Research Article Vol. 3, No. 1 / 25 February 2025 / Optica Quantum 111

OPTICA QUANTUM

High-speed source-device-independent quantum random number generator on a chip

Tommaso Bertapelle,[1] Marco Avesani,[1,2,*] Alberto Santamato,[3,4] Alberto Montanaro,[3,5] Marco Chiesa,[6,7] Davide Rotta,[6,7] Massimo Artiglia,[3,5] Vito Sorianello,[3] Francesco Testa,[5] Gabriele De Angelis,[3,5] Giampiero Contestabile,[5] Giuseppe Vallone,[1,2] Marco Romagnoli,[2] and Paolo Villoresi[1,2]

[1]Dipartimento di Ingegneria dell'Informazione, Università degli Studi di Padova, via Gradenigo 6B, 35131 Padova, Italy
[2]Padua Quantum Technologies Research Center, Università degli Studi di Padova, via Gradenigo 6A, 35131 Padova, Italy
[3]Photonic Networks and Technologies Lab - CNIT, 56124 Pisa, Italy
[4]Now at Nu Quantum Ltd., Broers Building, 21 JJ Thomson Avenue, Cambridge CB3 0FA, UK
[5]Scuola Superiore Sant'Anna, 56124 Pisa, Italy
[6]InPhoTec, Integrated Photonic Technologies Foundation, 56124 Pisa, Italy
[7]CamGraPhIC srl, 56124 Pisa, Italy
*marco.avesani@unipd.it

Received 9 May 2024; revised 15 October 2024; accepted 7 November 2024; published 10 February 2025

A wide range of applications require, by hypothesis, to have access to a high-speed, private, and genuine random source. Quantum random number generators (QRNGs) are currently the sole technology capable of producing true randomness. However, the bulkiness of current implementations significantly limits their adoption. In this work, we present a high-performance source-device-independent QRNG leveraging a custom-made integrated photonic chip. The proposed scheme exploits the properties of a heterodyne receiver to enhance security and integration to promote spatial footprint reduction while simplifying its implementation. These characteristics could represent a significant advancement toward the development of generators better suited to meet the demands of portable and space applications. The system can deliver secure random numbers at a rate greater than 20 Gbps with a reduced spatial and power footprint.

© 2025 Optica Publishing Group under the terms of the Optica Open Access Publishing Agreement

https://doi.org/10.1364/OPTICAQ.529746

1. INTRODUCTION

Random numbers generators (RNGs) are some of the most influential tools of the current information age. Many real-world applications, such as cryptography, simulations, gaming, and fundamental physics experiments, already exploit such devices [1]. However, their capability to deliver genuine randomness is a matter of great concern, especially in cryptography: most of the known classical, quantum, and post-quantum protocols demand, by hypothesis, to have access to an authentic random source. Violating such a core assumption exposes the system to exploitable vulnerabilities which can completely break their security. However, despite their key role for security applications, almost all the RNGs used nowadays are deterministic in nature: they rely either on computer algorithms or classical physics phenomena. Hence, the stream of numbers can only mimic a random behavior and definitely cannot be considered a real source of randomness.

Since randomness cannot arise from determinism, the probabilistic nature of quantum mechanics can provide a method to generate truly random numbers, thus rectifying one of the principal flaws of current cryptographic protocols [2]. Therefore, given the growing concerns about cyber-security, it is expected that the interest in such devices will increase in the near future [3]. Nonetheless, despite the premises, the unavoidable non-idealities and imperfections concerning the implementation of such quantum-based RNGs (QRNGs) must be carefully evaluated, especially when dealing with security applications [1]. Indeed, such non-idealities can be modeled as leaked information correlated with the QRNG itself (side information) and thus exploited to predict the generated numbers. From this point of view, QRNGs can be classified into three categories: fully trusted (FT), device-independent (DI), and semi-device-independent (Semi-DI).

FT-QRNGs are relatively simple to realize and provide some of the highest generation rates to date [4,5]. Nevertheless, everything concerning the system, including the imperfections of the hardware used, must be known and characterized, leading to generators with the lowest level of security. A complete device characterization may be challenging, as it sets many working assumptions, none of which must be breached. For example, for CV protocols, which are relevant to our work, Smith *et al.* [6] report an attack that could undermine the security of some of the mentioned systems. In contrast, DI schemes offer the highest

level of security since nothing concerning the device's physical implementation is trusted. However, DI-QRNGs are extremely difficult to realize as they request a loophole-free Bell test and are several orders of magnitude slower than FT devices [7–10]. Therefore, although they are the best choice in terms of offered security, they are not feasible for real-world scenarios due to the limitations discussed above. The Semi-DI approach, instead, aims to make a compromise between security and speed. To achieve such, Semi-DI only trusts specific aspects of the device, for instance, the quantum source [11], the measuring apparatus [12–16], the underlying Hilbert space dimension [17,18], the mean photon number [19–23], or the overlap bound [24] of the emitted states. Clearly, the Semi-DI strategy guarantees greater security since fewer assumptions are required to operate the QRNG, if compared with the FT framework, while still achieving several Gbps [25] in terms of generation rate, which is much higher than DI schemes and yet sufficient for current practical applications.

Alongside the particular protocol exploited to realize a QRNG, additional aspects must be also considered to target a wider range of use cases. Aside from sheer performance, several constraints such as cost, system integration, scalability, reliability, power, and space consumption must be addressed. In recent years, improvements in the integrated photonics field made such a technology an interesting solution for developing QRNGs capable of reaching the aforementioned goals. Research on these engineered generators is active [5,26–33], witnessing the transition from the bulkiness of the early prototypes to a newer generation able to better meet the demands set by real-world applications ranging from the Internet of Things (IoT) to satellite-based systems.

In particular, the requirements imposed by space applications are some of the hardest to achieve. Yet, several emerging technologies, such as satellite quantum key distribution (QKD) [34], demand on-board robust, secure, and fast QRNGs, up to several Gbps [35]. Fulfilling these requirements in such a harsh, space- and power-constrained environment is difficult with bulk devices. Integrated photonics, however, has already demonstrated itself to provide several advantages, for example, free-space and satellite QKD [36], allowing the aforementioned goals to be achieved.

