Real-Time Self-Testing Quantum Random Number Generator with Non-classical States

Thibault Michel[(1),(3)], Jing Yan Haw[(1),(2)], Davide G. Marangon[(4)], Oliver Thearle[(1)], Giuseppe Vallone[(4),(5)], Paolo Villoresi[(4),(6)], Ping Koy Lam[(1)], Syed M. Assad[(1)]

[(1)] CQC2T, Department of Quantum Science, The Australian National University, Canberra, ACT 0200, Australia
[(2)] Quantum Communications Lab, ECE, National University of Singapore, 117583 Singapore, elehjy@nus.edu.sg
[(3)] UPMC-Sorbonne Universités, CNRS, ENS-PSL Research University, Collège de France, 4 place Jussieu, 75252 Paris, France
[(4)] Dipartimento di Ingegneria dell'Informazione, Università degli Studi di Padova, Via Gradenigo 6B, 35131 Padova, Italy
[(5)] Dipartimento di Fisica e Astronomia, Università di Padova, via Marzolo 8, 35131 Padova, Italy
[(6)] Istituto di Fotonica e Nanotecnologie - CNR, Via Trasea 7, 35131 Padova, Italy,

Abstract *The certification of private randomness of quantum origin is paramount for cryptographic applications. By trusting the measurement device, conjugate quadrature measurements allows us to quantify insecure side-information on the measured state with bounded energy. We demonstrate a live self-checking random number generator using squeezed states.*

Introduction

Random Number Generators based on intrinsic quantum randomness play a pivotal role in quantum communication technologies, such as quantum key distribution which demands randomness independent from all pre-existing knowledge. The current realisations of quantum random number generators (QRNG) span a spectra of varying degrees of trust and generation rates, where there is a strong tradeoff between these factors. For instance, a laser-phase-noise QRNG with a fully characterised source and measurement can offer large amounts of raw quantum entropy, up to 68 Gbps[1]. On the other hand, given completely untrusted devices, device-independent QRNGs have reported up to 62 MBits of genuine, unpredictable randomness based on violation of Bell inequality in a loophole free manner, while taking a total time of 96 hours[2]. For practical purposes, intermediate approaches, such as semi-device-independent (SDI)-QRNGs try to gain the best of both worlds, and thus offer attractive solutions for near-future applications while still enjoying high bit-rate and secrecy.

For these SDI-QRNGs, which operate under a few reasonable assumptions, several features are desirable. Firstly, since the SDI-QRNG is not fully trusted, self-testing[3] is often required to validate the amount of secure randomness. Moreover, the device needs to be able to certify that the generated randomness is of quantum origin. Finally, in order for the device to qualify as a *fully operating, self-calibrating and secure* QRNG, the aforementioned operations (self-testing and certification), together the final random bits generation should all be performed in real-time.

In this work[4], we demonstrate such a protocol that fulfills the above conditions by measuring a quantum state with no classical counterpart, namely a squeezed state, to generate randomness. Under the assumptions that our measurements are reliable, we are able to certify the quantum origin of the randomness with active-quadrature-switching homodyne detection scheme. Furthermore, together with the practical assumption of having a finite input energy, we are able then to exploit the entropic uncertainty relation (EUR) upon conjugate quadratures ($\hat{Q}$ for the data quadrature and $\hat{P}$ for the checking quadrature), which allows us to quantify the extractable randomness from the quadrature of $\hat{Q}$ conditioned on any (classical or quantum) side information that a malicious eavesdropper may have intercepted.

