Quantum Digital Signatures Transmitted Over a Channel Loss Equivalent to 134 km

R.J. Collins[1], R. Amiri[1], M. Fujiwara[2], T. Honjo[3], K. Shimizu[3], K. Tamaki[3], M. Takeoka[2],
R.J. Donaldson[1], M. Sasaki[2], E. Andersson[1], 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 Advanced Development Center, 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

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

Extended Abstract

We live in an age where people are becoming increasingly comfortable with distributed and networked computer systems [1]. Many people now routinely carry around smartphones that offer numerous methods for electronic communication. However, this increasing flow of electronic information often requires some form of security to ensure that the interactions with the various distributed systems will remain private, unaltered, and be accepted as genuine by the authorized parties [2–4]. Digital signature schemes offer some of the functionality required in these interactions by providing a means to guarantee the authenticity and transferability of electronic messages. It is the property of transferability (the ability to forward signed messages to other parties and have a significantly high probability that they will also accept the signature) that distinguishes signature schemes from message authentication schemes where recipients are not guaranteed to be able to forward messages. Furthermore, signature schemes are different from encryption schemes but no less important.

Many of the widely used modern digital schemes rely on the conjectured computational complexity of inverting so-called "one-way" mathematical functions [2–4]. That is to say, the security offered only holds as long as inversion of the "one-way" functions is significantly computationally challenging as to outweigh the return for successfully carrying out the inversion. If a quantum computer is ever realized many of these widely used digital signature schemes based on "one-way" functions will be rendered insecure. However, these digital signature schemes are efficient and easy to use and have therefore gained widespread acceptance [5–7].

Unconditionally secure signature schemes, where the security does not rely on assumptions of available computational resources, have been developed, 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 [8,9] are another possible solution. Here, security relies on the laws of quantum mechanics, similar to how the security of quantum key distribution is guaranteed.

Quantum digital signatures were first proposed by Gottesman and Chuang in 2001 [9] but this protocol required quantum memory to store quantum states and experimentally challenging controlled-NOT gates to undertake the comparison between the signature quantum states. The first practical quantum signature protocol, operating using coherent states, was proposed in 2006 [10] and in 2012 we carried out the first experimental demonstration of quantum digital signatures [11], using this approach. This demonstration was limited to short distances ~5 meters and long durations to generate signatures.

Although the intervening years have seen the development of several revised quantum digital signature protocols [12–16], and subsequent experimental implementations [17–19], all of the previous experimental demonstrations, based on optical fiber, have been limited to relatively short transmission ranges in a laboratory environment. Here we present an experimental quantum digital signature system that operated over several kilometers of standard telecommunications optical fiber, installed above and below ground. This represents a significant advancement in the operational ranges of such systems. Furthermore, the system presented here offered significantly higher signature generation rates when compared to previous implementations in optical fiber. We will present performance parameters for the system in terms of signature lengths and generation rates, and a consideration of the security parameter. We will also briefly consider future prospects for the technology, reflecting on the increased potential for implementation that revised protocols offer.

The quantum digital signature (QDS) system was based on a differential phase shift (DPS) quantum key distribution (QKD) system, as shown in figure Figure 1, that formed one link in the Tokyo QKD network [20,21]. The physical hardware of the QKD system was unaltered from operation as a QKD system and the only difference was in the post-processing of the data [15]. The communications channel between Alice and Bob was composed of a fixed 45 km long link of installed optical fiber in a loopback configuration and further added attenuation to simulate additional fiber distances.

