From: D. J. Bernstein <djb@cr.yp.to>
Sent: Monday, June 24, 2019 1:39 PM
To: pqc-comments
Cc: pqc-forum
Subject: [pqc-forum] ROUND 2 OFFICIAL COMMENT: LEDAcrypt
Attachments: signature.asc

I mentioned this in separate discussions of lattice proofs, but I've realized that filing this as an official comment is better.

https://www.ledacrypt.org/documents/LEDAcrypt_spec_latest.pdf appeals to the HHK17 CCA theorems, but actually uses a different notion of failure probability, without commenting on the difference in the definitions.
It's not clear to me that this proof gap can be fixed.

---Dan

--