Experimental Demonstration of Quantum Digital Signatures

Patrick J. Clarke[1], **Robert J. Collins**[1], **Vedran Dunjko**[1], **Erika Andersson**[1], **John Jeffers**[2], **Gerald S. Buller**[1]

[1]*SUPA, School of Engineering and Physical Sciences, David Brewster Building, Heriot Watt University, Edinburgh, EH14 4AS, UK*
[2]*SUPA, Department of Physics, John Anderson Building, University of Strathclyde, 107 Rottenrow, Glasgow, G4 0NG, UK*

Some information transfer and processing tasks can be performed better by exploiting quantum effects. Ideally, the security foundations of protocols realizing these tasks can be upgraded from the conjectured difficulty of certain mathematical problems to information-theoretic grounds and the principles of quantum mechanics. A prime example is Quantum Key Distribution, which has been extensively studied for amost 30 years. Here we report an experimental demonstration of Quantum Digital Signatures (QDS) [1], the quantum answer to the task of the distribution and authentication of digital signatures.

In all message verification schemes the security is based on an asymmetry of specific knowledge, reserved to the honest sender alone. In QDS, this knowledge is the classical description of quantum states ('quantum signatures') which are distributed to recipients. The message authentication is performed by checking whether the later disclosed classical descriptions match initially distributed quantum signatures.

We have constructed an experimental system which permits sharing of quantum digital signatures [2], and subsequent message authentication. The quantum signatures comprise a sequence of coherent states, the phase of which is known to the sender Alice alone.

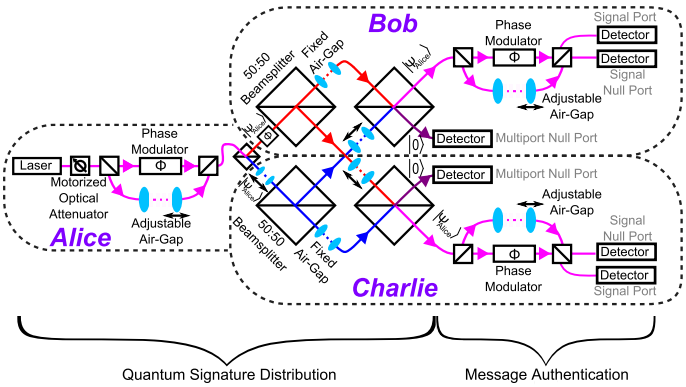

Figure 1: Fibre-based experimental demonstration of quantum digital signatures. Sender Alice generates time multiplexed phase signal and reference coherent pulses, split into recipients Bob's and Charlie's copies of quantum signatures. The quantum signatures are compared using a multiport, the four linked central balanced beam splitters. The comparison is required for security against message refutation. Finally, the signatures are validated in the Message Authentication component.

The QDS protocol ensures security against forging - no message devised by an unauthorised sender will be authenticated by the recipients, and against refutation - a message accepted by one recipient will also be accepted by all others. We have also performed a security analysis of our system. In the analysis of security against forging we show the desired exponential decay of successful forging probabilities in terms of the signature length L. For security against refutation the successful refutation probability also decays exponentially quickly in L, but depends on the imperfections of our experimental realisation. An upper bound of overall security of our system is dominated by the forging probability.

References

[1] D. Gottesman and I. Chuang, arXiv:quant-ph/0105032v2, 2001.
[2] E. Andersson, M. Curty, and I. Jex, Phys. Rev. A **74**, 022304, Aug 2006.