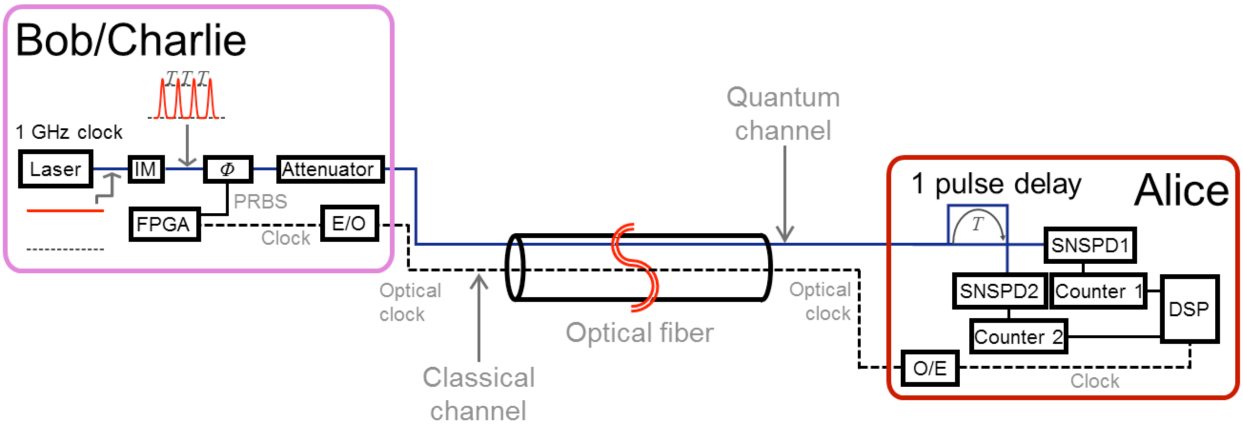

Figure 1. The DPS-QKD system used as the basis of the QDS experiment. FPGA is a master control field programmable gate array logical control unit, IM is an intensity modulator, DSP is a time-stamping digital signal processor, SNSPD is a superconducting single-photon detector, E/O is an electrical to optical encoder used to generate the synchronization clock signal and O/E is an optical to electrical decoder used to recover this synchronizing clock.

The QDS system was operated with several different additional attenuations to simulate several different optical fiber channel lengths, from 90 km [22] up to 134 km, and the time taken to sign a single bit at a failure probability (or "security level"), ε, of 10^{-4} is shown in Figure 2. Figure 2 also shows the optimal results from a previous laboratory-based demonstration of QDS to indicate the significant improvements offered by this new implementation. An ε of 10^{-4} is shown in order to provide a direct comparison between the different systems and the system has additionally been evaluated at an ε of 10^{-10} to provide a more direct comparison with QKD systems. At this more secure value of ε, the time taken to sign a single bit increased from ~0.2 s to ~0.5 s at 90 km and from ~11 s to ~27 s at 134 km. Previous laboratory-based demonstrators [18] were limited to an optimal single bit signing time of ~20 s over a 500-meter distance at an ε value of 10^{-4}.

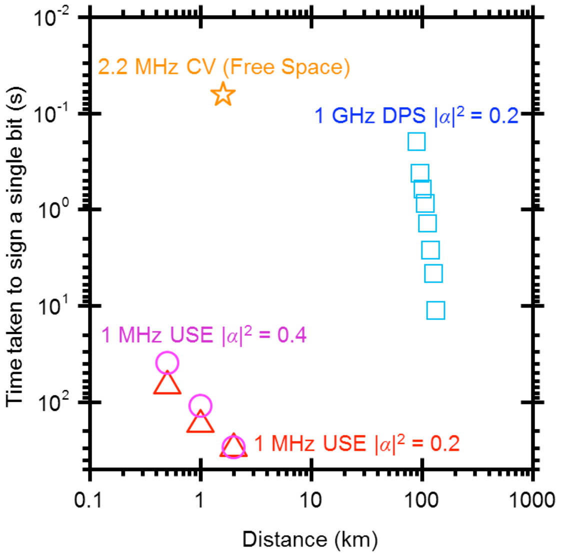

Figure 2. A comparison of results at an ε value of 10^{-4}, as used in previous QDS demonstrations.

