Secure Hardware-Efficient Realization of Lightweight Cryptography Algorithms

Summary

Lightweight cryptography (LWC) plays an important role to ensure integrity, confidentiality, and security of sensitive information on devices with limited resources, such as internet of things (IoT) and wireless sensor networks. In our project, we aim to (i) explore hardware-efficient realizations of lightweight cryptography algorithms taking into account performance, power, and area (PPA) requirements; (ii) secure these implementations against well-known attacks, such as side-channel analysis and fault injection, considering the PPA overhead; and (iii) demonstrate these LWC designs in an application-specific integrated circuit (ASIC) and embed them in a real-world IoT environment.

Research field:	Information and communication technology
Supervisor:	Levent Aksoy
Availability:	This position is available.
Offered by:	School of Information Technologies Department of Computer Systems
Application deadline:	Applications are accepted between October 01, 2024 00:00 and October 25, 2024 23:59 (Europe/Zurich)

Description

The research

An important shift from mainframe and personal computing to computing at edge nodes has led to significant growth in interconnected IoT devices that process and communicate information to a mobile device or a server over a wireless network. However, these devices are constrained in terms of implementation area, size of storage allocation, data rate, and energy consumption. To secure communication in an IoT environment, many LWC primitives have been introduced and standardized by national and international organizations, satisfying the IoT device requirements.

The main goal of this project is to implement hardware-efficient and secure LWC algorithms in ASIC. In this project, we will consider the LWC standards, such as PRESENT, Chaskey, and ASCON, and explore the hardware-efficient realization of their main blocks in terms of area, delay, and power dissipation. We will also secure our implementations against well-known attacks, such as side channel analysis and fault injection, using masking, blinding, and fault detection and mitigation techniques, considering the hardware complexity. Moreover, we will implement promising LWC designs in ASIC and use them in a real-world application.

Responsibilities and (foreseen) tasks:

- Describe LWC algorithms using hardware description languages, synthesize using commercial logic synthesis tools, and simulate and verify their behavior using commercial simulation tools
- Design LWC algorithms in ASIC including front-end, back-end, and tape-out phases
- Apply side-channel and fault injection attacks in all phases
- Disseminate the research findings in journal and conference publications

Applicants should fulfill the following requirements:

- Master’s degree in Computer Science, Electrical Engineering, or Computer Engineering
- Knowledge of hardware description languages Verilog/VHDL
- Knowledge of hardware design techniques targeting high performance and low power dissipation
- Experience in digital system design at RTL using Verilog/VHDL on FPGA/ASIC
- Knowledge of cryptography algorithms including block ciphers and hash functions
- Knowledge of hardware security including side-channel analysis and fault injection attacks

(The following experience is beneficial:)

- Experience in programming with C/C++

- Experience in the design of cryptography algorithms in hardware
- Experience in scripting languages, such as Perl, Tcl, and bash
- Relevant publications on cryptography and/or hardware security

We offer:

- 4-year PhD position in one of the largest, most internationalized and leading university in Estonia
- An opportunity to do high-level research with fellow researchers in this field
- Opportunities for international conferences, research stays and networking with well-known universities and research centers in this field

About the university and research centre

Tallinn University of Technology (TalTech) is the flagship in engineering and information technology science and education in Estonia, providing higher education at all levels in engineering and technology, economics, science, and maritime. TalTech's mission is to be a promoter of science, technology, and innovation and a leading provider of engineering and economic education in Estonia. The university has over 2000 employees and over 10,000 students, and approximately 70,000 alumni.

Centre for Hardware Security in the Department of Computer Systems focuses on research topics related to hardware security including hardware obfuscation, logic locking, cryptography, and side-channel analysis.

(Additional information)

Please include a cover letter including your interest in this position and your research plan in the application, for additional info, please contact Dr. Levent Aksoy by e-mail (levent.aksoy@taltech.ee).

To get more information or to apply online, visit https://taltech.glowbase.com/positions/851 or scan the the code on the left with your smartphone.