Progress in experimental quantum digital signatures

Progress in experimental quantum digital signatures

Robert J. Collins, Ross J. Donaldson, Gerald S. Buller

Robert J. Collins, Ross J. Donaldson, Gerald S. Buller, "Progress in experimental quantum digital signatures," Proc. SPIE 10771, Quantum Communications and Quantum Imaging XVI, 107710F (18 September 2018); doi: 10.1117/12.2319015

SPIE.

Event: SPIE Optical Engineering + Applications, 2018, San Diego, California, United States

Invited Paper

Progress in experimental quantum digital signatures

Robert J. Collins[a], Ross J. Donaldson[a], and Gerald S. Buller[a]

[a]Institute of Photonics & Quantum Sciences, and The Scottish Universities Physics Alliance, David Brewster Building, Gait 2, Heriot-Watt University, Edinburgh EH14 4AS, United Kingdom

ABSTRACT

There is ongoing research into information-theoretically secure digital signature schemes. Mathematically based approaches typically require additional resources such as anonymous broadcast and/or a trusted authority to achieve information-theoretical security. The principles of quantum mechanics can be applied to the problem to create the approach known as quantum digital signatures, which does not have these limitations. This presentation will provide an overview of the development of experimental quantum digital signatures. The evolution of experimental test-beds will be charted from small scale demonstrators to long distance implementations with commercial prototypes, along with overviews of the theoretical background of each stage.

Keywords: Quantum communications, quantum digital signature, quantum key distribution, photonics, digital signature, cryptography

1. INTRODUCTION

The humble handwritten *signature* has a long history of being used to guarantee the authenticity of the source of an item of communication.[1] By applying a (supposedly) unique mark to a statement or message the signatory can indicate that they are the source of that communication, and that they agree to be bound by the statements contained therein. Additionally, there is some understanding that a signed communiqué, can be passed to a third party and that they will subsequently also recognize the signature as genuine.

However, we now live in an age where digital communications are becoming increasingly common. A naive assumption may be that a handwritten signature could be converted into a digital graphical representation and appended to a message to indicate the same properties as the ink on paper counterpart. However, digital files can be copied an infinite number of times with no loss of fidelity, so the signature can be added to the end of any message, even those the "signatory" has no knowledge of. Clearly, some form of system or protocol is required that replicates a significant proportion of the functionality of handwritten signatures but can be applied to digital communications. Such schemes exist and are generally referred to as *digital signatures*, although those working in the field of quantum information research tend to refer to them as *classical digital signatures* to provide some separation from later quantum information based protocols.

Most classical digital signature schemes in widespread use employ what are referred to as "*trap-door one-way functions*", that is to say, functions which are computationally easy to compute "one-way" but comparatively difficult to invert without additional knowledge that forms the "trap-door".[2–4] Many of these signature schemes do not offer proven long-term security. There currently exist no publicly known proofs that the "one-way" computations will always be hard to invert - some schemes previous believed to be secure[5] have subsequently been proven to have flaws,[6] and some schemes may be broken in shorter times by quantum computers.[7–9] Nevertheless, classical digital signatures have gained widespread acceptance as a modern method of signing digital communications.[10]

Further author information: (Send correspondence to R.J.C.)
R.J.C.: E-mail: r.j.collins@hw.ac.uk, Telephone: +44 (0)131 451 3056
R.J.D.: E-mail: r.donaldson@hw.ac.uk, Telephone: +44 (0)131 451 4687
G.S.B.: E-mail: g.s.buller@hw.ac.uk, Telephone: +44 (0)131 451 3069

Quantum Communications and Quantum Imaging XVI, edited by Ronald E. Meyers, Yanhua Shih, Keith S. Deacon, Proc. of SPIE Vol. 10771, 107710F · © 2018 SPIE
CCC code: 0277-786X/18/$18 · doi: 10.1117/12.2319015

Quantum digital signatures aim to utilize the uncertainty relations of quantum mechanics to generate digital signatures. Quantum digital signatures were first proposed in 2001[11,12] but that scheme requires an experimentally complex[13] *Controlled-Not* (*CNOT*) gates[14] ,which may be though of a partial quantum mechanical analog of the classical exclusive OR (XOR) gate, to be implemented in the swap test.[15] This requirement for CNOT gates meant that practical implementation of the protocol was a significant challenge and there was a drive to identify simpler protocols that had the potential to be experimentally implemented.

2. EXPERIMENTAL APPROACHES

2.1 Experimentally Realizable Approach

The first protocol for quantum digital signatures that could be experimentally realized with relative ease, given the limitations of available experimental technologies, was proposed[16] in 2006. This protocol employed coherent state[17] mixing on a bulk optical 50:50 beam splitter cube,[18] the basic principles of which are shown in Fig 1(a), to permit the generation of signatures between three parties. Coherent states are comparatively easy to generate and manipulate, making them a far more practical choice for use in quantum information protocols than single-photons,[19] and bulk optical beam splitter cubes are a widely available commercial component.

The signature is encoded as a phase change on a series of coherent states. Unlike *quantum key distribution*,[20] where one post-processed binary digit (derived from approximately a single-photon) is used to secure one binary digit of the message,[21] quantum digital signatures uses a sequence of many phase encoded states to sign a single binary digit of the message. Each sequence is assigned to sign either a single binary 0 or 1 and is used only once for that single digit before being discarded. Messages consisting of multiple binary digits may be signed using one of a selection of variations of the protocol, such as iterating the process for a single binary digit - although more complex methods exist.[22] The exact length of the sequence is one of many parameters considered in the detailed analysis of the security of quantum digital signature protocols. The exact details of the security analysis vary from protocol to protocol and a full discussion of the subtleties of each analysis is beyond the scope of this work. The curious reader is encouraged to examine the original theoretical works outlining each protocol before considering the papers reporting the experimental work.

Three conditions must be considered in a quantum digital signature system, $P\,(\text{Honest Rejection})$ which is the probability that an honest signature will be incorrectly rejected, $P\,(\text{Successful Forgery})$ which is the probability of successful forgery of a signature, and $P\,(\text{Repudiation})$ which is the probability that a transferred signature is rejected by one party having been accepted by the other. Bounds for these parameters can be computed by considering the probability inequalities for sums of bounded random variables.[23] For the protocols reported in this work, we assume that the users of the system are equally concerned about each of these failures and set them all equal such that

$$\left[P\,(\text{Honest Rejection}) = P\,(\text{Successful Forgery}) = P\,(\text{Repudiation})\right] \leq \varepsilon, \tag{1}$$

where ϵ is a security parameter and we say that a system is *secure to a level of* ε if the condition outlined in Eq (1) is met.

