1163-94-441 **María Isabel González Vasco**, **Ángel Pérez del Pozo**, **Rainer Steinwandt*** (rsteinwa@fau.edu) and **Adriana Suárez Corona**. *Password-Authenticated Key Establishment in the Advent of Scalable Quantum Computing.*

To address the impact of large-scale quantum computing, new designs for cryptographic key establishment protocols now commonly integrate tools from post-quantum cryptography. A standard approach is to rely entirely on cryptographic tools, e.g., post-quantum signatures, for which no efficient quantum cryptanalytic attacks are known.

Available quantum resource estimates to implement, e.g., Shor's algorithm, suggest that quantum cryptanalytic attacks are not an imminent threat yet, and this talk focuses on a *quantum future* scenario. Here, an adversary is restricted to classical computation during (today's) protocol execution, but can leverage quantum computing after the protocol execution has ended (in the future). Such a security model opens up the possibility to *temporarily* rely on established hardness assumptions, even if in the long-term a quantum cryptanalytic attack becomes feasible. The talk shows how password-authenticated (group) key establishment can be realized efficiently in such a setting.

This presentation is based on work supported by NATO SPS project G5448 and by NSA Grant Number H98230-20-1-0295. (Received September 07, 2020)