1176-94-317 **Rainer Steinwandt*** (rs0141@uah.edu), University of Alabama in Huntsville, College of Science, 301 Sparkman Drive, Huntsville, AL 35899. *Group key establishment in transition to a post-quantum scenario.*

This presentation discusses a (password-authenticated) group-key establishment protocol that we explored within a NATO Science for Peace and Security Programme project. The protocol is designed for a *quantum-future* scenario, i.e., we assume that the adversary does not have access to a large-scale quantum computer during the protocol execution. However, the secrecy of an established session key remains guaranteed even if the adversary can perform large-scale quantum computations in the future. This scenario enables an efficient 2-round solution combining a Diffie-Hellman-based design with a post-quantum key encapsulation mechanism.

The presentation is based on joint work with M. I. González Vasco and Á. L. Pérez del Pozo, and this work has been supported by NATO SPS through project G5448. (Received January 25, 2022)