Certification of quantum networks
from Bell's theorem

P. Sekatski, J.-D. Bancal, S. Wagner and N. Sangouard

Quantum Optics Theory Group, University of Basel, CH-4056 Basel, Switzerland
E-mail: nicolas.sangouard@unibas.ch

Device-independent certification aims to guarantee that a given device behaves as instructed without any knowledge of its internal working. It relies on Bell's theorem, which is no longer of purely fundamental interest but is leading to unexpected applications, including the characterization of quantum many-body systems [1]-[2], the certification of random number generators [2]-[3] or quantum key distribution protocols [5].

In this talk, I will show how Bell's theorem can be used to certify all the components of quantum computers that are used to store, transfer and process quantum information. Our certification methods are very robust to experimental noise and can be readily used to certify that today's devices can be used in tomorrow's quantum networks.

References

[1] J. Tura, R. Augusiak, A.B. Sainz, T. Vertesi, M. Lewenstein, and A. Acin, Science **344**, 1256 (2014)

[2] R. Schmied, J.-D. Bancal, B. Allard, M. Fadel, V. Scarani, P. Treutlein, and N. Sangouard, Science **352**, 6284 (2016)

[3] R. Colbeck, Quantum and Relativistic Protocols for Secure Multi-Party Computation, PhD dissertation, Univ. Cambridge (2007)

[4] S. Pironio, A. Acin, S. Massar, A. Boyer de la Giroday, D.N. Matsukevich, P. Maunz, S. Olmschenk, D. Hayes, L. Luo, and C. Monroe, Nature **464**, 1021 (2010)

[5] A. Acin, N. Brunner, N. Gisin, S. Massar, S. Pironio, and V. Scarani, Phys. Rev. Lett. **98**, 230501 (2007)