From: Doge Protocol <dogeprotocol1@gmail.com> via pqc-forum@list.nist.gov
To: pqc-forum <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 imementations), 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.