Title: Overview of Post-Quantum Hash-Based Signature Schemes

Speaker: Nathan Manohar, Research Scientist, IBM Research

Abstract:

In this talk, I will overview post-quantum hash-based signature schemes in the recently announced CNSA Suite 2.0 for firmware and software signing. These schemes are stateful, meaning that the signer must maintain a state, and proper state management is required for security. I will also overview SPHINCS+, a stateless post-quantum hash-based signature scheme recently recommended for standardization by NIST that extends the previous schemes.

Bio: