# Scalable authentication in a quantum network

Naomi Solomons,[1] Alasdair Fletcher,[2] Stefano Pirandola,[2] Natarajan Venkatachalam,[3]
Djeylan Aktas,[3] Sören Wengerowsky,[4] Martin Lončarić,[5] Sebastian Philipp Neumann,[4]
Bo Liu,[6] Željko Samec,[5] Laurent Kling,[1] John G. Rarity,[3] and Siddarth Koduru Joshi[3]

[1] *Quantum Engineering Technology Labs & Quantum Engineering Centre for Doctoral Training, Centre for Nanoscience and Quantum Information, University of Bristol*
[2] *University of York*
[3] *Quantum Engineering Technology Labs & Department of Electrical and Electronic Engineering, University of Bristol*
[4] *Institute for Quantum Optics and Quantum Information - Vienna (IQOQI) & Vienna Center for Quantum Science and Technology (VCQ), Vienna, Austria*
[5] *Photonics and Quantum Optics Research Unit, Center of Excellence for Advanced Materials and Sensing Devices, Ruđer Bošković Institute, Zagreb, Croatia*
[6] *College of Advanced Interdisciplinary Studies, NUDT, Changsha, China*

The mathematically perfect security of quantum communication comes from the immutable laws of physics but assumes the authentication of all classical communication between any two users, based on pre-shared keys. This is impractical in any large quantum network. We present a linearly scalable method to distribute authentication keys that removes this significant barrier preventing quantum networks from growing. We discuss the implementation of this protocol on an 8-user quantum network test-bed and show how partially and temporarily trusting some nodes for ≈1 min can be used to distribute initial authentication keys between new end users while maximising the security of communications.

**Keywords:** QKD, networks, flooding, authentication

Current quantum key distribution (QKD) protocols include the requirement for classical communication alongside sending qubits, which can be public, but should not be tampered with by a malicious party [1]. This is prevented using an authentication scheme, typically the Wegman-Carter (WC) scheme, which requires that both parties share an initial secret, random key [2, 3]. Although the security of authentication protocols is widely assumed (see for example Ref. [4]), the issue of relying on a classical protocol is considered to be drawback of QKD implementations and was the major flaw addressed in the recent National Cyber Security Centre (NCSC) white paper [5]. Furthermore, the necessity of distributing these initial keys is a significant overhead cost that discourages commercial involvement.

As quantum networks grow, authentication keys between two users could be established via referral from mutually trusted nodes. Typically, when end users choose to use trusted nodes in quantum networks they must then place complete trust in those nodes forever. For long term data security this is neither viable nor practical. We instead focus on the possibility for end users to place partial and/or temporary trust in intermediary nodes in a quantum network (following from work done in [6]). We also consider using multiple paths for authentication key distribution, and the possibility of combining with flooding protocols (such as in [7]) to maximise end-to-end key transmission.

We have shown that using one intermediate trusted node to transfer the initial authentication key does not provide a long term security weakness, assuming that our secure inaugural transfer protocol is followed. We show that $n_k = \frac{(c_a+2)(c_a+1)}{2} + (n - c_a - 2)(c_a + 2)$ initial keys must be distributed in a fully connected network in which $n$ is the number of users, and $c_a$ is a constant based on the estimated capabilities of an adversary that can corrupt multiple nodes. Data from a previous 8-user experiment [8] was used to show that (following the protocol we describe), an intermediate user only needs to be trusted for approximately one minute.

[1] C. Bennett and G. Brassard, Theoretical Computer Science - TCS **560**, 175 (1984).

[2] M. N. Wegman and J. L. Carter, Journal of Computer and System Sciences **22**, 265 (1981).

[3] R. Renner and S. Wolf, in *Advances in Cryptology - EUROCRYPT 2004*, edited by C. Cachin and J. L. Camenisch (Springer Berlin Heidelberg, Berlin, Heidelberg, 2004) pp. 109–125.

[4] H.-K. Lo *et al.*, Nature Photonics **8**, 595–604 (2014).

[5] N. C. S. C., *Quantum security technologies*, Tech. Rep. (2020).

[6] L. Salvail *et al.*, Journal of Computer Security **18**, 61 (2010).

[7] S. Pirandola, Communications Physics **2**, 1 (2019).

[8] S. Koduru Joshi *et al.*, arXiv preprint arXiv:1907.08229 (2019), in press: Science Advances.