COSADE Conference Series

Past, Present, and Future

Sorin A. Huss

Initiators

- Werner Schindler

Bundesamt
für Sicherheit in der
Informationstechnik

- Sorin Alexander Huss

TECHNISCHE
UNIVERSITÄT
DARMSTADT

CASED

Constructive Side-Channel Analysis and Secure Design

Time Period	Locations
2010 to 2019	Darmstadt, Paris, Berlin, Graz, Singapore

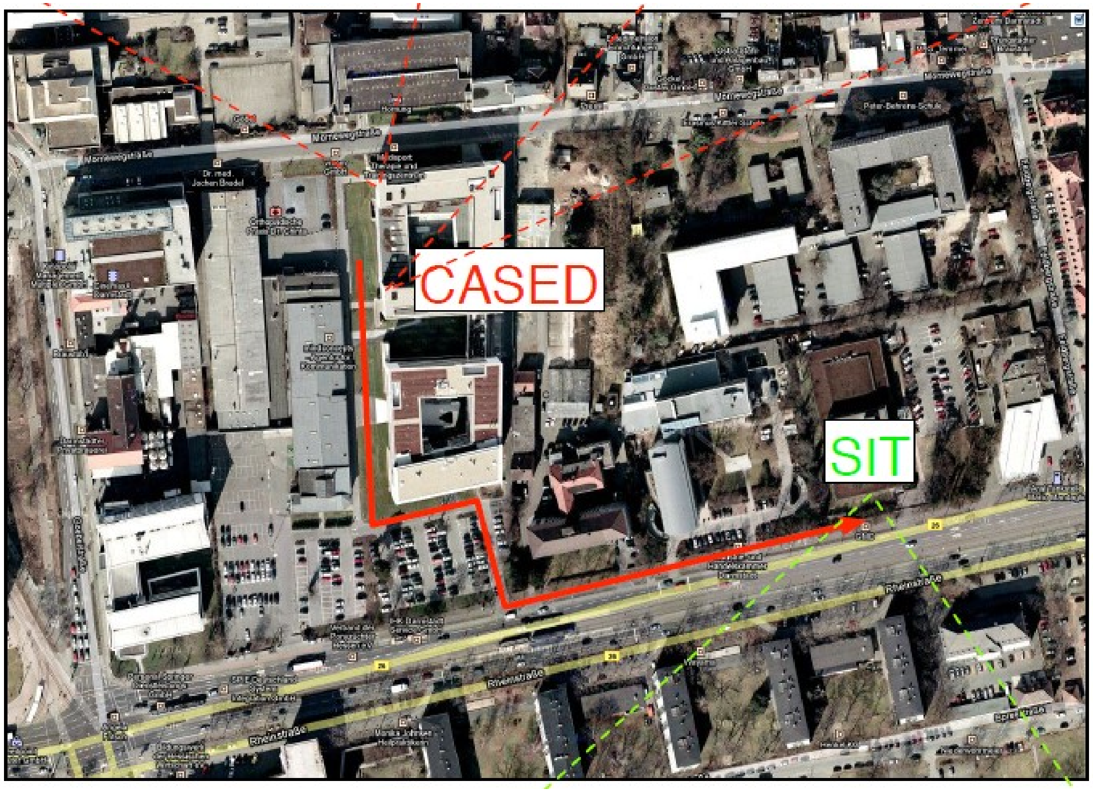
1st COSADE Conference ...

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.

1st COSADE Conference ...

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:

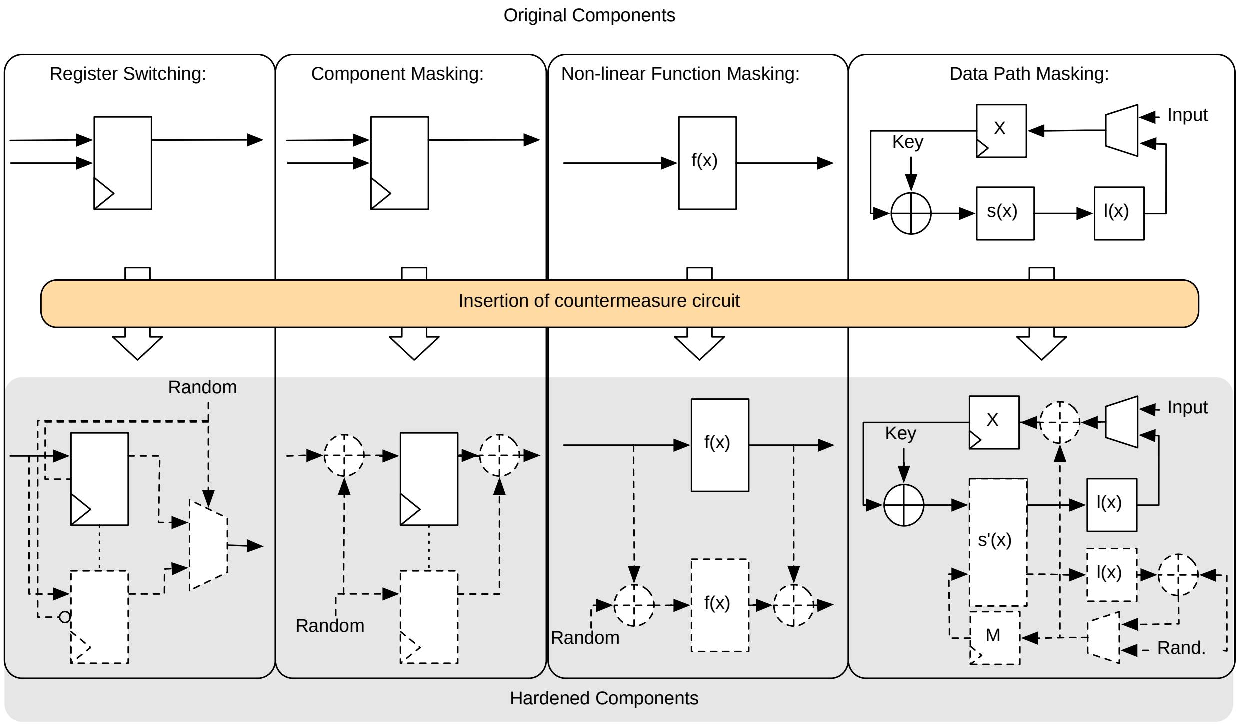
  Cryptographic blocks (including post-quantum and lightweight ciphers), random number generators, ...
- Implementation attack-resilient architectures and schemes:

  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



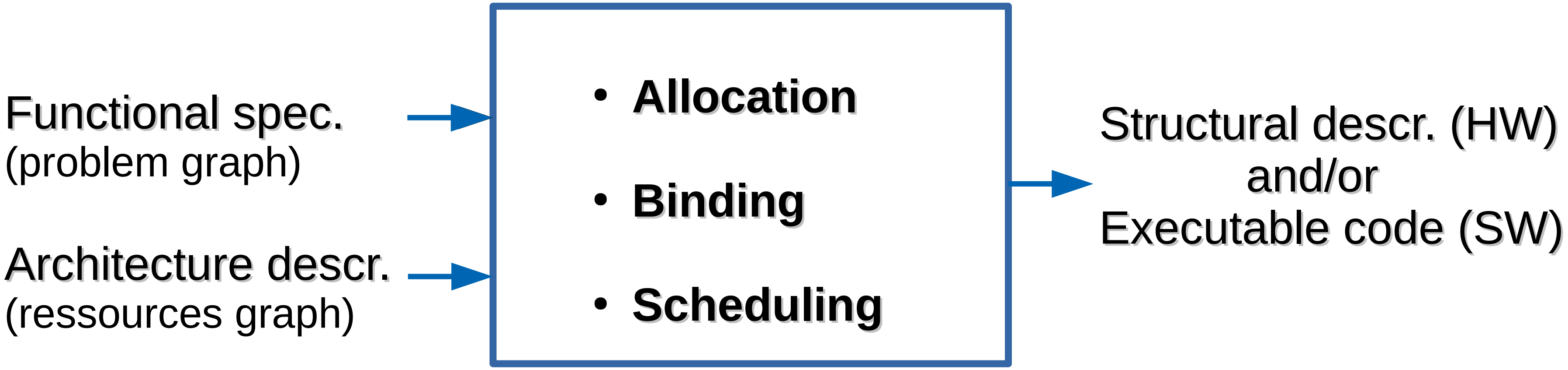
M. Zohner, M. Stöttinger, S. A. Huss, and O. Stein, „An Adaptable, Modular, and Autonomous Side-Channel Vulnerability Evaluator”, IEEE HOST, 2012.

S. A. Huss and O. Stein, „A Novel Design Flow for a Security-driven Synthesis of Side-channel hardened Cryptographic Modules“, J. Low Power Electron. Appl., 7, 4, 2017.