Only sender Alice can provide a full classical description of exactly which phase encodings were used on each coherent state so receivers Bob and Charlie can verify that the message was signed by Alice by comparing the classical list of phases to the phase encodings of the optical coherent states that they received. If the number of discrepancies is greater than a certain threshold, Bob and Charlie would determine that the signature was not transmitted by Alice and make a decision on progression based on the details of the protocol.

Through application of the coherent state mixing process shown in Fig 1(a), it is possible to create a multiport consisting of four 50:50 beam splitters in a network, as shown in Fig 1(b) , it was possible for sender Alice and receivers Bob and Charlie to generate a shared signature. This multiport carried out a process of symmeterization, ensuring that both receivers shared the same signature. In addition, if the same signature was transmitted to both Bob and Charlie, no light exited through the middle ports of the multiport (denoted by $|0\rangle$ in Fig 1(b)). The multiport essentially performs a non-demolition comparison of identical coherent states. Therefore, if Bob

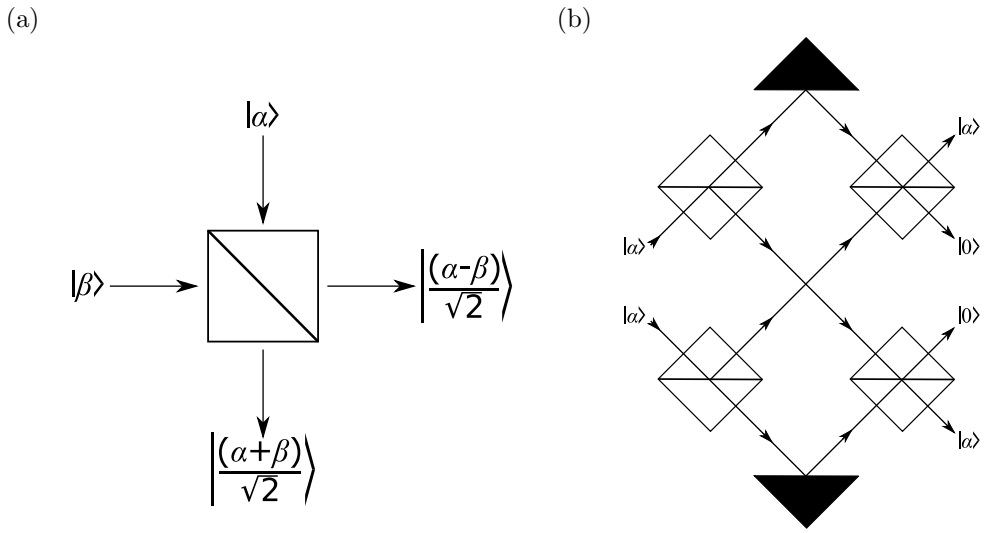

Figure 1. (a) Linear mixing of two coherent states on a 50:50 beam splitter.$|\alpha\rangle$ and $|\beta\rangle$ represent input optical coherent states.[18] (b) The bulk optical multiport that permits verification of quantum digital signatures for two receivers.[16] $|\alpha\rangle$ denotes an optical coherent state, two identical copies of which enter the multiport as indicated on the left-hand side. By reference to Fig 1(a), it can be seen that if the system is perfect (no loss, equal beam splitting ratios, exactly matched optical path lengths, etc) and the two copies of $|\alpha\rangle$ are identical, a copy of $|\alpha\rangle$ will exit from the top and bottom ports on the right-hand side and no light will exit through the middle pair of $|0\rangle$ ports. If the two input optical coherent states are different in any way, some light will exit through the middle pair of ports and a pair of photon detectors situated there will register an event.

and Charlie detected any light at these ports, they knew that Alice sent them differing signatures and acted accordingly as determined by the protocol.

This protocol was first implemented experimentally[24] in 2012, as shown in Fig 2. Sender Alice generated an attenuated laser pulse to serve as the initial, unmodulated coherent state, which was subsequently split into two equal amplitude components at a 50:50 beam splitter. One component served as a delayed unmodulated phase reference while the phase of the other was modulated by amount selected at random from a shared, predetermined set of possible phases.[25] The delay for the phase reference was chosen to be half of the inter-pulse period of the laser, in this case giving a delay of 5 ns. The delayed, unmodulated phase reference and the phase modulated signal were recombined in a single spatial mode at a second 50:50 beam splitter and transmitted from Alice into the multiport. The receivers, Bob and Charlie, had a similar system which delayed part of the signal by 5 ns relative to the reference, cancelling out the relative delay introduced by Alice and ensuring that signal and reference arrived on a final 50:50 beam splitter at the same time. In this first implementation, there was no enforced routing of photons into optically interfering spatial paths so inter-symbol interference from the non-optically-interfering paths increased the number of errors in the system.

This implementation used thick junction silicon single-photon avalanche diodes (Si-SPADs) and operated at a wavelength of 850 nm. Operating at a wavelength of 850 nm had the benefit that the single-photon detector technologies are relatively mature and had fewer deleterious afterpulsing (due to a lower electric field used in the p-n junction) and dark count effects that those at the so called telecommunications wavelengths of 1300 nm and 1550 nm.[26–28]There has been a long history of quantum information experiments performed at a wavelength of 850 nm and using silicon single photon avalanche diodes (Si-SPADs) as the detectors[19,29–33] due to the relatively high detection efficiencies and low spurious count rates. Si-SPADS also typically do not require extensive cryostat based cooling systems or complex external electronics to operate. There is a large field of expertise in fabrication of silicon based semiconductor technologies and this can potentially be applied to the production of single-photon detector technologies use at other wavelengths.[34] One potential drawback of operating at this wavelength is that the transmission losses exhibited by light with a wavelength of 850 nm in standard telecommunications optical fiber are higher at 2.2 db/km when compared to the losses of 0.22 db/km experienced by light of wavelength

