Gigahertz quantum signatures compatible with telecommunication technologies

Matthew Thornton,[1] Callum Croal,[1] Imran Khan,[2,3] Christoph Marquardt,[2,3] Gerd Leuchs,[2,3] and Natalia Korolkova[1]

[1]School of Physics and Astronomy, University of St. Andrews,
North Haugh, St. Andrews, Fife, KY16 9SS, Scotland
[2]Max Planck Institute for the Science of Light, Staudstraße 2, Erlangen, Germany
[3]Institute of Optics, Information and Photonics,
University of Erlangen-Nuremberg, Staudtstraße 7/B2, Erlangen, Germany

Modern cryptography covers much more than encryption of messages in order to keep them secret. Many other cryptographic primitives exist, and it is important to consider how the security of these will be affected in a quantum future. Digital Signatures are a widely used cryptographic primitive, found eg. in e-mail, e-commerce and digital banking, and they form the basis for larger protocols. A signature σ_m appended to a classical message m ensures the authenticity and transferability of the message, whilst preventing forgery and repudiation. By employing quantum mechanics to distribute the σ_m between recipients, unconditionally secure signature schemes can be constructed [1–4].

As the development of quantum security progresses, one must consider how to implement these schemes using currently existing technology. To this end, we present a continuous-variable quantum signature scheme with an emphasis on compatibility with existing telecommunication technologies. Our scheme is information-theoretically secure against repudiation attacks and collective forging attacks, and can be implemented even when some QKD-based signature protocols fail. We note that this is the first implemented continuous-variable quantum signature scheme which does not require secure quantum channels between participants, though discrete-variable protocols have been proposed and will soon be implemented [5].

In the simplest scenario, quantum digital signature (QDS) schemes involve three parties: Alice, who wishes to sign m, and two recipients, Bob and Charlie. In a Distribution stage, Alice forms sequences of quantum states, ρ_B^m and ρ_C^m, and sends them to Bob and Charlie, who measure the states and record their outcomes. The quantum states can be thought of as Alice's "public key". Her corresponding "private key", containing classical information about which states she sent, is used as the signature σ_m. Crucially, since a QDS scheme relies on quantum measurement, recipients gain only partial information about σ_m. Later, in an entirely classical Messaging stage Alice sends (m, σ_m). Bob and Charlie compare σ_m to their measurement results, and accept or reject m accordingly.

We have implemented our scheme by distributing an alphabet of phase-modulated coherent states over a 20 km optical fiber, and have devised the corresponding security proof. In particular, we prove that a dishonest forger who interacts with the quantum states cannot then declare some σ_m' which will be accepted by honest recipients, except with negligible probability (security against forging). The probability of successful forgery is related to the smooth min-entropy, which can be interpreted as the uncertainty that an eavesdropper has about an honest participant's measurement outcomes [6]. Hence, by estimating a lower bound for the smooth min-entropy we prove security of our protocol, taking into account the finite-size effects intrinsic to signatures. As tighter bounds are developed these can readily be incorporated. Furthermore, Bob's and Charlie's measurement outcomes are symmetrised with respect to Alice, which makes it unlikely that a dishonest Alice can find some σ_m'' which Bob will accept but that she can later deny sending (security against repudiation).

Our system is built from telecom components running at a wavelength of 1553.33 nm and is completely fiber-integrated. The coherent states are distributed by Alice at a rate of 10 GHz and are measured using homodyne detection at Bob/Charlie. With our security proof the signature lengths are of the order of 10^6 to sign m with a 0.01% chance of failure, meaning a 1 bit message can be signed in 0.1 ms. This opens up the possibility of efficiently distributing quantum signatures on a large scale with minimal installation cost, and makes our scheme competitive in a landscape where both practicality and security are important.

[1] D. Gottesman and I. Chuang, "Quantum Digital Signatures," 0105032 [quant-ph] .

[2] R. J. Collins, R. J. Donaldson, V. Dunjko, P. Wallden, P. J. Clarke, E. Andersson, J. Jeffers, and G. S. Buller, Phys. Rev. Lett. **113**, 040502 (2014).

[3] V. Dunjko, P. Wallden, and E. Andersson, Phys. Rev. Lett. **112**, 040502 (2014).

[4] C. Croal, C. Peuntinger, B. Heim, I. Khan, C. Marquardt, G. Leuchs, P. Wallden, E. Andersson, and N. Korolkova, Phys. Rev. Lett. **117**, 100503 (2016).

[5] R. Amiri, P. Wallden, A. Kent, and E. Andersson, Phys. Rev. A **93**, 032325 (2016).

[6] R. König, R. Renner, and C. Schaffner, IEEE Trans. Inf. Theory **55**, 4337 (2009).