This work proposes and realizes a high-performance source-device-independent QRNG system designed to reduce encumbrance while promoting simplicity. Such goals are achieved by leveraging a custom-made integrated photonic chip that operates at the standard 1550 nm telecom wavelength without any active feedback stabilization control loop, and that is mounted on a dedicated radio frequency printed circuit board (RF PCB) with all the electronics required for its operation. The generator exploits the protocol described in [25], allowing the certification of private and secure randomness with no assumption concerning the quantum source. Overall, the device combines high speed and security, and reaches a generation rate greater than 20 Gbps with a reduced spatial footprint, which makes it the first source-device-independent QRNG on-chip and currently the fastest Semi-DI QRNG. In light of such, we believe our device represents a significant step forward for QRNG systems that can aim for both portable and space applications with high-speed QKD as the primary target.

The paper is structured as follows: Section 2 briefly outlines the source-device-independent QRNG protocol used; Section 3 provides details concerning the device design, fabrication, and packaging; Section 4 describes the experimental setup adopted to characterize and estimate the QRNG performances; and Section 5 reports the obtained results.

2. HETERODYNE SOURCE-DI PROTOCOL

In the context of cryptographic-oriented QRNGs, the device must be resilient against an attacker, often known as Eve, whose aim is to predict the latter outcomes. To do so, the malicious adversary will exploit every knowledge about the generator implementation and any classical or quantum resource available, known as side-information E, to maximize its probability of correctly guessing the outcome X conditioned on E.

The source-device-independent protocol exploited in this work divides the QRNG into two sub-systems: the quantum source and the heterodyne receiver (measuring apparatus). While the first is assumed to be totally controlled by the malicious adversary, the latter is trusted and fully characterized. It is important to note that the receiver's trustfulness does not preclude the attacker's awareness of its operation details. Indeed, it is presumed that the adversary knows the set of positive operator value measurements (POVMs) implemented by the measuring apparatus. Therefore, to maximize the chances of correctly guessing the outcome X at each round of the QRNG protocol, Eve prepares and sends to the receiver a state $\hat{\rho}_A$ that can be written as an incoherent superposition $\hat{\rho}_A = \int d\beta\, p(\beta)\, \hat{\tau}_\beta^A$ of states τ_β^A with probability $p(\beta)$. As already shown in [25,37], such a conditional guessing probability, $P_{\text{guess}}(X|E)$, is upper-bounded by

$$P_{\text{guess}}(X|E) \leq \max_{\hat{\Pi}_A,\, \hat{\tau}_A} \text{Tr}[\hat{\Pi}_A \hat{\tau}_A], \tag{1}$$

with $\hat{\Pi}_A$ the discretized version of the heterodyne's POVM. Thus, given the receiver's resolution δ_q, δ_p, and that $\text{Tr}[\hat{\Pi}_A\, \hat{\tau}_A] \leq 1/\pi$ for every quantum state $\hat{\tau}_A$ injected, the previous bound becomes

$$P_{\text{guess}}(X|E) \leq \max_{\hat{\Pi}_A,\, \hat{\tau}_A} \text{Tr}[\hat{\Pi}_A \hat{\tau}_A] \leq \frac{\delta_q \delta_p}{\pi}. \tag{2}$$

Such a $P_{\text{guess}}(X|E)$ bound forbids the attacker to correctly guess the heterodyne outcome (raw randomness) with a probability greater than $\delta_q\delta_p/\pi$ even with complete knowledge of the system and holding the side-information E. Consequently, the amount of truly random bits that can be distilled from each measurement, quantified by the quantum conditional min-entropy $H_{\min}(X|E)$, is

$$H_{\min}(X|E) = -\log_2 P_{\text{guess}}(X|E) \geq -\log_2 \frac{\delta_q \delta_p}{\pi}. \tag{3}$$

The analysis just outlined is valid for individual attacks. However, it can be extended to encompass the more general coherent scenario, as shown in [25]. Considering that a collection of QRNG measurement outcomes can be written as $\hat{\Pi}_{x_1} \otimes \hat{\Pi}_{x_2} \otimes \ldots \hat{\Pi}_{x_n}$ and that the attacker can now prepare a general n-partite state $\hat{\rho}^{(n)}$, the latter conditional guessing probability becomes

$$\begin{aligned} P^{(n)}_{\text{guess}}(X|E) &= \max_{x_i} \max_{\hat{\rho}^{(n)}} \text{Tr}[\hat{\Pi}_{x_1} \otimes \hat{\Pi}_{x_2} \otimes \ldots \hat{\Pi}_{x_n} \hat{\rho}^{(n)}] \\ &= \prod_{n=1}^{n} \max_{x_i, \hat{\rho}_i} \text{Tr}[\hat{\Pi}_{x_i} \hat{\rho}_i]. \end{aligned} \tag{4}$$

This is because maximization over $\hat{\rho}^{(n)}$ corresponds to the maximum eigenvalue of the tensor-product operator, which is

composed of semi-definite positive Hermitian operators. Note that in the last equality, the term inside the product is the single-shot $P_{\text{guess}}(X|E)$ valid for individual attacks. Hence, the overall quantum conditional min-entropy is

$$H_{\min}^{(n)}(X|E) = n\, H_{\min}(X|E)\ . \tag{5}$$

Finally, to extract such randomness, a universal hashing function compliant with the constraints dictated by the "*Leftover Hashing Lemma*" [38] can be adopted.

3. DESIGN, FABRICATION, AND PACKAGING OF THE INTEGRATED CHIP

An image illustrating the photonic integrated circuit (PIC) implementing the heterodyne receiver is presented in Fig. 1. The PIC is fabricated using InPhoTec 220 nm silicon on insulator (SOI) technology, providing 220 × 480 nm photonic waveguides for optical routing. The heterodyne quadratures q and p are separated using a 90° optical hybrid realized with a 4 × 4 multi-mode interferometer (MMI), which mixes the quantum signal with an intense coherent state. It is important to note that since silicon photonics cannot integrate these sources directly into the chip substrate, hybrid integration or external light provision is necessary. Although the former offers a smaller footprint, it presents numerous challenges, such as the requirement for exact sub-micrometer alignment between the source and the PIC. Nevertheless, to demonstrate our chip's optimal performance, we chose to avoid the complexities associated with hybrid integration. The quadratures are then detected by a pair of balanced photodiodes. Compared with 90° optical hybrids realized with optical splitters and phase shifters, a 4 × 4 MMI allows us to obtain a smaller circuit that does not need any active phase control [39]. However, the absence of the latter must be compensated with a robust technology that can guarantee the fabrication of

