Theoretical model of an experimental quantum digital signature system

Klaudia Kleczkowska[1], John Jeffers[2], Robert J. Collins[1], and Gerald S. Buller[1]

[1]*SUPA, Institute of Photonics and Quantum Sciences, School of Engineering and Physical Sciences, David Brewster Building, Heriot-Watt University, Edinburgh, EH14 4AS, United Kingdom*
[2]*SUPA, Department of Physics, University of Strathclyde, John Anderson Building, 107 Rotten Row, Glasgow, G4 0NG, United Kingdom*

We present a theoretical model of a quantum digital signatures experiment. Our model suggests that further improvements and refinements of the experimental system design are required to optimize the protocol. Small physical imperfections in the experimental system can significantly affect the results. This detailed theoretical model has been developed both to determine the main causes of error in present experimental implementations and indicate possible solutions.

Quantum digital signatures (QDS) are a protocol which allows for unconditionally secure authentication and verification of the communication (messages) between sender and receiver. Quantum digital signatures are a potential quantum equivalent of classical digital signatures, which are mathematical constructs used to demonstrate that the transmitted digital message is authentic ie. that the message was not altered in transit and came from a known source[1, 2]. They provide non-repudiation, so that the sender cannot deny that they are the source of a message, and integrity, which guarantees that nobody tampered with the transmitted data. In particular, we require from the signature scheme, that recipient can check, without contacting another recipient, whether a message would likely be accepted as authentic by that other recipient. The first recipient can also ensure that the probability of acceptance is high.The security of classical digital signatures is based on the the present mathematical complexity of so called "trap-door one way functions", which are currently understood to be computationally difficult to invert without prior knowledge. The most known classical digital signature schemes are RSA[3], DES[4] and ECDSA algorithm[5]. In the case of QDS, the security of the protocol is based on laws of physics which offer unconditional security independent of technical advances in computer science. As opposed to QDS, security in classical signatures depends on the time needed to compute the inverse of the functions they are based on. The development of better algorithms for solving the problems on which trap-door functions are based, or ongoing development and construction of much faster or significantly different (ie. quantum) computers, might make most of the currently used classical schemes insecure. The protocol outlined by Andersson *et al.*[6] uses non-orthogonal coherent states as a communications medium, which cannot be perfectly distinguished from each other during measurement. The first experimental demonstration of a QDS protocol was successfully realized by Clarke *et al.*[7], and subsequently developed further by the same researchers[8, 9, 10]. This approach used phase encoded coherent states selected from a set of four states: $|\alpha\rangle$, $|\exp(i\frac{\pi}{2})\alpha\rangle$, $|\exp(i\pi)\alpha\rangle$ and $|\exp(i\frac{3\pi}{2})\alpha\rangle$.

Current experimental demonstrations of QDS systems typically take of the order of three hours to generate a signature with sufficient security, taken to be a probability of 0.01% of the protocol failing to secure a message. There is, therefore, a requirement for further improvements of the design of the experimental system. Misrouting of photons due to imperfections in the optics or imbalances introduced by differing losses in different optical paths negatively impact on the probability of the signature being authenticated and verified, in case of all parties being honest and therefore increases the length of time taken to generate the signature with sufficient security.

To highlight possible paths to improvements in the current experimental set-up, a detailed theoretical model of the entire system, including system imperfections and loss has been developed. Construction of this model has allowed us to predict the performance of the experimental system under different operating parameters, and offered guidance on routes to enhance it to a level which will offer faster operation - significantly enhancing the practicality of experimental implementations of such QDS schemes.

The behavior of the system is non-trivial, and its performance cannot be predicted with high accuracy. To explain these irregularities, a theoretical model of the optical elements and associated imperfections was developed. This computer simulation allowed us to gain an insight into the potential operation of the experimental optical system under different conditions. Our theoretical model includes non-perfect coherent state generation, and test the correlation between offset of states and asymmetry in