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**

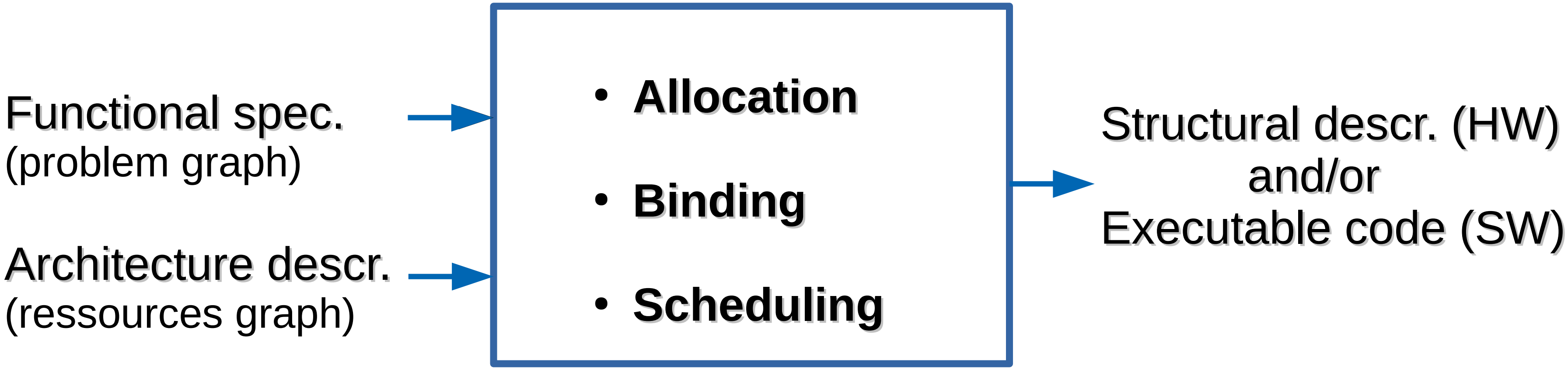
Structural descr. (HW)
and/or
Executable code (SW)

