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:
Nathan Manohar is a Research Scientist in Cryptography, Security, and Privacy and a member of the Cryptography Research Group at the IBM T.J. Watson Research Center. His main research interests are cryptography, computer security, and, more broadly, theoretical computer science. He recently received his PhD in Computer Science from UCLA, where he was advised by Amit Sahai. Previously, he received a bachelor's degree in Computer Science and Mathematics and a master's degree in Computer Science from Harvard University in 2016.