Research Square

Preprints are preliminary reports that have not undergone peer review.
They should not be considered conclusive, used to inform clinical practice,
or referenced by the media as validated information.

Quantum True Random Number Generation via Schmidt-Mode-Filtered SPDC with Finite-Size Security Constraints

Tawfik Ismail

tismail@taibahu.edu.sa

Taibah University

Ala Sabeeh

Taibah University

Research Article

Keywords: Quantum true random number generator (QTRNG), spontaneous parametric down-conversion (SPDC), single-photon avalanche diode (SPAD), joint spectral intensity (JSI), Schmidt decomposition, spectral purity, min-entropy, quantum randomness, finite-size security, quantum key distribution (QKD)

Posted Date: July 30th, 2025

DOI: https://doi.org/10.21203/rs.3.rs-7041346/v1

License: This work is licensed under a Creative Commons Attribution 4.0 International License.
Read Full License

Additional Declarations: No competing interests reported.

Quantum True Random Number Generation via Schmidt-Mode-Filtered SPDC with Finite-Size Security Constraints

Tawfik Ismail[1,2†], Ala H. Sabeeh [1,3*],
[1]Energy, Industry, and Advanced Technologies Research Center, Taibah University, P.O. Box 344, Medina, Saudi Arabia
[2]Department of Telecommunication Engineering, College of Engineering, Taibah University, P.O. Box 344, Medina, Saudi Arabia
[3]Department of Electrical Engineering, College of Engineering, Taibah University, P.O. Box 344, Medina, Saudi Arabia
Email addresses: *tismail@taibahu.edu.sa, †asabeeh@taibahu.edu.sa,

Abstract

This work proposes a quantum true random number generator (QTRNG) architecture based on spontaneous parametric down-conversion (SPDC) photon sources, single-photon avalanche diodes (SPADs), and Schmidt-mode-resolved joint spectral intensity (JSI) filtering. The system employs a numerically optimized spectral filter to isolate the dominant Schmidt mode, effectively suppressing spectral entanglement and enhancing source-level purity. Simulation results confirm that the optimized configuration achieves a Schmidt number of 1.0008, spectral purity of 0.9992, and entanglement entropy of 0.0052 bits. The bitstream generated from coincidence detections demonstrates ideal statistical properties, including a min-entropy per bit of $H_\infty = 0.9997$ and a total of 17.85 million extractable bits, without requiring post-processing. The randomness output passes all tests in the NIST SP 800-22 and Dieharder suites with a 100% success rate, confirming its unpredictability and cryptographic suitability. The system is also computationally efficient, with a runtime of 320 seconds and memory usage of 12.83 MB for 10^9 pulses, making it suitable for real-time embedded applications. This study establishes a scalable and physically secure QTRNG framework grounded in spectral mode engineering and finite-size security certification.

Index Terms

Quantum true random number generator (QTRNG), spontaneous parametric down-conversion (SPDC), single-photon avalanche diode (SPAD), joint spectral intensity (JSI), Schmidt decomposition, spectral purity, min-entropy, quantum randomness, finite-size security, quantum key distribution (QKD)

I. Introduction

The generation of true random numbers is fundamental to cryptographic systems, secure communications, and large-scale simulations, where unpredictability and entropy quality are essential. Classical pseudo-random number generators (PRNGs), although efficient and cost-effective, are inherently deterministic and thus unsuitable for high-security applications. In contrast, quantum random number generators (QRNGs) exploit the intrinsic randomness of quantum measurements—such as photon detection, vacuum fluctuations, or phase noise—to produce unpredictable outcomes governed by the fundamental laws of quantum mechanics [1]. These quantum true random number generators (QTRNGs) offer superior entropy characteristics and security guarantees, making them ideal for quantum-safe cryptographic infrastructures.

Ahmed et al. [2] introduced a chaos-based true random number generator (TRNG) using semiconductor lasers with external optical feedback to address two major challenges: high peak-to-average power ratio (PAPR) and parameter variation tolerance (PVT). Non-linear quantization via μ-law companding was applied to mitigate PAPR effects, while an AES-based post-processing stage enhanced randomness quality and enabled tolerance to $\pm 20\%$ variation in key system parameters such as mirror reflectivity, cavity length, and injection current. The generated bitstreams passed both NIST SP 800-22 [3] and Dieharder [4] statistical tests across all tested configurations, demonstrating robustness and cryptographic suitability under diverse operating conditions.

Christ et al. [5] investigated multimode quantum state characterization using second-order correlation functions applied to squeezed light from spontaneous parametric down-conversion (SPDC). Their approach enabled precise analysis of spatial-temporal quantum correlations in light fields, directly supporting TRNG designs that leverage SPDC-generated entangled photon pairs for randomness extraction.

The methodology provided a framework for evaluating spectral and temporal photon pair correlations, reinforcing the use of joint spectral intensity (JSI)-based filtering to ensure high-quality photon pair selection. The results validated the ability of SPDC sources to produce well-characterized, strongly correlated photon pairs suitable for secure quantum information protocols.

Rutz et al. [6] reviewed recent advances in entangled-photon pair sources and single-photon avalanche diodes (SPADs) operating in the short-wave infrared (SWIR) band, highlighting their relevance to quantum communication, sensing, and random number generation technologies. The review highlighted improvements in SPDC-based photon sources tailored for telecom wavelengths, including increased spectral purity, brightness, and collection efficiency. It also detailed progress in InGaAs/InP SPADs with reduced timing jitter and dark count rates, enabling high-fidelity photon detection. These advancements align closely with the design goals of QRNG systems by enhancing source-detector performance and randomness throughput in the SWIR band.

