

---

**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](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

--

You received this message because you are subscribed to the Google Groups "pqc-forum" group.  
To unsubscribe from this group and stop receiving emails from it, send an email to [pqc-forum+unsubscribe@list.nist.gov](mailto:pqc-forum+unsubscribe@list.nist.gov).  
To view this discussion on the web visit <https://groups.google.com/a/list.nist.gov/d/msgid/pqc-forum/20190624173910.25888.qmail%40cr.yp.to>.