# Machine-Learning Side-Channel Analysis on Lattice-based Signature Schemes

Soundes Marzougui
Technische Universität Berlin

33th Crypto Day, 17 September 2021

Machine-learning-based side-channel analysis is an emerging threat to the security of cryptographic algorithms [1, 5, 4]. Machine-learning techniques enable attackers to find dependencies in raw data, bypass many existing side-channel countermeasures, and break protected implementations [2]. Security against side-channel attacks is a major concern for schemes, especially those meant for real-world deployment. Therefore, the National Institute of Standards and Technology (NIST) has listed the side-channel resistance of implementations as one of the criteria for its standardization process [3].
This work proposes an innovative application of machine-learning side-channel attacks to recover the secret key of lattice-based signature schemes by targeting specific routines. The attack is mounted in two phases. In the profiling phase, we train machine-learning classifiers on a device identical to the device under attack. The training data consists of the input to the targeted routines and the corresponding power consumption traces. In the attack phase, the trained classifiers are then used to recover those inputs with high accuracy, culminating in a key recovery attack. We demonstrate the leakages by running the targeted schemes on a Cortex-M4 and provide proof-of-concept data and implementation for our attacks.

## References

[1] T. Kubota, K. Yoshida, M. Shiozaki, and T. Fujino. Deep learning side-channel attack against hardware implementations of aes. In *2019 22nd Euromicro Conference on Digital System Design (DSD)*, pages 261–268, 2019.

[2] Kalle Ngo, Elena Dubrova, and Thomas Johansson. Breaking masked and shuffled cca secure saber kem by power analysis. Cryptology ePrint Archive, Report 2021/902, 2021. `https://ia.cr/2021/902`.

[3] National Institute of Standards and Technology. Post-quantum cryptography pqc. `https://csrc.nist.gov/projects/post-quantum-cryptography`.

[4] Emmanuel Prouff, Rémi Strullu, Ryad Benadjila, Eleonora Cagli, and C. Canovas. Study of deep learning techniques for side-channel analysis and introduction to ascad database. *IACR Cryptol. ePrint Arch.*, 2018:53, 2018.

**crypto day matters 33** (2021)
Beiträge vom 33. Kryptotag, 17.09.2021, online.
doi:10.18420/cdm-2021-33-12

[5] H. Wang, M. Brisfors, S. Forsmark, and E. Dubrova. How diversity affects deep-learning side-channel attacks. In *2019 IEEE Nordic Circuits and Systems Conference (NORCAS): NORCHIP and International Symposium of System-on-Chip (SoC)*, pages 1–7, 2019.