Neural Network Architectures for Second Order Side Channel Attacks

Graduate internship (Master 2), Summer 2026

Location	PQShield SAS, Paris 8 Rue des Pirogues de Bercy WeWork Bercy 75012 Paris
Contact	Timo Zijlstra
Starting date and duration	Q2 (flexible) 2026, 6 months
Gross salary	1350 euros per month

Contents

Internship

Background

In order to compute key exchanges or digital signatures, embedded cryptographic devices require the use of a secret key that must remain confidential. Side channel attacks (SCA) exploit statistical dependencies between the power consumption of a cryptographic device and the value of data on which it computes in order to recover the secret key.

Countermeasures against SCA, such as masking, rely on the randomization of secret data during the computation of the cryptographic algorithm.

The use of machine learning in SCA on masked implementations has become increasingly popular over the last decade (https://eprint.iacr.org/2025/471). Neural networks seem particularly well suited for modeling how the data inside a processor impacts its power consumption. In particular, recent works have tried to design specific neural network architectures to attack masked implementations.

Scope of the internship

The intern will use PQShield's tools to design neural networks and test their effectiveness on existing datasets that consist of power measurements of PQShield's post quantum cryptographic hardware accelerator and/or open source implementations.

This project comprises the following phases:

1. **Literature review**
    - Understand the background of the datasets: SCA
    - Review the supervised machine learning methods used in the state of the art
2. **Practical Evaluations**
    - Explore the hyperparameter space for neural networks and design neural network architectures by taking into account the specifics of the power measurements within the datasets
    - Compare the effectiveness of supervised learning methods other than neural networks
    - Analyse the effectiveness of the various neural network architectures on datasets generated from implementations protected by various SCA countermeasures

About PQShield

PQShield is a cybersecurity scaleup that specialises in post-quantum cryptography, protecting information from today's attacks while readying organisations for the threat landscape of tomorrow. PQShield is headquartered in Oxford, with additional teams in the Netherlands, Germany, Belgium and France.

PQShield comprises a world-class collaboration of post-quantum cryptographers, engineers, and researchers. We've helped shape all of the first international PQC NIST standards, and we were the first cybersecurity company to develop quantum-safe cryptography on chips, in applications, and in the cloud.

Requirements and how to apply

Ideal candidates should possess:

- Prior experience in supervised machine learning methods for classification problems, including neural networks
- Proficiency in Python and experience with Keras/Tensorflow
- Some familiarity with cryptography
- Excellent communication skills
- Optional but big plus: familiarity with SCA

Supervision and Mentorship: The intern will be mentored by members of PQShield's Product Security Team in our office in Paris, with frequent progress meetings to facilitate knowledge exchange and to track progress.

To apply, please send your CV to the contact point listed at the top of this document.