Kilometer Transmission Range Quantum Digital Signatures

R.J. Collins[1], R.J. Donaldson[1], R. Amiri[1], M. Fujiwara[2],
T. Honjo[3], K. Shimizu[3], K. Tamaki[3],
M. Takeoka[2], P. Wallden[4], V. Dunjko[5],
M. Sasaki[2], E. Andersson[1], J. Jeffers[6], G.S. Buller[1].

1. Institute of Photonics & Quantum Sciences and Scottish Universities Physics Alliance, School of Engineering and Physical Sciences, David Brewster Building, Gait 2, Heriot-Watt University, Edinburgh EH14 4AS, United Kingdom
2. Quantum ICT Laboratory, National Institute of Information and Communications Technology (NICT), 4 2 1 Nukui Kitamachi, Koganei, Tokyo 184-8795, Japan
3. NTT Basic Research Laboratories, NTT Corporation, 3-11 Morinosato Wakamiya, Atsugi, Kanagawa 180-8585, Japan
4. School of Informatics, The University of Edinburgh, Information Forum, 10 Crichton Street, Edinburgh, EH8 9AB, United Kingdom
5. Institute for Quantum Optics and Quantum Information, Austrian Academy of Sciences, Technikerstr. 21A, A-6020 Innsbruck, Austria
6. Department of Physics and Scottish Universities Physics Alliance, John Anderson Building, University of Strathclyde, 107 Rottenrow, Glasgow, G4 0NG, United Kingdom

Keywords: quantum digital signatures, quantum communications, photon counting, fiber optics and optical communications,

Extended Abstract

In the age of interconnected electronic systems, it is not surprising to us that we can access and transmit digital information in a variety of different ways. We have reached the level of comfort with digital communication that in some countries votes in elections for the highest governmental office(s) can be made electronically [1]. To undertake these processes requires confidence that our interactions with the various systems will remain private, unaltered and be accepted by the parties responsible [2]. Digital signature schemes provide some of the functionality required in these interactions by providing a means to guarantee the authenticity and transferability of electronic messages. Signature schemes are different from encryption schemes but no less important.

Transferability means that a signed message is unlikely to be both accepted by one recipient, and if forwarded, subsequently rejected by another recipient. This property distinguishes signature schemes from message authentication schemes, where recipients are not guaranteed to be able to forward messages. Many modern widely used digital signature schemes rely on public-key cryptography, where security relies on the conjectured computational complexity of so-called “one-way” functions [3–5]. In other words, security is only computational. However, these digital signature schemes are efficient and easy to use and have therefore gained widespread acceptance.

If quantum computers can be built, this would render existing public-key cryptosystems insecure. It is therefore of interest to investigate signature schemes where security does not rely on computational assumptions. ”Classical” unconditionally secure signature schemes exist, but require additional resources such as an authenticated broadcast channel or a trusted third party, or at the very least pairwise shared secret keys among all parties. Quantum signature schemes [6,7] are another possible solution. Here, security relies on the laws of quantum mechanics, similar to how the security of quantum key distribution is guaranteed.

The first quantum digital signature scheme was proposed by Gottesman and Chuang in 2001 [6] but this required non-trivial components (controlled-NOT gates) to realize quantum comparison between the signature elements. In 2006, Andersson, Curty, and Jex proposed an approach to the comparison of optical coherent states that could be applied to an experimentally realizable quantum digital signature scheme [8] and in 2012 we carried out the first experimental demonstration of quantum digital signatures [9], using this approach. The intervening years have seen the development of several revised quantum digital signature protocols [10–14] and subsequent experimental implementations [15–17].

To date, all of our experimental implementations of quantum digital signatures have featured one sender (Alice) and two receivers (Bob and Charlie). This is the simplest case for a signature scheme since two recipients are needed for a message to be transferred from one recipient to another. Our demonstrations of quantum digital signatures have all used phase-encoded coherent states of light and have borrowed operational design ideas from quantum key distribution while employing additional components unique to quantum digital signatures. In these previous systems, the sender randomly selects coherent states with different phases and fixed amplitude. The number of possible phases will affect the security analysis, and determining the optimal number of states and amplitude is highly non-trivial. A full description of the quantum digital signature protocols is beyond the scope of this work but may be found in [8,10–12,18,13].

Our previous demonstrations of quantum digital signatures relied on an experimentally complex system of two intertwined interferometers, referred to as a multiport, to carry out an optical swap test between signature elements held by two receivers [9,15]. The challenges associated with this multiport limited the operational transmission distances between sender and receivers in these systems to around 5 meters. Removing the multiport [13] offers the potential to extended the transmission distance to several kilometers by employing approaches similar to those demonstrated in quantum key distribution thereby providing an already established set of experimental resources that can be applied to this complementary security technology [19,20,17].

Here we will present an experimental quantum digital signature system that operated over several kilometers of standard telecommunications optical fiber. This represents a significant advancement in the operational lengths of such systems. Furthermore, the presented system offered higher signature generation rates when compared to previous implementations. We will present performance parameters for the system in terms of signature lengths and generation rates, and a consideration of the security parameters that affected operation. We will also briefly consider future prospects for the technology, reflecting on the increased potential for implementation that revised protocols offer.

