Towards Provable Remote Data Deletion Through Quantum Entanglement

Jon Crowcroft
University of Cambridge

Gerard Briscoe
Queen Mary University London

ABSTRACT

A continuing challenge in computing is how to retain control of shared information, given the ease of loss-less copying that is possible. This challenge is becoming increasingly acute as the ease of distributing information continues to grow exponentially. Quantum Computing, which makes use of quantum mechanical phenomena, may offer a solution through the property of *quantum entanglement*. This property occurs when particles interact physically and then become separated, resulting in each of the pair having the same quantum mechanical description (state). So, we could utilise quantum bits (qubits), which are a unit of quantum information and analogous to classical bits, with the property of quantum entanglement to control the distribution of information. Therefore, if two qubits are connected via quantum entanglement [3], the value of one could be controlled by the other so that shared secrets can be destroyed (deleted) remotely. The approach becomes feasible as the number of qubits constructed continues to grow, with a qubyte (composed of eight quantum bits) being constructed in 2005. However, scaling to multiple remote copies would require multiple source copies, because the *quantum-no-deleting principle* implies that the ability to delete can drop exponentially with the number of copies to be deleted [1]. Also, given that quantum entanglement is yet to exceed 144 km [2], the approach would not yet scale globally.

BODY

If we connect two qubits via quantum entanglement, the fate of one can be controlled by the other so shared secrets can be deleted remotely.

REFERENCES

[1] A. K. Pati and S. L. Braunstein. Impossibility of deleting an unknown quantum state. *Nature*, 404(6774):164–165, 2000.

[2] R. Ursin, F. Tiefenbacher, T. Schmitt-Manderbach, H. Weier, T. Scheidl, M. Lindenthal, B. Blauensteiner, T. Jennewein, J. Perdigues, P. Trojek, et al. Entanglement-based quantum communication over 144 km. *Nature Physics*, 3(7):481–486, 2007.

[3] W. K. Wootters. Entanglement of formation of an arbitrary state of two qubits. *Physical Review Letters*, 80(10):2245–2248, 1998.

Volume 2 of Tiny Transactions on Computer Science