# Advances in Experimental Quantum Digital Signatures

R.J. Donaldson[1], R.J. Collins[1], K. Kleckowska[1], R. Amiri[1], P. Wallden[2], V. Dunjko[3], E. Andersson[1], J. Jeffers[4], 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. School of Informatics, The University of Edinburgh, Information Forum, 10 Crichton Street, Edinburgh, EH8 9AB, United Kingdom
3. Institute for Quantum Optics and Quantum Information, Austrian Academy of Sciences, Technikerstr. 21A, A-6020 Innsbruck, Austria
4. 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, unambiguous state elimination, unambiguous state discrimination, quantum state elimination

## Extended Abstract

Modern society relies heavily on electronic communications. Digital signature schemes are widely used in electronic communication to guarantee the authenticity and transferability of messages. Transferability means that a signed message is unlikely to be 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. Signature schemes are different from encryption schemes, but no less important. 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. In other words, security is only computational. On the other hand, the digital signature schemes are efficient and easy to use.

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 currently proposed such schemes require additional resources such as an authenticated broadcast channel or a trusted third party. Quantum signature schemes is another possible solution. Here, security relies on the laws of quantum mechanics, similar to how the security of quantum key distribution is guaranteed.

Quantum key distribution, which aims to generate a shared secret key for the encryption of messages, is a commercially available technology that makes use of quantum mechanics to ensure that any eavesdropping attempt can be detected. A recently proposed protocol for quantum digital signatures uses only the same components as quantum key distribution, making this a viable quantum signature scheme. Ideal protocols are often phrased in terms of single photons. Although there have been significant advances in the field of single-photon generation, it still remains significantly easier to generate a low-photon number coherent state by attenuating the optical output of a pulsed laser. Both quantum key distribution and quantum digital signatures can use such weak coherent states instead of single photons. In quantum digital signature schemes, many pulses are used to sign an individual binary digit, in much the same way as several coherent states or single qubits are transmitted in quantum key distribution in order to generate a single shared secret bit. Also, as in quantum key distribution, the average photon number of the coherent states in quantum digital signature schemes should be selected low enough so that a malicious party cannot gain too much information about the state that was sent.

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. The sender randomly selects coherent states with different phases and affixed 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 QDS protocols is beyond the scope of this work but may be found in [1-4].

Initial designs [1], such as that shown in Figure 1, used a multiport consisting of four 50/50 beamsplitters to symmetrize the signature states sent by Alice to Bob and Charlie. At each receiver the signature from Alice is split into two components with equal amplitude, and one of these is shared with the other receiver, who performs the same action on their copy of the signature. The retained component of the signature is then mixed on a beamsplitter with the component transmitted from the other receiver. It can be seen that if the two components are the same then the original signature will be recovered through one port of the beamsplitter and a vacuum state $|0\rangle$ will be generated at the other. No matter what the input state sent by Alice is, the output of the multiport is a symmetrization of the input state. This provides transferability of the signature, since it means that Bob and Charlie will obtain the same measurement statistics.

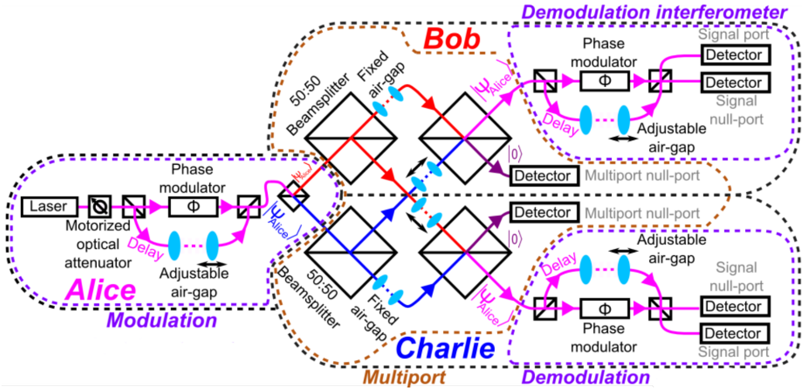

*Figure 1. A schematic of the fiber-based experimental demonstration of quantum digital signatures. VCSEL is a vertical cavity surface emitting laser and SPAD is a single-photon avalanche diode. An honest Alice should send the same signature to Bob and Charlie, but this setup can be modified to test situation where different signatures are sent to different parties in a simple attempt for Alice to be dishonest.*

Alice encodes the coherent state using a phase modulator in one arm of the system while an unmodulated phase reference is provided by a second arm that introduces a delay of duration half the inter-pulse period. This means that the input to the multiport is a time-multiplexed sequence of pairs of pulses consisting of a phase-modulated signal followed by the corresponding unmodulated phase reference. At the receivers, the signal is delayed by half the inter-pulse period, while the phase of the reference is modulated so that both delayed signal and modulated reference arrive at the final beamsplitter at the same time and interfere. Adjustable air-gaps allow for compensation of any small optical-path-length drift in the system.

