A REVIEW OF HYBRID QUANTUM–CLASSICAL RANDOMNESS-AS-A-SERVICE ARCHITECTURES FOR SECURE APPLICATIONS

K. Gangadhara Rao
Assistant Professor, Dept. of IT
Chaitanya Bharathi Institute of Technology
Hyderabad, India
Kgangadhar_it@cbit.ac.in

T. Satyanarayana Murthy
Associate Professor, Dept. of IT
Chaitanya Bharathi Institute of Technology
Hyderabad, India
tsmurthy_it@cbit.ac.in

R. M. Krishna Sureddi
Associate Professor, Dept. of IT
Chaitanya Bharathi Institute of Technology
Hyderabad, India
krishna.murali564@gmail.com

Udvik Konduru
Department of Information Technology
Chaitanya Bharathi Institute of Technology
Hyderabad, India
ugs22186_it.udvik@cbit.org.in

Jitesh Kumar
Department of Information Technology
Chaitanya Bharathi Institute of Technology
Hyderabad, India
ugs22199_it.jitesh@cbit.org.in

Namani Pravardhan
Department of Information Technology
Chaitanya Bharathi Institute of Technology
Hyderabad, India
ugs22188_it.pravardhan@cbit.org.in

***Abstract*—The generation of quality random numbers with strong trustworthiness is required for the modern cryptographic and security services. Random number generation by software is widespread and may be deterministic, while true random number quantum generators are only available currently at prohibitive cost. This paper examines hybrid quantum/classical number generation approaches and proposes the Hybrid QRaaS architecture which utilizes Qiskit-based quantum entropy and entropy from a classical operating system in a governance hybrid layer that handles mixing and real time health checks of the sampling rather than the self-contained generator; this architecture is service-oriented and includes health logging. The paper examines earlier developments in classical pseudo-random number generation, practical quantum random number generation applications, and service-oriented architectures with an emphasis on security. This work presents a hybrid entropy architecture designed to enhance the reliability, robustness, and trustworthiness of random number generation for cryptographic key generation, authentication, and distributed security applications.**

***Index Terms*—Hybrid Random Number Generation, Quantum Randomness, Randomness-as-a-Service, Entropy Validation, Cryptographic Security**

I. INTRODUCTION

The generation of sufficiently high-quality random values is an essential requirement for modern digital security ecosystems. Cryptographic protocols, secure communication channels, authentication mechanisms, and distributed computing systems depend on values that exhibit a high degree of unpredictability and minimal bias. Randomness can be harvested from physical sources; however, in the real world, most computing environments rely on pseudo-random number generators (PRNG), often for efficiency, portability, and convenience. PRNGs are algorithmic, and their security depends on the quality of the entropy that seeds them [1].In the scenario that the seed values are weak, reused or partially compromised, the output values can become predictable, and the cryptographic primitives become insecure. This threat is especially relevant in key-generation applications, in where partial exposure of certain secret values can render attacks feasible under certain circumstances [2].

Classical entropy pools based on system-dependent operational properties (when it was used, who used it, how hardware interrupts were handled) remain the primary source of entropy in many modern computing environments. While pragmatic entropy is provided, the volume and quality of entropy remains highly workload, sensitivity, and environment-dependent. This demonstrates shortcomings of classical entropy pooling and implies an emergent need for systems that can provide consistent and verifiable randomness quality irrespective of usage constraints.

Hybrid entropy architectures are used to improve the reliability and availability of entropy by combining multiple independent sources of entropy. Quantum random number generators (QRNGs) take advantage of the inherent probabilistic nature of quantum measurements to produce truly random outputs [3]. The entropies of both quantum and classical

system reduces the risk of losing any one source. Such hybrid approaches can include entropy mixing, keeping score of what is generated, and lightweight statistics to ensure quality of randomness is maintained. The advent of service-oriented computing has also given rise to RaaS (Randomness-as-a-Service) which can supply secure randomness to applications via a standard interface.

