UNIVERSITÄT ZU LÜBECK
INSTITUT FÜR TECHNISCHE INFORMATIK

Bachelor and Master Project / Bachelor- und Masterarbeit

Designing and Implementing
a Class of Side-Channel Attacks Resilient S-boxes

Introduction: The substitution box (S-Box) is a non- linear mapping used in block ciphers to induce confusion in data. The role of the S-Boxes is to obscure the relation between the cipher- secret key and the input data (Plaintext). The efficient and secure S-box design is the one that provides a block cipher with a high level of confusion. On the other hand, applying Side-Channel Attacks (SCAs) on a block cipher aims to exploit the physical characteristics of the cipher-implementation to extract and recover the cipher-secret key. SCAs are considered as the most powerful attacks against block ciphers. To increase the resilience and resistance of the block ciphers against such a type of attack, the used S-boxes in the block cipher design should meet specific cryptographic requirements.

Furthermore, implementing secure S-boxes with a small input length is very necessary to minimize the area used in realizing a block cipher design. A block cipher utilizes such low complexity S-Boxes is called a lightweight cipher. Therefore, a special class of Low-Complexity and SCAs resilient S-boxes is required, research on such a class has gained recently more interest, especially for the internet of things (IoT) applications.

Project Plan: The work plan contains three steps as follow:

1) Studying and reviewing the cryptographic properties of S-boxes that allow designing a new class of S-boxes and understand the concept of Low-Complexity implementations.
2) Devising an algorithm to provide and generate Low-Complexity S-boxes with negligible success probabilities of specific well-known SCAs.
3) Implementing the resulting S-boxes on System-on-Chip (SoC) and check the complexity.

Applications of the research results:
Such S-boxes are expected to be used in a block cipher design for resource constrained devices.

Prerequisites/Requirements: Students should have good background in algorithms and programming languages, 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.