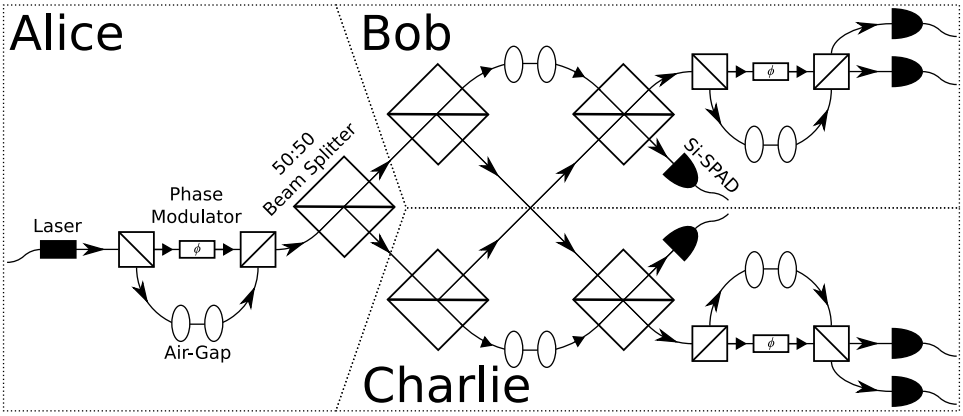

Figure 2. The first experimental demonstration of quantum digital signatures.[24] The laser emitted coherent state pulses at a repetition rate of 100 MHz and a wavelength of 850 nm. The system was assembled from polarization maintaining optical fiber that supported a single optical mode a wavelength of 850 nm. Computer controlled adjustable delay air-gaps allowed for small scale optical path-length changes to be corrected. A phase modulator could be inserted into one of the input arms of the multiport to examine the effects of different signatures in the system .

1550 nm. This means that systems employing light with a wavelength of 850 nm in standard telecommunications optical fiber are limited to shorter transmission distances than those operating with a wavelength of 1550 nm.

The quantum digital signature system was assembled from polarization maintaining optical fiber that supports a single spatial optical mode at a wavelength of 850 nm. Optical fiber was chosen as the construction medium since it offered easier interconnection with the existing optical fiber telecommunications network. Specialist polarization maintaining fiber was used since it offered improved interferometric visibility and, consequently, a significantly reduced number of errors. Adjustable air-gaps, monitored by an iterative feedback loop control system, made small adjustments to the relative optical path lengths to ensure that a relatively high interferometric visibility was maintained throughout the system.[35] However, the multiport was still a complex optical system that limited the overall transmission distance to approximately 5 m. Despite the challenges of such a system, it took approximately 10 seconds to sign a single bit with an ε of 10^{-4}.

2.2 Removal of Quantum Memory

The first implementation of quantum digital signatures, shown in sec 2.1, required some form of quantum memory at receivers Bob and Charlie, rendering it impractical for use in a deployed experimental quantum digital signature system. In a practical digital signature system, the sender Alice would ideally like to be able to send the signature first and then send the message at some indeterminate time in the future. The quantum digital signature system shown in Fig 2 required sender Alice to transmit the message immediately after the corresponding coherent states had been transmitted since receivers Bob and Charlie only had short lengths of optical fiber to delay the coherent states before they were measured with by comparison with a delayed and phase shifted reference.

This requirement for quantum memory was lifted in 2014[36,37] and the corresponding system is shown in Fig 3. Although the revised protocol could have been implemented using phase modulators at the receivers, as in Fig 2, the decision was made to apply the relatively new technology of quantum unambiguous state elimination[38,39] to examine the prospects of passive state discrimination. In this application, quantum unambiguous state elimination seeks to use partial information on the quantum properties of a state to bound the security of the system. By employing a pair of delay systems at the receiver, one with a fixed delay corresponding to a phase shift of $\frac{\pi}{2}$, partial information regarding the quantum state can be measured. The detector event patterns are shown in Table 1 for a set of four phase encodings. In the case of Table 1, if three detectors were to register an event while one did not, the phase encoding of the state would be fully determined and this would be unambiguous state discrimination.

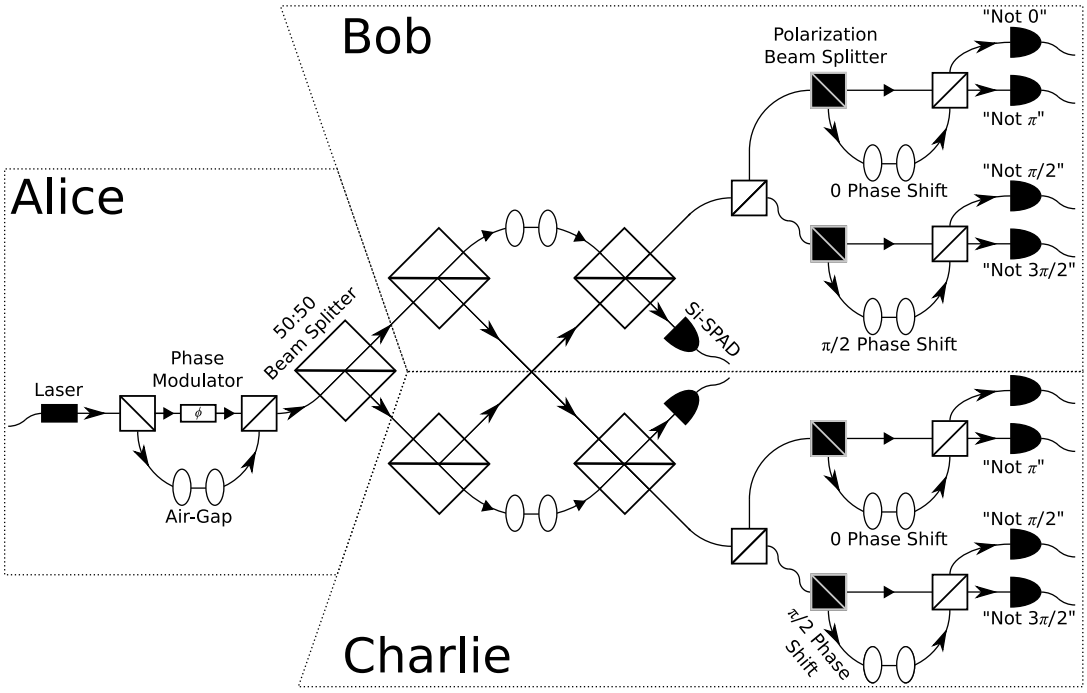

Figure 3. The application of quantum unambiguous state elimination[38,39] to quantum digital signatures[36] without quantum memory.[37] The laser emitted coherent state pulses at a repetition rate of 100 MHz and a wavelength of 850 nm. The system was assembled from polarization maintaining optical fiber that supported a single optical mode a wavelength of 850 nm. Computer controlled adjustable delay air-gaps allowed for small scale optical path-length changes to be corrected. Polarization routing[40] was used to reduce the effects of intra-symbol interference from non-interfering paths .