II. Background

A. Classical Random Number Generation

Within nearly all computing environments, randomness is provided by pseudo-random number generators (PRNG). PRNGs are deterministic algorithms that generate statistically uniform sequences of numbers. The seeds of these sequences are filled with entropy from operating system events, including fluctuations in timing, hardware interrupts, and even user interactions. Their resourcefulness and scalability render PRNGs a viable candidate for in-application use. The strength of these applications is dependent on the entropy produced from the events that fill these seeds. Biased or insufficient entropy may lead to suboptimal sequences with reduced levels of unpredictability, compromising the keys' strength. [1], [4].Considering that entropy generation is mostly software-based in the case of modern devices, however, the question of ensuring uniform quality of the entropy across different environments still remains.

B. Quantum Random Number Generation

To overcome the limitations of deterministic algorithms, many techniques for true random number generation based on physical processes have been explored. quantum random number generators (QRNG) rely on the inherent unpredictability of quantum measurements to produce statistically unbiased random bit strings [3], [5], [6]. Many realizations have relied on optical quantum events like photon counting or beam splitting, extracting randomness from physical events [7].

QRNGs provide stronger randomness assurances than classical random number generators and are being explored for security sensitive applications such as cryptographic key generation. The practical use of QRNG technology, however, is still at an early stage because of the requirement for specialized hardware and challenges in integrating quantum devices with standard computers.

C. Hybrid Entropy Architectures and Service-Oriented Randomness

To improve resilience and availability of RNG, recent work has explored hybrid entropy architectures that build on multiple independent entropy sources. By augmenting quantum entropy with OS-level entropy, hybrid architectures reduce the chance that compromising one source has an outsized impact on the quality of the output. Hybrid architectures typically use mixing, monitoring, and lightweight, non-intrusive statistical tests. Related work in the area of service-oriented computing has spawned Randomness-as-a-Service (RaaS) solutions that provide validated RNG via a service-oriented interface. These hybrid and service-oriented approaches aim to improve a modern security infrastructure's resilience, auditability, and scalability, while remaining compatible with prevailing software ecosystems.

III. Related Work

A. Classical Randomness Generation and Standards

while later research proved that a deterministic pseudo-random sequence generator could create a sequence that possessed the same desirable qualities of a random sequence, thus being useful for modeling natural phenomena. [8]. Standardized deterministic random bit generation mechanisms, such as those described in NIST SP 800-90A, continue to form the basis for randomness generation in modern operating systems and security libraries [1]. Subsequent guidelines addressing entropy sources emphasize the need for reliable entropy collection and validation [4]. Additionally, classical studies in numerical computation provide widely adopted techniques for pseudo-random generation [9]. Real-world analyses have also demonstrated that insufficient entropy during key generation can lead to practical cryptographic failures [10].

B. Security Implications of Weak Randomness

The connection between randomness quality and cryptographic security has been extensively studied. Researchers have demonstrated that partially exposed or predictable secret parameters degrade the security of otherwise secure ciphers. The results of [2] demonstrate that partial exposure of private key blocks is sufficient to enable RSA attacks on cryptographic implementations to make a point about securing sufficient entropy even in non hostile environments. The results justify the need of designing next generation architectures for randomness generation that are resilient to unpredicted scenarios

C. Quantum Random Number Generation Research

To escape the deterministic limitations of classical methods, quantum random number generators (QRNGs) are employed as an unpredictably-fundamental source of entropy. Survey papers provide implementations involving quantum measurement [3]. Experimental demonstrations using optical systems confirm the feasibility of extracting entropy from photon detection and beam-splitting mechanisms [7]. Further research has explored certified quantum randomness and device-independent generation approaches capable of providing stronger security guarantees [11], [12]. Advances in ultrafast QRNG implementations continue to improve throughput and reliability [5], [13], [14].

D. Validation and Statistical Testing of Randomness

To guarantee quality of generated random sequences, tests must be performed to ascertain validity of the generated data. Statistical test suites, such as that of NIST SP 800-22, are

often used to evaluate randomness properties and test for bias or predictability . [15]. These validation techniques are essential for assessing both classical and quantum entropy sources before deployment in security-sensitive applications.

