

Practical Authenticated Quantum Teleportation and Anonymous Transmission

Simon Neves¹, Anupama Unnikrishnan²,
Iordanis Kerenidis³, Damian Markham¹, and Eleni Diamanti¹

¹ LIP6, CNRS, Sorbonne Université, 75005 Paris, France

² Department of Atomic and Laser Physics, Clarendon Laboratory, University of Oxford, Oxford OX1 3PU, UK

³ IRIF, CNRS, Université Paris Diderot, Sorbonne Paris Cité, 75013 Paris, France

Abstract

In this work, we are interested in the design and implementation of advanced quantum communication protocols in a cryptographic context, in particular of Authenticated Quantum Teleportation and Anonymous Transmission. We present practical protocols for achieving these tasks, which include verification procedures of the initial entangled resource, hence enabling to bound the success probabilities of such protocols. We also discuss progress towards their experimental implementation.

Quantum Teleportation [1] has raised a lot of interest in the past decades, as it ensures long-distance qubit transmission. Combined with multipartite entanglement, it also enables the Anonymous Transmission of a qubit in a network, as was initially described by Christandl and Wehner [3]. Indeed, multipartite entangled states, such as GHZ states, provide anonymous Bell pair distribution between a sender and a receiver, and anonymous broadcast of classical bits; such resources therefore enable Quantum Teleportation while preserving the anonymity of the sender and the receiver.

In this work, we design protocols for practical Quantum Teleportation and Anonymous Transmission, in realistic experimental conditions. We use first the self-testing method [4] in order to authenticate the measurements and Bell pairs in the Quantum Teleportation protocol. In this way, we can derive bounds on the success probability of the teleportation in different settings, namely the one-sided or fully device independent settings.

Furthermore, we build an experimentally accessible Quantum Anonymous Transmission protocol by defining the notion of ε -anonymity: A protocol ensures ε -anonymity if dishonest parties can guess the identity of the sender and/or the receiver with a probability of $\frac{1}{k} + \varepsilon$ at most, where k is the number of honest parties. The protocol ensures perfect anonymity as long as $\varepsilon = 0$. Our protocol combines the Christandl-Wehner protocol with a verification protocol, which tests an untrusted source of GHZ states in the presence of dishonest parties [5]. Using this verification procedure, we can ensure a certain fidelity of the generated states with respect to the expected GHZ state. This allows us to certify the security of our ε -anonymous protocol, where ε is bounded depending on this fidelity.

Finally, we address the central element of our experiments tailored for the implementation of these protocols, namely our source of entangled pairs of photons, which is based on a PPKTP crystal in a Sagnac interferometer. Our source is designed for telecom wavelength emission of the generated pairs and high spectral purity to ensure high quality GHZ-state generation [6], while we also use a temporal multiplexer [7], to increase the protocol repeatability.

- [1] C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W. K. Wootters, *Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels*, Phys. Rev. Lett. **70**, 1895 (1993).
- [2] D. Bouwmeester *et al.*, *Experimental quantum teleportation*, Nature **390**, 575-579 (1997).
- [3] M. Christandl and S. Wehner, *Quantum Anonymous Transmissions*, Advances in Cryptology - ASIACRYPT, 217-235 (2005).
- [4] D. Mayers and A. Yao, *Self testing quantum apparatus*, Quantum Information and Computation, vol. **4**, no. **4** (2004).
- [5] W. McCutcheon, A. Pappa, B. A. Bell, A. McMillan, A. Chailloux, T. Lawson, M. Mafu, D. Markham, E. Diamanti, I. Kerenidis, J. G. Rarity, and M. S. Tame, Nature Communication **7**, 13251 (2016).
- [6] R.-B. Jin, R. Shimizu, K. Wakui, H. Benichi, and M. Sasaki, *Widely tunable single photon source with high purity at telecom wavelength*, Optics Express, vol. **21**, no. **9**, 10659 (2013).
- [7] C. Greganti, P Schiаны, I. A. Calafell, L. M. Procopio, L. A. Rozema, and P. Walther, *Tuning single-photon sources for telecom multi-photon experiments*, Optics Express, Vol. **26**, No. **3**, 3286 (2018).