Table 1. Unambiguous state elimination when applied to quantum digital signatures with four possible phase encodings. If the complete set of detector events described in a row occur then unambiguous state discrimination has been achieved an the phase encoding of the state is known. This table only considers a perfect system, including detectors that do not exhibit dark counts or after-pulsing.[26–28]

Transmitted State	**Detector**			
	Not 0	**Not** $\frac{\pi}{2}$	**Not** π	**Not** $\frac{3\pi}{2}$
0	Not possible	Possible	Possible	Possible
$\frac{\pi}{2}$	Possible	Not possible	Possible	Possible
π	Possible	Possible	Not possible	Possible
$\frac{3\pi}{2}$	Possible	Possible	Possible	Not possible

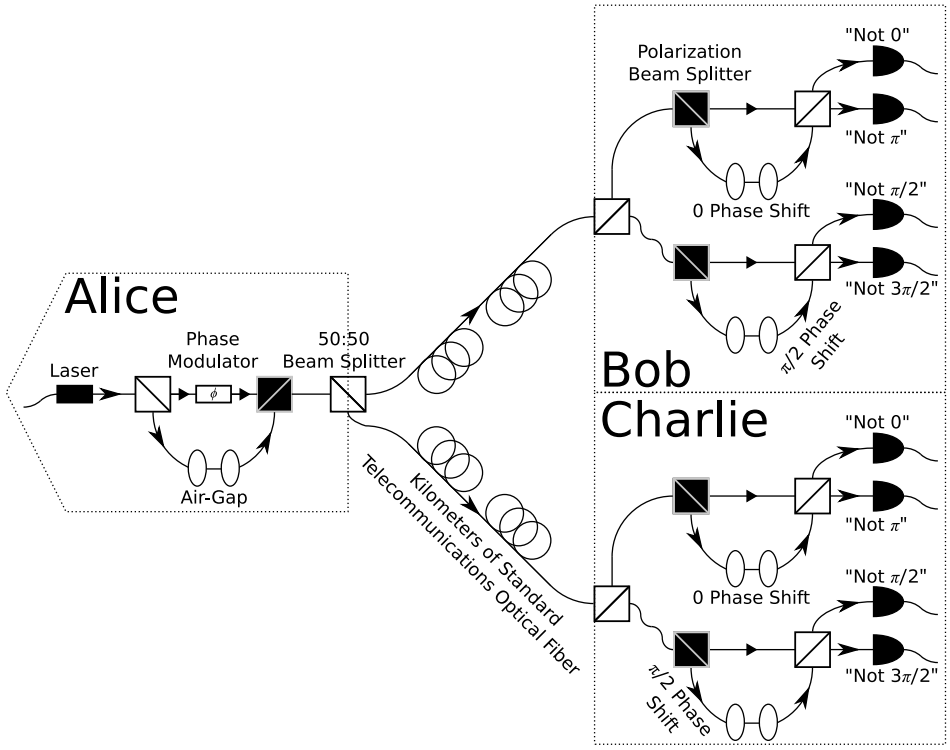

Figure 4. The application of quantum unambiguous state elimination[38,39] to kilometer scale transmission distance quantum digital signatures[41] without quantum memory.[43] The laser emitted coherent state pulses at a repetition rate of 100 MHz and a wavelength of 850 nm. Sender Alice and receivers Bob & Charlie used systems assembled from polarization maintaining optical fiber that supported a single optical mode a wavelength of 850 nm. The communications channel was standard telecommunications optical fiber that supported aa single optical mode at a wavelength of 1550 nm and multiple modes at a wavelength of 850 nm. Mode manipulation techniques[29] were used to suppress the higher order modes. Computer controlled adjustable delay air-gaps allowed for small scale optical path-length changes to be corrected. Polarization routing[40] was used to reduce the effects of intra-symbol interference from non-interfering paths

2.3 Kilometer Scale Transmission Distances

The removal of the requirement for quantum memory paved the way for the transmission distance to be increased to kilometer scale lengths. The process of the symmetrization of the information between receivers Bob and Charlie can be carried out classically over a channel between them which has been secured by quantum key distribution, thereby removing the requirement for a complex multiport. This opens the prospect of implementing quantum digital signatures using quantum key distribution hardware,[41] some of which is now commercially available,[42] significantly improving the practicality of the protocols. If Bob and Charlie conduct quantum key distribution with Alice up to the point of basis set reconciliation and sifting but excluding any error correction and privacy amplification they share a partially correlated sequence of quantum state with Alice. The sequence is only partially correlated since it includes any errors introduced during transmission.

Quantum digital signatures were demonstrated over kilometer scale transmission distances of up to 2 km of laboratory based fiber[43] in 2016 using a variation of the unambiguous state elimination system, as shown in Fig 4. This system took approximately 10^6 seconds to sign a single bit with an ε of 10^{-4}.

With the transmission distance limitation removed, the logical progression was to conduct tests of quantum digital signatures using installed optical fiber. In 2016, Quantum digital signatures were first demonstrated[44] over installed optical fiber in the Tokyo Quantum Key Distribution Network[45] using a differential phase shift quantum key distribution system developed by the Nippon Telegraph and Telephone Corporation (NTT) in collaboration with the National Institute of Information and Communications Technology (NICT).[46] Quantum

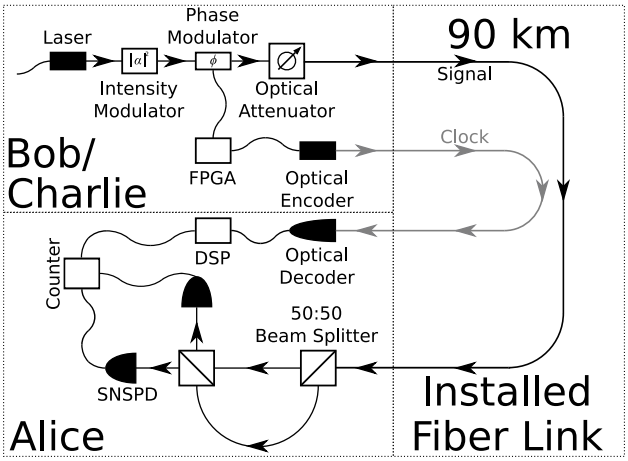

Figure 5. The application of differential phase shift quantum key distribution[46,48] to kilometer scale transmission distance quantum digital signatures[44] over installed optical fiber forming part of the Tokyo Quantum Key Distribution Network.[45] FPGA denotes a *Field Programable Gated Array* , DSP denotes a *Digital Signal Processor*, and SNSPD denotes a *Superconducting Nanowire Single Photon Detector*.[49] The continuous wave laser emitted at a wavelength of 1550 nm and the optical output was converted to pulses at a repetition rate of 1 GHz by an optical intensity modulator. Although the optical fiber link was of fixed length 90 km, additional attenuation could be introduced to simulate longer transmission distances.[47] The quantum signal and synchronization clock were transmitted through optical fiber while the classical data exchange was conducted over Ethernet.[50]

digital signatures were generated between sender Alice and two receivers situatedin the same NICT laboratory but connected to each other by an installed optical fiber link. These experiments were carried out at a wavelength of 1550 nm, which is different to the 850 nm wavelength used in previous demonstrations of quantum digital signatures.

