Unconditionally secure quantum signatures

Ryan Amiri[1], Ittoop Puthoor[1], Petros Wallden[2], Adrian Kent[3,4], John Jeffers[5] and Erika Andersson[1] (theory)
Ross Donaldson[1], Robert J. Collins[1], Klaudia Kleczkowska[1], and Gerald Buller[1] (experiments)
[1]*SUPA, Institute of Photonics and Quantum Sciences, Heriot-Watt University, Edinburgh EH14 4AS, United Kingdom*
[2]*LFCS, School of Informatics, University of Edinburgh, 10 Crichton Street, Edinburgh EH8 9AB, United Kingdom*
[3]*Centre for Quantum Information and Foundations, DAMTP, Centre for Mathematical Sciences, University of Cambridge, Wilberforce Road, Cambridge, CB3 0WA, United Kingdom*
[4]*Perimeter Institute for Theoretical Physics, 31 Caroline Street North, Waterloo, ON N2L 2Y5, Canada*
[5]*SUPA, Department of Physics, John Anderson Building, University of Strathclyde, 107 Rottenrow, Glasgow, G4 0NG, United Kingdom*

Signature schemes are widely used in modern communication, for example in e-mail, software updates and electronic commerce, to guarantee that messages cannot be forged or tampered with. Additionally, messages are transferrable, which, broadly speaking, distinguishes digital signatures from message authentication. Transferrability means that messages can be forwarded; in other words, that a sender is unlikely to be able to make one recipient accept a message which is subsequently rejected by another recipient if the message is forwarded. Modern cryptography encompasses much more than encryption of secret messages. Signatures give another cryptographic functionality, different from encryption, but which is no less important or useful.

Since messages can be forwarded, the simplest setting for a signature scheme is the three-party scenario with a sender, Alice, and two recipients, Bob and Charlie. Any participant may be dishonest, but there are restrictions on how many dishonest participants there can be. With three participants, for example, two dishonest parties working together can trivially cheat, and thus one assumes that at most one party is dishonest.

Similar to public-key cryptography, the security of commonly used signature schemes relies on the assumed computational difficulty of problems such as finding discrete logarithms or factoring large primes. With quantum computers, such assumptions would no longer be valid. Partly for this reason, it would be desirable to develop signature schemes with unconditional or information-theoretic security. Quantum signature schemes, including the original quantum digital signature (QDS) scheme proposed in [1], are one possible solution. Similar to quantum key distribution, their unconditional security relies only on the laws of quantum mechanics. Early quantum signature protocols required long-term quantum memory [1, 2], but later schemes have become increasingly practical [3–7], needing essentially the same experimental components as quantum

key distribution (QKD), which is already commercially available.

Unconditionally secure "classical" signature schemes are also possible, but need, at the very least, shared secret keys, unless there is a third party trusted by everybody (who effectively can provide each participant with secret information) [5, 8–10]. Shared secret keys can of course be securely generated by QKD, so that one could proceed by first performing standard QKD, and then running e.g. the "classical" signature protocol referred to as "P2" in [5]. Unconditionally secure "direct" quantum signature schemes proceed without first distilling highly secure shared secret keys [1–7], aiming directly at signing messages. It is an open question what the best signature schemes are, with respect to signature length, trust assumptions, requirements on communication channels, and so on. Intuitively, the best "direct" quantum signature schemes should be at least as efficient as those that proceed via the intermediate step of distilling a highly secure key. "Direct" quantum signature schemes have indeed already been shown to have advantages over protocols that rely on standard QKD, in that the"direct" scheme proposed in [7] tolerates more noise in the quantum channels than standard QKD does.

Unconditionally secure signatures are a relatively little investigated research field, and this talk aims to stimulate interest in the topic by explaining how quantum signature schemes work and reviewing progress so far.

References

[1] D. Gottesman and I. Chuang, *"Quantum Digital Signatures"*, arXiv:quant-ph/0105032v2 (2001).

[2] P. J. Clarke et al., *"Experimental demonstration of quantum digital signatures using phase-encoded coherent states of light"*, Nat. Commun. **3**, 1174 (2012).

[3] V. Dunjko, P. Wallden, E. Andersson, *"Quantum Digital Signatures without Quantum Memory"*, Phys. Rev. Lett. **112**, 040502 (2014).

[4] R. Collins et. al, *"Realization of Quantum Digital Signatures without the requirement of quantum memory"*, Phys. Rev. Lett. **113**, 040502 (2014).

[5] P. Wallden, V. Dunjko, A. Kent, E. Andersson, *"Quantum digital signatures with quantum-key-distribution components"*, Phys. Rev. A **91**, 042304 (2015).

[6] R. Donaldson et al., *"Experimental demonstration of kilometre-range quantum digital signatures"*, in preparation.

[7] R. Amiri, P. Wallden, A. Kent and E. Andersson, *"Secure quantum signatures using insecure quantum channels"*, arXiv:quant-ph/1507.02975 (2015).

[8] D. Chaum and S. Roijakkers, *"Unconditionally-secure digital signatures"*, Advances in Cryptology-CRYPTO'90, LNCS, Santa Barbara, USA, 1990, vol. **537**, pp. 206-2014 (1991).

[9] G. Hanaoka, J. Shikata, Y. Zheng, and H. Imai, *"Unconditionally secure digital signature schemes admitting transferability"*, Advances in Cryptology-ASIACRYPT 2000, LNCS, Kyoto, Japan, 2000, vol. **1976**, pp. 130-142 (2000).

[10] C. M. Swanson, and D. R. Stinson, *"Unconditionally secure signature schemes revisited"*, Information Theoretic Security, Proceedings of ICITS 2011, LNCS, Amsterdam, vol. **6673**, pp. 100-116 (2011).