Short Cycles in Quasi-Cyclic Code-Based Cryptosystems

Emily McMillon

Rice University, USA

Bit Flipping Key Encapsulation (BIKE) is a code-based cryptosystem based on quasi-cyclic moderate density parity-check (QC-MDPC) codes paired with an iterative decoder. A major issue preventing adoption of this standard is that decoding failures have been demonstrated to lead to an attack that recovers the BIKE private key. The decoder failure rate of these codes is difficult to determine, as their capabilities are governed by the code's graphical representation as opposed to traditional, more well-understood code parameters. In this talk, I will highlight the connection between short cycles in the Tanner graph corresponding to private keys and higher decoder failure rates. I will discuss possible design and weak key filter strategies to alleviate some decoder failures.

In Special Session 55 on Post-Quantum Cryptography at the Mathematical Congress of the Americas 2025.

MCA 2025 internal code: SS55-T11