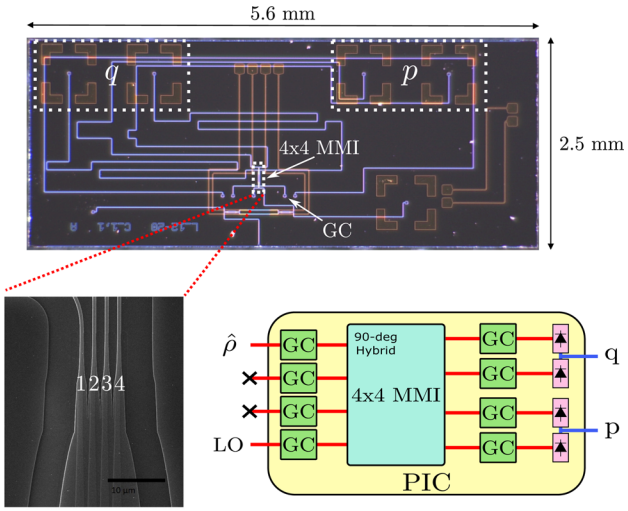

Fig. 1. Image of the integrated photonic circuit implementing the heterodyne receiver. The 4 × 4 multi-mode interferometer (MMI) can be accessed through grating couplers with the four outputs, p and q, indicated with dashed lines. The routing between the latter grating coupler and the 4 × 4 MMI is done with waveguides of the same length and number of curves. The bottom left inset shows an enlarged view of the 4 × 4 MMI outputs; the shallow etch should be noted. The bottom right inset displays a high-level depiction of the PIC functioning as a heterodyne receiver. Notice that the photodiodes are hybridly integrated in the PIC.

MMIs with minimum phase error between the four channels. Additionally, this technology must also maintain minimal differential losses among these channels. For this reason, we designed a shallow-etched ridge waveguide-based MMI, see Fig. 1 (bottom left inset), to ensure low deviations from specifications [39]. Sixteen dedicated interferometric test structures were used to characterize the fabricated MMIs. The results revealed a mean phase spacing between the four channels of ~ 89.99 ° with a standard deviation of 3.24 °. One test structure also underwent thermal variations analysis, with temperatures spanning from 15 °C to 80 °C. Findings indicated a maximum deviation of <6% at 80°C compared with at standard 25°C room temperature, while <3% degree deviations for temperatures below 60°C. The optical inputs and outputs of the PIC were realized with grating couplers (GCs). Particular attention was given when routing each MMI's output with its corresponding GC. As can be seen from Fig. 1, the p-path 1–4 and q-path 2–3 have identical length and curve counts to minimize delays and relative losses. Moreover, optical crossings were avoided to prevent cross talk effects. GCs and waveguides losses were estimated by fabricating and evaluating dedicated test chips. Measurements revealed an average coupling loss between GCs and single-mode fibers of 4 dB, and an average waveguide propagation loss of ~ 2 dB/cm. The latter was estimated with the cut-back method [40]. The four MMI inputs are accessed with a single-mode fiber array pigtailed on the chip and coupled to the input GCs, see Fig. 2(a). To align the former fiber block to the MMIs input GCs, the latter are arranged linearly between two extra GCs connected back-to-back, forming a loop. This loop is commonly used for aligning fiber blocks onto photonic integrated circuits [41,42]. Specifically, during the process, light is injected through the fiber array to one of the two GCs composing the loop while connecting the other to a power meter. Then, a six-axes, three linear and three rotational, industrial fiber alignment system exploits such feedback to optimize the fiber's block position. Once aligned, a polymeric glue (also acting as a refractive index matching material) is dispensed and cured with UV light to hold the fiber array in position. Of the aforementioned MMI inputs, one of such serves as the heterodyne local oscillator (LO) optical inlet. To convert the extracted quadratures in electrical signals, two couples of high-speed photodiodes (PDs) (Kiosemi KPDEH20LC) with responsivity ~ 0.8 A/W were hybridly integrated with the chip using a pick-and-place technique at the level of output GCs (Fig. 2(a), top enlarged view) via vertical coupling. Each PD pair was electrically connected to form a balanced photodiode (BPD) as detailed in the enlarged view at the top of Fig. 2(a). Hybrid integration was necessary due to the unavailability of active devices within our in-house technology. Based on simulations, a nominal coupling loss of 2.5 dB between the PDs and GCs was expected. By also incorporating the alignment tolerances due to PDs to GCs misalignment (±5 µm) during integration, the coupling loss was estimated not to exceed 3 dB. This loss can be almost eliminated using integrated photodiodes. Simulations also indicated a maximum optical power unbalance of 0.5 dB between the two PDs composing each BPD.

The chip, alongside its fiber array and PDs, was then assembled on a custom-made RF PCB, which houses the electronics for readout, as shown in Fig. 2. The interface design between the PIC and the external electronic circuit is crucial to ensure proper signal amplification and conditioning when working with bandwidths in the GHz range. In the present system, this interface comprises the balanced photodiodes (BPDs) on the PIC