Recently, significant progress has been made in the certification of quantum randomness through device-independent protocols. In particular, Seguinard et al. [7] experimentally demonstrated the generation of more than one bit of certified quantum randomness in a two-input, two-output Bell scenario, establishing a robust framework for randomness certification that does not rely on assumptions about the internal workings of the devices. This experimental validation reinforces the theoretical foundation for high-assurance quantum random number generation, especially in photonic systems where spectral and temporal correlations must be carefully managed.

In this work, we propose a novel QTRNG architecture that advances quantum randomness extraction by integrating Schmidt-mode-resolved JSI filtering with SPDC photon-pair generation and SPAD-based single-photon detection. The key innovation lies in applying a mode-selective spectral filter derived from the biphoton wavefunction's Schmidt decomposition to isolate the dominant spectral mode and suppress higher-order spectral correlations. This source-level spectral engineering enhances purity and reduces entanglement entropy, enabling the extraction of high-quality quantum randomness directly from the physical layer. The system design incorporates a full simulation framework that models SPDC dynamics, Schmidt-mode decomposition, SPAD non-idealities, and finite-size entropy bounds under adversarial conditions. Key contributions include: (1) a physically accurate simulation model incorporating spectral filtering and photon detection effects; (2) entropy enhancement through optimized spectral mode shaping; (3) complete statistical validation using standardized randomness test suites; and (4) computationally efficient implementation suitable for real-time and resource-constrained environments.

This paper is organized as follows: Section II introduces the system architecture, including SPDC-based biphoton generation, Schmidt-mode-resolved JSI filtering, and SPAD-based single-photon detection. Section III details the simulation framework, including the optimization routine, entropy analysis, and statistical validation using the NIST SP 800-22 and Dieharder test suites. Section IV summarizes the key contributions, highlights the advantages of the proposed system, and outlines directions for future research.

II. System Design and Security Framework

Figure 1 illustrates the schematic of the proposed QTRNG architecture, which integrates SPDC-based photon-pair generation, Schmidt-mode-resolved JSI filtering, and SPAD-based single-photon detection. The system is based on a physically realistic model of SPDC dynamics and applies mode-selective spectral filtering to isolate the dominant Schmidt mode. This design enhances spectral purity and enables reduction of frequency-domain entanglement entropy, which is critical for generating high-quality quantum randomness [5]. A dedicated analysis of entanglement entropy is included to characterize spectral separability and quantify the number of effectively contributing modes. To maintain this spectral purity under fluctuating pump or environmental conditions, an adaptive JSI filtering mechanism is introduced for real-time Schmidt-mode tracking. Finally, a finite-size smooth min-entropy framework is employed to certify the randomness of the generated bitstream under quantum side information and adversarial constraints.

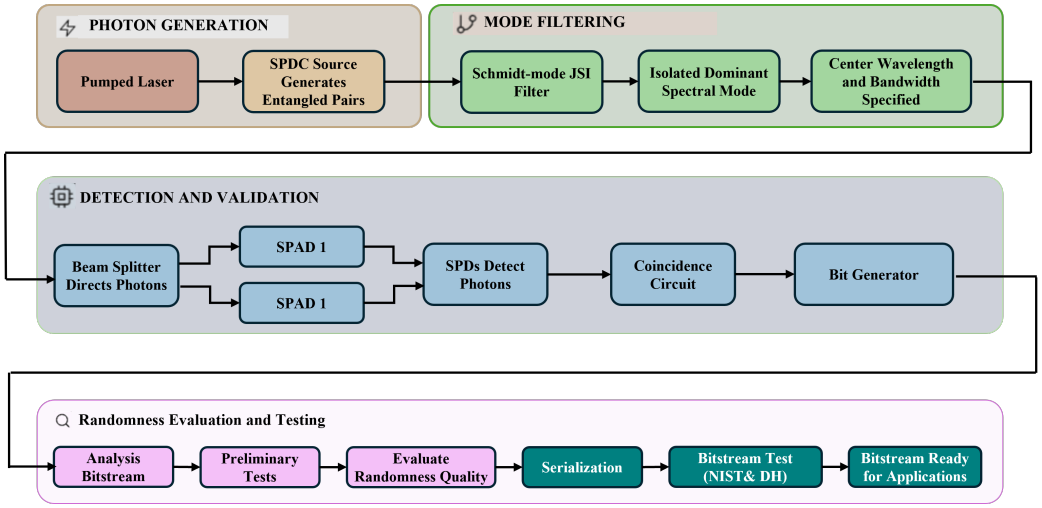


Fig. 1: Schematic diagram of a QTRNG based on SPDC and SPADs, integrated with JSI filter.

A. SPDC-Based QTRNG Architecture

1) Nonlinear Crystal (SPDC Source): The heart of the system is the nonlinear crystal where SPDC occurs. A high-energy pump photon (γ_p) enters the crystal and, with a small probability, splits into two lower-energy photons: a signal photon (γ_s) and an idler photon (γ_i), as presented in Eqs. (1a) and (1b). This process obeys conservation laws, ensuring that the generated photons are entangled in properties such as polarization, time-energy, or spatial modes [8]:

$$\hbar\omega_p = \hbar\omega_s + \hbar\omega_i \ \leftarrow \text{(Energy Conservation)} \tag{1a}$$

$$\vec{k}_p = \vec{k}_s + \vec{k}_i \ \leftarrow \text{(Momentum Conservation)} \tag{1b}$$

where ω_p, ω_s, and ω_i denote the angular frequencies of the pump, signal, and idler photons, respectively, and $\vec{k}_p$, $\vec{k}_s$, and $\vec{k}_i$ represent their corresponding wave vectors [9].