E. Toward Hybrid Randomness Architectures

The latest developments in randomness generation involve combining multiple entropy sources for resilience and fault tolerance. Hybrid designs combining quantum-derived entropy and OS-level entropy minimize dependence on a single entropy source while increasing practicality. These designs illustrate the growing trend of service-oriented randomness generation that provides quality-controlled entropy to applications throughout a distributed network.

IV. Methodology

This work adopts a system-oriented methodology to design and analyze a Hybrid Quantum Randomness-as-a-Service (HyQRaaS) framework that combines classical and quantum entropy sources.

A. Entropy Source Integration

The proposed architecture assumes two independent sources of entropy. Classical randomness uses OS entropy sources with standardised DRBG protocols [1], [4]. Simultaneously, a Hadamard circuit-based quantum circuit in the Qiskit simulation environment generates quantum-based randomness with qubit measurements resulting in probabilistic bit strings serving as the source of quantum entropy. [3], [5].

In the current implementation, quantum entropy is generated from the Qiskit simulator for hardware-agnostic development. This will ultimately progress to the use of hardware-based quantum entropy sources for even stronger assurance of unpredictability.

B. Hybrid Mixing Mechanism

The output from the classical source and the output from the quantum source are combined using a bitwise exclusive OR (XOR) operation. The concept of hybrid entropy mixing has been extensively studied for applications of security and entropy preservation [9]. The hybrid controller oversees entropy accumulation, stream mixing, and bit stream synchronization to produce the output random bit string. Such a system architecture is designed to maintain adequate randomness even if one source is only partially deactivated.

C. Randomness Validation

For output quality evaluation, outputs are intended to be validated through lightweight statistical validation measuring frequency distribution, and entropy estimation and testing evaluation theory follows known statistical testing theories [15]. The system produces a health score that provides real-time feedback regarding entropy quality.

D. Service-Oriented Delivery

The validated hybrid random data is exposed over a service interface enabling applications to request random bytes on demand using well-defined API calls. This Randomness-as- a-Service paradigm enables auditability, scalability, and integration into distributed security applications.

This study focuses on architectural design and literature analysis; empirical benchmarking will be conducted in future work.

Comparative Analysis

Randomness generation techniques can be divided into classical pseudo-random number generators, physical true random number generators, and quantum entropy sources. Each of these has advantages and disadvantages in terms of their lack of predictability, their availability, efficiency and implementation complexity.

Classical pseudo-random number generators (PRNGs) are widely used due to their computational efficiency and scalability [9]. However, deterministic nature makes them dependent on entropy source quality with predictable results in where entropy is lacking [1]. Real-world analyses have demonstrated that weak randomness during key generation can compromise cryptographic security [10].

True random number generators (TRNG) based on physical processes have higher entropy quality but require special hardware and may exhibit environmental variability. Quantum random number generators (QRNG) offer inherently unpredictable output based on quantum measurement processes [3], [5]. Experimental implementations have demonstrated strong statistical properties, though deployment cost and integration complexity remain significant challenges [7], [13].

Hybrid entropy architectures aim to combine the benefits of multiple sources for increased robustness and availability. By melding together OS entropy and quantum randomness, hybrid architectures reduce dependence on a single source while providing a consistent output quality.

A. Summary of Methods

TABLE I
Comparison of Randomness Generation Approaches

Method	Advantages	Primary Limitation
PRNG	Fast, scalable, easy to deploy	Deterministic; depends on seed quality
TRNG (Physical)	Higher entropy from physical noise	Hardware dependence and variability
QRNG	Fundamentally unpredictable output	Integration cost and device complexity
Hybrid RNG	Improved reliability and availability	Requires coordination of multiple sources

B. Discussion

The comparison indicates that there is no gold-standard randomness source meeting the performance, availability and strong entropy requirements. Classical sources are efficient but potentially or fully predictable, while quantum has stronger guarantees but deployment difficulties. Hybrid entropy sources offer a practical compromise – combining independent sources

and testing the quality of the output to provide greater confidence in the use of randomness for security-sensitive applications.

V. Challenges

Despite the advantages offered by hybrid randomness gen- eration systems, several technical and operational challenges remain that must be addressed for reliable real-world deploy- ment.