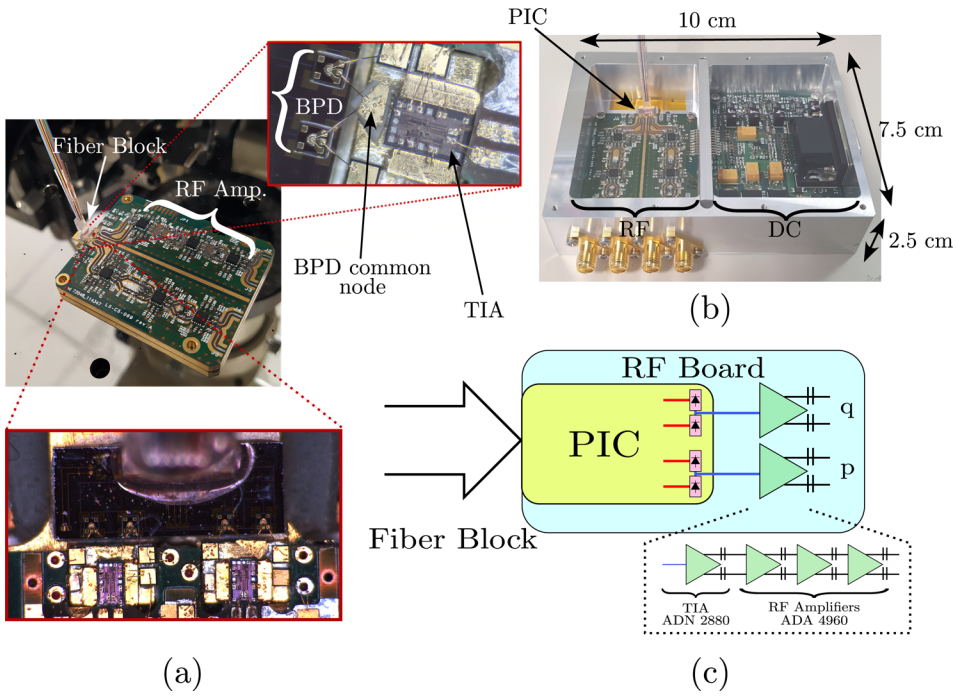

Fig. 2. (a) Assembly of the PIC with the RF electronics and fiber block for optical input. The upper inset displays a close-up view of two hybrid-integrated photodiodes forming a balanced photodiode. The latter is connected to the transimpedance amplifier through short wire bonds. In the bottom inset, an enlarged view of the fiber block pigtailed on the PIC. (b) Complete assembly, comprising also the DC control, inside the metallic package. High-level block diagram of the interconnection between the fiber block, PIC, and RF board.

end and low-noise transimpedance amplifiers (TIAs) on the RF PCB side. The TIAs serve as the initial amplification stage, boosting the BPD currents. TIAs and BPDs were interconnected through ball-wedge wire bonds of $\sim 700\,\mu$m. Balanced detection of the two quadratures is achieved by wiring the cathode of one PD of the couple with the anode of the other, as illustrated in the top enlarged view of Fig. 2(a). Since high-speed operations necessitate broad bandwidths, a higher degree of noise is introduced compared with lower-frequency systems. Such a noise increase degrades the receiver's sensitivity. Moreover, wire bonds introduce parasitic inductances that may limit the operating bandwidth while generating unwanted oscillations of the active electronic components [43]. Therefore, considering all the aforementioned constraints, the interface was designed to best compromise between noise, bandwidth, and gain values to approach shot-noise limited measurements.

The TIAs (Analog Devices ADN 2880), depicted in the inset of Fig. 2(a), feature a bandwidth of 2.5 GHz, 4400 Ω differential transimpedance gain, and an input referred noise of 315 nA. Each TIA was then coupled to a chain of amplifiers to match the subsequent analog-to-digital converter voltage range. The latter amplification chain frequency response was oversized to preserve the operating frequency window set by the TIAs and minimize classical correlations. Specifically, the amplification chain is three-staged, each of which (Analog Devices ADA 4960) has a bandwidth of 5 GHz. This choice made negligible impact on the receiver's SNR since this is dominated by the TIAs noise as by Friis' formula [44]. The amplification system, including the TIA, provides an overall differential gain of 281, 600 Ω. Calculations indicated a total input referred electronic noise level of $\sim 6\,\mathrm{PA}/\sqrt{\mathrm{Hz}}$ when neglecting the small contribution of the photodiode's dark current and Johnson noise. From this, it was determined that the clearance is upper limited by 11 dB when 1 mW reaches each photodiode, which translates to roughly 20 mW at the heteordyne's input after considering insertion losses and the power splitting contribution of the MMI. Such an estimation presumes that the MMI outputs are perfectly balanced, the PDs' responsivity deviates minimally from the nominal value of 0.8 A/W, and the PDs/GCs are perfectly aligned. The 11 dB upper-bound is consistent with the experimental value of ~ 9 dB reported in Section 4. Discrepancies are due to violations of the ideal working hypothesis discussed above. A DC electronic board was designed and manufactured to manage and supply the necessary electrical biases for the RF electronics and BPDs. Finally, as shown in Fig. 2(b), the PIC, the RF PCB, and the DC control electronics were integrated inside a metallic enclosure to ensure EMI protection, insulate the heterodyne receiver from external disturbances, and maintain the high sensitivity level needed to detect quantum signals. The fully assembled module, shown in Fig. 2(c), outputs two pairs of differential electrical signals (q and p) via SMA connectors. The module's overall dimensions are $7.5 \times 10 \times 2.5$ cm, as indicated in Fig. 2(b).

4. EXPERIMENTAL IMPLEMENTATION

A schematic representation of the experimental setup used to run the heterodyne-based source-device-independent QRNG protocol is presented in Fig. 3. The LO is an external 1550 nm distributed feedback (DFB) laser, whose power and polarization are controlled by a polarization controller (PC) and a variable optical attenuator (VOA) before the injection of the former light into the photonic chip. Subsequently, a beam splitter (BS) routes

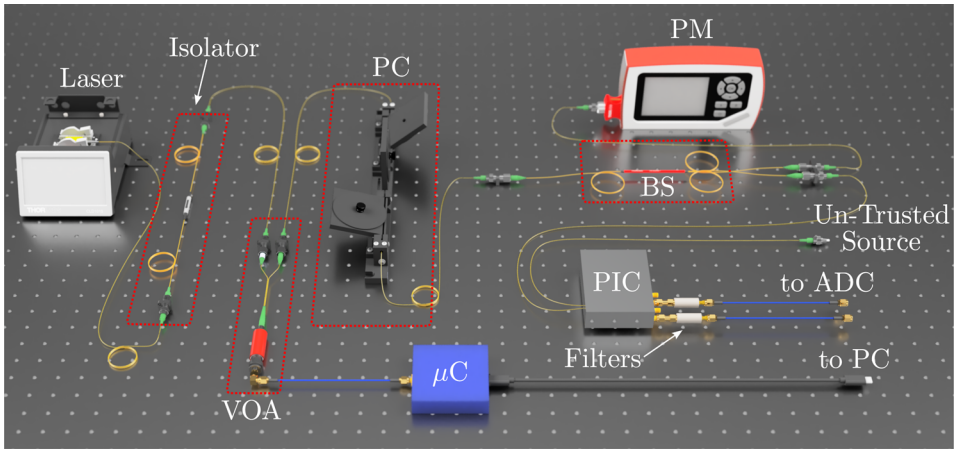

Fig. 3. Schematic representation of the experimental setup used. The latter consists of a 1550 nm laser acting as a local oscillator (LO) for the optical heterodyne receiver. The isolator prevents backreflections causing laser instabilities, the polarization controller (PC) aligns the LO polarization before coupling it into the photonic integrated circuit (PIC), the variable optical attenuator (VOA) is used to scan the LO power during the calibration phase to estimate the conditional min-entropy parameter, and through the beam splitter (BS) (99:1 splitting ratio) the optical power injected into the PIC is determined. The device's RF signals are provided as differential pairs. For each of such, one is terminated to 50 Ω, and the other is filtered with analog filters and digitized by an analog-to-digital converter (ADC) connected to the PC. This is because the ADC used only accepts single-ended signals. Moreover, the PC controls everything concerning the calibration to automatize the procedure.