2) Schmidt-Mode-Based JSI Filtering: To reduce entanglement entropy and increase spectral purity, the biphoton wavefunction is filtered using Schmidt-mode decomposition. The joint spectral amplitude (JSA) is modeled as:

$$\text{JSA}(\omega_s, \omega_i) = \alpha(\omega_s + \omega_i) \cdot \phi(\omega_s, \omega_i) \tag{2}$$

where α is the pump envelope and ϕ is the phase-matching function. The JSI is given by:

$$\text{JSI}(\omega_s, \omega_i) = |\text{JSA}(\omega_s, \omega_i)|^2 \tag{3}$$

Spectral correlations are decomposed using Schmidt decomposition:

$$\text{JSA}(\omega_s, \omega_i) = \sum_k \sqrt{\lambda_k}\, u_k(\omega_s)\, v_k(\omega_i) \tag{4}$$

where λ_k are Schmidt coefficients and u_k, v_k are orthonormal spectral modes [10], [11]. Dominance of $\lambda_1 \gg \lambda_{k>1}$ ensures high spectral purity [5].

3) Beam Splitting and SPAD Detection: Following SPDC and JSI filtering, the entangled photon pair is spatially separated via a beam splitter [12]. The signal photon is directed to Detector A, and the idler photon to Detector B. This separation enables independent detection and facilitates coincidence-based bit generation in the TRNG system. Each photon path terminates at a SPAD operating in Geiger mode, capable of detecting individual photons with high sensitivity. However, SPADs exhibit non-ideal characteristics such as dead time and dark counts [13]. The overall detection efficiency, incorporating both coupling efficiency η_c and internal detection efficiency η_d, is given by:

$$\eta_{\text{total}} = \eta_c \cdot \eta_d \tag{5}$$

where η_c is the coupling efficiency, representing the fraction of photons successfully coupled into the detection path, and η_d is the detection efficiency, which denotes the probability that an incident photon triggers an avalanche in the detector.

Due to the presence of dead time τ_d, the effective detection rate of a SPAD is reduced. The relationship is expressed as:

$$R_{\text{eff}} = \frac{R_0}{1 + R_0 \cdot \tau_d} \tag{6}$$

where R_0 denotes the incident photon count rate in the absence of dead time, and τ_d represents the detector's dead time, which is the minimum interval required between two successive valid detection events to avoid overlap or saturation effects.

Additionally, thermally induced dark counts occur at a certain rate, contributing to false detection events during the gate window. The probability of a dark count within the detection gate is given by:

$$P_{\text{dark}} = R_{\text{dark}} \cdot T_{\text{gate}} \tag{7}$$

where R_{dark} is the dark count rate of the detector, representing the number of false detection events per second, and T_{gate} is the gate window width, defining the duration within which a photon detection event is considered valid.

4) Coincidence Detection and Bit Generation: Coincidence events are identified when both SPADs detect photons within the same temporal gate window τ. These events indicate successful detection of an entangled photon pair. The probability of observing such a coincidence is governed by the overall efficiency and temporal resolution of the system and can be approximated as follows:

$$P_{\text{coinc}} \approx \eta_{\text{pair}} \cdot (\eta_c \cdot \eta_d)^2 \cdot (1 - e^{-T_{\text{gate}}/\tau}) \tag{8}$$

where τ denotes the width of the coincidence window, η_{pair} is the probability of generating SPDC pairs, η_c is the coupling efficiency and η_d is the detection efficiency of the SPADs. Only detections that fall within the defined window are accepted as valid coincidences. Random bits are then generated from valid coincidence events. The origin of this randomness is fundamentally quantum, stemming from vacuum fluctuations and wavefunction collapse during detection [14]. The bitstream is then passed to post-processing and security validation stages.

While the described system architecture ensures high spectral purity and randomness at the physical layer, real-world deployment requires both dynamic spectral adaptability and rigorous security validation. The next subsection addresses adaptive Schmidt-mode filtering under varying conditions, followed by a finite-size entropy framework that quantifies the certifiable randomness per bit in the presence of quantum side information.

B. Entanglement Entropy Reduction

In the spectral domain, the degree of entanglement between signal and idler photons is quantified by two key metrics derived from the Schmidt decomposition in Eq. (4): the entanglement entropy S and the Schmidt number K [15]. The entanglement entropy is defined as the Shannon entropy of the Schmidt eigenvalue distribution:

$$S = -\sum_k \lambda_k \log_2 \lambda_k \tag{9}$$

where λ_k denotes the probability weight of the k-th Schmidt mode. A higher value of entanglement entropy S implies a broader distribution of significant Schmidt modes, indicating increased spectral entanglement and reduced separability of the biphoton state. In the context of QTRNG, such spectral correlations introduce statistical dependencies that compromise the uniformity and unpredictability of the extracted bits. Therefore, minimizing S is essential for enhancing spectral purity and ensuring that the randomness originates from a well-isolated quantum mode, yielding higher min-entropy and stronger security guarantees.

Complementarily, the Schmidt number K provides a measure of the effective number of contributing spectral modes:

$$K = \frac{1}{\sum_k \lambda_k^2} \tag{10}$$

Eq. (10) provides a quantitative measure of the effective number of Schmidt modes contributing to the biphoton state. In the context of QTRNG, achieving a Schmidt number close to unity ($K \to 1$) is highly desirable, as it indicates a nearly pure, single-mode spectral profile with minimal entanglement-induced correlations. A low K enhances the spectral separability of photon pairs and ensures that the measured outcomes are fundamentally random and uncorrelated. The reduction in entanglement entropy and Schmidt number, facilitated by spectral shaping and Schmidt-mode filtering, directly increases the quality of the generated bitstream in terms of balance, unpredictability, and certifiable entropy. Therefore, optimizing the system toward minimizing K is essential for maximizing the extractable randomness and satisfying the stringent statistical requirements of QTRNG protocols.