A. Entropy Quality and Consistency

A primary challenge is the consistent quality of entropy from different sources. Classical operating system entropy pools are subject to variation in usage and environmental factors, potentially diminishing their stochastic properties [1], [4]. It also has an impact on the entropy of quantum sources. Regularly performing statistical tests is therefore needed to check for the presence of flaws or degradation in the outputs produced [15].

B. Integration Complexity

There are practical difficulties in mixing quantum and classical entropy sources. There is a processing overhead to synchronize the bit streams from the different sources and to carry out the mixing steps. There is also an additional implementation "cost" in having to connect the quantum bits generation with classical software. [3], [5].

C. Performance and Scalability

Hybrid systems using entropy tests and validation can have increased latencies for high-volume random data. In high-load scenarios, Randomness-as-a-Service services need to balance sampling volume with real-time assurance. Optimising for performance while having strong quality assurance is a research topic.

D. Security and Reliability

Randomness extraction also needs to defend itself against means of behavioral exploitation that learned about the extracted data. If the learned behavioral patterns can be exploited, then the generated randomness cannot be considered truly random [2], [10]. Ensuring fault tolerance, auditability, and protection against entropy manipulation is therefore critical for secure deployment.

VI. Future Directions

While the Hybrid QRaaS framework provides the foundation for trustworthy entropy generation, several enhancements can be applied to its implementation and operation.

A. Hardware-Based Quantum Integration

Future implementations might extend not only to simulation-based quantum circuits but to hardware dedicated qrngs. Optical or device-independent qrng modules can provide higher entropy rates with enhanced guarantees [5], [12], [13]. Incorporating hardware-based quantum sources would improve the trustworthiness of the generated randomness in security-critical environments.

B. Advanced Statistical Validation

Further developments can include full statistical testing suites based on established evaluation suites. Continuous val- idation against NIST tests can be automated to keep track of and in real-time detect entropy degradation [15]. Machine- learning-based anomaly detection techniques may also be explored for identifying irregular entropy patterns.

Scalable Randomness-as-a-Service Deployment

Future versions of distributed Randomness-as-a-Service systems could be made to scale and be highly available. By distributing hybrid entropy nodes across geolocations, it would be possible to balance loads, have redundancy and fault tolerance. This architecture could accommodate globally distributed, bounded applications that need continuous secure RNG.

C. Optimization of Hybrid Mixing Strategies

Other work could investigate other forms of mixing beyond simple XORing. Adaptive mixing based on the varying quality of the sources of entropy could also enhance the irreducibility of the system and its resistance to entropy loss.

VII. System Architecture of the Hybrid Quantum Randomness Framework

This section will describe the Hybrid QRaaS Architecture. This encompasses a combination of two different entropy sources (classical OS entropy and quantum derived entropy), a hybrid mixer controller, a quality validation and monitoring module, and an audit-compliant service interface. Figures 1 and 2 summarize the end-to-end pipeline and the controller's internal workflow. The XOR-based mixing process is designed to help ensure that even if one entropy source becomes partially degraded, the combined output retains high unpredictability.This study focuses on the design and evaluation of a hybrid randomness architecture; a full-scale production deployment and empirical benchmarking are left for future work

A. End-to-End Architecture

As shown in Fig. 1, HyQRaaS integrates (i) a classical entropy source based on the operating system's cryptographically secure random generator, and (ii) a quantum entropy source produced via a Hadamard-based circuit executed in Qiskit. Both streams are forwarded to the hybrid controller. The controller is responsible for synchronizing the bit streams, aligning lengths, and performing the mixing operation. The mixed output is then validated, assigned a runtime health score, and made available to clients through a service endpoint. Logging and audit trails are maintained to support traceability and post-generation inspection when required.The current implementation relies on simulated quantum circuits; integrating

hardware QRNG modules is planned to further strengthen entropy guarantees

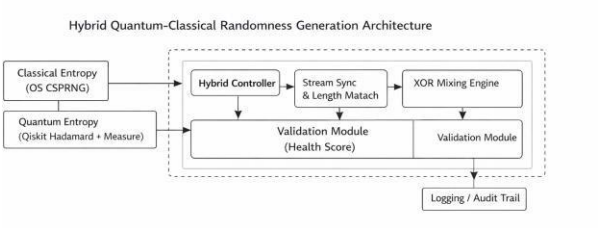

Fig. 1. Hybrid Quantum–Classical Randomness Generation Architecture.