1% of the LO power to an optical power meter (PM, Thorlabs PM100D with S122C) connected to a computer, while the remaining 99% is sent to the heterodyne receiver. The power meter and the VOA are required only during the calibration phase in which $H_{\min}(X|E)$ is estimated. The PC, instead, is necessary to maximize the amount of optical power coupled into the PIC due to its sensitivity to polarization. The integrated device then performs a heterodyne measurement on the incoming quantum state, yielding two pairs of RF differential signals with a bandwidth of 2.5 GHz each. To interface it with a single-ended RF chain and ADC, we kept one of the channels while terminating the other to 50 Ω. Finally, these are filtered by an analog high-pass filter with a 48 MHz cutoff frequency to eliminate low-frequency spectral noise from the LO, sampled by an oscilloscope at a rate of 25 GSps with an 8-bit resolution per channel and transferred to a computer off-line for digital processing. The latter step accounts for a pre-processing procedure, based on [25], that extracts the portion of the spectrum of the measurements for random number generation and random extraction.

Before operating the QRNG, the heterodyne receiver must be characterized and the pre-processing parameters defined.

The former is achieved when its phase-space resolution δ_q and δ_p is estimated. To do this, we observe that the photo-current associated with each quadrature is proportional to the local oscillator's power P_{LO}. Therefore, if the system behaves linearly with respect to such a power, then the ADC measures can be re-scaled from their original units $V_{q,p}$ into the phase-space vacuum units with a constant value $k_{q,p}$. To determine the latter, we injected the vacuum state into the device's signal port while scanning P_{LO} from zero up to the maximum applied value of 21.15 ± 0.01 mW. For every local oscillator power used, we acquired 10 million data-points for both quadratures, and computed their variance $\sigma^2_{V_{q,p}}$. The resulting P_{LO}-$\sigma^2_{V_{q,p}}$ trend, see Fig. 4, exhibits a linear behavior. For each quadrature, the re-scaling factor is given by $k_{q,p} = 2\, m_{q,p} P_{\mathrm{LO}}$, with $m_{q,p}$ the angular coefficients of the P_{LO}-$\sigma^2_{V_{q,p}}$ fitted straight lines. The $\delta_{q,p}$ values can be then obtained

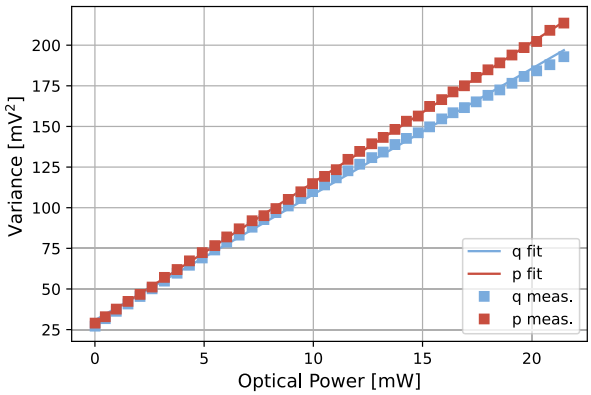

Fig. 4. Relation between the LO optical power and the measured signal variance for both processed RF channels, representing the q, p quadratures. The plot shows a linear relationship between the two quantities over the entire LO power range, with a similar trend for both channels. The parameters of the linear fit are used in the calibration procedure to convert from digitized units to vacuum units (VU).

by re-scaling the measurements' resolution, which is set by the ADC range and bit-width, with the retrieved $k_{q,p}$, as described in [25]. From the data reported in Fig. 4, the estimated $m_{q,p}$ coefficients are different. The discrepancy is mostly due to LO power unbalance between the two homodynes measuring the q and p quadrature, and variations and tolerances in the detector's responsivity and the system's amplification gain. Nevertheless, the calibration purpose is to consider such variations to map the measurements in vacuum units, and compensate for such imperfections. Hence, we highlight that the different $m_{q,p}$ do not represent a problem from the protocol's perspective; they only capture the responses of the photodetection systems for proper rescaling. Yet, some imperfections remain challenging to address, and a refined heterodyne receiver model is essential for

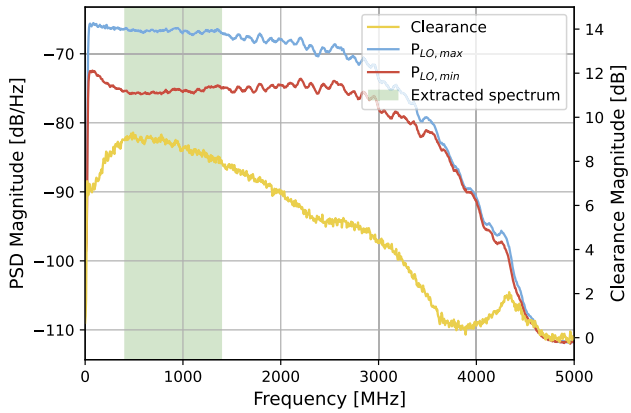

Fig. 5. Typical heterodyne receiver's clearance, in yellow, and PSDs (before digital pre-processing) either with no and maximum (21 mW) LO power respectively in red and blue. Notice that only of the two channels is reported for reference, since performances are similar for both. Notice that the device clearance is greater than 4 dB within the entire operational bandwidth (2.5 GHz) reaching ∼ 9 dB at its maximum. Moreover, the figure also highlights (in green) the portion of the spectrum exploited for the random extracting procedure during the experiments.