The optical fiber link was 45 km of installed dark fiber configured with a loop-back so that the total transmission distance was 90 km. Approximately half of the length of the optical fiber link was installed in underground ducting while the other half was mounted on overhead poles. The deployed nature of this fiber meant that the channel loss was between 28.7 dB and 31 dB, significantly more than the 19.8 dB that may be expected from the widely accepted "standard" loss of 0.22 db/km quoted for such optical fibers. Consequently, when additional lengths we subsequently simulated by purposefully introducing additional loss to the channel, the simulated length was calculated using the 0.32 db/km loss measured for this fiber at the time of experimentation.[47] The results obtained from this system are shown in Fig 7. This system[47] was able to sign a single bit in approximately 27 seconds with an ε of 10^{-10} at a distance of 134 km using a clock rate of 1 GHz, or approximately two bits per second at a distance of 90 km.

3. PARALLEL DEVELOPMENTS

3.1 Free Space Transmission Channel

Since the generation of quantum key digital signatures can be conducted using the same experimental hardware as quantum key distribution,[41] there is no fundamental reason that transmission of a quantum digital signature cannot take place over a free-space link, and this may lead to the distribution of quantum digital signatures by satellite. There has been a significant experimental examination of the feasibility of free-space quantum key distribution links in a range of different environments and for many different applications[52–54] and the field is highly advanced.[55]

In 2016, a continuous variable[56,57] free-space quantum key distribution system was applied to quantum digital signatures,[51] as shown in Fig 6. *Continuous variable* quantum key distribution differs from the more common "*discrete variable*" quantum key distribution[20] in that the information that forms the key is encoded in continuous quantum variables, such as the quadratures of quantized electromagnetic modes such as coherent

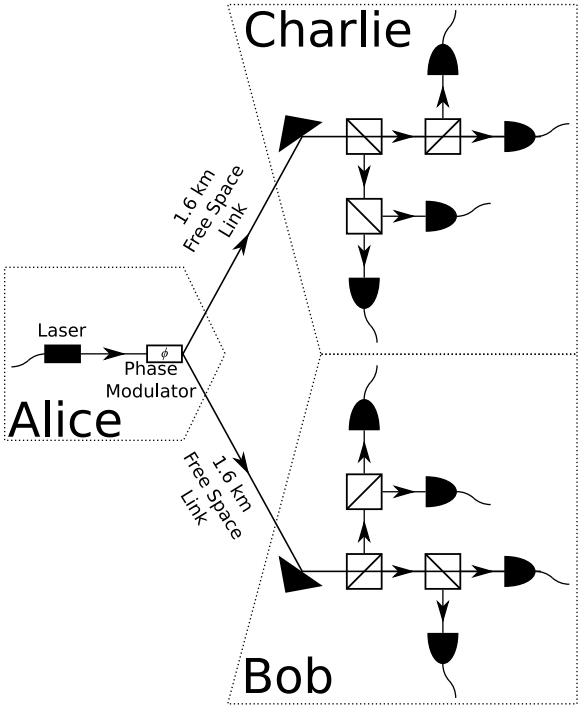

Figure 6. Free space quantum digital signatures based around a continuous variable quantum key distribution system.[51]

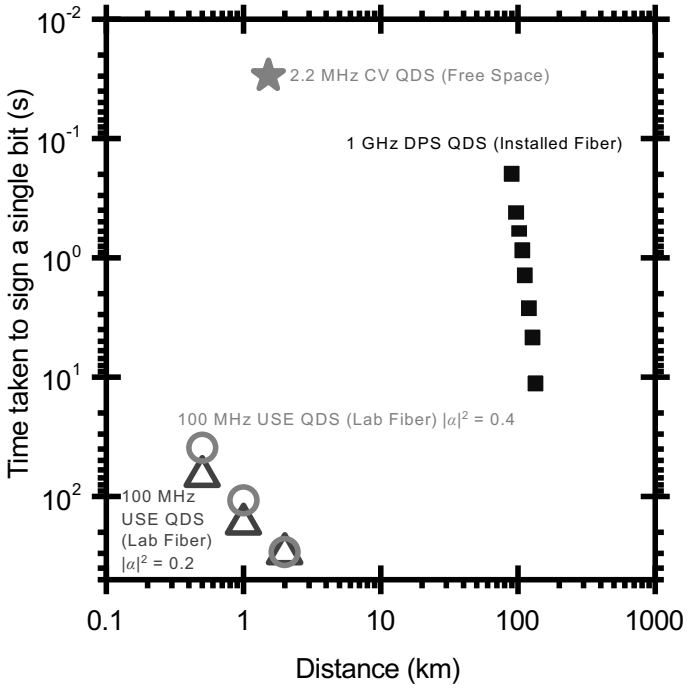

Figure 7. Comparison of the time taken to sign a single bit for three different quantum digital signature systems: a lab based system operating of kilometers of optical fiber with unambiguous state elimination (USE),[43] a free space system based on continuous variable quantum key distribution (CV QKD),[51] and a differential phase shift (DPS) quantum key distribution based system operating over kilometers of installed optical fiber and intentionally introduced additional losses to simulate longer lengths.[47]

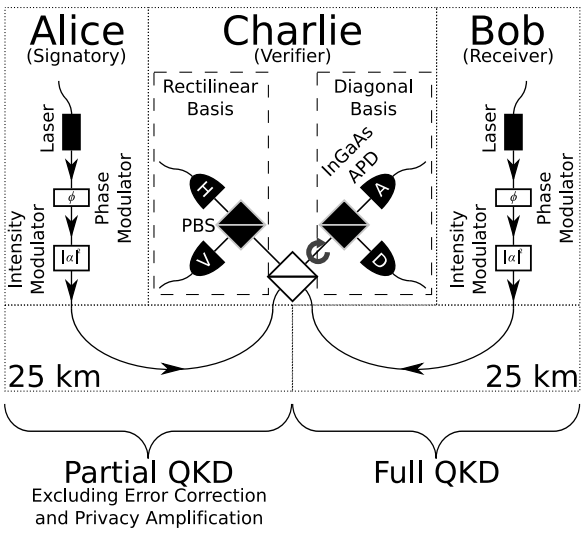

Figure 8. MDI QDS as demonstrated over 25 km of fiber in a laboratory.[62] H denotes horizontal, V denotes vertical, D denotes diagonal, and A denotes anti-diagonal.

states or squeezed states. In addition, instead of the relatively complex single-photon detectors used in discrete variable quantum key distribution, continuous variable quantum key distribution can employ the same homodyne detector schemes[58] used in the classical communications field,[59] making it simpler to implement.