B. Hybrid Controller Workflow

The hybrid controller is the central coordinating component and the primary novelty of the proposed system. Figure 2 illustrates its workflow. First, entropy is acquired from both the OS and quantum pipelines. Next, stream synchronization and length matching ensure that the controller combines comparable segments from both sources.The XOR mixing engine does bitwise mixing to eliminate dependence on any one source and to eliminate the bias that a partially corrupted stream would impart. The mixed stream is then finally written to an output buffer that rate-limits and burst fulfills requests from applications. If desired, logging/auditing metadata can be written.

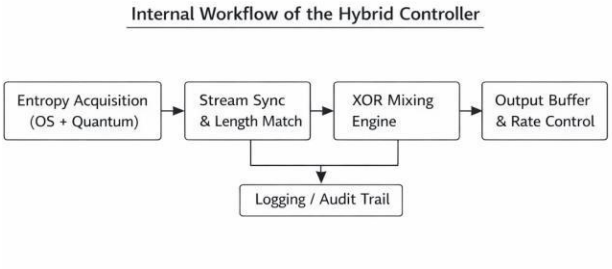

Fig. 2. Internal Workflow of the Hybrid Controller.

C. Validation and Service Delivery

Before delivery, generated sequences are subject lightweight statistical tests and assigned a health score to convey the quality of output. The Randomness-as-a-Service API provides endpoints for applications to request random bytes as needed making the framework appropriate for use in security-sensitive applications such as the generation of authentication tokens, key material and session IDs. The use of service-oriented notions also enables centralized monitoring whilst the dual-entropy framework protects the approach from entropy depletion and the failure of one source in particular. A REST endpoint such as \verb—/random/bytes?n=32— can be employed to obtain vetted random byte sequences.

VIII. Feasibility Analysis and Practical Considerations

This section evaluates the practical feasibility of deploy- ing the proposed Hybrid Quantum Randomness-as-a-Service (HyQRaaS) architecture by examining technical viability, cost implications, and operational considerations.

A. Technical Feasibility

The proposed hybrid randomness system is considered technically feasible based on existing technologies because it relies on well-established components that are already widely available in modern computing environments.

- Classical Entropy Availability: Most OSs provide cryptographically secure rng based on entropy pools gathered from OS events; these implementations are standard/recommended for secure apps [1], [4].
- Quantum Entropy Production: Quantum randomness can be generated by elementary quantum circuits exploit- ing measurement-induced uncertainty (e.g., Hadamard circuits) Available work and simulators (e.g., Qiskit) show that optical hardware requirements are not a must to achieve hardware-efficient quantum-based randomness [3], [5].
- Hybrid integration: mixture of independent entropy sources is a feasible approach to improve the strength and availability of the overall entropy source generic software interfaces can handle entropy harvesting, provide conditioning and XOR mixing; no special-purpose hardware required

B. Cost and Deployment Considerations

The economic feasibility of the HyQRaaS system depends on both initial setup costs and ongoing operational requirements.

- Initial Infrastructure: The primary deployment requirement is a modest server capable of executing quantum simulation workloads and managing entropy streams. Since the classical entropy source is already present in the operating system, additional hardware requirements are minimal.
- Operational Overhead: Recurring costs mainly include computational resources and maintenance. Quantum entropy generation via simulation does not require expensive dedicated hardware, reducing operational expenses compared to optical QRNG implementations.
- Scalability: The service-oriented architecture enables a single deployment to serve multiple applications simultaneously through an API interface, distributing cost across multiple use cases such as authentication services, secure communication, and token generation.

C. Performance and Reliability Considerations

This hybrid architecture is expected to strengthen reliability weaknesses of a single entropy source. Continuous statistical

testing and health scoring can signal if the quality of random- ness has degraded. Beating and rate-limiting features ensure a consistent supply of randomness despite request bursts. These characteristics make it possible to deploy in numerous envi- ronments without interfering with existing crypto operations.

