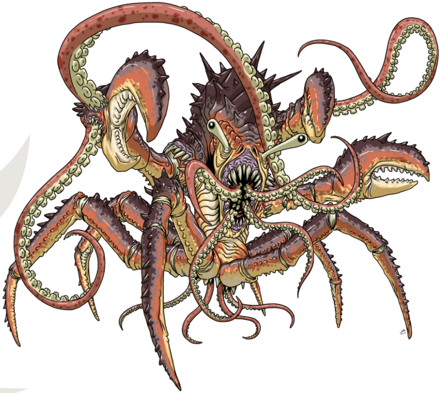
10 September 2018

PQCzoo: Post-Quantum Beasts and Where to Find Them

James Howe, Marco Martinoli



- On which embedded device does Frodo fit?

- On which embedded device does Frodo fit?
- Can you fault Dilithium?

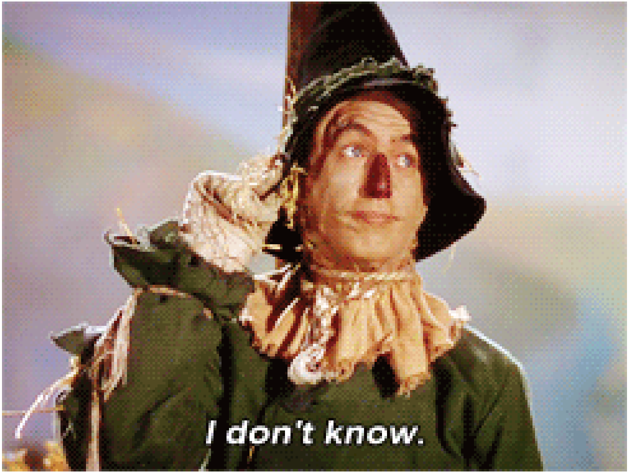
- On which embedded device does Frodo fit?
- Can you fault Dilithium?
- Does NewHope suffer cold (boot attacks)?

- On which embedded device does Frodo fit?
- Can you fault Dilithium?
- Does NewHope suffer cold (boot attacks)?
- Does a hardware design of a code-based scheme exist?

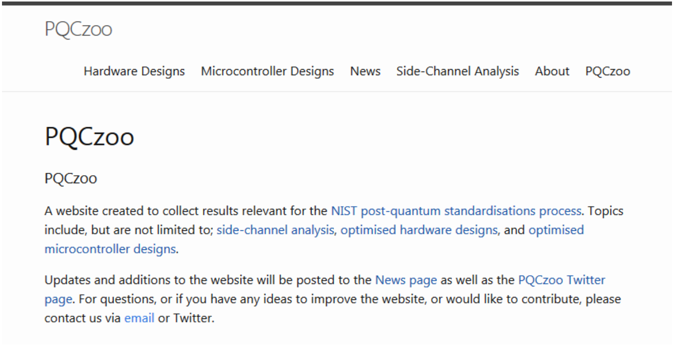
OPPA

GOPPA

CODES


I don't know.

Introducing: PQCzoo!



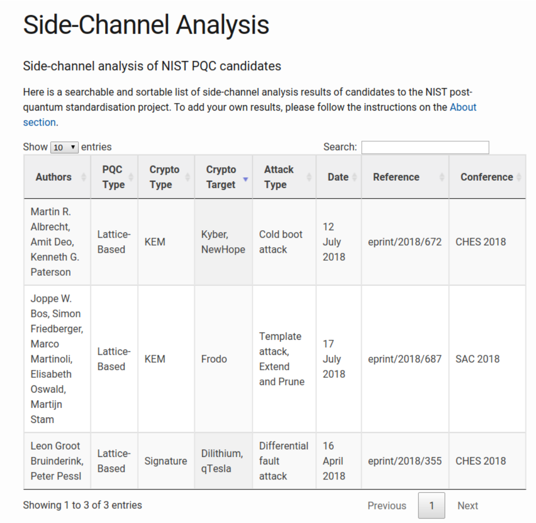
PQCzoo

PQCzoo

A website created to collect results relevant for the NIST post-quantum standardisations process. Topics include, but are not limited to; side-channel analysis, optimised hardware designs, and optimised microcontroller designs.