To be practically usefully, the protocol realized with the setup shown in Figure 1 would also require long-term quantum memory between the multiport and the receivers' demodulation systems. In a practical system, there will be a considerable delay (weeks, months) between signature distribution and sending a signed message. The system shown in Figure 1 required immediate transmission of the signed message following the signature, as long-term quantum memory is impractical with current technology.

The quantum memory requirement was removed in the system shown in Figure 2 and described in more detail in [2]. In this approach each receiver has two of the demodulation systems of Figure 1 without the phase modulator, but they are set to induce a particular fixed phase difference between signal and reference at the final beamsplitter. While it may initially seem intuitively logical to perform unambiguous quantum state discrimination on the received signals to unambiguously determine which of the phases was selected by Alice, this is inefficient and results in an extremely low transmission rate. Far better is to employ unambiguous state elimination, as described in [3], where the receiver can gain full correct information about the phase but is also usually able to unambiguously eliminate certain possibilities.

Both of the experimental systems shown in Figure 1 and Figure 2 still employ the multiport to symmetrize the states Alice sends to Bob and Charlie in order to provide transferability. The multiport is a high-loss component and it can be difficult to stabilize the relative optical path-lengths during operation of the system. Revised protocols exist that remove the requirement for the multiport (see, for example [4]) and these are the next logical candidates for experimental examination.

To conclude, quantum digital signatures is an exciting emerging application of quantum mechanics to digital security that offers the prospect of many more progressive developments in future.

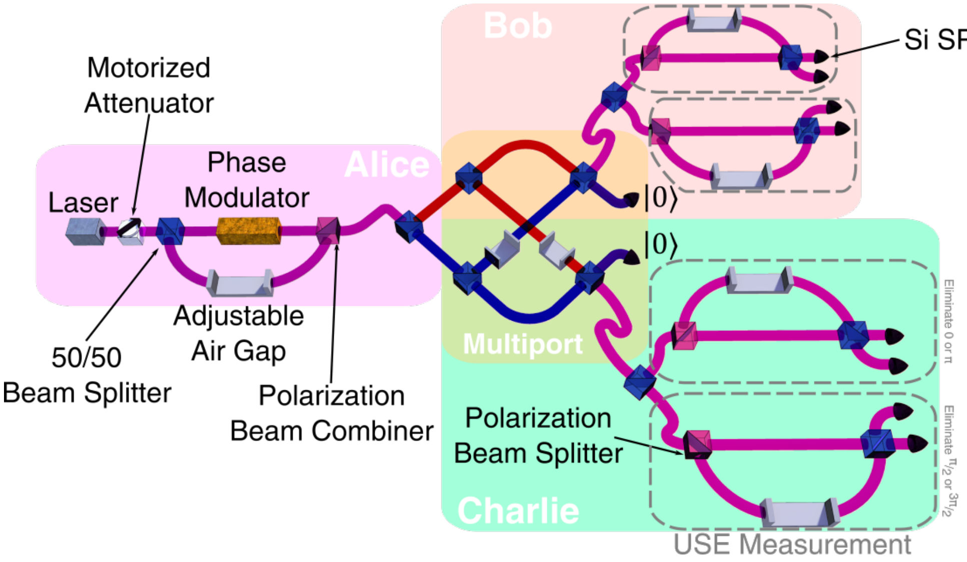

*Figure 2. A schematic of the fiber-based experimental demonstration of quantum digital signatures without the requirement for quantum memory. This system uses four phase encodings. USE is unambiguous state elimination.*

[1] P.J. Clarke, R.J. Collins, V. Dunjko, E. Andersson, J. Jeffers, G.S. Buller, Nature Communications **3**,1174 (2012).

[2] R. Collins, R.J. Donaldson, V. Dunjko, P. Wallden, P.J. Clarke, E. Andersson, J. Jeffers, G.S. Buller, Physical Review Letters, **113**(4), 040502 (2014).

[3] V. Dunjko, P. Wallden, E. Andersson, Physical Review Letters, **112**(4), 040502 (2014).

[4] P. Wallden, V. Dunjko, A. Kent, E. Andersson, Physical Review A, **89**(4), 042304 (2015).