Theory

Given an input quantum state ρ_A that may be mixed and correlated to a malicious party E, i.e. $\rho_A = \mathrm{Tr}_E(\rho_{AE})$, the goal of our real-time SDI-QRNG protocol is to quantify the min-entropy from the discretised data quadrature $\hat{Q}_{\delta q}$ of the state ρ_A conditioned upon on the side-information accessible to an eavesdropper E. However, the

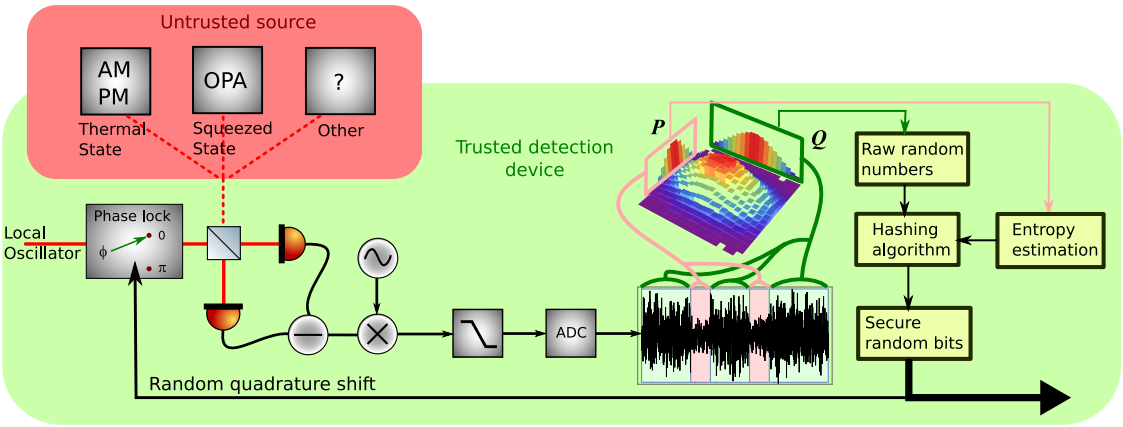

Fig. 1: Scheme and protocol of the SDI-QRNG. A local oscillator whose phase is locked to measure the *check* quadrature is interfered with an untrusted entropy source which can be a squeezed, thermal or some unknown state. The checking quadrature dictates the secure randomness to be extracted from the data quadrature. By performing randomness extraction on-line, part of the random bits can be resupplied into the system for random basis switching, thus allowing the device to operate in a fully self-testing manner. Figure from[4]

system E is generally inaccessible in experiments, and hence a worst case estimate would have to be made, by performing a full tomography of ρ_A and subsequently optimising all compatible states, which is intractable for a generic infinite-dimensional system. Fortunately, by using the EUR, the quantity of interest can be lower bounded by the following equation:

$$H_{\min}(Q_{\delta q}|E) \geq H_{\text{low}}(P_{\delta p}) \\ := -H_{\max}(P_{\delta p}) - \log_2 c(\delta q, \delta p) \quad (1)$$

where $c(\delta q, \delta p)$ is a measure of the incompatibility between the two quadrature measurements dependent on the bin sizes δp and δq. Interestingly, the bound $H_{\text{low}}(P_{\delta p})$ can be obtained *unconditionally* by simply measuring the discretised check quadrature $\hat{P}_{\delta q}$ and evaluate the max-entropy $H_{\max}(P_{\delta p})$. In practice, the detection has a finite range, so we assume that the input states ρ_A are limited in phase space and have no support in the two extreme bins. In other words, by bounding the energy of the input state, we alleviate the need to perform a full tomography upon an uncharacterized source.

Experiment

Figure 1 shows a schematic of our real-time SDI-QRNG protocol. To demonstrate the self-testing feature and robustness of our protocol, we operate the device with two distinct states: a non-classical squeezed state and a classical thermal state. The 3 dB-squeezed state was generated with a seeded doubly resonant optical parametric amplifier in a bow-tie geometry[5]. Thermal states with different variances were generated using a pair of amplitude and phase electro-optic modulators, driven by two independent function generators with white-noise signals. At the measurement stage, the homodyne detector is first phased-locked to the checking quadratures to estimate lower bound of the secure randomness $H_{\text{low}}(P_{\delta p})$. Subsequently, by locking to the data-quadrature, Toeplitz hashing is then performed on the acquired raw random bits ($n = 16000$ 12-bit datapoints) to extract the amount randomness estimated during the checking round. Finally, some of the secure random bits obtained are loaded back into the system for random switching between the check and data measurement stages. We note that prior to each check measurement, the dark noise, shot noise and the bin-size are re-evaluated to ensure that our entropy estimation is stable with respect to experimental conditions. As a result, our protocol is self-testing, self-sustaining and self-calibrating.