Updates and additions to the website will be posted to the News page as well as the PQCzoo Twitter page. For questions, or if you have any ideas to improve the website, or would like to contribute, please contact us via email or Twitter.

Introducing: PQCzoo!



Side-Channel Analysis

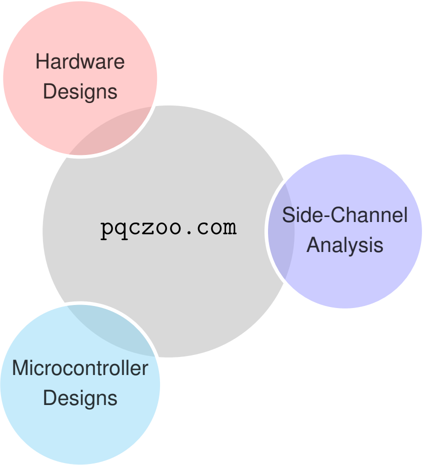
Side-channel analysis of NIST PQC candidates

Here is a searchable and sortable list of side-channel analysis results of candidates to the NIST post-quantum standardisation project. To add your own results, please follow the instructions on the About section.

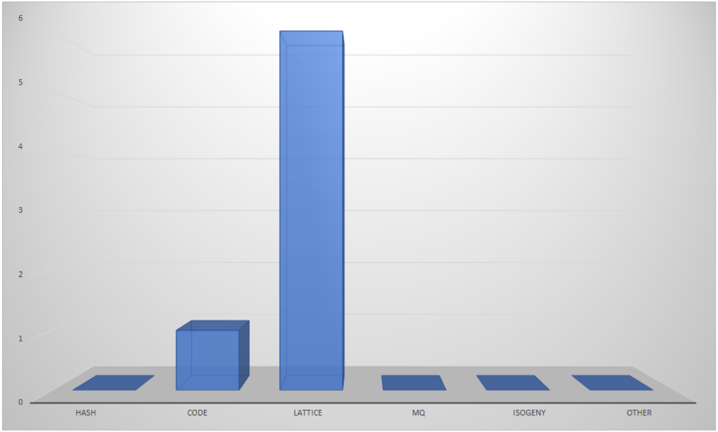
Authors	PQC Type	Crypto Type	Crypto Target	Attack Type	Date	Reference	Conference
Martin R. Albrecht, Amit Deo, Kenneth G. Paterson	Lattice-Based	KEM	Kyber, NewHope	Cold boot attack	12 July 2018	eprint/2018/672	CHES 2018
Joppe W. Bos, Simon Friedberger, Marco Martinoli, Elisabeth Oswald, Martijn Stam	Lattice-Based	KEM	Frodo	Template attack, Extend and Prune	17 July 2018	eprint/2018/687	SAC 2018
Leon Groot Bruinderink, Peter Pessl	Lattice-Based	Signature	Dilithium, qTesla	Differential fault attack	16 April 2018	eprint/2018/355	CHES 2018

Showing 1 to 3 of 3 entries

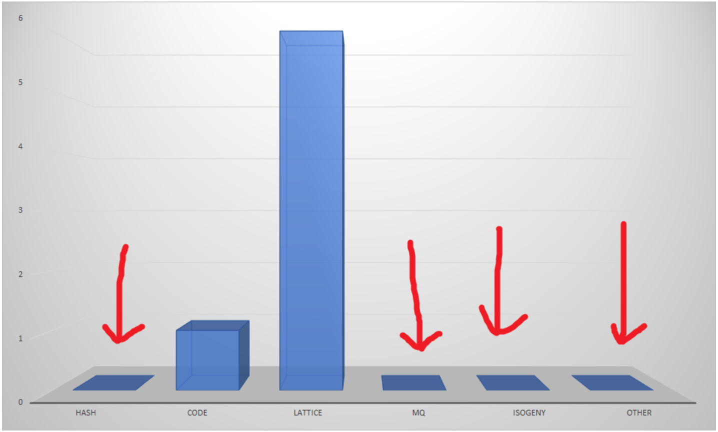
Introducing: PQCzoo!



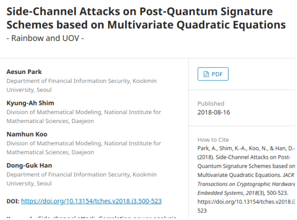
Represented Classes



(Under)Represented Classes



Awaiting submissions...