Not dependent on abstraction level
or on application domain

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

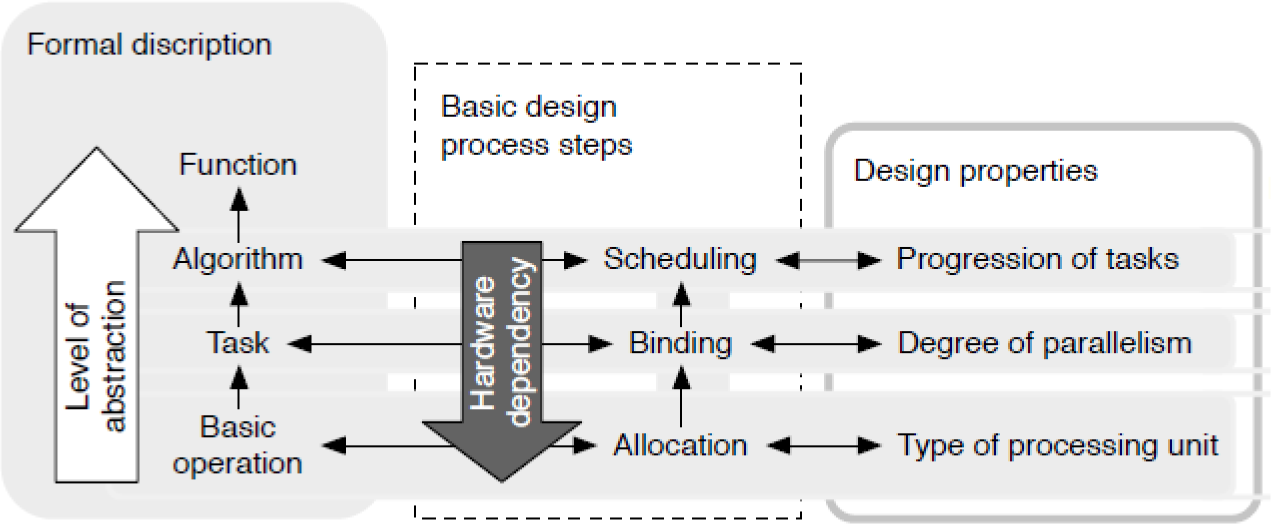
HW HW/SW SW

Static Architectures

implemented on ASIC, FPGA, or MPSoC

Mutating Runtime Architecture

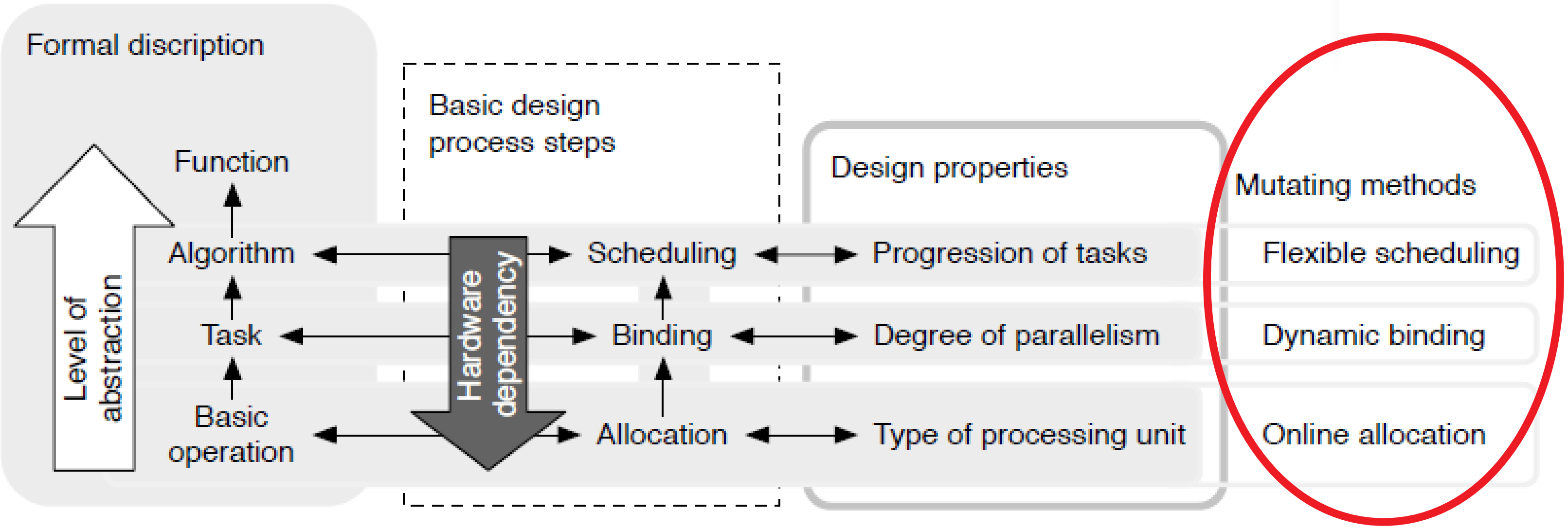
Concept: *Refinement* of the basic HW/SW codesign construction methods by means of *exploiting the reconfiguration abilities* offered by advanced FPGA platforms resulting in a *Mutating Runtime Architecture*.



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*.

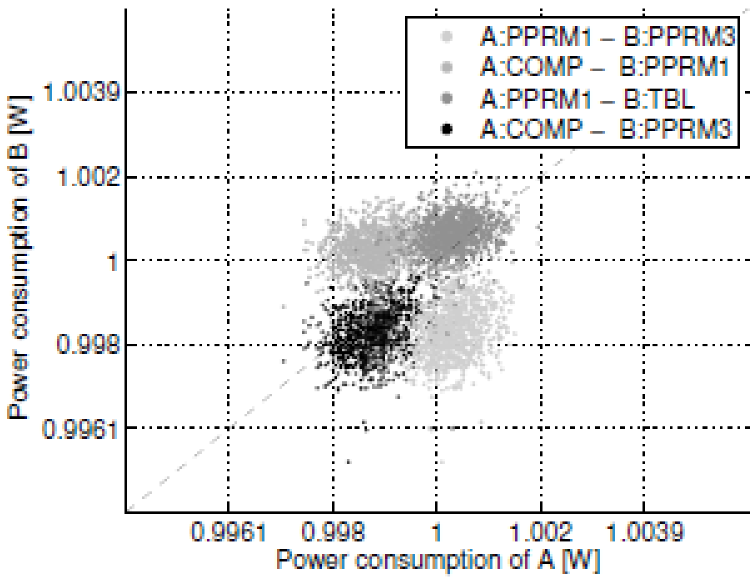
Goal: Countermeasures to side-channel power attacks to be introduced *implicitely* during the HW/SW codesign process thus resulting in an architecture with a *considerably reduced* leakage.



