EHTv3 and EHTv4: On-ramp Digital Signature Candidates for the NIST PQC Standardization Process

...
Martin Feussner and Igor Semaev
University of Bergen
...

Abstract

This seminar delves into EHTv3 and EHTv4, digital signature schemes that were submitted to the additional round of the NIST Post-Quantum Cryptography (PQC) standardization process. It outlines the schemes' design rationales, providing some intuition on how the components come together to establish the protocols. The discussion extends to a general overview of the key generation, signature generation, and verification protocols. Furthermore, a comparative analysis with other leading submissions in the NIST PQC initiative is provided, focusing on performance metrics and storage requirements. The presentation concludes by identifying areas for further research and potential improvements in the future work of these schemes.