Free-space quantum signatures using heterodyne measurements

Callum Croal,[1] Matthew Thornton,[1] Christian Peuntinger,[2,3,4] Bettina Heim,[2,3] Imran Khan,[2,3] Christoph Marquardt,[2,3] Gerd Leuchs,[2,3] Petros Wallden,[5] Erika Andersson,[6] and Natalia Korolkova[1]

[1] *School of Physics & Astronomy, University of St. Andrews, North Haugh, St. Andrews, KY16 9SS, UK*
[2] *Max Planck Institute for the Science of Light, Günther-Scharowsky-Str. 1/Bldg. 24, Erlangen, Germany*
[3] *IOIP, University of Erlangen-Nuremberg, Staudtstraße 7/B2, Erlangen, Germany*
[4] *Department of Physics, University of Otago, 730 Cumberland Street, Dunedin, New Zealand*
[5] *School of Informatics, University of Edinburgh, 10 Crichton Street, Edinburgh, EH8 9AB, UK*
[6] *SUPA, Institute of Photonics and Quantum Sciences, School of Engineering and Physical Sciences, Heriot-Watt University, David Brewster Building, Edinburgh, EH14 4AS, UK*

Modern cryptography encompasses much more than encryption of messages in order to keep them secret. Many other important cryptographic primitives exist, and it is possible to extend the use of quantum key distribution (QKD) systems to encompass more than the transmission of a secret shared key. One such example are digital signatures, which are widely used e.g. in e-mail and internet commerce to ensure authenticity and transferability of messages. Analogous to how the security of QKD is guaranteed by quantum mechanics, unconditionally secure quantum signature schemes are possible (see e.g. [1]).

Many possible implementations of Quantum Digital Signatures (QDS) are related to QKD in terms of experimental components. However, since the functionalities of QKD and QDS are different, the classical post-processing, the security assumptions, and the security analysis are different. In the first successful realizations of discrete variable (DV) QDS [2, 3], signature lengths were prohibitively long, due in part to experimental imperfections, but also since theoretical techniques need developing. To increase data rates and to render QDS fully compatible with standard telecommunication networks, we here develop QDS scheme where heterodyne measurements replace single-photon detectors [4]. Our scheme is thus closer to a fully continuous variable (CV) QDS scheme. Heterodyne detection is widely used in classical optical communications, reducing experimental errors and improving the message transmission rate. Therefore, it may be possible to use a commercially-compatible real-world experimental platform.

In the simplest scenario, signature schemes involve three parties, Alice, Bob and Charlie. Quantum signature schemes run in two stages. In a distribution stage, sequences of quantum states are distributed among the participants. In an entirely "classical" messaging stage, which can occur much later, Alice sends signed messages to Bob or Charlie. In the type of scheme we employ, Alice first distributes sequences of phase-encoded coherent states, randomly selected between four possible non-orthogonal states, to the possible recipients Bob and Charlie. There is one sequence corresponding to each possible one-bit message (0 or 1). The classical information which fully describes these sequences can be viewed as Alice's "private keys". Only Alice has exact knowledge of these "private key" sequences. Bob and Charlie, or any malicious party, are only able to obtain partial information about these sequences, no matter what type of quantum measurements they are using. In the messaging stage, Alice sends the message together with the corresponding private key, that is, the classical description of what states the corresponding sequence contained. Bob and Charlie compare the private key with their measurement results and reject or accept the message accordingly. The details of the protocol are presented in [4]. The main difference to existing schemes is the use of heterodyne detection, i. e., quadrature measurements, for the "quantum state elimination" in the distribution stage.

We have implemented this quantum signature scheme over a real-world free space link of 1.6 km and developed a security proof. The required signature sequence length per message bit in this experiment was of the order of 10^5, as compared to 10^9 reported in [3], which is an important step forward. The difference between the required signature length in the corresponding ideal schemes, not taking experimental imperfections into account, is one order of magnitude. Until recently [5], all QDS schemes assumed a secure, authenticated quantum channel. Towards removing this restriction, we have devised another CV QDS scheme based on two non-orthogonal states and developed a conceptually new security proof, in the spirit of CV QKD schemes. This new scheme, which uses an unauthenticated quantum channel and is secure against forgery, repudiation and passive eavesdropping attacks, leads to further decrease in signature lengths and is more robust to losses which is confirmed in the experiment.

---

[1] P. J. Clarke *et al.*, Nat. Commun. **3**, 1174 (2012).
[2] R. J. Collins *et al.*, Phys. Rev. Lett. **113**, 040502 (2014).
[3] R. Donaldson *et al.*, Phys. Rev. A **93**, 012329 (2016).
[4] C. Croal, Ch. Peuntinger, B. Heim, I. Khan, Ch. Marquardt, G. Leuchs, P. Wallden, E. Andersson, N. Korolkova: Free-space quantum signatures using heterodyne measurements, arXiv:1604.03708 [quant-ph].
[5] R. Amiri, P. Wallden, A. Kent and E. Andersson, Phys. Rev. A **93**, 032325 (2016).