Development of a high-speed integrated quantum random number generator employing vacuum fluctuations

Momtchil Peev[1], Christoph Pacher[1], Philipp Grabenweger[1], Bernhard Schrenk[1], Imran Khan[2,3], Dominique Elser[2,3], Christoph Marquardt[2,3] and Gerd Leuchs[2,3]

1. Digital Safety & Security Department, AIT Austrian Institute of Technology, Donau-City-Straße 1, 1220 Vienna, Austria
2. Max Planck Institute for the Science of Light, Guenther-Scharowsky-Str. 1/Bldg. 24, 91058 Erlangen Germany
3. Institute of Optics, Information and Photonics, University of Erlangen-Nuernberg, Staudtstraße 7/B2, 91058 Erlangen, Germany

We present the state of development of the TIQUAR project that was already introduced in QCRYPT 2014. In this poster we focus predominantly on the theoretical approaches we pursue in our research.

Quantum Random Number Generation (QRNG) is a vital tool in many quantum information based application. For this reason many groups are devising and implementing QRNG devices. It is well known that quantum mechanics inherently gives rise to “irreducible randomness”, i.e. randomness that cannot be reduced to any principally attainable knowledge. However it turns out to be pretty difficult to discriminate reducible from irreducible randomness. Indeed only the latter can be the source of a True QRNG device that is unpredictable in principle. The former could in fact be used as a predictive tool in the hands of an unbounded adversary.

Frauchiger et al. [1] devised a well-founded theoretic scheme for separation of both types of randomness and extracting the irreducible ingredient alone and ultimately calculating the reduction factor in the randomness extraction stage. Their results are essentially restricted to single photon detection schemes (discrete variables). We have extended these to the case of homodyne detection based measurement of vacuum fluctuations (continuous variables), following the experimental scheme of Gabriel et al. [2]. We estimate the min-entropy of the quantum measurement conditioned on the potential knowledge of the eavesdropper and its transformation after the classical electronic processing that outputs the raw random string. On this basis we calculate the reduction factor that determines the output length of the (seeded) randomness extraction algorithm that yields a true random string.

In addition to the theoretical results we will report on the progress made in the development of the advanced photonic and electronic device integration scheme that is the implementation basis of the TIQUAR QRNG.

[1] D. Frauchiger, R. Renner and M. Troyer, arXiv:1311.4547.
[2] C. Gabriel, C. Wittmann, D. Sych, R. Dong, W. Mauerer, U. L. Andersen, C. Marquardt and G. Leuchs, Nature Photonics **4**, 711 (2010).