A NEW SEMI-QUANTUM CONFERENCE KEY AGREEMENT PROTOCOL

R. BARREIRO, W. KRAWEC, P. MATEUS, N. PAUNKOVIĆ, AND A. SOUTO*

Abstract. The constructions of (quantum) secure applications and communications are a reality for the near future Quantum internet. Quantum Key Distribution (QKD) protocols are one of the most studied communication protocols in the literature and despite the existence of theoretical perfectly secure QKD's, these protocols do not scale properly with the number of users. Furthermore, they require that all the parties in the protocol have a quantum device. In this talk I will be presenting a new Semi-Quantum Conference Key Agreements protocol that, on one hand, being quantum, its security does not depend on mathematical hardness assumptions; secondly, is an extension of QKD for several users; and also, being only semi-quantum, i.e., requiring only one of the parties involved in the protocol to be fully quantum and all the others classical, uses less (quantum) expensive resources.

Introduction

The major thread of quantum computing to classical public-key cryptography is due to Shor's algorithm [1]. This algorithm reduced to (quantum probabilistic) polynomial time the difficulty to break cryptographic systems commonly used nowadays like RSA and Elliptic-curve cryptography. Therefore new quantum-resistant communication protocols are being seriously studied for the last decades. Quantum mechanics brought to computer science and especially cryptography a fresh perspective on one can deal with the security and privacy of communications. In particular, the replacement of hardness mathematical assumptions (e.g., factoring a n bit number is not possible with a probabilistic-polynomial time algorithm) by laws of physics to ensure secrecy is the most relevant advantage of using a quantum-based approach to cryptography.

One of the most basic communication protocols aims to achieve a common key between two parties which is called key distribution. Diffie-Hellman protocol [4] (that relies on the hardness of computing the discrete logarithm) is probably the most well-known example of this kind of protocol. Although, Shor's algorithm turns this protocol vulnerable to quantum computers. In 1984, Charles Bennett and Gilles Brassard developed the first-ever QKD, known as, the BB84 protocol [3], following Wiesner's ideas [2] of multiplexing to generate quantum money that could not be copied. It is known that BB84 is secure [5]. However, the QKDs are not suitable for real-world scenarios where users want to establish a common key among all of them since it does not scalable with the number of users.

[*] Speaker

This work was supported by FCT through the Instituto de Telecomunicações research unit under ref. UIDB/EEA/50008/2020 and by the LASIGE research unit under ref. UIDB/00408/2020 and ref. UIDP/00408/2020.

The concept of Quantum Conference Key Agreements (QCKAs) came from the idea of extending QKDs to several users and several direct protocols have been proposed (see [6] for a recent survey). The proposed solutions solve the scalability problem but have the characteristic that the more parties are involved the more quantum resources are needed. To reduce the number of quantum devices necessary and to enable the possibility of seeing the QCKA a quantum service the idea of semi-quantum QKD's [7, 8] and semi-quantum QCKA's [9, 10, 11] was considered in the literature.

Semi-quantum QKD's were introduced by Boyer et. al in 2007 and in this type of protocol the two parties Alice and Bob are, in terms of resources, different. Furthermore, these protocols have the advantage of lower costs for practical implementation. Alice is a fully quantum agent while Bob is limited to being classical having access to a measurement device (much cheaper quantum hardware). Alice prepares quantum states and Bob can either measure and resend the result as a basic quantum state or reflect the state to Alice. The high-level description of our proposal is the following:

(1) *Alice* (quantum entity) prepares a $|GHZ_{N+1}\rangle$ (i.e., an entangled quantum state of $N+1$ particles), where N is the number of *Bobs* (classical entities).
(2) *Alice* sends to each *Bob* a particle of this entangled quantum state through a quantum communication channel and keeps to herself the first one.
(3) Each *Bob*, according to a (small) pre-shared key, will either choose to reflect the undisturbed qubit to *Alice* (`CTRL` operation) or measure the qubit in the computational basis and sends back to her the measurement result as an encoded state prepared in the same classical state found (`SIFT` operation).
(4) The `CTRL` rounds are used for spotting eavesdropping, while the `SIFT` rounds are used to establish the final conference key.