OnlineAllocation

Type of Processing Unit

Power consumption scatter plot of some SBox design variants



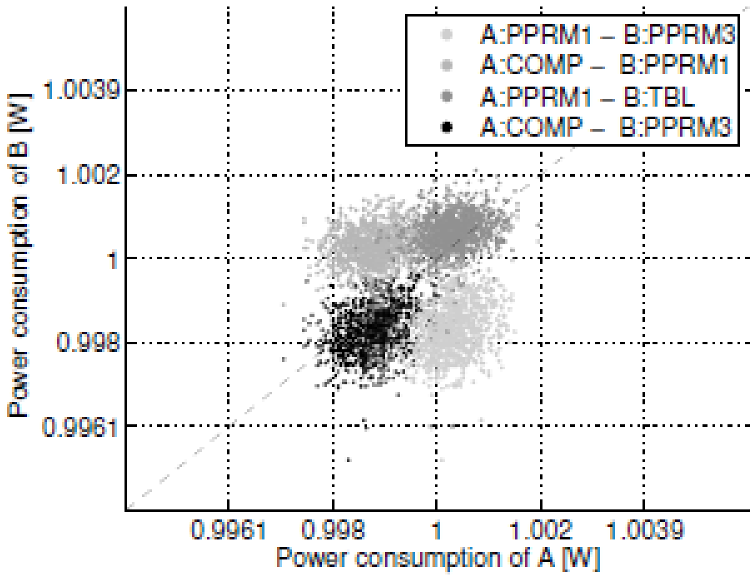
Example: Allocation of the SBox operation to a ressource over time

Point in Time	Design Variant
i	COMP
j	PPRM1
k	PPRM3
l	TBL

OnlineAllocation

Type of Processing Unit

Power consumption scatter plot of some SBox design variants



Implementation of OnlineAllocation on top of an FPGA by means of

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

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

Point in Time	Design Variant
i	COMP
j	PPRM1
k	PPRM3
l	TBL

S. A. Huss and M. Stöttinger, „A Novel Mutating Architecture for Embedding Multiple Countermeasures Against Side-Channel Attacks“, in P. Mishra, S. Bhunia, M. Terhanipoor (eds.), „Hardware IP Security and Trust“, Springer, 2017.

M. Stöttinger, „Mutating Runtines Architectures as a Countermeasure Against Power Analysis Attacks“. PhD thesis, Techn. Univ. Darmstadt, 2012.

DynamicBinding

Degree of Parallelism

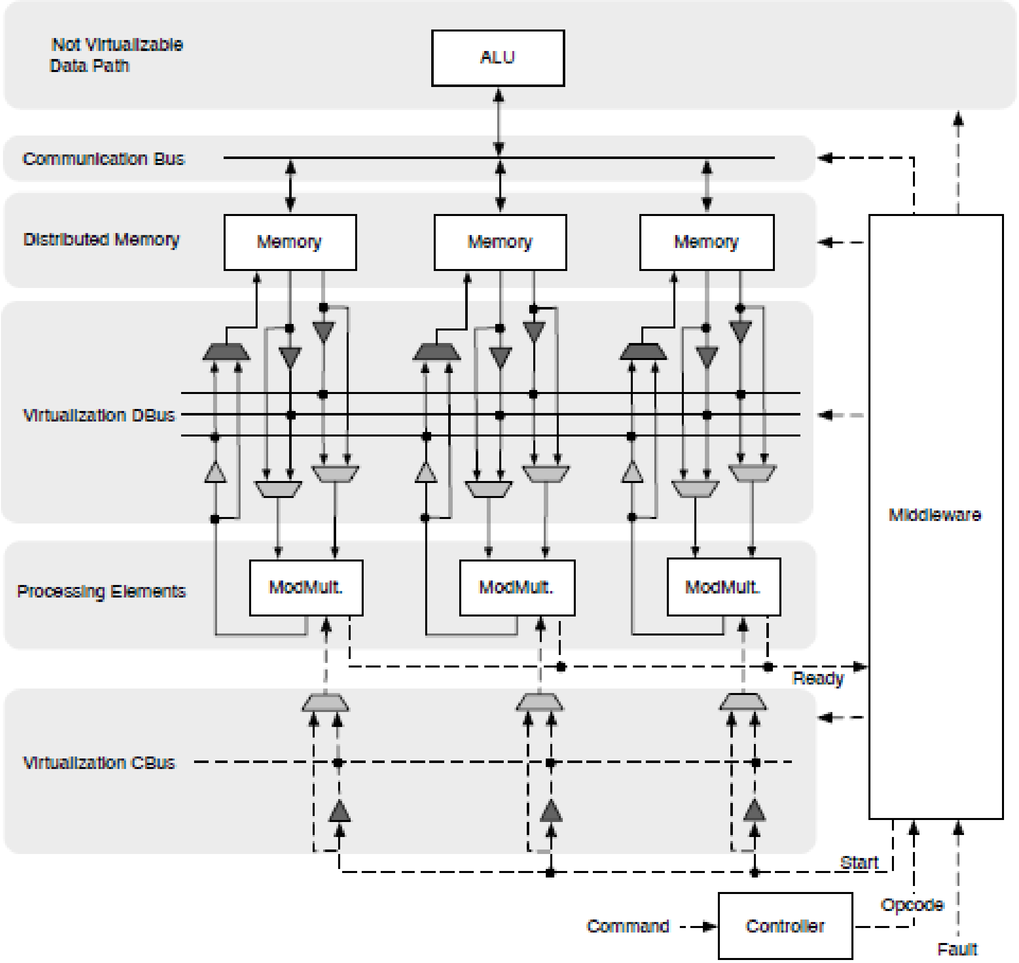
Change at runtime the link between activity and ressource instance(s) by

