

Artifacts of

Avengers assemble!

Supervised learning meets lattice reduction – A single power trace attack against CRYSTALS-Kyber Key Generation
Pierre-Alain Fouque, Damien Marion, Quyen Nguyen Alexandre Wallet

<https://gitlab.inria.fr/capsule/avengers-assemble>



Data

Available on zenodo:
records n°17058125

- numpy format: raw traces, pre-treated traces and models.
- text format: results and guesses.

Code

- acquisition (C, python): based on Lib6dromel.
- analysis (python): pre-treatments, classifiers and post-treatments.
- key-recovery (sage): linear algebra, LLL and BKZ.

Artifacts of

Avengers assemble!

Supervised learning meets lattice reduction – A single power trace attack against CRYSTALS-Kyber Key Generation
Pierre-Alain Fouque, Damien Marion, Quyen Nguyen Alexandre Wallet

<https://gitlab.inria.fr/capsule/avengers-assemble>



Lessons learned for next time

- propose an easier way to deploy the environment (maybe with docker).
- keep track of updates of software and libraries used.
- beta test and deploy on clean machine before submitting artifacts.

Feel free to fork, use and modify, any question, contact us:
damien.marion@irisa.fr