From: Daniel Apon <dapon.crypto@gmail.com> via pqc-forum@list.nist.gov
To: pqc-forum <pqc-forum@list.nist.gov>
Subject: [pqc-forum] A new Rowhammer attack on Frodo
Date: Monday, July 25, 2022 12:50:11 PM ET

Dear PQC Researchers,

We'd like to announce our recent paper (https://eprint.iacr.org/2022/952.pdf), "When Frodo Flips: End-to-End Key Recovery on FrodoKEM via Rowhammer."

In this work, we experimentally recover the private key material of FrodoKEM by using Rowhammer to flip bits during the key generation process, followed by a tailored decryption failure attack.

We are happy to answer scientific questions about our work in this thread.

Best regards,
The FrodoFlips team

--