To support this spectral separability objective, we define an optimization problem that jointly minimizes the Schmidt number K and the entanglement entropy S by adjusting the physical parameters of the SPDC process. The objective function is formulated as:

$$\min_{L,\,\sigma_p} \; \mathcal{C}(L, \sigma_p) = w_1 \cdot (K(L, \sigma_p) - 1)^2 + w_2 \cdot S(L, \sigma_p)^2 \tag{11}$$

subject to the physical constraints:

$$L_{\text{min}} \leq L \leq L_{\text{max}}$$
$$\sigma_{p,\text{min}} \leq \sigma_p \leq \sigma_{p,\text{max}}$$

where L is the nonlinear crystal length, σ_p is the pump bandwidth, and w_1, w_2 are non-negative weights that determine the relative importance of purity and entropy suppression. The functions $K(L, \sigma_p)$ and $S(L, \sigma_p)$ represent the Schmidt number and entanglement entropy, respectively, derived from the spectral decomposition of the biphoton wavefunction. Solving this constrained optimization problem yields SPDC parameters that minimize spectral correlations and promote a nearly separable biphoton state with $K \approx 1$ and $S \approx 0$.

C. Adaptive JSI Filtering for Schmidt Mode Optimization

In practical SPDC-based QTRNG systems, variations in experimental conditions—such as pump power, spectral drift, and thermal instability—can alter the joint spectral amplitude (JSA) and degrade the purity of the dominant Schmidt mode. To address this, we introduce an adaptive Schmidt-mode filtering mechanism that dynamically aligns the JSI with the dominant eigenmode. The goal is to maintain high spectral purity by maximizing the weight of the first Schmidt coefficient λ_1 through a tunable spectral filter function $F(\omega)$:

$$\max \left\{ \lambda_1(F(\omega)) \right\} \tag{12}$$

This optimization ensures robust alignment with the dominant Schmidt mode under time-varying conditions. The filter profile $F(\omega)$ can be controlled by a feedback loop driven by real-time measurements of spectral correlations, marginal distributions, or coincidence rates. This adaptive mechanism is preceded by a numerical optimization stage, introduced in Section II-B, which determines a near-separable JSA by minimizing the Schmidt number K and entanglement entropy S as functions of the SPDC parameters (L, σ_p). Once the optimal pair (L^*, σ_p^*) is identified, the adaptive filter maintains mode alignment in the presence of environmental fluctuations. Together, the numerical and adaptive stages form a robust spectral engineering framework that ensures long-term spectral purity and entropy stability, enabling consistent, high-fidelity quantum randomness generation.

D. Finite-Size Security Analysis and Extractable Entropy

To quantify the certifiable randomness of the generated bitstream under realistic conditions, we apply the *smooth min-entropy* framework, which accounts for finite sample size and potential quantum side information held by an adversary [16]. Let $\mathbf{X} \in \{0,1\}^n$ denote the raw bitstream of length n, and let ε be the security failure probability. The ε-smooth min-entropy conditioned on side information $\mathbf{E}$ is lower bounded by:

$$H_{\min}^{\varepsilon}(\mathbf{X}|\mathbf{E}) \geq n \cdot H_{\infty}(\mathbf{X}) - \Delta(n,\varepsilon) \tag{13}$$

where, $H_{\infty}(\mathbf{X})$ is the min-entropy (worst-case unpredictability) per bit, given by:

$$H_{\infty}(\mathbf{X}) = -\log_2\left(\max\{P_0, P_1\}\right) \tag{14}$$

and the finite-size correction term is:

$$\Delta(n,\varepsilon) = 7 \cdot \sqrt{\frac{\log(2/\varepsilon)}{2n}} \tag{15}$$

This bound ensures that, even in the presence of statistical fluctuations, a provable number of uniformly random bits can be securely extracted from the raw bitstream. In quantum key distribution (QKD) protocols such as BB84 and E91, high-quality randomness is essential for basis selection, bit encoding, and decoy state modulation. If the QKD system depends on a quantum TRNG (QTRNG) for this randomness, then any bias, autocorrelation, or entropy deficiency in the TRNG can directly affect the security of the final key and reduce the achievable secret key rate (SKR) [17]. To account for this, the SKR under collective attacks and finite-size effects can be expressed as [18]:

$$\text{SKR} = R \cdot \left[\frac{H_{\min}^{\varepsilon}(\mathbf{X}|\mathbf{E})}{n} - f \cdot h(Q)\right] \tag{16}$$

where R is the raw bit generation rate, n is the block size, f is the error correction efficiency, $h(Q)$ is the binary entropy function of the quantum bit error rate (QBER) Q, and $H_{\min}^{\varepsilon}(X|E)/n$ is the average extractable entropy per bit. This term is directly influenced by the quality of the physical random source.

To enhance this, our system includes a parameter optimization stage that selects the nonlinear crystal length L and pump bandwidth σ_p to minimize the Schmidt number K and entanglement entropy S. This ensures that the generated photon pairs are nearly unentangled in frequency, i.e., the JSA becomes approximately separable. As a result, the per-bit min-entropy $H_{\infty}(X)$ approaches its ideal value of 1, and the extractable randomness is maximized even under finite-size constraints. Consequently, the extractable entropy in Eq. (13) remains close to the theoretical limit, minimizing the required finite-size correction $\Delta(n,\varepsilon)$ and eliminating the need for post-processing or entropy distillation.

