# Secure heterodyne-based quantum random number generator at 17 Gbps

*M. Avesani*[1], *D. G. Marangon*[1], *G. Vallone*[1,2], *P. Villoresi*[1,2]

[1]*Dipartimento di Ingegneria dell'Informazione, Università degli Studi di Padova, Via Gradenigo 6B - 35131 Padova, Italia*
[2]*Istituto di Fotonica e Nanotecnologie - CNR, Via Trasea 7 - 35131 Padova, Italia*

Random numbers are an invaluable resource in many different fields, ranging from simulations in fundamental science to security applications. Quantum random number generators (QRNGs), exploit the intrinsic randomness of quantum mechanics for the generation of genuine random numbers. However, in some critical cases such as classical and quantum cryptography, the random numbers are also required to be private, meaning that they must be known only by the legitimate user. In fact, imperfections, malfunctions or backdoors, could leak *(quantum) side information* that could be used by an eavesdropper to guess the random sequence. Even in presence of side information, randomness can still be extracted [1], but it is necessary to bound it, usually requiring assumptions on the inner working of the generators. While all the commercial QRNGs need to fully trust their devices, Device-Independent (DI) protocols exploit Bell nonlocality to generate private randomness without any assumption on the components. Unfortunately, such experimental realization is extremely demanding since it requires a loophole-free violation of a Bell inequality, and the generation rate is too low to be useful in practical scenarios [2,3].
A promising approach, that combines the speed of commercial QRNG and the security of DI-QRNG, is given by Semi-Device-Independent (Semi-DI) protocols: with respect to common trusted QRNG, they require weaker assumptions on the devices (e.g, only on the source or on the measurement side), but they can achieve a generation rate dramatically larger than DI-QRNG [4,5].

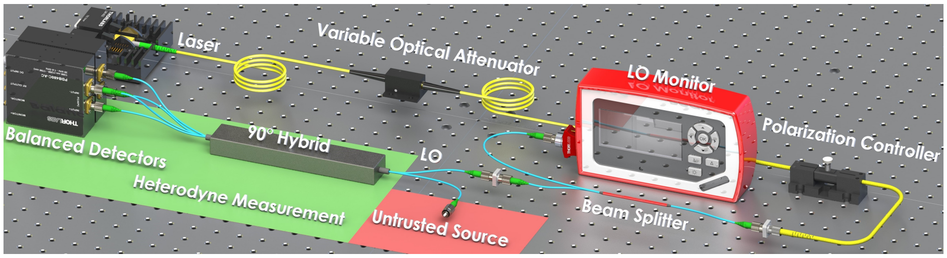

Figure 1: Schematic representation of the experimental setup.

In our work we introduce a QRNG belonging to the family of the Semi-DI generators [6]: in particular, we describe a novel source-device independent (SDI) protocol based on generic Positive Operator Valued Measurements (POVM). We exploit the structure of the POVM to naturally bound the private extractable randomness without any assumption on the source, which can be even fully controlled by an adversary. The analysis takes into account both classical and quantum side information. Unlike previous secure QNRG, the amount of extractable randomness does not depend on the data, but only on the structure of the measurement. Moreover, the bound on the min-entropy is valid also in the non-asymptotic regime, i.e. for finite block size. All previously known Semi-DI or DI protocols needed to randomly switch between two basis, thus requiring an external randomness source. For this reason they are actually randomness expansion protocols. Being free of the strong assumption on the given external randomness, our protocol removes a critical side-channel, improving the security and making it able to operate as a standalone random number generator. Then, we experimentally implemented the protocol, using for the first time continuous variable (CV) and heterodyne measurement. The advantage of CV is twofold: firstly, it can increase the amount of entropy extractable per measurement, secondly, it allows to use standard commercial off-the-shelves telecom devices. This last aspect is particularly interesting for the realization of an integrated QRNG, since it is already compatible with today's fabrication technology, developed for classical communication devices. Combining our protocol with high bandwidt telecom components, we were able to experimentally demonstrate a secure generation rate greater than 17 Gbit/s: to our knowledge, the fastest random generation rate for a Semi-DI QRNG obtained so far. Hence, our QRNG combines simplicity, ultrafast-rates and high security with low cost components compatible with standard photonic integration technologies, paving the way to new practical solutions for integrated random number generation.

## References

[1] M. Tomamichel, C. Schaffner, A. Smith, and R. Renner, Leftover Hashing Against Quantum Side Information", IEEE Transactions on Information Theory, vol. 57, pp. 55245535 (2011)

[2] P. Bierhorst, E. Knill, S. Glancy, Y. Zhang, A. Mink, S. Jordan, A. Rommal, Y.-K. Liu, B. Christensen, S. W.Nam,et al., Experimentally generated randomness certified by the impossibility of superluminal signals, Nature, vol. 556 (2018)

[3] Y. Liu, X. Yuan, M.-H. Li, W. Zhang, Q. Zhao, J. Zhong, Y. Cao, Y.-H. Li, L.-K. Chen, H. Li, T. Peng, Y.-A.Chen, C.-Z. Peng, S.-C. Shi, Z. Wang, L. You, X. Ma, J. Fan, Q. Zhang, and J.-W. Pan, High-speed device-independent quantum random number generation without a detection loophole,Phys. Rev. Lett., vol. 120 (2018)

[4] D. G. Marangon, G. Vallone, and P. Villoresi, Source-Device-Independent Ultrafast Quantum Random Number Generation,Physical Review Letters, vol. 118, (2017).

[5] J. B. Brask, A. Martin, W. Esposito, R. Houlmann, J. Bowles, H. Zbinden, and N. Brunner, Megahertz-ratesemi-device-independent quantum random number generators based on unambiguous state discrimination,Phys. Rev. Applied, vol. 7, (2017)

[6] M. Avesani, D. G. Marangon, G. Vallone, and P. Villoresi, Secure heterodyne-based quantum random number-generator at 17 Gbps, Preprint at arXiv:1801.04139 (2018)