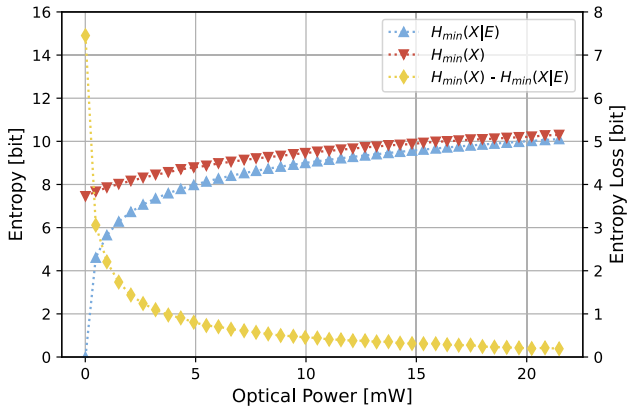

Fig. 6. Relation between the LO optical power, the quantum conditional min-entropy $H_{\min}(X|E)$, and the classical min-entropy $H_{\min}(X)$. Since $H_{\min}(X)$ upper-bounds the $H_{\min}(X|E)$, also their difference is reported, showing that for increasing LO powers, this quantity (entropy loss) reduces to a fraction of a bit.

assessing the impact on performance, such as the non-perfect orthogonality between quadrature measured. This is why we required the implementation of the MMI as a 90° hybrid to minimize its deviation from ideality, as reported in Section 3. Such a requirement should guarantee negligible effects on performance, but its theoretical inclusion in a security proof is an area of ongoing research, and we are planning to incorporate it into our methods in future works. It is worth noticing that with the calibration procedure adopted, the electronic noise, assumed classical and thus predictable, is untrusted. The approach makes the random estimation more conservative but secure against an attacker's manipulation of such a noise.

Following the characterization of the receiver, the local oscillator power P_{LO} was established and consequently the pre-processing parameters were defined. Since the generation rate increases as $\delta_{q,p}$ decreases, P_{LO} was set to its maximum value (21 mW). Then, from the heterodyne measurements, their power spectral densities (PSDs) and clearance were computed; see Fig. 5 for reference. As can be seen, we decided on a spectral window ranging from 400 to 1400 MHz. Such a choice rejects the technical noise present at lower frequencies, is sufficiently far from the system cutoff frequency (2.5 GHz at −3 dB), and ensures that the signals used for the random extraction possess a clearance of at least 8 dB.

5. RESULTS

After the QRNG phase-space resolution $\delta_{q,p}$ has been estimated, the conditional quantum min-entropy was determined for each local oscillator's power P_{LO} used; the results are reported in Fig. 6. In the case of maximum P_{LO} (∼ 21 mW), $H_{\min}(X|E)$ lower-bounds to 10.106 ± 0.005 bit, the randomness that can be extracted from a 16-bit heterodyne measurement (8-bit per channel). Therefore, the achievable secure generation rate is

$$R_{sc} = R_{rw} H_{\min}(X|E) = 20.212 \text{ Gbps}, \quad \textbf{(6)}$$

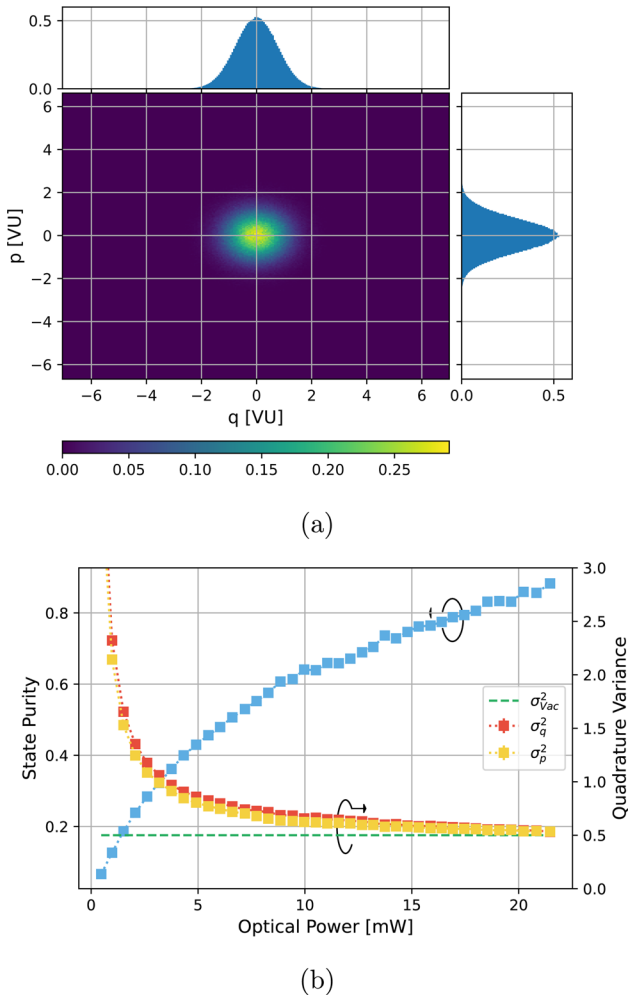

Fig. 7. (a) Experimental source (vacuum) state tomography with maximum LO power. On the axes sides, the associated marginal distributions are reported. (b) Relation between the LO optical power, the estimated quadratures variances, and the purity of the measured state. Since the classical noise is considered untrusted, as the LO power increases, the variances approach the expected vacuum values (1/2) and the purity tends to one.

with R_{rw} the equivalent ADC sampling rate after the off-line pre-processing procedure digital re-sampling (2 GSps). Notice that even with low P_{LO}, $475 \pm 10\,\mu\mathrm{W}$, the device can deliver more than 4 Gbps of secure random bits. Such sensitivity can be further enhanced with integrated photodetectors [45] to eliminate the coupling losses due to hybrid integration. Additionally, incorporating integrated optical sources or gain chips butt-coupled to the PIC can reduce the coupling losses associated with grating couplers [45]. These modifications could increase the coupling efficiency by at least fourfold, which would correspondingly improve the sensitivity by a comparable amount.

For comparison in Fig. 6, the unconditional classical min-entropy $H_{\min}(X)$, a quantity that upper-bounds $H_{\min}(X|E)$, is also reported. The gap between the two possesses a decreasing trend with respect to P_{LO}, reaching 0.191 ± 0.005 bit when the latter is set to the maximum tested power. Since the vacuum state was injected while running the experiments, the latter discrepancy has a straightforward interpretation. Indeed, when calibrating the receiver, its classical noise was deemed as untrusted. Consequently, there is an additional contribution to the vacuum's quadrature variances of 1/2. This is exemplified in Fig. 7, where we depicted the state's estimated purity and the corresponding variances of the quadratures $\sigma^2_{q,p}$ relative to the local oscillator power. As it can be observed, higher levels of P_{LO} correspond to an increase in the purity. At the highest LO power, the purity peaks at a value of 0.883 ± 0.003 with $\sigma^2_q = 0.5317 \pm 0.0013$ and $\sigma^2_p = 0.5347 \pm 0.0013$. Such a trend stems from the fact that for increasing LO power, the ratio between the quantum signal and the classical noise (clearance) improves.