III. Simulation and Analysis

The proposed QTRNG system is implemented in MATLAB, incorporating realistic models of SPDC dynamics, Schmidt-mode-based joint spectral intensity (JSI) filtering, SPAD detection behavior, and finite-size security analysis. The simulation workflow encompasses biphoton generation, spectral decomposition, dominant-mode filtering, coincidence-based detection, and entropy estimation. Table I summarizes the complete set of simulation parameters along with the key spectral and entropy metrics used to evaluate system performance. As part of the simulation, the system employs a numerical optimization procedure to adjust the pump bandwidth σ_p and the nonlinear crystal length L in order to minimize the Schmidt number $K \approx 1$ and the entanglement entropy $S \approx 0$, which maximize spectral purity and improve the quality of source-level randomness.

Figure 2 illustrates the weight of the dominant Schmidt mode (λ_1) over time, comparing performance with and without adaptive filtering. Without adaptation, fluctuations in experimental conditions cause λ_1 to degrade below 0.95, leading to reduced spectral purity. In contrast, when adaptive Schmidt-mode alignment is employed, λ_1 remains consistently above 0.99, demonstrating robust maintenance of spectral separability. This adaptive mechanism ensures that higher-order modes are suppressed, achieving near-zero contributions from these modes. These results confirm a significant reduction in frequency-domain entanglement entropy to $S = 0.0052$ bits and demonstrate the feasibility of generating nearly separable biphoton states using optimized pump bandwidth ($\sigma_p = 10^{13}$ Hz) and crystal length ($L = 10^{-4}$ m). This improvement aligns with the spectral optimization goals discussed in Section II-B, where minimizing K and S directly enhances the quality of source-level randomness.

Figure 3 presents the finite-size entropy analysis for increasing bitstream lengths, illustrating both the theoretical min-entropy bound (dashed line) and the simulated extractable entropy (solid line) computed under the optimized Schmidt-mode filtering scheme. The results demonstrate that the estimated min-entropy per bit, H_{∞}, consistently exceeds 0.9997, closely tracking the theoretical bound across all tested scales. Also, the curve includes a critical marker indicating the point at which the system, after generating 17.85 million bits, achieves $H_{\infty} \approx 0.9997$ with a finite-size correction $\Delta(n,\epsilon) = 0.004462$. This stability validates the filtering optimization described in Section II-B/II-C and confirms that the system can securely extract high-quality randomness, even under finite-size constraints.

TABLE I: Simulation Parameters and Optimized Metrics

Parameter	Value	Description
Simulation Parameters		
Total SPDC Pulses (N_{pulses})	10^7, 10^8, 10^9	Number of pump pulses used to generate photon pairs in each simulation run.
Coupling Efficiency (η_c)	0.8	Fraction of photons successfully coupled into the detection path.
Detector Quantum Efficiency (η_d)	0.6	Probability that a photon reaching the detector triggers an avalanche event.
Pump Refractive Index (n_p)	1.87	Refractive index of the nonlinear crystal at the pump wavelength.
Signal Refractive Index (n_s)	1.83	Refractive index at the signal photon wavelength.
Idler Refractive Index (n_i)	1.81	Refractive index at the idler photon wavelength.
JSI Frequency Range	± 2 THz	Frequency span for evaluating the joint spectral intensity.
JSI Matrix Size	300×300	Resolution of the JSI frequency grid used in Schmidt decomposition.
Detection Gate Window (T_{gate})	1 ns	Time window during which detection events are accepted.
Coincidence Window (τ)	1 ns	Maximum allowed delay between detections on both SPADs for a coincidence event.
SPAD Dead Time (τ_d)	50 ns	Recovery time required after a SPAD detection before it can register another event.
Dark Count Rate (R_{dark})	100 Hz	Rate of false detection events due to thermal noise or dark current.
Run Counts	30	Number of simulation repetitions performed for statistical averaging.
Optimized Metrics		
Crystal Length (L)	-	Optimized nonlinear crystal length for minimizing spectral correlations.
Pump Bandwidth (σ_p)	-	Spectral width of the pump laser, optimized for low entanglement entropy.
Schmidt Number (K)	-	Measure of the effective number of independent spectral modes; ideal value is 1.
Spectral Purity ($1/K$)	-	Inverse of Schmidt number; quantifies single-mode spectral quality.
Entanglement Entropy (S)	-	Shannon entropy of the Schmidt eigenvalue distribution; lower values indicate purer states.
Min-Entropy per Bit (H_∞)	-	Worst-case per-bit unpredictability estimate.
Extractable Entropy	-	Number of provably random bits extractable under finite-size constraints.
Security Correction ($\Delta(n, \epsilon)$)	-	Finite-size entropy reduction term for security parameter.

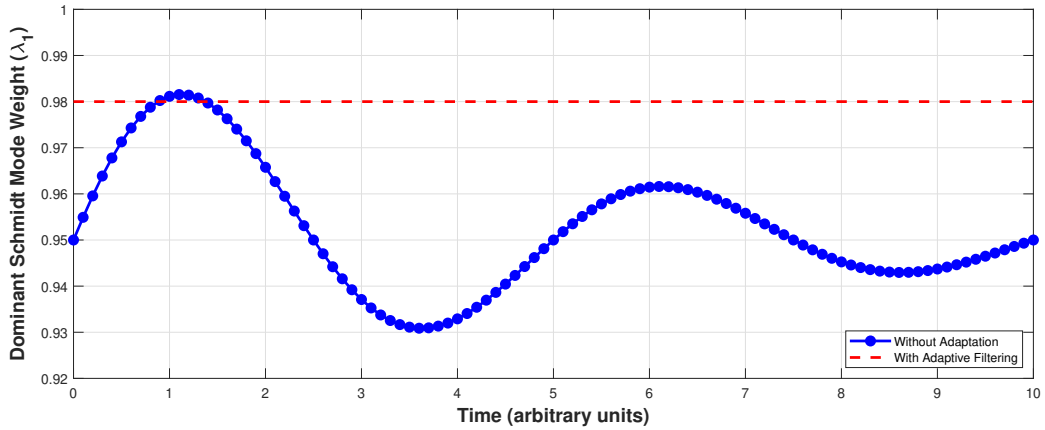


Fig. 2: Dominant Schmidt mode weight (λ_1) with and without adaptive filtering

.