- Random concurrent binding
- Virtualization

on top of an executive layer, which organizes the links beween achivities and executing ressources.

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

Example: Virtualized ECC cypher under Middleware control



M. Stöttinger, A. Biedermann, S. A. Huss, „Virtualization within a Parallel Array of Homogenous Processing Units“, In P. Sirisuk, F. Morgan, T. A. El-Ghazawi, H. Amano (eds.), ARC, LNCS, vol. 5992, Springer, 2010.

A. Biedermann, S. A. Huss, „A Methodology for Invasive Programming on Virtualizable Embedded MPSoC Architectures“, ICCS, Elsevier, 2013.

FlexibleScheduling

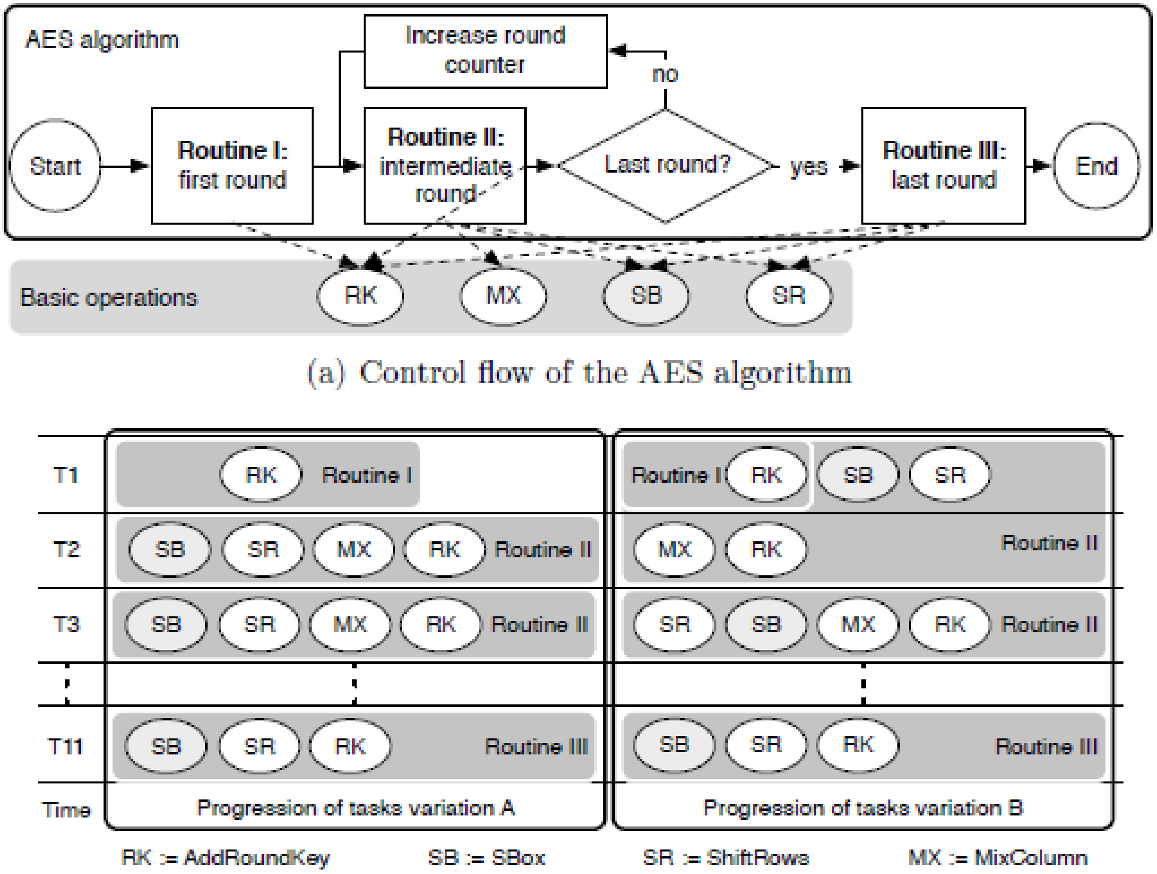
Progression of Tasks

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



(a) Control flow of the AES algorithm

(b) Example of rearranged basic operations in a routine

FlexibleScheduling

Progression of Tasks

Goal

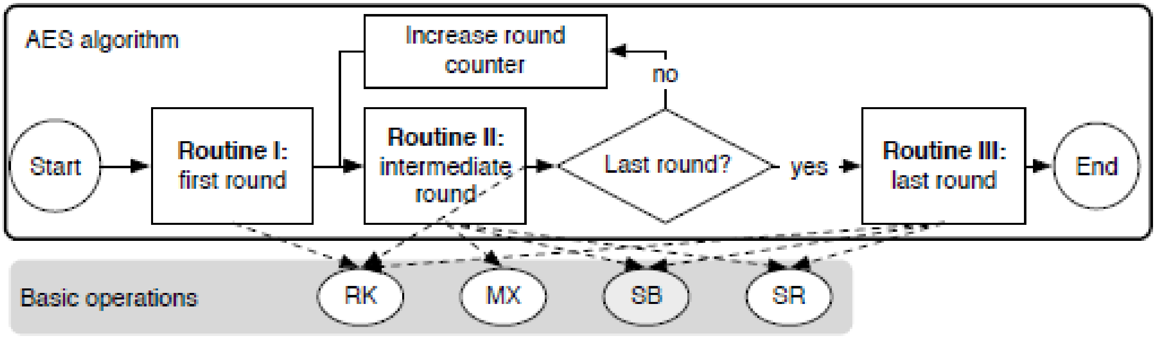
Change execution behavior during runtime by manipulated sequences of data-independent basic operations (‚shuffling‘)

Approach

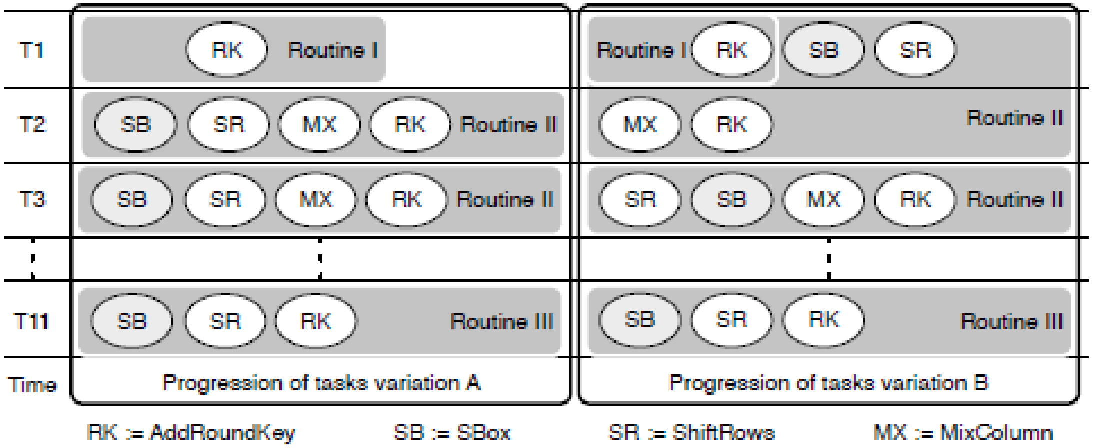
- Execute basic operations on mutable, online relocable processing units
- Modify frequently the number of in-parallel operating units by applying a dynamic binding

