FACULTY
OF INFORMATION
TECHNOLOGY
CTU IN PRAGUE

Assignment of bachelor's thesis

Title:	Physical unclonable functions on ESP32
Student:	Ondřej Staníček
Supervisor:	Ing. Jiří Buček, Ph.D.
Study program:	Informatics
Branch / specialization:	Computer Security and Information technology
Department:	Department of Computer Systems
Validity:	until the end of summer semester 2022/2023

Instructions

Physical unclonable functions are an emerging cryptographic primitive that can be used for device identification, authentication, and key generation in digital devices.

* Study the topic of physical unclonable functions (PUFs). Focus primarily on SRAM PUF.
* Design and implement a simple SRAM based PUF on a suitable ESP32 microcontroller.
* Experiment with the microcontroller's internal registers to find a suitable mechanism for SRAM power state control.
* Test the function of the PUF on several devices.
* Evaluate relevant PUF parameters (especially bit stability and uniqueness).
* Evaluate the distribution of SRAM bit values depending on operating temperature and power-off time.

Electronically approved by prof. Ing. Pavel Tvrdík, CSc. on 10 January 2022 in Prague.