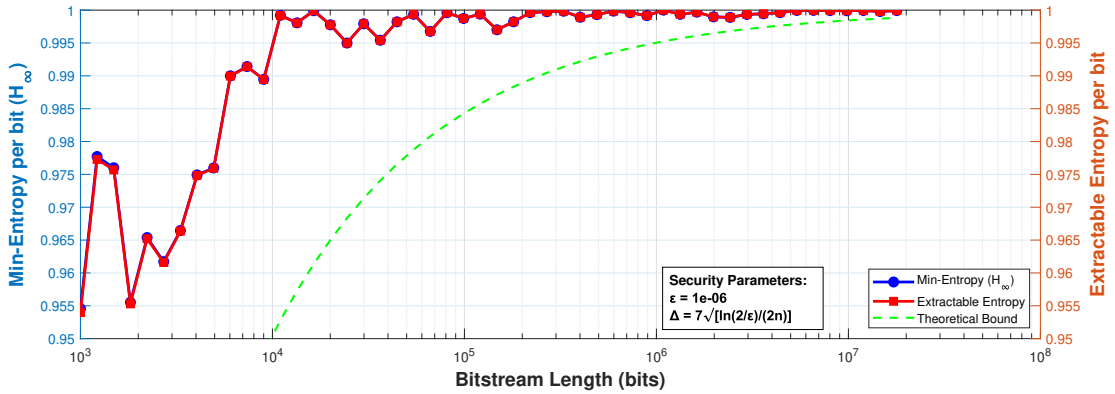


Fig. 3: Finite-Size Entropy Analysis with Optimized Filter

Figure 4 compares the JSI profiles before and after Schmidt-mode filtering. Panel (a) displays the original JSI of the SPDC-generated photon pairs, revealing strong spectral correlations across the signal and idler frequency axes. In contrast, Panel (b) presents the filtered JSI obtained through Schmidt-mode decomposition, which isolates the dominant spectral mode. The resulting JSI exhibits a highly localized peak along the diagonal with suppressed off-diagonal correlations, reflecting a spectral purity of approximately 0.9992 (i.e., $1/K$). These results validate the effectiveness of the adaptive filtering approach

in maintaining long-term stability and directly supporting entropy stability.

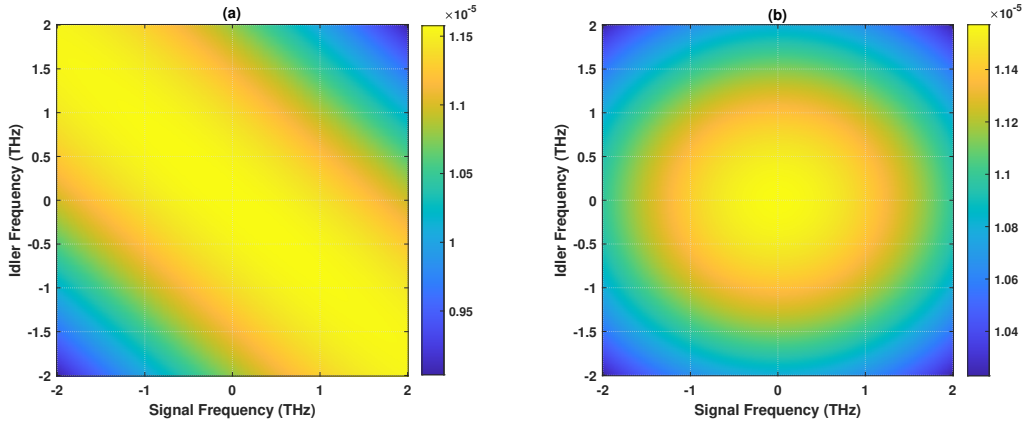


Fig. 4: Joint Spectral Intensity (a) Original JSI and (b) Filtered JSI (Dominant Schmidt Mode).

