Multiparty Quantum Signatures Schemes

Juan Miguel Arrazola,[1] Petros Wallden,[2] and Erika Andersson[3]
[1]*Institute for Quantum Computing, University of Waterloo,*
200 University Avenue West, Waterloo, Ontario, N2L 3G1, Canada
[2]*School of Informatics, University of Edinburgh, 10 Crichton Street, Edinburgh EH8 9AB, UK*
[3]*SUPA, Institute of Photonics and Quantum Sciences,*
Heriot-Watt University, Edinburgh, EH14 4AS, United Kingdom

Digital signatures are important cryptographic building-blocks that are widely used to provide security in electronic communications. They achieve three main cryptographic goals: authentication, non-repudiation, and transferability. These properties make them suitable for securing important tasks such as financial transactions, software updates, and legal contracts. When quantum communication is allowed, it becomes possible to construct signature schemes whose information-theoretic security is based on fundamental principles of quantum mechanics. These are known as quantum signature schemes (QSSs).

Recently, several practical QSS protocols have been reported and experimentally demonstrated [1–4]. Nevertheless, these schemes have not been generalized to more than three participants and their security goals have been only informally defined. Many applications of signature schemes inherently involve more than three participants, since one may need to transfer a message more than once. Moreover, in the multiparty case, one must deal very carefully with the presence of coalitions of adversaries as well as the transferability of messages. This makes it crucial to provide a fully rigorous security framework for quantum signature schemes suitable for multiple participants. Such a security framework has not yet been proposed, and suggestions for corresponding frameworks for classical signature schemes do not directly apply to quantum schemes.

In our work, we accomplish the following main results:

1. We provide detailed and rigorous security definitions for multiparty quantum signature schemes by generalizing the work of Swanson and Stinson [5] to the quantum case and introducing a formal definition of transferability.

2. We prove several properties that QSS protocols must satisfy in order to achieve their security goals. This clarifies the aspects of these protocols that are responsible for their security and provides a valuable tool for the design of new protocols.

3. We generalize a protocol of Wallden et. al [1] to the multiparty case and prove its security against forging, repudiation and non-transferability. **Notably, this protocol can be implemented from any point-to-point QKD network and therefore it is ready to be experimentally demonstrated**.

Our new QSS protocol can be thought of as a classical protocol that requires secret channels between participants, which are then established using quantum key distribution (QKD). This is remarkable because participants could behave dishonestly during the QKD stage, but we prove that this does not affect the security of the protocol. Moreover, this implies that all security proofs related to the quantum communication in the protocol can be completely outsourced to QKD, where a vast literature of security proofs already exists. This is not only helpful in analyzing the security of the protocol, but it also takes care of its practicality: since this protocol can be implemented from any point-to-point QKD network, it is already a practical.

Overall, our results imply that for signature schemes, the situation is analogous to that of secure communication, where a classical protocol—the one time-pad—can guarantee information-theoretic security at the expense of shared secret keys. Quantum communication is then used to establish these secret keys via unsecured quantum channels. Similarly, for signature schemes, there exist a classical protocol—our QSS protocol—that provides information-theoretic security at the expense of shared secret keys, which are established using QKD.

A detailed presentation of our work can be found in Ref. [6].

[1] P. Wallden, V. Dunjko, A. Kent, and E. Andersson, Phys. Rev. A **91**, 042304 (2015).

[2] V. Dunjko, P. Wallden, and E. Andersson, Phys. Rev. Lett. **112**, 040502 (2014).

[3] J. M. Arrazola and N. Lütkenhaus, Phys. Rev. A **90**, 042335 (2014).

[4] R. J. Collins, R. J. Donaldson, V. Dunjko, P. Wallden, P. J. Clarke, E. Andersson, J. Jeffers, and G. S. Buller, Phys. Rev. Lett. **113**, 040502 (2014).

[5] C. M. Swanson and D. R. Stinson, Information Theoretic Security pp. 100–116 (2011).

[6] J. M. Arrazola, P. Wallden, and E. Andersson, arXiv preprint arXiv:1505.07509 (2015).