.

Tackling these challenges by collaborating across disciplines, between quantum physics, hardware engineering and cybersecurity policy, we can finally see QRNGs realize their potential of building the foundation of digital security on the unchanging laws of nature, paving the way to a sustainable, quantum-safe world..

REFERENCES

[1] Maurício J. Ferreira ,Nuno A. Silva ,Armando N. Pinto and Nelson J. Muga, “Characterization of a Quantum Random Number Generator Based on Vacuum Fluctuations” MDPI, August 2021. Available: https://www.mdpi.com/2076-3417/11/16/7413

[2] Marcin M. Jacak, Piotr Jóźwiak, Jakub Niemczuk & Janusz E. Jacak, ”Quantum generators of random numbers” scientific reports, August 2021.Available: https://www.nature.com/articles/s41598-021-95388-7b

[3] Weinan Huang, Yichen Zhang, Ziyong Zheng, Yang Li, Bingjie Xu, and Song Yu, “Practical security analysis of a continuous-variable quantum random-number generator with a noisy local oscillator” APS, July, 2020. Available: https://journals.aps.org/pra/abstract/10.1103/PhysRevA.102.012422

[4] Marco Avesani, Davide G. Marangon, Giuseppe Vallone & Paolo Villoresi, “Source-device-independent heterodyne-based quantum random number generator at 17 Gbps” nature communications , December 2018. Available: https://www.nature.com/articles/s41467-018-07585-0

[5] Vaishnavi Kumar, John Bosco Balaguru Rayappan, Rengarajan Amirtharajan, Padmapriya Praveenkumar, “Quantum true random number generation on IBM’s cloud platform” ScienceDirect, September 2022. Available: https://www.sciencedirect.com/science/article/pii/S1319157822000283

[6] Miguel Herrero-Collantes, Juan Carlos Garcia-Escartin, “Quantum Random Number Generators” arxiv, Oct 2016. Available: https://arxiv.org/abs/1604.03304v2

[7] Guangshen Lin, Huanbo Feng, Shizhuo Li, Feng Xie, Zhenrong Zhang, Hongbang Liu, Kejin Wei, “X-ray-driven multi-bit quantum random number generator” PubMed, July 2024. Available: https://pubmed.ncbi.nlm.nih.gov/39538883

[8] Xiongfeng Ma, Xiao Yuan, Zhu Cao, Bing Qi & Zhen Zhang, “Quantum random number generation” npj, June 2016. Available: https://www.nature.com/articles/npjqi201621

[9] Hongyi Zhou, “Numerical Framework for Semi-Device-Independent Quantum Random Number Generators” arxiv, July 2022. Available: https://arxiv.org/abs/2207.02611

[10] Qian Li, Xiaoming Sun, Xingjian Zhang, Hongyi Zhou, “Improved Real-time Post-Processing for Quantum Random Number Generators” arxiv, Jan 2024. Available: https://arxiv.org/abs/2301.08621

[11] Maksim Iavich, Sergiy O. Gnatyuk, Andriy Fesenko, Tamari Kuchukhidze, “Novel Certification Method for Quantum Random Number Generators” ResearchGate, June 2021. Available: https://www.researchgate.net/publication/352686099_Novel_Certification_Method_for_Quantum_Random_Number_Generators

[12] Yang Liu, Qi Zhao, Ming-Han Li, Jian-Yu Guan, Yanbao Zhang, Bing Bai, Weijun Zhang, Wen-Zhao Liu, Cheng Wu, Xiao Yuan, Hao Li, W. J. Munro, Zhen Wang, Lixing You, Jun Zhang, Xiongfeng Ma, Jingyun Fan, Qiang Zhang, Jian-Wei Pan, ” Device independent quantum random number generation” arxiv, Jul 2018. Available: https://arxiv.org/abs/1807.09611

[13] Leilei Huang, Hongyi Zhou, Kai Feng & Chongjin Xie, “Quantum random number cloud platform” npj, July 2021. Available: https://www.nature.com/articles/s41534-021-00442-x

[14] John T. Kavulich, Brennan P. Van Deren, Maximilian Schlosshauer, "Searching for evidence of algorithmic randomness and incomputability in the output of quantum random number generators" arxiv, Jan 2021. Available: https://arxiv.org/abs/2101.01238

[15] Emil Simion, "Entropy And Randomness: From Analogic To Quantum World" ResearchGate, April 2020 . Available: https://www.researchgate.net/publication/340813821_Entropy_And_Randomness_From_Analogic_To_Quantum_World

[16] Jialin Cheng, Shaocong Liang, Jiliang Qin, Jiatong Li, Baiyun Zeng, Yi Shi, Zhihui Yan, and Xiaojun Jia, "Quantum randomness introduced through squeezing operations and random number generation" Optics Express, May 2024. Available: https://opg.optica.org/oe/fulltext.cfm?uri=oe-32-10-18237&id=549811

