Initiators

- Werner Schindler
- Sorin Alexander Huss
Constructive Side-Channel Analysis and Secure Design

Time Period
2010 to 2019

Locations
Darmstadt, Paris, Berlin, Graz, Singapore
We expected not more than 30 persons to attend this event, but 49 attendees registered in total, 16 of them during the last two days before the conference was to start. So, we urgently needed to take some actions on the fly.
We expected not more than 30 persons to attend this event, but 49 attendees registered in total, 16 of them during the last two days before the conference was to start. So, we urgently needed to take some actions on the fly.

- Move the location of the venue from the CASED building to the Fraunhofer SIT institute.
- Generate road signs as to inform the participants how to get from CASED to SIT.
- Reshape the catering of the COSADE event.
COSADE Call for Papers

2013:
- Constructive side-channel analysis and implementation attacks
- Semi-invasive, invasive and fault attacks
- Leakage models and security models for side-channel analysis
- Cache-attacks and micro-architectural analysis
- Decapsulation and preparation technique
- Side-channel based reverse engineering
- Leakage resilient implementations
- Evaluation methodologies for side-channel resistant designs
- Secure designs and countermeasures
- Evaluation platforms and tools for testing of side-channel characteristics

2019:
- Implementation attacks and exploitations:
  Side-channel analysis, fault-injection attacks, probing and read-out, hardware Trojans, ...
- Secure implementation:
  Cryptographic blocks (including post-quantum and lightweight ciphers), random number generators, ...
- Implementation attack-resilient architectures and schemes:
  Trusted environment (Secure boot, execution, storage, isolation, virtualization, firmware update), ...
- Secure design and evaluation:
  Security and leakage models, formal analysis of secure implementations, design automation and tools, ...
Secure Design and Evaluation

Countermeasure insertion within the AMASIVE high-level (re-)synthesis and evaluation tool set


Synthesis in a Nutshell

**Synthesis**: Mapping of a functional specification onto a structural description

**Fundamental Principle**: Order all activities in space and time

- Allocation
- Binding
- Scheduling

Functional spec. (problem graph) → \[\text{Not dependent on abstraction level or on application domain}\] → Architecture descr. (ressources graph) → Structural descr. (HW) and/or Executable code (SW)
Synthesis in a Nutshell

Synthesis: Mapping of a functional specification onto a structural description

Fundamental Principle: Order all activities in space and time

Functional spec. (problem graph)

Architecture descr. (ressources graph)

- Allocation
- Binding
- Scheduling

Structural descr. (HW) and/or Executable code (SW)

Not dependent on abstraction level or on application domain

Static Architectures
implemented on ASIC, FPGA, or MPSoC
Mutating Runtime Architecture

Concept: *Refinement* of the basic HW/SW codesign construction methods by means of exploiting the reconfiguration abilities offered by advanced FPGA platforms resulting in a *Mutating Runtime Architecture*. 
Mutating Runtime Architecture

Concept: Refinement of the basic HW/SW codesign construction methods by means of exploiting the reconfiguration abilities offered by advanced FPGA platforms resulting in a Mutating Runtime Architecture.

Goal: Countermeasures to side-channel power attacks to be introduced implicitly during the HW/SW codesign process thus resulting in an architecture with a considerably reduced leakage.
Online Allocation

Power consumption scatter plot of some SBox design variants

Example: Allocation of the SBox operation to a resource over time

<table>
<thead>
<tr>
<th>Point in Time</th>
<th>Design Variant</th>
</tr>
</thead>
<tbody>
<tr>
<td>i</td>
<td>COMP</td>
</tr>
<tr>
<td>j</td>
<td>PPRM1</td>
</tr>
<tr>
<td>k</td>
<td>PPRM3</td>
</tr>
<tr>
<td>l</td>
<td>TBL</td>
</tr>
</tbody>
</table>
OnlineAllocation

Power consumption scatter plot of some SBox design variants

Example: Allocation of the SBox operation to a resource over time

<table>
<thead>
<tr>
<th>Point in Time</th>
<th>Design Variant</th>
</tr>
</thead>
<tbody>
<tr>
<td>i</td>
<td>COMP</td>
</tr>
<tr>
<td>j</td>
<td>PPRM1</td>
</tr>
<tr>
<td>k</td>
<td>PPRM3</td>
</tr>
<tr>
<td>l</td>
<td>TBL</td>
</tr>
</tbody>
</table>

Implementation of OnlineAllocation on top of an FPGA by means of

- Dedicated switching network
- Partial reconfiguration (if avail.)


