KyberSlash: division timings depending on secrets in Kyber software

Various Kyber software libraries in various environments leak secret information into timing, specifically because

- these libraries include a line of code that divides a secret numerator by a public denominator,
- the number of CPU cycles for division in various environments varies depending on the inputs to the division, and
- this variation appears within the range of numerators used in these libraries.

The KyberSlash pages

- track which Kyber libraries have this issue;
- include a FAQ about the issue;
- provide demos showing that KyberSlash is sometimes exploitable; and
- host a paper on KyberSlash.

Contributors (alphabetical order)

- Daniel J. Bernstein (University of Illinois at Chicago, USA; Academia Sinica, Taiwan)
- Karthikeyan Bhargavan (Inria; Cryspen)
- Shivam Bhasin (Temasek Labs and National Integrated Center for Evaluation, Nanyang Technological University, Singapore)
- Anupam Chattopadhyay (College of Computing and Data Science, Nanyang Technological University, Singapore)
- Tee Kiah Chia (Temasek Labs, Nanyang Technological University, Singapore)
- Matthias J. Kannwischer (Quantum Safe Migration Center, Chelpis Quantum Tech, Taiwan)
- Franziskus Kiefer (Cryspen)
- Thales Paiva (University of Sao Paulo, Fundep, CASNAV)
- Prasanna Ravi (Temasek Labs and College of Computing and Data Science, Nanyang Technological University, Singapore)
- Goutam Tamvada (Cryspen)

URL

The permanent link for the KyberSlash pages is https://kyberslash.cr.yp.to. Currently the pages are also available at http://kyberslash.cr.yp.to (without redirection to HTTPS) to support very old browsers.

Version: This is version 2024.06.24 of the "Introduction" web page.