In conclusion, we have presented the longest equivalent transmission distance for an experimental demonstration of QDS and have achieved this over mainly installed optical fiber using existing QKD hardware. This represents a significant step forward for practical implementations of QDS as it demonstrates the ability for existing systems to undertake the complementary security process of QDS in addition to QKD.

References

1. M. Hilbert and P. López, "The world's technological capacity to store, communicate, and compute information," Science (New York, N.Y.) **332**, 60–65 (2011) doi:10.1126/science.1200970.
2. O. Goldreich, *Foundations of Cryptography: Volume I Basic Techniques*, 2nd ed. (Cambridge University Press, 2003) ISBN:0511041209.
3. O. Goldreich, *Foundations of Cryptography: Volume II Basic Applications*, 1st ed. (Cambridge University Press, 2001) ISBN:9780511546891.
4. D. R. Stinson, *Cryptography: Theory and Practice*, Third (Chapman & Hall/CRC, 2006) ISBN:1-58488-508-4.
5. D. Kahn, *The Codebreakers: The Comprehensive History of Secret Communication from Ancient Times to the Internet*, 2nd ed. (Simon & Schuster, 1997) ISBN:978-0684831305.
6. S. Singh, *The Code Book*, 1st ed. (Fourth Estate, 2000) ISBN:1-85702-889-9.
7. B. Schneier, *Secrets & Lies* (Wiley Publishing Inc, 2004) ISBN:0-471-45380-3.
8. D. Gottesman and I. L. Chuang, "Quantum digital signatures," arXiv:quant-ph/0105032 (2001).
9. D. Gottesman and I. Chuang, "Quantum digital signatures," U.S. patent US 2002/0199108 A1 (2002).
10. E. Andersson, M. Curty, and I. Jex, "Experimentally realizable quantum comparison of coherent states and its applications," Physical Review A **74**, 22304 (2006) doi:10.1103/PhysRevA.74.022304.
11. 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.
12. 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.
13. V. Dunjko, P. Wallden, and E. Andersson, "Quantum Digital Signatures without quantum memory," Physical Review Letters **112**, 40502 (2014) doi:10.1103/PhysRevLett.112.040502.
14. R. Amiri, P. Wallden, A. Kent, and E. Andersson, "Secure quantum signatures using insecure quantum channels," Physical Review A **93**, 32325 (2016) doi:10.1103/PhysRevA.93.032325.
15. P. Wallden, V. Dunjko, A. Kent, and E. Andersson, "Quantum digital signatures with quantum-key-distribution components," Physical Review A **89**, 42304 (2015) doi:10.1103/PhysRevA.91.042304.
16. J. M. Arrazola, P. Wallden, and E. Andersson, "Multiparty Quantum Signature Schemes," Quantum Information And Computation **16**, 0435–0464 (2016).
17. 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**, 40502 (2014) doi:10.1103/PhysRevLett.113.040502.
18. 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**, 12329 (2016) doi:10.1103/PhysRevA.93.012329.
19. C. Croal, *et al.*, "Free-Space Quantum Signatures Using Heterodyne Measurements," Physical Review Letters **117**, 100503 (2016) doi:10.1103/PhysRevLett.117.100503.
20. K. Inoue, E. Waks, and Y. Yamamoto, "Differential Phase Shift Quantum Key Distribution," Physical Review Letters **89**, 37902 (2002) doi:10.1103/PhysRevLett.89.037902.
21. M. Sasaki, *et al.*, "Field test of quantum key distribution in the Tokyo QKD Network.," Optics Express **19**, 10387–10409 (2011) doi:10.1364/OE.19.010387.
22. R. J. Collins, R. Amiri, M. Fujiwara, T. Honjo, K. Shimizu, K. Tamaki, M. Takeoka, E. Andersson, G. S. Buller, and M. Sasaki, "Experimental transmission of quantum digital signatures over 90 km of installed optical fiber using a differential phase shift quantum key distribution system," Optics Letters **41**, 4883 (2016) doi:10.1364/OL.41.004883.