Dynamic Binding

Change at runtime the link between activity and resource instance(s) by

- Random concurrent binding
- Virtualization

on top of an executive layer, which organizes the links between activities and executing resources.

This layer is quite similar to the Middleware concept in SW system architectures.


Flexible Scheduling

Goal
Change execution behavior during runtime by manipulated sequences of data-independent basic operations (‘shuffling’)

Approach
- Execute basic operations on mutable, online relocable processing units
- Modify frequently the number of in-parallel operating units by applying a dynamic binding
Flexible Scheduling

Goal
Change execution behavior during runtime by manipulated sequences of data-independent basic operations (‘shuffling’)

Approach
- Execute basic operations on mutable, online relocable processing units
- Modify frequently the number of in-parallel operating units by applying a dynamic binding

Result
Complex power distribution acting as an additional countermeasure by combining effects from DynamicBinding and OnlineAllocation manipulations
Application Example
Block Cipher AES 128 bit

Design objectives

- Change dynamically the degree of in-parallel operating SBox units
- Execute SBox operation on different unit designs
- Merge round operations into one clock cycle
- Manipulate the word-width being processed during one clock cycle
Highly Configurable Data Path and Key Scheduler

- Scalable degree of in-parallel processed data from 8 to 128 bit in byte-wise steps
- Next round key in-parallel calculation on 128 bit at once or on 96, 64, or 32 bit wide chunks
SCA Results

- SASEBO-GII board
- 450k traces in profiling phase of Stochastic Approach
- 50k traces in attack phase
SCA Results

- SASEBO-GII board
- 450k traces in profiling phase of Stochastic Approach
- 50k traces in attack phase

Future Requirements

- **Fundamental innovations are required** to improve current practices in computer security if we want to **increase the acceptance** of IT techniques by the public.
Future Requirements

Secure Design

- **Fundamental innovations are required** to improve current practices in computer security if we want to **increase the acceptance** of IT techniques by the public.

- We therefore need to **change our perspective** on attacks, models, and design methods to a **holistic view on secure devices** because built-in countermeasures have to jointly cover a **variety of attack scenarios**.

- In general, countermeasures **shall not harden a device against just a single attack method** and at the same time **leave doors open** for many other ones.
Future Requirements

**Secure Design**

- **Fundamental innovations are required** to improve current practices in computer security if we want to **increase the acceptance** of IT techniques by the public.

- We therefore need to **change our perspective** on attacks, models, and design methods to a **holistic view on secure devices** because built-in countermeasures have to jointly cover a **variety of attack scenarios**.

- In general, countermeasures **shall not harden a device against just a single attack method** and at the same time **leave doors open** for many other ones.

- There is a **lot of research work still to be done** and **COSADE** is the **premier place** to present and to discuss new models, methods, and approaches stemming from the proposed change of perspective.
Future Requirements

Secure Design

- **Fundamental innovations are required** to improve current practices in computer security if we want to **increase the acceptance** of IT techniques by the public.

- We therefore need to **change our perspective** on attacks, models, and design methods to a **holistic view on secure devices** because built-in countermeasures have to jointly cover a **variety of attack scenarios**.

- In general, countermeasures **shall not harden a device against just a single attack method** and at the same time **leave doors open** for many other ones.

- There is a **lot of research work still to be done** and **COSADE** is the **premier place** to present and to discuss new models, methods, and approaches stemming from the proposed change of perspective.

**So, let us open our minds and enlarge considerably the focus of our research!**