The result obtained from this system over a communication link length of 1.6 km is given in Fig 7.

3.2 Measurement Device Independent

Measurement device independent quantum key distribution[57,60] offers the prospect of quantum key distribution where the measurement apparatus is not trusted. As quantum key distribution hardware can be applied to quantum digital signatures,[61] there have been two significant experiments using measurement device independent quantum key distribution for quantum digital signatures. The first used 25 km reels of fiber in a laboratory[62] whilst the second[63] employed between 17 km and 30 km of installed optical fiber in the metropolitan Hefei optical fiber network.[64] Fig 8 shows a schematic representation of the system which operated over 25 km in a laboratory but the concepts are the same as the system operating over installed fiber.

The laboratory based experiment[62] was able to secure around 13 bit/second (approximately one bit every 74 ms) with an ε of 10^{-10} at a clock rate of 1 GHz. The system operating over the installed Hefei optical fiber network[64] was able to sign a single bit at an ε of $\approx 8 \times 10^{-10}$ in around 40 hours at a clock rate of 75 MHz. While these times are relatively long in comparison to the times obtained from other quantum digital signature systems, it is important to note that measurement device independent quantum key distribution is a comparatively new field of research, so there has been limited research focused on improving transmission rates, and it offers improved security compared to other forms of quantum key distribution.

4. CONCLUSIONS

The field of quantum digital signatures has advanced significantly over the last six years. Efforts by both theorists and experimentalists working together have resulted in the progression of quantum digital signatures from somewhat impractical systems confined to the laboratory[24] to more practical systems utilizing the hardware of commercially available quantum key distribution systems.[44,47]

In a relatively short period of time, the field of quantum digital signatures has advanced to achieve a comparable technological readiness level to that of quantum key distribution. Indeed, since it has been demonstrated that quantum digital signatures and quantum key distribution can share the same hardware,[44,47] there are excellent

prospects for commercialization of the technology by those companies that have already invested in developing commercial quantum key distribution hardware.

ACKNOWLEDGMENTS

The authors thank Professor Erika Andersson & Dr Ittoop Vergheese Puthoor (both Heriot-Watt University), Dr Petros Wallden (University of Edinburgh), Dr Vedran Dunjko (Max-Planck Institute for Quantum Optics), Dr Ryan Amiri & Dr Patrick Joseph Clarke (both formerly Heriot-Watt University), Professor John Jeffers (University of Strathclyde), Dr Toshimori Honjo, Dr Kaoru Shimizu & Dr Kiyoshi Tamaki (all NTT), and Dr Masahide Sasaki, Dr Masahiro Takeoka, & Dr Mikio Fujiwara (all NICT) for their invaluable contributions to the work reported here.

This work was funded in part by the UK Engineering and Physical Sciences Research Council (EPSRC) under grants EP/M013472/1, EP/G009821/1, EP/K022717/1, EP/L015110/1, EP/K015338/1, and the EPSRC Doctoral Prize fellowship grant, COST Action MP1006, the ImPACT Program of Council for Science, Technology and Innovation (a department of the Cabinet Office, Government of Japan), the Daiwa Anglo-Japanese Foundation under grant 10803/11543, and the British Embassy in Tokyo.

The authors are researchers within The UK Quantum Technology Hub for Quantum Communications and gratefully acknowledge the support and funding provided by that partnership.

REFERENCES

[1] "Charles II, 1677: An act for prevention of frauds and perjuryes," in [*Statutes of the Realm*], Raithby, J., ed., **5**, 839–842, Great Britain Record Commission (1819).

[2] Goldreich, O., [*Foundations of Cryptography: Volume I Basic Techniques*], Cambridge University Press, Cambridge, United Kingdom, 2nd ed. (2003).

[3] Goldreich, O., [*Foundations of Cryptography: Volume II Basic Applications*], Cambridge University Press, Cambridge, United Kingdom, 1st ed. (2001).

[4] Stinson, D. R., [*Cryptography: theory and practice*], Chapman & Hall/CRC, Boca Raton, Florida, United States of America, third ed. (2006).

[5] "Data encryption standard." National Bureau of Standards (U.S.), Federal Information Processing Standards Publication 46 (1977).

[6] Curtin, M., [*Brute Force: Cracking the Data Encryption Standard*], Springer, New York, New York, United States of America (2005).

[7] Shor, P. W., "Algorithms for quantum computation: discrete logarithms and factoring," in [*IEEE Symposium on Foundations of Computer Science*], 124–134, IEEE, IEEE, Santa Fe, New Mexico, United States of America (1994).

[8] Shor, P. W., "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer," *SIAM Journal on Computing* **26**(5), 1484–1509 (1997).

[9] Grover, L. K., "A fast quantum mechanical algorithm for database search," in [*Proceedings, 28th Annual ACM Symposium on the Theory of Computing (STOC)*], 212–219, ACM (1996).

[10] "Regulation (EU) no 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC," *Official Journal of the European Union* , L 257/73–114 (August 2014).

[11] Gottesman, D. and Chuang, I. L., "Quantum digital signatures." arXiv preprint: quant-ph/0105032 (2001).

[12] Gottesman, D. and Chuang, I., "Quantum digital signatures." US Patent US20020199108A1 (2002).

[13] Monroe, C., Meekhof, D. M., King, B. E., Itano, W. M., and Wineland, D. J., "Demonstration of a fundamental quantum logic gate," *Physical Review Letters* **75**, 4714–4717 (1995).

[14] Barenco, A., Deutsch, D., Ekert, A., and Jozsa, R., "Conditional quantum dynamics and logic gates," *Physical Review Letters* **74**, 4083–4086 (1995).

[15] Buhrman, H., Cleve, R., Watrous, J., and de Wolf, R., "Quantum fingerprinting," *Physical Review Letters* **87**, 167902 (2001).

[16] Andersson, E., Curty, M., and Jex, I., "Experimentally realizable quantum comparison of coherent states and its applications," *Physical Review A* **74**(2), 022304 (2006).

[17] Glauber, R., "Coherent and incoherent states of the radiation field," *Physical Review* **131**(6), 2766–2788 (1963).

[18] Loudon, R., [*The quantum theory of light*], Oxford science publications, Clarendon Press (1983).