IX. Conclusion

This paper has presented an architectural and literature re- view of Hybrid Quantum–Classical Randomness-as-a-Service (HyQRaaS) architectures capable of enhancing the availability and fault tolerance of cryptographic random number genera- tion. Classical pseudo-random number generation is vulner- able to the quality of entropy sources in varied operational environments. To address this problem, a hybrid architecture combining classical OS-level entropy with quantum random- ness is introduced to improve resilience against entropy source failure.

The study provides the means to understand the operation of a hybrid controller that coordinates the mixing of the entropy sources, performs the XOR mixing, and outputs a high-quality random stream for applications.The lightweight statistical tests and health scoring are also able to monitor real-time randomness quality making deployment in security-sensitive applications safe.

The service-oriented architecture of HyQRaaS demonstrates how a randomness generator can be exposed via a service- oriented architecture to securely connect to authentication, cryptography, and distributed compute backends and by com- bining classical and quantum entropy sources, the architecture increases robustness, auditability, and scalability over single- source generators.

Directions for future work might involve using hardware- based quantum entropy sources, optimization of mixing and validation, and more exhaustive statistical testing with estab- lished testing suites to quantify performance against realistic workloads.

References

1. National Institute of Standards and Technology, “Recommendation for random number generation using deterministic random bit generators,” 2015, nIST Special Publication 800-90A. [Online]. Available https://csrc.nist.gov/publications/detail/sp/800-90a/rev-1/final
2. S. K. Ravva, K. L. N. C. Prakash, and S. R. M. Krishna, “Partial key exposure attack on rsa using some private key blocks,” Journal of Computer Virology and Hacking Techniques, vol. 20, pp. 185–193, 2024
3. M. Herrero-Collantes and J. C. Garcia-Escartin, “Quantum random number generators,” Reviews of Modern Physics, vol. 89, no. 1, p. 015004, 2017
4. National Institute of Standards and Technology, “Recommendation for the entropy sources used for random bitgeneration,” 2018, nIST Special Publication 800-90B [Online]. Available https://csrc.nist.gov/ publications/detail/sp/800-90b/final
5. . Ma, X. Yuan, Z. Cao, B. Qi, and Z. Zhang, “Quantum random number generation,” *npj Quantum Information*, vol. 2, p. 16021, 2016
6. Xu and X. Ma, “Practical quantum random number generation: Advances and challenges,” *IEEE Access*, 2022
7. Stefanov, N. Gisin, O. Guinnard, L. Guinnard, and H. Zbinden, “Optical quantum random number generator,” *Journal of Modern Optics*, vol. 47, no. 4, pp. 595–598, 2000
8. E. Shannon, “Communication theory of secrecy systems,” *Bell System Technical Journal*, vol. 28, no. 4, pp. 656–715, 1949.
9. E. Knuth, *The Art of Computer Programming, Volume 2: Seminu- merical Algorithms*. Addison-Wesley, 1997
10. K. Lenstra *et al.*, “Ron was wrong, whit is right,” *IACR Cryptology ePrint Archive*, vol. 2012, p. 064, 2012 [Online]. Available: https://eprint.iacr.org/2012/064
11. S. Pironio *et al.*, “Random numbers certified by bell’s theorem,” *Nature*, vol. 464, pp. 1021–1024, 2010
12. P. Bierhorst, E. Knill, S. Glancy, Y. Zhang, A. Mink, S. Jordan *et al.*, “Experimentally generated randomness certified by the impossibility of superluminal signals,” *Nature*, vol. 556, pp. 223–226, 2018
13. A. Abbott, C. S. Calude, J. Conder, and K. Svozil, “Strong exper- imental guarantees in ultrafast quantum random number generation,” *Physical Review X*, vol. 6, no. 4, p. 041004, 2016
14. M. M. Jacak, L. Jacak, and W. A. Jacak, “Quantum generators of random numbers,” *Scientific Reports*, vol. 11, p. 16108, 2021
15. National Institute of Standards and Technology, “A statistical test suite for random and pseudorandom number generators,” 2010 [Online] Available https://csrc.nist.gov/publications/detail/sp/800-22/rev-1a/final