

From: Doge Protocol <dogeprotocol1@gmail.com> via pqc-forum@list.nist.gov
To: [pqc-forum](mailto:pqc-forum@list.nist.gov) <pqc-forum@list.nist.gov>
CC: Doge Protocol <dogeprotocol1@gmail.com>
Subject: [pqc-forum] Re: HertzBleed : power side channel attacks on SIKE
Date: Tuesday, June 14, 2022 03:44:04 PM ET

Typo: implementations*

On Tuesday, June 14, 2022 at 12:42:28 PM UTC-7 Doge Protocol wrote:

Came across this today <https://www.hertzbleed.com/herzbleed.pdf>

The paper describes a side channel chosen-ciphertext attack on SIKE (even on constant-time implementations), allowing full key extraction via remote timing.

Has this been already discussed in this forum? Didn't see any previous references in this forum, hence sharing.

--

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.

To view this discussion on the web visit <https://groups.google.com/a/list.nist.gov/d/msgid/pqc-forum/f425ef27-17ab-4d91-9bc1-e147428beebfn%40list.nist.gov>.