[19] Collins, R. J., Clarke, P. J., Fernandez, V., Gordon, K. J., Makhonin, M. N., Timpson, J. A., Tahraoui, A., Hopkinson, M., Fox, A. M., Skolnick, M. S., and Buller, G. S., "Quantum key distribution system in standard telecommunications fiber using a short wavelength single photon source," *Journal of Applied Physics* **107**(7), 073102 (2010).

[20] Bennett, C. H. and Brassard, G., "Quantum cryptography: public key distribution and coin tossing," in [*Proceedings of the International Conference on Computers, Systems & Signal Processing*], 175–179, IEEE, Bangalore, India (1984).

[21] Grönberg, P., "Key reconciliation in quantum key distribution," Tech. Rep. FOI-R– 1743 –SE, FOI Defence Research Agency (2005).

[22] Wang, T.-Y., Ma, J.-F., and Cai, X.-Q., "The postprocessing of quantum digital signatures," *Quantum Information Processing* **16**(1), 19 (2016).

[23] Hoeffding, W., "Probability inequalities for sums of bounded random variables," *Journal of the American Statistical Association* **58**(301), 13–30 (1963).

[24] Clarke, P. J., Collins, R. J., Dunjko, V., Andersson, E., Jeffers, J., and Buller, G. S., "Experimental demonstration of quantum digital signatures using phase-encoded coherent states of light," *Nature Communications* **3**, 1174 (2012).

[25] Townsend, P. D., Rarity, J. G., and Tapster, P. R., "Enhanced single photon fringe visibility in a 10km-long prototype quantum cryptography channel," *Electronics Letters* **29**(14), 1291–1293 (1993).

[26] Collins, R. J., Hadfield, R. H., and Buller, G. S., "Commentary: New developments in single photon detection in the short wavelength infrared regime," *Journal of Nanophotonics* **4**(1), 040301 (2010).

[27] Buller, G. S. and Collins, R. J., "Single-photon generation and detection," *Measurement Science and Technology* **21**(1), 012002 (2010).

[28] Buller, G. S. and Collins, R. J., "Single-Photon Detectors for Infrared Wavelengths in the Range 11.7 μm," in [*Springer Series on Fluorescence: Methods and Applications: Advanced Photon Counting*], Kapusta, P., Wahl, M., and Erdmann, R., eds., ch. 3, Springer Berlin Heidelberg (2014).

[29] Gordon, K. J., Fernandez, V., Townsend, P. D., and Buller, G. S., "A short wavelength gigahertz clocked fiber-optic quantum key distribution system," *IEEE Journal of Quantum Electronics* **40**(7), 900–908 (2004).

[30] Bienfang, J. C., Gross, a. J., Mink, A., Hershman, B. J., Nakassis, A., Tang, X., Lu, R., Su, D. H., Clark, C. W., Williams, C. J., Hagley, E. W., and Wen, J., "Quantum key distribution with 1.25 Gbps clock synchronization," *Optics Express* **12**(9), 2011–2016 (2004).

[31] Meyer-Scott, E., Hubel, H., Fedrizzi, A., Erven, C., Weihs, G., and Jennewein, T., "Quantum entanglement distribution with 810 nm photons through telecom fibers," *Applied Physics Letters* **97**(3), 031117 (2010).

[32] Dada, A. C., Leach, J., Buller, G. S., Padgett, M. J., and Andersson, E., "Experimental high-dimensional two-photon entanglement and violations of generalized Bell inequalities," *Nature Physics* **7**(9), 677–680 (2011).

[33] Donaldson, R. J., Collins, R. J., Eleftheriadou, E., Barnett, S. M., Jeffers, J., and Buller, G. S., "Experimental Implementation of a Quantum Optical State Comparison Amplifier," *Physical Review Letters* **114**(12), 120505 (2015).

[34] Warburton, R. E., Intermite, G., Myronov, M., Allred, P., Leadley, D. R., Gallacher, K., Paul, D. J., Pilgrim, N. J., Lever, L. J. M., Ikonic, Z., Kelsall, R. W., Huante-Ceron, E., Knights, A. P., and Buller, G. S., "Ge-on-Si Single-Photon Avalanche Diode Detectors: Design, Modeling, Fabrication, and Characterization at Wavelengths 1310 and 1550 nm," *IEEE Transactions on Electron Devices* **60**(11), 3807–3813 (2013).

[35] Clarke, P. J., Collins, R. J., Hiskett, P. A., Townsend, P. D., and Buller, G. S., "Robust gigahertz fiber quantum key distribution," *Applied Physics Letters* **98**(13), 131103 (2011).

[36] Dunjko, V., Wallden, P., and Andersson, E., "Quantum Digital Signatures without quantum memory," *Physical Review Letters* **112**(4), 040502 (2014).