Side-Channel Attacks on Post-Quantum Signature Schemes based on Multivariate Quadratic Equations

- Rainbow and UOV -

Aesun Park
Department of Financial Information Security, Kookmin University, Seoul

Kyung-Ah Shim
Division of Mathematical Modeling, National Institute for Mathematical Sciences, Daejeon

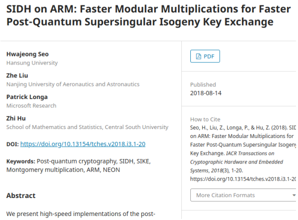
Namhun Koo
Division of Mathematical Modeling, National Institute for Mathematical Sciences, Daejeon

Dong-Guk Han
Department of Financial Information Security, Kookmin University, Seoul

DOI: https://doi.org/10.13154/tches.v2018.i3.500-523

Published
2018-08-16

How to Cite
Park, A., Shim, K.-A., Koo, N., & Han, D.-(2018). Side-Channel Attacks on Post-Quantum Signature Schemes based on Multivariate Quadratic Equations. *IACR Transactions on Cryptographic Hardware Embedded Systems, 2018*(3), 500-523. https://doi.org/10.13154/tches.v2018.i3-523



SIDH on ARM: Faster Modular Multiplications for Faster Post-Quantum Supersingular Isogeny Key Exchange

Hwajeong Seo
Hansung University

Zhe Liu
Nanjing University of Aeronautics and Astronautics

Patrick Longa
Microsoft Research

Zhi Hu
School of Mathematics and Statistics, Central South University

DOI: https://doi.org/10.13154/tches.v2018.i3.1-20

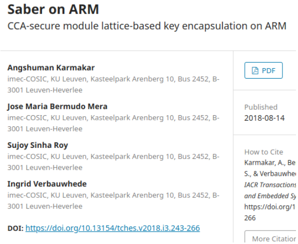
Keywords: Post-quantum cryptography, SIDH, SIKE, Montgomery multiplication, ARM, NEON

Abstract

We present high-speed implementations of the post-

Published
2018-08-14

How to Cite
Seo, H., Liu, Z., Longa, P., & Hu, Z. (2018). SID on ARM: Faster Modular Multiplications for Faster Post-Quantum Supersingular Isogeny Key Exchange. *IACR Transactions on Cryptographic Hardware and Embedded Systems, 2018*(3), 1-20. https://doi.org/10.13154/tches.v2018.i3.1-20



Saber on ARM

CCA-secure module lattice-based key encapsulation on ARM

Angshuman Karmakar
imec-COSIC, KU Leuven, Kasteelpark Arenberg 10, Bus 2452, B-3001 Leuven-Heverlee

Jose Maria Bermudo Mera
imec-COSIC, KU Leuven, Kasteelpark Arenberg 10, Bus 2452, B-3001 Leuven-Heverlee

Sujoy Sinha Roy
imec-COSIC, KU Leuven, Kasteelpark Arenberg 10, Bus 2452, B-3001 Leuven-Heverlee

Ingrid Verbauwhede
imec-COSIC, KU Leuven, Kasteelpark Arenberg 10, Bus 2452, B-3001 Leuven-Heverlee

DOI: https://doi.org/10.13154/tches.v2018.i3.243-266

Published
2018-08-14

How to Cite
Karmakar, A., Be S., & Verbauwhe *IACR Transactions and Embedded Sy* https://doi.org/1 266

Cool! How do I submit my paper?

- You need a GitHub account.
- Access PQCzoo's Git: `github.com/pqczoo/pqczoo.github.io`.
- Add an entry with your paper to the appropriate table (HW, SW, or SCA).
- Send a pull request and wait, the paper will be on soon! :)

Cool! How do I submit my paper?

- You need a GitHub account.
- Access PQCzoo's Git: `github.com/pqczoo/pqczoo.github.io`.
- Add an entry with your paper to the appropriate table (HW, SW, or SCA).
- Send a pull request and wait, the paper will be on soon! :)

Instructions on this are on the website's About section (`pqczoo.com/about`).
Otherwise, send me an email or catch me at the conference!