Machine Learning Resistant PUF Authentication Schemes

A Physical Unclonable Function (PUF) is a hardware element which uses subtle manufacturing variabilities to derive a device-unique secret. In the case of a multi-challenge PUF (or ‘strong PUF’), the PUF functions as a device-unique function, mapping challenges to PUF responses.

A PUF like this is very useful for authentication scenarios, where e.g. a server provides challenges to a device, which replies with the PUF response the server can now check against an internal model or response database.

Protocols like these, however, suffer from data leaks, allowing an attacker to create a model of a device’s PUF from captured challenge-response pairs. Thus, the ostensibly unclonable device may be replicated just by eavesdropping on authentication communication.

The aim of this work is to investigate novel approaches for PUF authentication procedures which plug data leaks with simple on-device preprocessing while still allowing for reliable authentication in the presence of measurement noise. A software implementation can then be evaluated e.g. against a more standard implementation in terms of performance, complexity or resistance against a machine learning attack.

This work can either be conducted in German or in English.

I am happy to provide more details and answer your questions upon request.

Prerequisites

- Necessary: Basic cryptography knowledge; mathematical background; programming skills
- favourably: Experience with machine learning techniques
- Optionally: Basic knowledge of error-correcting codes, PUFs

Contact

Jonas Ruchti, M.Sc.
Technical University of Munich, Chair of Security in Information Technology
Room N1014
E-Mail: j.ruchti@tum.de

Advisors

Jonas Ruchti