[37] Collins, R. J., Donaldson, R. J., Dunjko, V., Wallden, P., Clarke, P. J., Andersson, E., Jeffers, J., and Buller, G. S., "Realization of Quantum Digital Signatures without the Requirement of Quantum Memory," *Physical Review Letters* **113**(4), 040502 (2014).
[38] Barnett, S. M., [*Quantum Information*], Oxford University Press, Oxford, United Kingdom, first ed. (2009).
[39] Bandyopadhyay, S., Jain, R., Oppenheim, J., and Perry, C., "Conclusive exclusion of quantum states," *Physical Review A* **89**(2), 022336 (2014).
[40] Marand, C. and Townsend, P. D., "Quantum key distribution over distances as long as 30km," *Optics Letters* **20**(16), 1695–1697 (1995).
[41] Wallden, P., Dunjko, V., Kent, A., and Andersson, E., "Quantum digital signatures with quantum-key-distribution components," *Physical Review A* **89**(4), 042304 (2015).
[42] Shenoy-Hejamadi, A., Pathak, A., and Radhakrishna, S., "Quantum Cryptography: Key Distribution and Beyond," *Quanta* **6**(1), 1–47 (2017).
[43] Donaldson, R. J., Collins, R. J., Kleczkowska, K., Amiri, R., Wallden, P., Dunjko, V., Jeffers, J., Andersson, E., and Buller, G. S., "Experimental demonstration of kilometer-range quantum digital signatures," *Physical Review A* **93**(1), 012329 (2016).
[44] Collins, R. J., Amiri, R., Fujiwara, M., Honjo, T., Shimizu, K., Tamaki, K., Takeoka, M., Andersson, E., Buller, G. S., and Sasaki, M., "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**(21), 4883 (2016).
[45] Sasaki, M., Fujiwara, M., Ishizuka, H., Klaus, W., Wakui, K., Takeoka, M., Miki, S., Yamashita, T., Wang, Z., Tanaka, A., Yoshino, K., Nambu, Y., Takahashi, S., Tajima, A., Tomita, A., Domeki, T., Hasegawa, T., Sakai, Y., Kobayashi, H., Asai, T., Shimizu, K., Tokura, T., Tsurumaru, T., Matsui, M., Honjo, T., Tamaki, K., Takesue, H., Tokura, Y., Dynes, J. F., Dixon, A. R., Sharpe, A. W., Yuan, Z. L., Shields, A. J., Uchikoga, S., Legré, M., Robyr, S., Trinkler, P., Monat, L., Page, J.-B., Ribordy, G., Poppe, A., Allacher, A., Maurhart, O., Länger, T., Peev, M., and Zeilinger, A., "Field test of quantum key distribution in the Tokyo QKD Network.," *Optics Express* **19**(11), 10387–10409 (2011).
[46] Shimizu, K., Honjo, T., Fujiwara, M., Ito, T., Tamaki, K., Miki, S., Yamashita, T., Terai, H., Wang, Z., and Sasaki, M., "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**(1), 141–151 (2014).
[47] Collins, R. J., Amiri, R., Fujiwara, M., Honjo, T., Shimizu, K., Tamaki, K., Takeoka, M., Sasaki, M., Andersson, E., and Buller, G. S., "Experimental demonstration of quantum digital signatures over 43 dB channel loss using differential phase shift quantum key distribution," *Scientific Reports* **7**, 3235 (2017).
[48] Inoue, K., Waks, E., and Yamamoto, Y., "Differential Phase Shift Quantum Key Distribution," *Physical Review Letters* **89**(3), 037902 (2002).
[49] Miki, S., Yamashita, T., Fujiwara, M., Sasaki, M., and Wang, Z., "Multichannel SNSPD system with high detection efficiency at telecommunication wavelength.," *Optics letters* **35**(13), 2133–2135 (2010).
[50] IEEE Computer Society, "IEEE Std 802.3-2015: IEEE Standard for Ethernet," (2015).
[51] Croal, C., Peuntinger, C., Heim, B., Khan, I., Marquardt, C., Leuchs, G., Wallden, P., Andersson, E., and Korolkova, N., "Free-Space Quantum Signatures Using Heterodyne Measurements," *Physical Review Letters* **117**(10), 100503 (2016).
[52] Vasylyev, D., Semenov, A. A., Vogel, W., Günthner, K., Thurn, A., Bayraktar, Ö., and Marquardt, C., "Free-space quantum links under diverse weather conditions," *Physical Review A* **96**(4), 043856 (2017).
[53] García-Martínez, M. J., Denisenko, N., Soto, D., Arroyo, D., Orue, A. B., and Fernandez, V., "High-speed free-space quantum key distribution system for urban daylight applications.," *Applied Optics* **52**(14), 3311–7 (2013).
[54] Pugh, C. J., Kaiser, S., Bourgoin, J.-P., Jin, J., Sultana, N., Agne, S., Anisimova, E., Makarov, V., Choi, E., Higgins, B. L., and Jennewein, T., "Airborne demonstration of a quantum key distribution receiver payload," *Quantum Science and Technology* **2**(2), 024009 (2017).
[55] Yin, J., Cao, Y., Li, Y.-H., Ren, J.-G., Liao, S.-K., Zhang, L., Cai, W.-Q., Liu, W.-Y., Li, B., Dai, H., Li, M., Huang, Y.-M., Deng, L., Li, L., Zhang, Q., Liu, N.-L., Chen, Y.-A., Lu, C.-Y., Shu, R., Peng, C.-Z., Wang, J.-Y., and Pan, J.-W., "Satellite-to-Ground Entanglement-Based Quantum Key Distribution," *Physical Review Letters* **119**(20), 200501 (2017).

[56] Lorenz, S., Korolkova, N., and Leuchs, G., "Continuous-variable quantum key distribution using polarization encoding and post selection," *Applied Physics B* **79**(3), 273–277 (2004).

[57] Leverrier, A. and Grangier, P., "Unconditional Security Proof of Long-Distance Continuous-Variable Quantum Key Distribution with Discrete Modulation," *Physical Review Letters* **102**(18), 180504 (2009).

[58] Laudenbach, F., Pacher, C., Fung, C.-H. F., Poppe, A., Peev, M., Schrenk, B., Hentschel, M., Walther, P., and Hübel, H., "Continuous-Variable Quantum Key Distribution with Gaussian Modulation-The Theory of Practical Implementations," *Advanced Quantum Technologies* , 1800011 (2018).

[59] Kahn, J., "1 Gbit/s PSK homodyne transmission system using phase-locked semiconductor lasers," *IEEE Photonics Technology Letters* **1**(10), 340–342 (1989).

[60] Lo, H.-K., Curty, M., and Qi, B., "Measurement-Device-Independent Quantum Key Distribution," *Physical Review Letters* **108**(13), 130503 (2012).

[61] Puthoor, I. V., Amiri, R., Wallden, P., Curty, M., and Andersson, E., "Measurement-device-independent quantum digital signatures," *Physical Review A* **94**(2), 022328 (2016).

[62] Roberts, G. L., Lucamarini, M., Yuan, Z. L., Dynes, J. F., Comandar, L. C., Sharpe, A. W., Shields, A. J., Curty, M., Puthoor, I. V., and Andersson, E., "Experimental measurement-device-independent quantum digital signatures," *Nature Communications* **8**(1), 1–7 (2017).

[63] Yin, H. L., Wang, W. L., Tang, Y. L., Zhao, Q., Liu, H., Sun, X. X., Zhang, W. J., Li, H., Puthoor, I. V., You, L. X., Andersson, E., Wang, Z., Liu, Y., Jiang, X., Ma, X., Zhang, Q., Curty, M., Chen, T. Y., and Pan, J. W., "Experimental measurement-device-independent quantum digital signatures over a metropolitan network," *Physical Review A* **95**(4), 1–10 (2017).

[64] Tang, Y.-L., Yin, H.-L., Zhao, Q., Liu, H., Sun, X.-X., Huang, M.-Q., Zhang, W.-J., Chen, S.-J., Zhang, L., You, L.-X., Wang, Z., Liu, Y., Lu, C.-Y., Jiang, X., Ma, X., Zhang, Q., Chen, T.-Y., and Pan, J.-W., "Measurement-Device-Independent Quantum Key Distribution over Untrustful Metropolitan Network," *Physical Review X* **6**(1), 011024 (2016).