Abstract:

ARX-based cryptographic algorithms are composed of only three elemental operations—addition, rotation and exclusive or—which are mixed to ensure adequate confusion and diffusion properties. While ARX-ciphers can easily be protected against timing attacks, special measures like masking have to be taken in order to prevent power and electromagnetic analysis. Here we present a processor architecture for ARX based cryptography, that intrinsically guarantees first-order SCA resistance of any implemented algorithm. This is achieved by protecting the complete data path using a Boolean masking scheme with three shares. We evaluate our security claims by mapping an ARX-algorithm to the proposed architecture and using the common leakage detection methodology based on Student’s $t$-test to certify the side-channel resistance of our processor.

Existing system

Security plays a major role in many applications of the upcoming Internet of Things (IoT), in particular when security critical digital devices are also potentially exposed to physical attacks, such as side-channel analysis (SCA) and intentional fault-injection. ARX-based cryptography is denoting a set of symmetric constructions that are purely based on Additions (mod $2^n$), Rotations and XOR (ARX).

Proposed system

In this work, we present a novel co-processor subsystem that is designed as an Application-Specific Instruction-Set Processor (ASIP) for a specific class of cryptosystems with inherent hardware resistance against side-channel analysis. More precisely, our architecture and instruction set follows principles from the “Threshold Implementation” (TI) concept that is
known to provide provable security against power side-channel analysis. As an ASIP it can be loaded with software implementations of different symmetric ARX-based cryptographic primitives, such as stream and block ciphers or hash-functions without the need for adaption of the hardware. We show that a prototype of our design including a software implementation of Speck is not only secure against first-order side-channel analysis and timing attacks but can be realized at moderate costs that are even comparable against pure (protected) hardware implementations. Note that the hardware is designed to completely counter the aforementioned side channel attack which significantly relaxes the requirements for software engineers to handle complex constraints of physical side-channel security.

Applications

1) Communications
2) Digital signal processing

Advantages

Area, delay and power reduced

System Configuration:

In the hardware part a normal computer where Xilinx ISE 14.3 software can be easily operated is required, i.e., with a minimum system configuration

HARDWARE REQUIREMENT

Processor - Pentium –III

Speed - 1.1 GHz

RAM - 1 GB (min)

Hard Disk - 40 GB
Floppy Drive - 1.44 MB

Key Board - Standard Windows Keyboard

Mouse - Two or Three Button Mouse

Monitor - SVGA

SOFTWARE REQUIREMENTS


❖ Front End : Modelsim 6.3 for Debugging and Xilinx 14.3 for Synthesis and Hard Ware Implementation

This software’s where Verilog source code can be used for design implementation.