Result

Figure 2 shows the results from our experimental demonstration for squeezed states and thermal states. The entropy estimation is in excellent agreement with the numerical simulation based on our frequentist estimator. For comparison, the theoretical bound for the unconditional min-entropy $H^{\text{th}}_{\min}(Q_{\delta q})$ and $H^{\text{th}}_{\text{low}}(P_{\delta p})$ assuming discretized Gaussian distribution are plotted. The theoretical conditional curve for the conditional case is always lower than the unconditional case, as one would expect from a source with untrusted correlation or noise. For a thermal state, the higher the variance, the higher the min-entropy, which reflects the apparent random noise in the quadrature measurement, yet the condi-

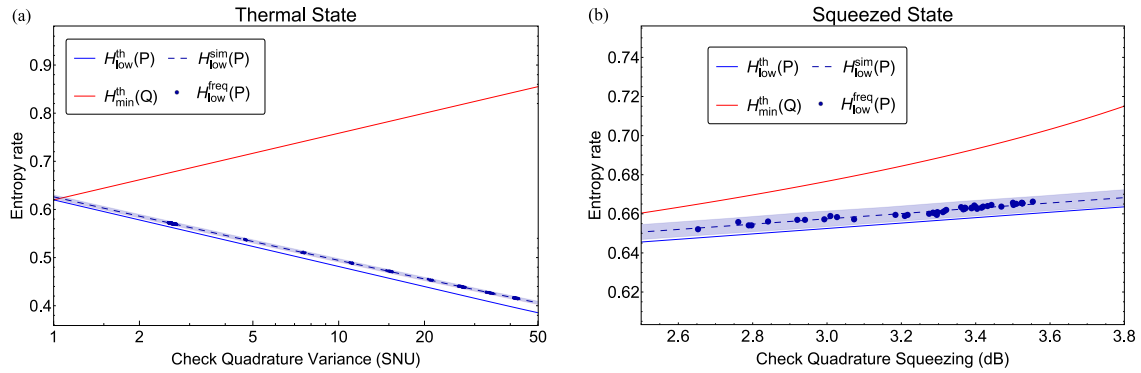

Fig. 2: Entropy bound for (a) thermal states (b) a $\hat{P}$-squeezed state with 33% loss. The red solid lines: the theoretical min entropy of the random-data quadrature $\hat{Q}$. The blue solid lines: the theoretical bound to the conditional min-entropy $H_{\min}(Q|E)$ obtained by the EUR. The blue points show the corresponding experimental data calculated in real-time using a frequentist estimator on data samples of length $n = 16000$. Dashed lines show the corresponding simulation results and the shaded area corresponds to a 5 standard deviation uncertainty region. Figure adapted from[4].

tional min-entropy is lower because the state may well be correlated with a mode obtained by Eve. Meanwhile, for a squeezed state, the purity of the state is scrutinized via the check quadrature, thus the entropy independent of increases as the squeezing value increases. The final average secret bit generation rate, taking into account the full measurement cycle into account is 8 kb/s.

Discussions

Notably, the novelty of our approach is two-fold:

1. **Using EURs in real-time randomness estimation.** While there have been previous demonstrations of EUR-based QRNG[6],[7], the randomness estimation was always evaluated offline. Here, we demonstrate the possibility to utilize the EUR techniques even in a real-time fashion, which is critical for the applicability of the QRNG in many cryptographic scenarios such as quantum key distribution. We show that it is possible to perform the full protocol (including dynamical quadrature switching, locking, entropy bound evaluation and randomness extraction) on the fly. This provides us the advantage point to uncover and subsequently resolve potential issues and challenges in estimating min-entropy with finite data length.
2. **Nonclassical state - squeezed state for more randomness.** In our protocol, the quantum origin of the randomness is guaranteed by the use of highly non-classical squeezed states. By checking the squeezed quadrature, we show that the anti-squeezed quadrature provides a higher bit-rate in the same protocol. Unlike in the thermal-noise case, this noise is not correlated with another system. For example, having 5 dB squeezing on the source increases the entropy rate by around 10% compared with the vacuum. To our knowledge, this is also the first experimental instance of utilising squeezing as a secure entropy source for a QRNG.

