Contribution ID: **79** Type: **Talk**

# Device-Independent Quantum Key Distribution Between Two Ion Trap Nodes

*Thursday 30 June 2022 11:45 (22 minutes)*

Private communication over shared network infrastructure is of fundamental importance to the modern world. In classical cryptography, shared secrets cannot be created with unconditional security; real-world key exchange protocols rely on computational conjectures such as the hardness of prime factorisation to provide security against eavesdropping attacks. Quantum theory, however, promises that measurements on two entangled systems can yield correlated outcomes that are fundamentally unpredictable to any third party, which forms the basis of quantum key distribution (QKD) [1]. The security of existing QKD implementations has relied on detailed knowledge of the states and measurements involved, however, enabling attacks that exploit imperfections in the quantum devices (e.g. [2]). Following the pioneering work of Ekert [3] proposing the use of entanglement to bound an adversary's information from Bell's theorem, we present the experimental realisation of a complete quantum key distribution protocol immune to these vulnerabilities.

The security of our protocol is device-independent [4]: we treat the systems as "black boxes", relying only on measurement statistics observed during the key generation process for the security analysis. This requires a great number of observations of a large, detection-loophole-free Bell inequality violation. We achieve this using two $^{88}\mathrm{Sr}^{+}$ ion trap nodes connected by an optical fibre link. A heralded entanglement generation scheme yields about one hundred Bell pairs per second with a fidelity of 96.0(1)%, a new record for optical entanglement of distant matter qubits.

We combine this experimental platform with theoretical advances in finite-statistics analysis, error correction, and privacy amplification to generate, for the first time, a shared key with device-independent security. Our result [5] demonstrates that provably secure cryptography is possible with real-world devices, and paves the way for further quantum information applications based on the device-independence principle.

[1] Gisin et al., Rev. Mod. Phys. 74, 145 (2002).
[2] Lydersen et al., Nat. Photonics 4, 686 (2010).
[3] A. K. Ekert, Phys. Rev. Lett. 67, 661 (1991).
[4] Mayers and Yao, Quantum Info. Comput. 4, 273–286 (2004).
[5] Nadlinger et al., arXiv:2109.14600 (2021).

**Primary author:** NADLINGER, David P. (University of Oxford)

**Co-authors:** DRMOTA, Peter (University of Oxford); NICHOL, Bethan C. (University of Oxford); ARANEDA, Gabriel (University of Oxford); MAIN, Dougal (University of Oxford); SRINIVAS, Raghavendra (University of Oxford); LUCAS, David M. (University of Oxford); BALLANCE, Chris J. (University of Oxford); IVANOV, Kirill (École Polytechnique Fédérale de Lausanne); TAN, Ernest Y.-Z. (ETH Zürich); SEKATSKI, Pavel (University of Geneva); URBANKE, Rüdiger L. (École Polytechnique Fédérale de Lausanne); RENNER, Renato (ETH Zürich); SANGOUARD, Nicolas (Université Paris-Saclay); BANCAL, Jean-Daniel (Université Paris-Saclay)

**Presenter:** NADLINGER, David P. (University of Oxford)

**Session Classification:** Quantum Information & Computing