Title

Stateful Hash-based Signatures: From Theory to Practice

Abstract

In this talk I will present a theoretical as well as a practical understanding of the standardized stateful hash-based signatures. RSA and ECC public key cryptographic algorithms formed the basis of digital signatures. However, their security was undermined with the advent of quantum computers. Consequently, Commercial National Security Algorithm (CNSA) Suite 2.0 replaced RSA and ECC-based digital signatures with hash-based signatures such as eXtended Merkle Signature Scheme (XMSS) and Leighton Micali Signature (LMS). These HBS schemes are stateful thus requiring the signer to maintain a state. The construction of these schemes and recommended parameters by NIST will also be covered in this talk.

Bio

Dr. Nimisha Limaye is a Staff Engineer in the Security IP R&D team within the Solutions Group at Synopsys, where she applies her expertise in hardware security. She joined Synopsys in July 2022, following the completion of her Doctorate in Electrical Engineering from the Tandon School of Engineering at New York University. Dr. Limaye has co-authored over 20 technical papers across esteemed conferences and journals, and her thesis work has been seamlessly integrated into Synopsys tools, demonstrating her practical impact in the field. Moreover, Dr. Limaye has played pivotal roles in organizing and judging various cyber security competitions, including NYU CSAW, HeLLO-CTF, and ICCAD CADAthlon.