From: Apon, Daniel C. (Fed)
To: Lichtinger, Jacob T. (Fed)
Subject: Sub-review request (PKC 2022)
Date: Saturday, September 25, 2021 1:01:05 AM
Importance: High

Hi Jacob,

Would be willing to sub-review this paper for me?

Sub-review deadline: Monday, October 18

Title: Multitarget decryption failure attacks and their application to Saber and Kyber

Abstract:
Many lattice-based encryption schemes are subject to a very small probability of decryption failures. It has been shown that an adversary can efficiently recover the secret key using a number of ciphertexts that cause such a decryption failure. In PKC 2019, D'Anvers et al. introduced 'failure boosting', a technique to speed up the search for decryption failures. In this work we first improve the state-of-the-art multitarget failure boosting attacks. We then improve the cost calculation of failure boosting and extend the applicability of these calculations to permit cost calculations of real-world schemes. Using our newly developed methodologies we determine the multitarget decryption failure attack cost for all parameter sets of Saber and Kyber, showing among others that the quantum security of Saber can theoretically be reduced from 172 bits to 145 bits in specific circumstances. We then discuss the applicability of decryption failure attack in real-world scenarios, showing that an attack might not be practical to execute.

Keywords: Post-Quantum Cryptography, Lattice-based cryptography, Decryption failure attacks, Failure boosting

Let me know; I'll forward you the paper/rubric/instructions/etc if you're interested.
(Btw, I assume comp sci conference review processes are new to you.. Generally, you would need to read the paper then write something like 3-5 paragraphs. Whatever seems appropriate. A line by line critique is useful but not required.)

--Daniel