Entanglement Verification in Quantum Recursive Networks with Tampered Nodes

Michele Amoretti[1,3], Stefano Carretta[2,3]

1: Dep. of Engineering and Architecture, University of Parma, Italy
2: Dep. of Mathematical, Physical and Computer Sciences, University of Parma, Italy
3: Quantum Information Science @ University of Parma — http://www.qis.unipr.it
Contact email: michele.amoretti@unipr.it

Abstract – Quantum repeater networks enable the sharing of quantum states between spatially separated systems. More specifically, the quantum recursive network architecture (QRNA) introduced by Van Meter *et al.* [1] supports the creation of entangled quantum states between node pairs, being them directly connected by a quantum channel or separated by multiple hops. Distributed quantum states are used, *e.g.*, in decision algorithms, distributed arithmetic, secure distributed function computation, quantum secret sharing, remote synchronization of clocks.

In this work, we focus on a particularly challenging case of security breach in QRNA-based distributed systems, namely the one where an attacker takes full control of a node and alters the configuration of the local quantum memory, either to make a denial-of-service attack or to reprogram the node. In such a scenario, entanglement verification over quantum memories is a means for detecting the intruder. Several approaches for entanglement verification have been proposed and studied, both analytically and experimentally, considering scenarios that are different from the one described in this work. Usually, the focus is either on untrusted sources of entangled qubits (photons, in most cases) or on eavesdroppers that interfere with the quantum channel while entangled qubits are transmitted. Instead, in this work we assume that the source of entanglement is trusted, but parties may be dishonest.

Looking for efficient entanglement verification protocols that require only classical channels and local quantum operations to work, we thoroughly analyze the one proposed by Nagy and Akl [2], that we denote as NA2010 for simplicity. Then, we propose and analyze two entanglement verification protocols based on teleportation (denoted as AC1 and AC2), characterized by increasing efficiency. Compared to NA2010, our AC1 and AC2 protocols are much more convenient in terms of intrusion detection probability, the sacrificed quantum resources being equal. Remarkably, the success probability p of AC2 is always $\geq 1/2$ and ≤ 1, for any measurement basis the intruder adopts to destroy the entanglement. If the intruder measured in the computational or diagonal basis, $p = 3/4$. Thus, to detect the intruder with high probability, it is necessary to sacrifice only a few qubit pairs.

A full version of this work is available on arXiv [3].

References

[1] R. Van Meter, J. Touch, C. Horsman, *Recursive Quantum Repeater Networks*, Progress in Informatics, no. 8, pp. 65-79 (2011)

[2] N. Nagy, M. Nagy, S. G. Akl, *Quantum security in wireless sensor networks*, Natural Computing, vol. 9, no. 4, pp. 819-830 (2010)
[3] M. Amoretti, S. Carretta, *Entanglement verification protocols for distributed systems based on the Quantum Recursive Network Architecture*, arxiv:1707.02895 (2017)

Acknowledgements
This work is supported by the University of Parma Research Fund - FIL 2016 - Project "NEXTALGO: Efficient Algorithms for Next-Generation Distributed Systems".