GROUP KEY EXCHANGE IN THE QUANTUM ERA

MARÍA ISABEL GONZÁLEZ VASCO, ÁNGEL LUIS PÉREZ DEL POZO, AND RAINER STEINWANDT

Abstract. In cryptography, key establishment protocols are often the starting point paving the way towards secure execution of different tasks. Namely, the parties seeking to achieve some cryptographic task, often start by establishing a common high-entropy secret that will eventually be used to secure their communication. In this talk, we will discuss a protocol we proposed in [?], which has been further implemented and tested in the context of our project *Secure Communication in the Quantum Era*. In particular, in our work we focus on the so-called *quantum-future* scenario (as defined by [?]), at which we consider adversaries that may execute efficient quantum algorithms, yet only once the execution of the protocol has concluded. For the case of GAKE this captures a situation in which keys are to be established in the present, while security guarantees must still be provided in the future when quantum resources may be accessible to a potential adversary. Our proposal uses password authentication and builds upon efficient and reasonably well understood primitives: a message authentication code and a post-quantum key encapsulation mechanism. In particular, one could use as building block any of the key encapsulation mechanisms that are currently considered for standarization (namely, Kyber, NTRU, Saber —lattice based– and Classic McEliece – code based). The hybrid structure dodges potential efficiency downsides, like large signatures, of some "true" post-quantum authentication techniques, making our protocol a potentially interesting fit for current applications with long-term security needs.

References

[1] , M. I. González Vasco and A. L. Pérez del Pozo and R. Steinwandt, Group Key Establishment in a Quantum-Future Scenario, *Informatica*, 31, 4 (2020), 751–768, https://doi.org/10.15388/20-INFOR427.

[2] N. Bindel, J. Brendel, M. Fischlin, B. Goncalves, D. Stebila. Hybrid Key Encapsulation Mechanisms and Authenticated Key Exchange *Post-Quantum Cryptography. PQCrypto 2019*, Lecture Notes in Computer Science, vol 11505, (2019), 206–226, https://doi.org/10.1007/978-3-030-25510-712.

[3] Author's name as it appears. Title of article. *Shortened Journal Title*, Volume Number, issue number, (Year of publication), page range, DOI.

María Isabel González Vasco, Ángel Luis Pérez del Pozo; MACIMTE - Universidad Rey Juan Carlos

Email address: {mariaisabel.vasco, angel.perez}@urjc.es

Rainer Steinwandt; College of Science, University of Alabama in Huntsville

Email address: rs0141@uah.edu

The first two authors have been partially supported by MINECO Grant CREEME - PID2019- 109379RB-100. All authors have been partially supported by NATO Science for Peace and Security Programme, Grant G5448.

The talk at the 8IMM 2022 has been given by the first author.