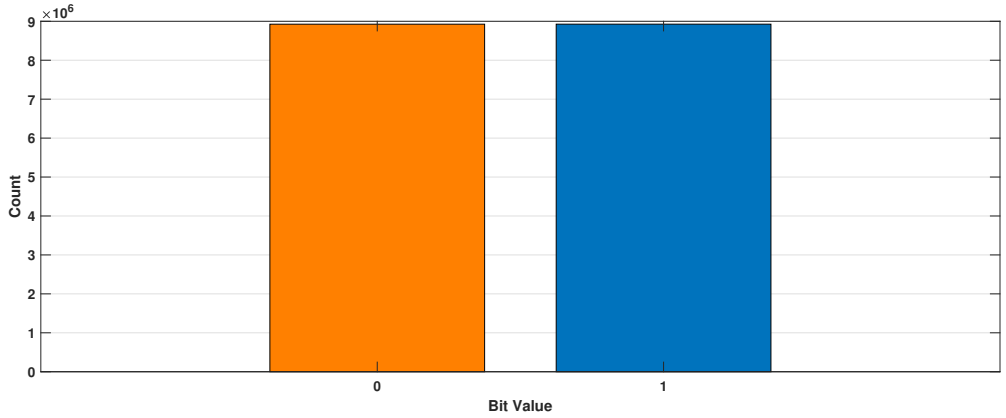


Fig. 5: Bits [0 1] distribution

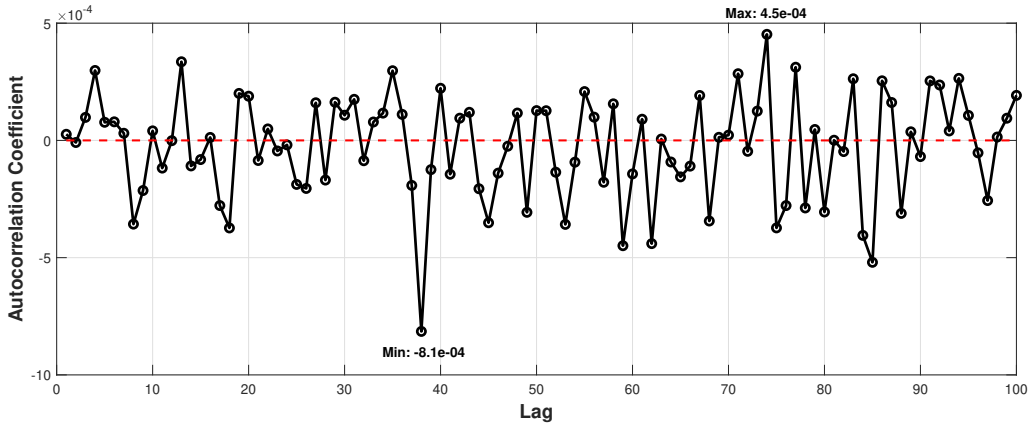


Fig. 6: Autocorrelation of bitstream (lag 1-100)

Figure 5 confirms the uniformity of the generated bitstream, showing an almost equal count of 0s and 1s across the entire dataset. This near-perfect balance reflects the high min-entropy value ($H_\infty = 0.9997$) obtained from the finite-size security analysis and validates the quantum origin of the randomness. According to the simulation results, the system generates a total of $17,851,486$ bits with an estimated entropy of > 0.9997, thereby ensuring compliance with cryptographic standards without the need for post-processing or hashing techniques. This outcome reinforces the conclusions presented in Section II-D, demonstrating the sufficiency of physical-layer randomness extraction in the proposed QTRNG architecture.

Figure 6 illustrates the autocorrelation coefficients of the generated bitstream across lags 1 to 100, revealing no statistically significant correlation between successive bits. All values lie within the range $[-8.1\times10^{-4}, 4.5\times10^{-4}]$, which is consistent with

ideal random behavior and confirms zero-lag independence. This result complements the earlier entropy analysis and supports the conclusion that the system produces truly unpredictable sequences suitable for secure communication and cryptographic protocols. In conjunction with the high spectral purity and low entanglement entropy achieved through optimized JSI filtering, these statistical properties validate the robustness of the proposed QTRNG architecture under realistic experimental constraints.

Furthermore, the generated bitstream was rigorously evaluated using the NIST SP 800-22 and Dieharder statistical test suites. All tests were passed with a 100% success rate, confirming the high fidelity, unpredictability, and cryptographic suitability of the generated random numbers. An additional key advantage of the proposed approach is its low computational complexity compared to other TRNG simulation methods. Unlike many classical or quantum-based TRNGs that require post-processing or entropy extraction techniques (e.g., hashing), this method directly generates high-quality random bits without any preprocessing or conditioning stages. This enables efficient execution even at large data sizes.

To evaluate runtime performance and memory consumption, three simulation runs were conducted at varying scales:

- $N_{\text{pulses}} = 10^7$, the system generated $178{,}514$ bits in 2.29 seconds, consuming only 0.60 MB of memory.
- $N_{\text{pulses}} = 10^8$, a total of 1.78 million bits were produced in 28.20 seconds, with memory usage of 0.46 MB.
- $N_{\text{pulses}} = 10^9$, the system outputs 17.85 million bits in 320.20 seconds, with memory usage increasing modestly to 12.83 MB.

This scalability analysis demonstrates that the proposed system maintains high computational efficiency and low memory overhead across a wide range of data sizes. As a result, it is well-suited for real-time cryptographic applications and deployment in resource-constrained embedded platforms that require fast, reliable, and continuous quantum random number generation.

IV. Conclusion

This work presented a high-fidelity QTRNG that integrates SPDC photon sources, SPAD-based photon detection, and JSI filtering based on Schmidt-mode decomposition for enhanced spectral purity and entropy performance. The system architecture was modeled and simulated under realistic constraints, including detector inefficiencies, dark counts, and dead time. By isolating the dominant spectral mode via Schmidt decomposition, the system achieved a spectral purity of 0.9992 and reduced frequency-domain entanglement entropy to $S = 0.0052$ bits. The optimized configuration, with a pump bandwidth of $\sigma_p = 10^{13}$ Hz and a nonlinear crystal length of $L = 10^{-4}$ m, resulted in a near-single-mode biphoton state characterized by a Schmidt number of $K = 1.0008$. The generated bitstreams were evaluated using both the NIST SP 800-22 and Dieharder statistical test suites, passing all tests with a 100% success rate. Finite-size security analysis further confirmed a min-entropy per bit of $H_\infty = 0.9997$, with an extractable entropy of 17.85 million bits from a 17.85 million-bit run and a security correction factor $\Delta(n, \epsilon) = 0.004462$. These results validate the quantum origin and certifiable unpredictability of the bitstream, without requiring any post-processing or entropy distillation. Additionally, the system demonstrated excellent scalability, generating up to 17.85 million bits in 320 seconds using only 12.83 MB of memory. The low computational and memory overhead confirms the system's suitability for real-time cryptographic applications and deployment in resource-constrained embedded systems. Future work will focus on extending the current simulation framework to experimental validation using real SPDC sources and SPAD detectors to benchmark the system's performance under practical conditions. In parallel, the implementation of the QTRNG on FPGA platforms will be explored to achieve ultra-low-latency and high-throughput randomness generation suitable for embedded and real-time applications. Another promising direction is the extraction of multiple independent random bitstreams in parallel by isolating orthogonal Schmidt modes within the biphoton wavefunction, thereby enhancing the total entropy rate and enabling parallel randomness delivery. Furthermore, the integration of the proposed QTRNG into QKD protocols will be investigated. These advancements aim to enhance both the scalability and applicability of the system across a wide range of quantum communication and security infrastructures.