Following the calibration of the QRNG receiver, approximately 50 GBytes of data was collected for random number extraction. For this purpose, the P_{LO} was settled to its peak value of 21.15 ± 0.01 mW reached during calibration. The 2-universal hashing function used was the Toeplitz bit-wise matrix-vector multiplication with $n = 17,600$ columns and $m = 11,008$ rows. These numbers guarantee a security parameter $\varepsilon' \sim 10^{-10}$ of the whole hashed data and approximate the ratio $m/n \sim H_{\min}(X|E)/2\,n_{\mathrm{bit}}$ to preserve generation efficiency:

$$R_{sc} = \left(\frac{m}{n}\right) 2\,n_{\mathrm{bit}}\,R_{rw} \approx 20.015\ \mathrm{Gbps}\,. \tag{7}$$

Finally, with our matrix dimension choice, we obtained 2.5 GBytes of hashed data from the original 50 GBytes of raw measurements. The latter were then analyzed with the standard NIST random test batteries suite; the results are reported in Table 1.

Table 1. NIST test results with an hashed file of approximately 2.5 Gbyte. The extractor, designed to ensure a security parameter $\varepsilon \sim 10^{-10}$ of the whole hashed data, is implemented as a Toeplitz matrix-vector modulo two multiplication with column and row dimensions respectively of 17,600 and 11,008.

Test	p-value	Test Result
Frequency	0.768	PASSED
BlockFrequency	0.559	PASSED
CumulativeSums	0.386	PASSED
Runs	0.533	PASSED
LongestRun	0.323	PASSED
Rank	0.091	PASSED
DFT	0.537	PASSED
NonOverlappingTemplate	0.646	PASSED
OverlappingTemplate	0.963	PASSED
Universal	0.342	PASSED
ApproximateEntropy	0.800	PASSED
LinearComplexity	0.748	PASSED
RandomExcursions	0.234	PASSED
RandomExcursionsVariant	0.628	PASSED
Serial	0.539	PASSED
LinearComplexity	0.809	PASSED

6. CONCLUSIONS

This work presents, to the best of our knowledge, the first source-device-independent QRNG scheme on a chip and currently the fastest among the Semi-DI class, capable of a secure generation rate greater than 20 Gbps. Such a result was possible by exploiting integrated photonics alongside fast electronics. Indeed, the latter combination allowed us to achieve a high generation efficiency, ensuring several Gbps even with the local oscillator power well below 1 mW. The generator was developed to promote system designs that are simpler, compact, and reliable. This is achieved through the 4×4 MMI interferometer upon which our heterodyne receiver is based. Indeed, no active feedback control loops are required to ensure the orthogonality of the measured quadratures. Moreover, the 4×4 MMI, being a fully passive structure, should make the optical receiver resistant to harsh operating conditions. Therefore, with the potential qualities mentioned before, the proposed solution should represent an appealing candidate to address the challenges posed by secure space applications, especially those that also require high-performance operations, such as satellite-based QKD. Indeed, given the demonstrated secure generation rate obtained in this paper, our module could power satellite QKD transmitters with a repetition rate higher than 5 GHz.

To conclude, our QRNG combines high security and record-high performance with the benefits of an integrated platform. We believe that this is a significant step forward for the exploitation of this technology in demanding real-world scenarios such as high-speed QKD, either ground or space based.

Funding. Agenzia Spaziale Italiana (ASI, Accordo n. 2017-31-H.0, project QRNG).

Acknowledgments. We acknowledge the Italian Space Agency for support. This work was funded by the project QRNG of the Italian Space Agency (ASI, Accordo n. 2017-31-H.0): "Realizzazione integrata di un generatore quantistico di numeri casuali". We thank the CloudVeneto facility for computational resources. We also thank CAPRI (University of Padova Strategic Research Infrastructure Grant 2017: "CAPRI: Calcolo ad Alte Prestazioni per la Ricerca e l'Innovazione") for computational resources.

Disclosures. The authors declare no conflicts of interest.

Data availability. Data supporting the results presented in this paper are available from the authors upon reasonable request.

REFERENCES

1. M. Herrero-Collantes and J. C. Garcia-Escartin, "Quantum random number generators," Rev. Mod. Phys. **89**, 015004 (2017).
2. A. Acín and L. Masanes, "Certified randomness in quantum physics," Nature **540**, 213–219 (2016).