Our proposal has the following characteristics. Having Alice as an interested party to also have a part in the shared key, brings a security advantage as we do not have to deal with the case of having a third party leading the process to be impersonated by an eavesdropper (see [12], for a more comprehensive discussion). Furthermore, it is possible to ensure security assuming that the size of the pre-shared key among all the participants is of the square root order of the new common secret binary string. Therefore, this kind of protocol is sometimes called *conference key extension.*

In this talk we discuss the security of our protocol. The proof of security used a reduction to a One-Way Fully-Quantum Key Distribution protocol a technique developed to prove the security of SQKD (Semi-Quantum Key Distribution) protocols [13]. We also discuss the key rate of our proposal and computed a lower bound for it.

References

[1] Shor, P.: "Algorithms for quantum computation: discrete logarithms and factoring". Proc. 35th Annual Symposium on Found. of Computer Science, pp. 124–134, 1994.

[2] Wiesner, S.: "Conjugate Coding". SIGACT News, vol. 15, pp. 78–88, 1983.

[3] Bennett, C., Brassard, G.: "Quantum cryptography: Public key distribution and coin tossing". Theoretical Computer Science, vol. 560, pp. 7–11, 1984.

[4] Diffie, W.; Hellman, M. . CiteSeerX 10.1.1.37.9720. New Directions in Cryptography. *IEEE Transactions on Information Theory. 22 (6): 644–654, 1976*

[5] Shor, P. and Preskill, J. Simple Proof of Security of the BB84 Quantum Key Distribution Protocol, Phys. Rev. Lett. 85 (2): 441–444, American Physical Society, 2000

[6] Murta, G., Grasselli, F., Kampermann, H., Bruß, D.: "Quantum Conference Key Agreement: A Review". Advanced Quantum Technologies, vol. 3 (11), 2020.

[7] Boyer, M., Kenigsberg, D., Mor, T.: "Quantum Key Distribution with Classical Bob". Phys. Rev., vol. 99, 2007.

[8] Lu, H., Cai, Q.: "Quantum key distribution with classical Alice". Int. Journal of Quantum Information, vol. 6, pp. 1195 – 1202, 2008.

[9] Xian-Zhou, Z., Wei-Gui, G., Yong-Gang, T., Zhen-Zhong, R., Tian, G.: "Quantum key distribution series network protocol with m-classical Bobs". Chinese Phys. B., vol. 18, 2009.

[10] Zhu, K., Zhou, N., Wang, Y., Wen, X.: "Semi-quantum key distribution protocols with ghz states". Int. Journal of Theoretical Phys., vol. 57, pp. 3621 – 3631, 2018.

[11] Zhou, N., Zhu, K., Zou, X.: "Multi-party semi-quantum key distribution protocol with four-particle cluster states". Annalen der Physik, 2019.

[12] Massa, F., Yadav, P., Moqanaki, A., Krawec, W. O., Mateus, P., Paunković, et al.: "Experimental Quantum Cryptography With Classical Users", 2019.

[13] Iqbal, H. and Krawec, W. High-Dimensional Semi-Quantum Cryptography, arXiv:1901.01611, arXiv.org perpetual, non-exclusive license, 2019

Rúben Barreiro; Universidade Nova Lisboa
Email address: r.barreiro@campus.fct.unl.pt

Walter O. Krawec; University of Connecticut
Email address: walter.krawec@uconn.edu

Paulo Mateus; Instituto Superior Técnico, Universidade de Lisboa and Instituto de Telecomunicações
Email address: pmat@math.ist.utl.pt

Nikola Paunković; Instituto Superior Técnico, Universidade de Lisboa and Instituto de Telecomunicações
Email address: npaunkov@math.ist.utl.pt

André Souto; Faculdade de Ciências, Universidade de Lisboa and LASIGE and Instituto de Telecomunicações...
Email address: ansouto@fc.ul.pt