Acknowledgment

This research is supported by a grant (No. CRPG-25-3143) under the Cybersecurity Research and Innovation Pioneers Initiative, provided by the National Cybersecurity Authority (NCA) in the Kingdom of Saudi Arabia.

References

[1] X. Ma, X. Yuan, Z. Cao, B. Qi, and Z. Zhang, "Quantum random number generation," *npj Quantum Information*, vol. 2, p. 16021, 2016.

[2] S. Ahmed, N. Alshaer, and T. Ismail, "Chaos-based rng using semiconductor lasers with parameters variation tolerance," *IEEE Conference on Transparent Optical Networks (ICTON)*, 2021.

[3] National Institute of Standards and Technology, "NIST special publication 800-22: A statistical test suite for random and pseudorandom number generators for cryptographic applications," 2010, available: https://csrc.nist.gov/pubs/sp/800/22/r1/upd1/final.

[4] R. G. Brown, D. E. Bernholdt, M. S. Cawood, and M. Jiang, "Dieharder: A random number test suite," 2020, available: https://www.phy.duke.edu/~rgb/General/dieharder.php.

[5] A. Christ, K. Laiho, A. Eckstein, K. N. Cassemiro, and C. Silberhorn, "Probing multimode squeezing with correlation functions," *New Journal of Physics*, vol. 13, no. 3, p. 033027, 2011.

[6] F. Rutz, T. Passow, A. Wörl, R. Müller, Q. Yang, V. Leidel, A. Bächle, E. Diwo-Emmer, J. Niemasz, S. Giudicatti, V. Daumer, and R. Rehm, "Advances in entangled-photon sources and single-photon avalanche diodes for quantum technologies in the SWIR," in *Advanced Photon Counting Techniques XVIII*, M. A. Itzler, J. C. Bienfang, and K. A. McIntosh, Eds., vol. 13025, International Society for Optics and Photonics. SPIE, 2024, p. 130250B.

[7] A. J.-M. Séguinard, A. Piveteau, P. Mironowicz, and M. Bourennane, "Experimental certification of more than one bit of quantum randomness in the two inputs and two outputs scenario," *New Journal of Physics*, vol. 25, no. 11, p. 113022, 2023.

[8] R. W. Boyd, "Nonlinear optics," 2020.
[9] R. van der Meer, J. J. Renema, B. Brecht, C. Silberhorn, and P. W. H. Pinkse, "Optimizing spontaneous parametric down-conversion sources for boson sampling," *Phys. Rev. A*, vol. 101, p. 063821, 2020.
[10] W. Grice, A. U'Ren, and I. Walmsley, "Eliminating frequency and space-time correlations in multiphoton states," *Physical Review A*, vol. 64, no. 6, p. 063815, 2001.
[11] A. Eckstein, A. Christ, P. J. Mosley, and C. Silberhorn, "Highly efficient single-pass source of pulsed single-mode twin beams of light," *Physical Review Letters*, vol. 106, no. 1, p. 013603, 2011.
[12] T. Jennewein, U. Achleitner, G. Weihs, H. Weinfurter, and A. Zeilinger, "A fast and compact quantum random number generator," *Review of Scientific Instruments*, vol. 71, no. 4, pp. 1675–1680, 2000.
[13] Y. Albeck, E. Greenberg, and T. Arusi-Parpar, "Dead-time effect on spad detection efficiency," *Appl. Opt.*, vol. 64, no. 9, pp. 2163–2168, 2025.
[14] A. Uchida, K. Amano, M. Inoue, K. Hirano, S. Naito, H. Someya, I. Oowada, T. Kurashige, M. Shiki, S. Yoshimori, K. Yoshimura, and P. Davis, "Fast physical random bit generation with chaotic semiconductor lasers," *Nature Photonics*, vol. 2, no. 12, pp. 728–732, 2008.
[15] Y. KanadaEnyo, "Entanglement entropy and schmidt number as measures of delocalization of α clusters in one-dimensional nuclear systems," *Progress of Theoretical and Experimental Physics*, vol. 2015, no. 4, p. 043D04, 2015.
[16] X. Zhang, Y. Zhang, Y. Zhao, X. Wang, S. Yu, and H. Guo, "Finite-size analysis of continuous-variable measurement-device-independent quantum key distribution," *Physical Review A*, vol. 96, no. 4, p. 042334, 2017.
[17] S. Ahmed, N. Alshaer, K. A. Alaghbari, and T. Ismail, "Security analysis of gaussian and discrete modulations in fso/cv-qkd systems employing llo under phase and amplitude attacks," *IEEE Access*, vol. 10, pp. 100 041–100 053, 2022.
[18] P. Jouguet, S. Kunz-Jacques, E. Diamanti, and A. Leverrier, "Analysis of imperfections in practical continuous-variable quantum key distribution," *Physical Review A*, vol. 86, no. 3, p. 032309, 2012.