[17] Michał Dudek, Grzegorz Siudem, Grzegorz Kwaśnik, Wojciech Żołnowski & Marek T. Życzkowski, "Optical fibre-based quantum random number generator: stochastic modelling and measurements" scientific reports , March 2025. Available: https://www.nature.com/articles/s41598-025-95414-y

[18] Nicolò Leone, Stefano Azzini, Sonia Mazzucchi, Valter Moretti, Lorenzo Pavesi, "Certified quantum random number generator based on single-photon entanglement" arxiv, Sep 2021. Available: https://arxiv.org/abs/2104.04452

[19] Anish Saini ,Athanasios Tsokanos andRaimund Kirner , "Quantum Randomness in Cryptography—A Survey of Cryptosystems, RNG-Based Ciphers, and QRNGs" MDPI, June 2022. Available: https://www.mdpi.com/2078-2489/13/8/358

[20] Wen-Bo Liu, Yu-Shuo Lu, Yao Fu, Si-Cheng Huang, Ze-Jie Yin, Kun Jiang, Hua-Lei Yin, and Zeng-Bing Chen , "Source-independent quantum random number generator against tailored detector blinding attacks" Optics Express , Mar 2023. Available: https://opg.optica.org/oe/fulltext.cfm?uri=oe-31-7-11292&id=528338

[21] Zhengeng Zhao, Xin Hua, Yongqiang Du, Chenyu Xu, Feng Xie, Zhenrong Zhang, Xi Xiao, and Kejin Wei , "Silicon-based quantum random number generator with untrusted sources and uncharacterized measurements " Optics Express, Oct 2024. Available: https://opg.optica.org/oe/fulltext.cfm?uri=oe-32-22-38793&id=561383

[22] Nhan Duy Truong, Jing Yan Haw; Syed Muhamad Assad; Ping Koy Lam; Omid Kavehei, "Machine Learning Cryptanalysis of a Quantum Random Number Generator" IEEE, February 2019). Available: https://ieeexplore.ieee.org/document/8396276

[23] Janusz E. Jacak, Witold A. Jacak, Wojciech A. Donderowicz & Lucjan Jacak , "Quantum random number generators with entanglement for public randomness testing" Scientific Reports, January 2020. Available: https://www.nature.com/articles/s41598-019-56706-2

[24] Yongqiang Du, Xin Hua, Zhengeng Zhao, Xiaoran Sun, Zhenrong Zhang, Xi Xiao & Kejin Wei ,"Source-independent quantum random number generators with integrated silicon photonics" communications physics, January 2025. Available: https://www.nature.com/articles/s42005-024-01917-x

[25] Xing Lin, Shuang Wang, Zhen-Qiang Yin, Guan-Jie Fan-Yuan, Rong Wang, Wei Chen, De-Yong He, Zheng Zhou, Guang-Can Guo & Zheng-Fu Han , "Security analysis and improvement of source independent quantum random number generators with imperfect devices" npj , December 2020. Available: https://www.nature.com/articles/s41534-020-00331-9

[26] Stefano Pironio, Serge Massar , "Security of practical private randomness generation" arxiv, Dec 2012. Available: https://arxiv.org/abs/1111.6056

[27] Peter Bierhorst, Emanuel Knill, Scott Glancy, Yanbao Zhang, Alan Mink, Stephen Jordan, Andrea Rommal, Yi-Kai Liu, Bradley Christensen, Sae Woo Nam, Martin J. Stevens, Lynden K. Shalm , "Experimentally Generated Randomness Certified by the Impossibility of Superluminal Signals" arxiv, Feb 2018. Available: https://arxiv.org/abs/1803.06219

[28] Aldo C. Martínez, Aldo Solis, Rafael Díaz Hernández Rojas, Alfred U'Ren, "Advanced Statistical Testing of Quantum Random Number Generators" ResearchGate,November 2018. Available: https://www.researchgate.net/publication/329114447_Advanced_Statistical_Testing_of_Quantum_Random_Number_Generators

[29] Sahil Verma, Varich Boonsanong, Minh Hoang, Keegan E. Hines, John P. Dickerson, Chirag Shah, "Counterfactual Explanations and Algorithmic Recourses for Machine Learning: A Review" axivr, Nov 2022. Available: https://arxiv.org/pdf/2010.10596

[30] Shaohua Kan, Kohei Nakajima, Yuki Takeshima, Tetsuya Asai, Yuji Kuwahara, Megumi Akai-Kasaya, "Simple Reservoir Computing Capitalizing on the Nonlinear Response of Materials: Theory and Physical Implementations" Physical Review Applied, February 2021. Available: https://journals.aps.org/prapplied/abstract/10.1103/PhysRevApplied.15.024030