References

1. D. A. Gritzalis, ed., *Secure Electronic Voting*, 1st ed. (Springer, 2003) ISBN:978-1-4020-7301-4.
2. B. Schneier, *Secrets & Lies* (Wiley Publishing Inc, 2004) ISBN:0-471-45380-3.
3. D. R. Stinson, *Cryptography: Theory and Practice*, Third (Chapman & Hall/CRC, 2006) ISBN:1-58488-508-4.
4. O. Goldreich, *Foundations of Cryptography: Basic Techniques*, Second (Cambridge University Press, 2003) ISBN:0511041209.
5. O. Goldreich, *Foundations of Cryptography: Volume II Basic Applications*, First (Cambridge University Press, 2001), Vol. 1 ISBN:9780511546891.
6. D. Gottesman and I. L. Chuang, "Quantum digital signatures," arXiv:quant-ph/0105032 (2001).
7. D. Gottesman and I. Chuang, "Quantum digital signatures," U.S. patent US 2002/0199108 A1 (2002).
8. E. Andersson, M. Curty, and I. Jex, "Experimentally realizable quantum comparison of coherent states and its applications," Physical Review A **74**, 022304 (2006) doi:10.1103/PhysRevA.74.022304.
9. P. J. Clarke, R. J. Collins, V. Dunjko, E. Andersson, J. Jeffers, and G. S. Buller, "Experimental demonstration of quantum digital signatures using phase-encoded coherent states of light," Nature Communications **3**, 1174 (2012) doi:10.1038/ncomms2172.
10. P. Wallden, V. Dunjko, and E. Andersson, "Minimum-cost quantum measurements for quantum information," Journal of Physics A: Mathematical and Theoretical **47**, 125303 (2013) doi:10.1088/1751-8113/47/12/125303.
11. V. Dunjko, P. Wallden, and E. Andersson, "Quantum Digital Signatures without quantum memory," Physical Review Letters **112**, 040502 (2014) doi:10.1103/PhysRevLett.112.040502.
12. R. Amiri, P. Wallden, A. Kent, and E. Andersson, "Secure quantum signatures using insecure quantum channels," Physical Review A **93**, 032325 (2016) doi:10.1103/PhysRevA.93.032325.
13. P. Wallden, V. Dunjko, A. Kent, and E. Andersson, "Quantum digital signatures with quantum-key-distribution components," Physical Review A **89**, 042304 (2015) doi:10.1103/PhysRevA.91.042304.
14. J. M. Arrazola, P. Wallden, and E. Andersson, "Multiparty Quantum Signature Schemes," Quantum Information And Computation **16**, 0435–0464 (2016).

15. R. J. Collins, R. J. Donaldson, V. Dunjko, P. Wallden, P. J. Clarke, E. Andersson, J. Jeffers, and G. S. Buller, "Realization of Quantum Digital Signatures without the Requirement of Quantum Memory," Physical Review Letters **113**, 040502 (2014) doi:10.1103/PhysRevLett.113.040502.

16. R. J. Donaldson, R. J. Collins, K. Kleczkowska, R. Amiri, P. Wallden, V. Dunjko, J. Jeffers, E. Andersson, and G. S. Buller, "Experimental demonstration of kilometer-range quantum digital signatures," Physical Review A **93**, 012329 (2016) doi:10.1103/PhysRevA.93.012329.

17. C. Croal, C. Peuntinger, B. Heim, I. Khan, C. Marquardt, G. Leuchs, P. Wallden, E. Andersson, and N. Korolkova, "Free-space quantum signatures using heterodyne detection," arXiv:1604.03708 [quant-ph] (2016).

18. R. Amiri and E. Andersson, "Unconditionally Secure Quantum Signatures," Entropy **17**, 5635–5659 (2015) doi:10.3390/e17085635.

19. M. Sasaki, M. Fujiwara, H. Ishizuka, W. Klaus, K. Wakui, M. Takeoka, S. Miki, T. Yamashita, Z. Wang, A. Tanaka, K. Yoshino, Y. Nambu, S. Takahashi, A. Tajima, A. Tomita, T. Domeki, T. Hasegawa, Y. Sakai, H. Kobayashi, T. Asai, K. Shimizu, T. Tokura, T. Tsurumaru, M. Matsui, T. Honjo, K. Tamaki, H. Takesue, Y. Tokura, J. F. Dynes, A. R. Dixon, A. W. Sharpe, Z. L. Yuan, A. J. Shields, S. Uchikoga, M. Legré, S. Robyr, P. Trinkler, L. Monat, J.-B. Page, G. Ribordy, A. Poppe, A. Allacher, O. Maurhart, T. Länger, M. Peev, and A. Zeilinger, "Field test of quantum key distribution in the Tokyo QKD Network.," Optics Express **19**, 10387–10409 (2011) doi:10.1364/OE.19.010387.

20. K. Shimizu, T. Honjo, M. Fujiwara, T. Ito, K. Tamaki, S. Miki, T. Yamashita, H. Terai, Z. Wang, and M. Sasaki, "Performance of long-distance quantum key distribution over 90-km optical links installed in a field environment of Tokyo metropolitan area," Journal of Lightwave Technology **32**, 141–151 (2014) doi:10.1109/JLT.2013.2291391.