Conclusions

In summary, we have successfully demonstrated a real-time SDI-QRNG incorporating measurement-basis switching and hashing using a squeezed state. This protocol produces a fully automated entropy validation, which is robust against source impurities and imperfections, thus offering the user a peace of mind after switching the device on.

A strongly appealing aspect of our approach is that the generation speed can be readily scale up by incorporating high speed randomness extraction[8], non-mechanical optical switching and using a broadband squeezed light[9]. Furthermore, in view of miniaturisation, on-chip squeezing[10] is an promising avenues for our SDI-QRNG protocol to be implemented, realising a bona-fide random number generator with no classical counterpart.

Acknowledgements

This work was funded by the Australian Research Council Centre of Excellence and Laureate Fellowship schemes (CE110001027 and FL150100019). The research is also supported by The Defence Industry and Innovation Next Generation Technologies Fund.

References

[1] Y.-Q. Nie, L. Huang, Y. Liu, F. Payne, J. Zhang, and J.-W. Pan, "The generation of 68 gbps quantum random number by measuring laser phase fluctuations", *Review of Scientific Instruments*, vol. 86, no. 6, p. 063 105, 2015.

[2] Y. Liu, Q. Zhao, M.-H. Li, J.-Y. Guan, Y. Zhang, B. Bai, W. Zhang, W.-Z. Liu, C. Wu, X. Yuan, *et al.*, "Device-independent quantum random-number generation", *Nature*, vol. 562, no. 7728, pp. 548–551, 2018.

[3] T. Lunghi, J. B. Brask, C. C. W. Lim, Q. Lavigne, J. Bowles, A. Martin, H. Zbinden, and N. Brunner, "Self-Testing Quantum Random Number Generator", en, *Physical Review Letters*, vol. 114, no. 15, Apr. 2015.

[4] T. Michel, J. Y. Haw, D. G. Marangon, O. Thearle, G. Vallone, P. Villoresi, P. K. Lam, and S. M. Assad, "Real-time source-independent quantum random-number generator with squeezed states", *Physical Review Applied*, vol. 12, no. 3, p. 034 017, 2019.

[5] H. M. Chrzanowski, S. M. Assad, J. Bernu, B. Hage, A. P. Lund, T. C. Ralph, P. K. Lam, and T. Symul, "Reconstruction of photon number conditioned states using phase randomized homodyne measurements", *Journal of Physics B: Atomic, Molecular and Optical Physics*, vol. 46, no. 10, p. 104 009, May 2013.

[6] G. Vallone, D. G. Marangon, M. Tomasin, and P. Villoresi, "Quantum randomness certified by the uncertainty principle", en, *Physical Review A*, vol. 90, no. 5, Nov. 2014.

[7] D. G. Marangon, G. Vallone, and P. Villoresi, "Source-device-independent Ultra-fast Quantum Random Number Generation", en, *Physical Review Letters*, vol. 118, no. 6, Feb. 2017.

[8] X.-G. Zhang, Y.-Q. Nie, H. Zhou, H. Liang, X. Ma, J. Zhang, and J.-W. Pan, "Note: Fully integrated 3.2 Gbps quantum random number generator with real-time extraction", *Review of Scientific Instruments*, vol. 87, no. 7, p. 076 102, Jul. 2016.

[9] S. Ast, M. Mehmet, and R. Schnabel, "High-bandwidth squeezed light at 1550 nm from a compact monolithic PPKTP cavity", EN, *Opt. Express, OE*, vol. 21, no. 11, pp. 13 572–13 579, Jun. 2013.

[10] F. Mondain, T. Lunghi, A. Zavatta, E. Gouzien, F. Doutre, M. De Micheli, S. Tanzilli, and V. DâAuria, "Chip-based squeezing at a telecom wavelength", *Photonics Research*, vol. 7, no. 7, A36–A39, 2019.