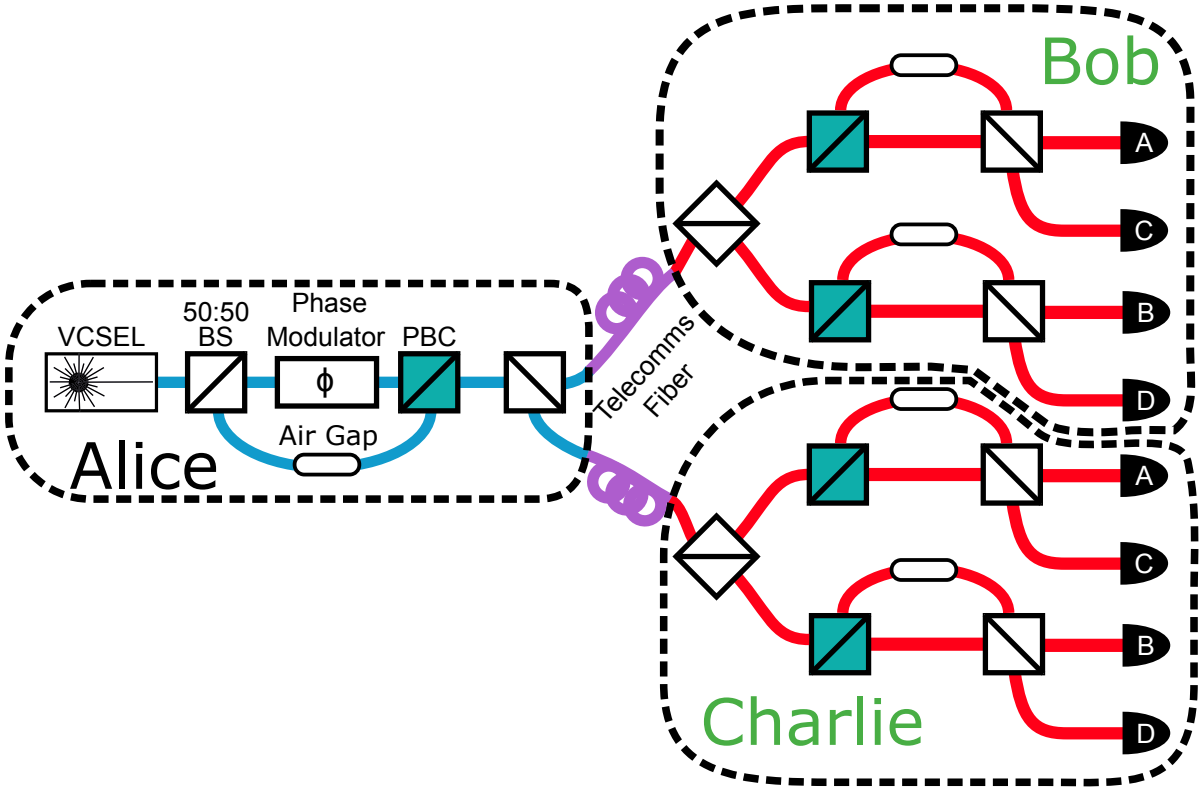

Figure 1: Schematic for the experimental QDS set-up. Alice sends phase-encoded states to receivers Bob and Charlie. Letters A, B, C and D mark detectors accordingly such that A is $D_{event}(\neg 0)$, B is $D_{event}(\neg\frac{\pi}{2})$, C is $D_{event}(\neg\pi)$ and D is $D_{event}(\neg\frac{3\pi}{2})$.

cost matrices. The simulation models asymmetric and lossy beam splitters, and takes into account loss in fiber and loss on fiber couplers.

The successful experimental realization of the latest QDS protocol strongly depends on quality of the results of the unambiguous state elimination (USE) measurement that lies at the heart of the approach [8]. In the simpler unambiguous state discrimination (USD) protocol, we try to determine exactly which state was transmitted by the sender, and to do so with high certainty we need to rule out all of the other states. At low photon numbers per pulse this leads to a significant number of partial records (where only some of the alternatives were ruled out) being discarded. USE, on the other hand, uses this previously discarded partial information to eliminate some of the states as possible candidates for the transmitted state. It is perhaps obvious that the USE approach will have a higher success probability than the standard USD measurement.

An example of a USE measurement result is shown in table 1, where columns correspond to sent coherent states $|exp(i\theta)\alpha\rangle$, and rows corresponds to the detectors $D_{event}(\neg\theta)$ (where $\neg$ denotes negation or "not" and θ is the phase angle).