3. "Quantum random number generators: Market and technology assessment 2023-2032," Inside Quantum Technology, Report: IQT-QRNG2023-1222 (2022), https://www.insidequantumtechnology.com/product/quantum-random-number-generators-market-and-technology-assessment-2023-2032/.
4. Y.-Q. Nie, L. Huang, Y. Liu, *et al.*, "The generation of 68 Gbps quantum random number by measuring laser phase fluctuations," Rev. Sci. Instrum. **86**, 063105 (2015).
5. C. Bruynsteen, T. Gehring, C. Lupo, *et al.*, "100-Gbit/s integrated quantum random number generator based on vacuum fluctuations," PRX Quantum **4**, 010330 (2023).
6. P. R. Smith, D. G. Marangon, M. Lucamarini, *et al.*, "Simple source device-independent continuous-variable quantum random number generator," Phys. Rev. A **99**, 062326 (2019).
7. S. Pironio, A. Acín, S. Massar, *et al.*, "Random numbers certified by Bell's theorem," Nature **464**, 1021–1024 (2010).
8. B. G. Christensen, K. T. McCusker, J. B. Altepeter, *et al.*, "Detection-loophole-free test of quantum nonlocality, and applications," Phys. Rev. Lett. **111**, 130406 (2013).
9. P. Bierhorst, E. Knill, S. Glancy, *et al.*, "Experimentally generated randomness certified by the impossibility of superluminal signals," Nature **556**, 223–226 (2018).
10. Y. Liu, X. Yuan, M.-H. Li, *et al.*, "High-speed device-independent quantum random number generation without a detection loophole," Phys. Rev. Lett. **120**, 010503 (2018).
11. Z. Cao, H. Zhou, and X. Ma, "Loss-tolerant measurement-device-independent quantum random number generation," New J. Phys. **17**, 125011 (2015).
12. G. Vallone, D. G. Marangon, M. Tomasin, *et al.*, "Quantum randomness certified by the uncertainty principle," Phys. Rev. A **90**, 052327 (2014).
13. S. Gómez, A. Mattar, E. S. Gómez, *et al.*, "Experimental nonlocality-based randomness generation with nonprojective measurements," Phys. Rev. A **97**, 040102 (2018).
14. D. G. Marangon, G. Vallone, and P. Villoresi, "Source-device-independent ultrafast quantum random number generation," Phys. Rev. Lett. **118**, 060503 (2017).
15. Z. Cao, H. Zhou, X. Yuan, *et al.*, "Source-independent quantum random number generation," Phys. Rev. X **6**, 011020 (2016).
16. F. Xu, J. H. Shapiro, and F. N. C. Wong, "Experimental fast quantum random number generation using high-dimensional entanglement with entropy monitoring," Optica **3**, 1266–1269 (2016).
17. T. Lunghi, J. B. Brask, C. C. W. C. W. Lim, *et al.*, "Self-testing quantum random number generator," Phys. Rev. Lett. **114**, 150501 (2015).
18. P. Mironowicz, G. Ca nas, J. Cari ne, *et al.*, "Quantum randomness protected against detection loophole attacks," Quantum Inf Process. **20**, 39 (2021).
19. T. V. Himbeeck, E. Woodhead, N. J. Cerf, *et al.*, "Semi-device-independent framework based on natural physical assumptions," Quantum **1**, 33 (2017).
20. D. Rusca, T. Van Himbeeck, A. Martin, *et al.*, "Self-testing quantum random-number generator based on an energy bound," Phys. Rev. A **100**, 062338 (2019).
21. M. Avesani, H. Tebyanian, P. Villoresi, *et al.*, "Semi-device-independent heterodyne-based quantum random-number generator," Phys. Rev. Appl. **15**, 034034 (2021).
22. H. Tebyanian, M. Avesani, G. Vallone, *et al.*, "Semi-device-independent randomness from d -outcome continuous-variable detection," Phys. Rev. A **104**, 062424 (2021).
23. H. Tebyanian, M. Zahidy, M. Avesani, *et al.*, "Semi-device independent randomness generation based on quantum state's indistinguishability," Quantum Sci. Technol. **6**, 045026 (2021).
24. J. B. Brask, A. Martin, W. Esposito, *et al.*, "Megahertz-rate semi-device-independent quantum random number generators based on unambiguous state discrimination," Phys. Rev. Appl. **7**, 054018 (2017).
25. M. Avesani, D. G. Marangon, G. Vallone, *et al.*, "Source-device-independent heterodyne-based quantum random number generator at 17 Gbps," Nat. Commun. **9**, 5365 (2018).
26. C. Abellan, W. Amaya, D. Domenech, *et al.*, "Quantum entropy source on an InP photonic integrated circuit for random number generation," Optica **3**, 989–994 (2016).
27. F. Raffaelli, G. Ferranti, D. H. Mahler, *et al.*, "A homodyne detector integrated onto a photonic chip for measuring quantum states and generating random numbers," Quantum Sci. Technol. **3**, 025003 (2018).
28. T. Roger, T. Paraiso, I. D. Marco, *et al.*, "Real-time interferometric quantum random number generation on chip," J. Opt. Soc. Am. B **36**, B137–B142 (2019).
29. B. Haylock, D. Peace, F. Lenzini, *et al.*, "Multiplexed quantum random number generation," Quantum **3**, 141 (2019).
30. J. F. Tasker, J. Frazer, G. Ferranti, *et al.*, "Silicon photonics interfaced with integrated electronics for 9 GHz measurement of squeezed light," Nat. Photonics **15**, 11–15 (2021).
31. B. Bai, J. Huang, G.-R. Qiao, *et al.*, "18.8 Gbps real-time quantum random number generator with a photonic integrated chip," Appl. Phys. Lett. **118**, 264001 (2021).
32. L. Li, M. Cai, T. Wang, *et al.*, "On-chip source-device-independent quantum random number generator," Photonics Res. **12**, 1379–1394 (2024).
33. T. Wang, P. Huang, L. Li, *et al.*, "High key rate continuous-variable quantum key distribution using telecom optical components," New J. Phys. **26**, 023002 (2024).
34. S.-K. Liao, H.-L. Yong, C. Liu, *et al.*, "Long-distance free-space quantum key distribution in daylight towards inter-satellite communication," Nat. Photonics **11**, 509–513 (2017).
35. F. Grunenfelder, A. Boaron, D. Rusca, *et al.*, "Performance and security of 5 GHz repetition rate polarization-based quantum key distribution," Appl. Phys. Lett. **117**, 144003 (2020).
36. M. Avesani, L. Calderaro, M. Schiavon, *et al.*, "Full daylight quantum-key-distribution at 1550 nm enabled by integrated silicon photonics," npj Quantum Inf. **7**, 93 (2021).
37. M. Avesani, H. Tebyanian, P. Villoresi, *et al.*, "Unbounded randomness from uncharacterized sources," Commun. Phys. **5**, 273 (2022).
38. M. Tomamichel, C. Schaffner, A. Smith, *et al.*, "Leftover hashing against quantum side information," IEEE Trans. Inform. Theory **57**, 5524–5535 (2011).
39. R. Halir, G. Roelkens, A. Ortega-Monux, *et al.*, "High-performance 90° hybrid based on a silicon-on-insulator multimode interference coupler," Opt. Lett. **36**, 178–180 (2011).
40. D. B. Keck and A. R. Tynes, "Spectral response of low-loss optical waveguides," Appl. Opt. **11**, 1502–1506 (1972).
41. L. Zimmermann, G. B. Preve, T. Tekin, *et al.*, "Packaging and assembly for integrated photonics–a review of the epixpack photonics packaging platform," IEEE J. Sel. Top. Quantum Electron. **17**, 645–651 (2011).
42. R. Marchetti, C. Lacava, L. Carroll, *et al.*, "Coupling strategies for silicon photonics integrated chips," Photonics Res. **7**, 201–239 (2019).
43. Z. Xuan, R. Ding, Y. Liu, *et al.*, "A low-power hybrid-integrated 40-Gb/s optical receiver in silicon," IEEE Trans. Microwave Theory Tech. **66**, 589–595 (2018).
44. H. Friis, "Noise figures of radio receivers," Proc. IRE **32**, 419–422 (1944).
45. S. Y. Siew, B. Li, F. Gao, *et al.*, "Review of silicon photonics technology and platform development," J. Lightwave Technol. **39**, 4374–4389 (2021).

193.205.81.5 2025-11-11 11:09:56 14