Bachelor and Master Project / Bachelor- und Masterarbeit

RISC-V Cryptographic Vector Extensions for Secure and Efficient Hash-Engine

Introduction: RISC-V is an open-source instruction set architecture (ISA) using reduced instruction set computer principles. This instruction set is considered an abstract model describing computer components. For instance, certain instructions of RISC-V lead to the implementation and realization of a specific cryptographic engine such as AES or SHA engines. Recently several vendors have started using RISC-V. The number of products using the RISC-V CPU core is expected to be 62.4 billion by 2025.
This project will show first the current capability of RISC-V in implementing a hash function. Then, it will show how to develop a new cryptographic RISC-V extensions for efficient hash implementation . This project aims to develop a secure RISC-V hash engine by deploying the principles of "Security by Design".

Research Objectives: The work plan contains four steps as follow:

1) Studying and reviewing the recent cryptographic vector extensions.
2) Studying and investigating one of the standard hash function.
3) Devising new RISC-V cryptographic vector extensions for the chosen hash.
4) Implementing the designed RISC-V cryptographic vector extensions and compare the resulting hash engine with the state-of-art .

Applications of the research results:
Jupiter.

Prerequisites/Requirements: Students should have good background in processor design or security , and they should be interested in hardware-implementations.

Starting Date: To be agreed on with the interested party.

Interested students are kindly asked to contact:

- **Instructor and adviser**: Saleh Mulhem, mulhem@iti.uni-luebeck.de
- **Supervisor:** Prof. Dr-Ing, Mladen Berekovic.

Institut für Technische Informatik,
Gebäude 64, 2. Stock,
Universität zu Lübeck
Ratzeburger Allee 160,
23562 Lübeck.