Tables of counts from USE measurements, such as are shown in table 1, can be used to provide sets of numbers called cost matrices. It is convenient to use these cost matrices to determine the transmitted information in a QDS system. In a real QDS experiment we observe irregularities that affect the overall performance of the system and these are reflected in asymmetry in the cost matrix.

Apparent asymmetry in these tables restricts choices for the thresholds of authentication and verification.Threshold of authentication provides bounds on the percentage of signature length that can contain errors in the case of receiving signature straight from the source, and threshold of verification [8], which is a percentage of signature length allowed to have errors in case of forwarding the message from one recipient to another, to be within smaller interval. This makes the probability of the successful authentication and verification of the message smaller when all parties are honest.

The theoretical simulation model was created using the "Quantum Toolbox in Python" (QuTiP)[11], and was supported by detailed numerical analysis of experimental results performed in MatLab [12]. The simulation provides us with information on how the entries of the cost-matrix are affected by imperfect state generation, and how the imbalance in loss in the system disturbs the terms. It has allowed us

		Alice Sends $\|exp(i\theta)\alpha\rangle$			
		0	$\frac{\pi}{2}$	π	$\frac{3\pi}{2}$
Bob Measures	Not 0	0	0.25	0.5	0.25
	Not $\frac{\pi}{2}$	0.25	0	0.25	0.5
	Not π	0.5	0.25	0	0.25
	Not $\frac{3\pi}{2}$	0.25	0.5	0.25	0

		Alice Sends $\|exp(i\theta)\alpha\rangle$			
		0	$\frac{\pi}{2}$	π	$\frac{3\pi}{2}$
Bob Measures	Not0	0.015	0.288	0.487	0.285
	Not $\frac{\pi}{2}$	0.268	0.046	0.298	0.493
	Not π	0.525	0.224	0.004	0.209
	Not $\frac{3\pi}{2}$	0.193	0.443	0.210	0.013

Table 1: a) An example of a theoretical perfect, normalized result of USE measurement. b) Experimentally achieved USE results.

to determine which components give the greatest contribution to the asymmetry in the table of USE measurements. By adjusting the parameters of the components we were able to simulate improvements to the performance of our protocol, hence ensuring its robustness.

Refinements to the theoretical model of this QDS system are still ongoing and the ultimate goals are to identify the experimental elements responsible for lowering cost matrix quality and to offer indicators of potential areas of improvement. This model will also permit examination of other potential implementations while they are still at the planning stage so that they may be sufficiently evaluated before experiments commence.

References

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

[2] O. Goldreich, *Foundations of Cryptography: Volume II Basic Applications*, 1st ed. Cambridge: Cambridge University Press, 2001.

[3] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Communications of the ACM*, vol. 21, no. 2, pp. 120–126, 1978.

[4] E. Biham and A. Shamir, "Differential cryptanalysis of DES-like cryptosystems," *Journal of Cryptology*, vol. 4, no. 1, pp. 3–72, 1991.

[5] D. Johnson and A. Menezes, "The elliptic curve digital signature algorithm (ECDSA)," Certicom Research and University of Waterloo, Tech. Rep., 1999.

[6] E. Andersson, M. Curty, and I. Jex, "Experimentally realizable quantum comparison of coherent states and its applications," *Physical Review A*, vol. 74, no. 2, p. 022304, 2006.

[7] 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*, vol. 3, p. 1174, 2012.

[8] 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*, vol. 113, no. 4, p. 040502, 2014.

[9] V. Dunjko, P. Wallden, and E. Andersson, "Quantum Digital Signatures without quantum memory," *Physical Review Letters*, vol. 112, no. 4, p. 040502, 2014.

[10] P. Wallden, V. Dunjko, A. Kent, and E. Andersson, "Quantum digital signatures with quantum-key-distribution components," *Physical Review A*, vol. 89, no. 4, p. 042304, 2015.

[11] J. Johansson, P. Nation, and F. Nori, "Qutip 2: A python framework for the dynamics of open quantum systems," *Computer Physics Communications*, vol. 184, no. 4, pp. 1234 – 1240, 2013.

[12] Mathworks, "MATLAB 2014b (8.4.0.118713)," Natick, Massachusetts, 2014.