Result

Complex power distribution acting as an additional counter-measure by combining effects from DynamicBinding and OnlineAllocation manipulations



(a) Control flow of the AES algorithm

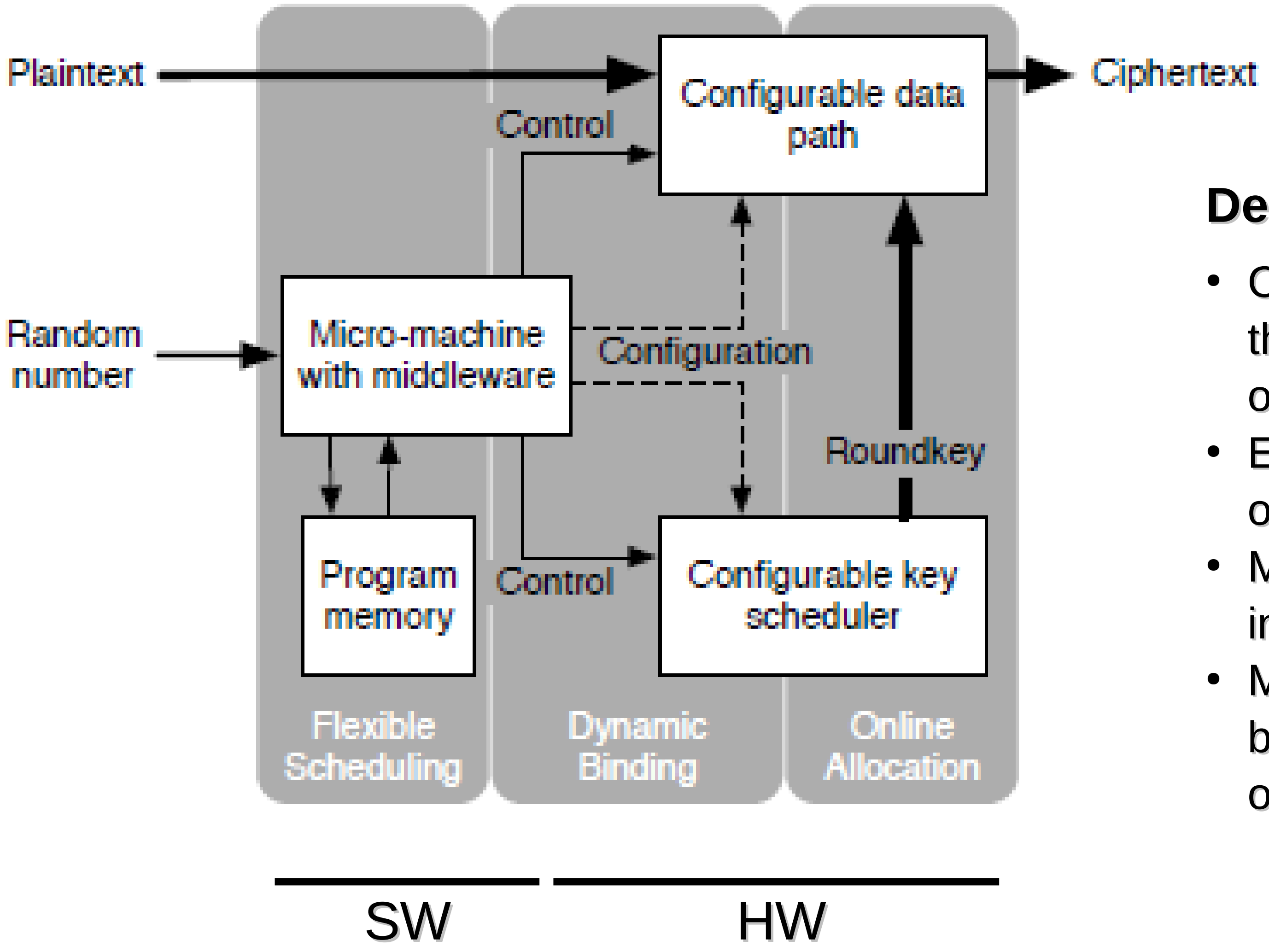


(b) Example of rearranged basic operations in a routine

Application Example

Block Cipher AES 128 bit

HW/SW Architecture of AES Mutate



Design objectives

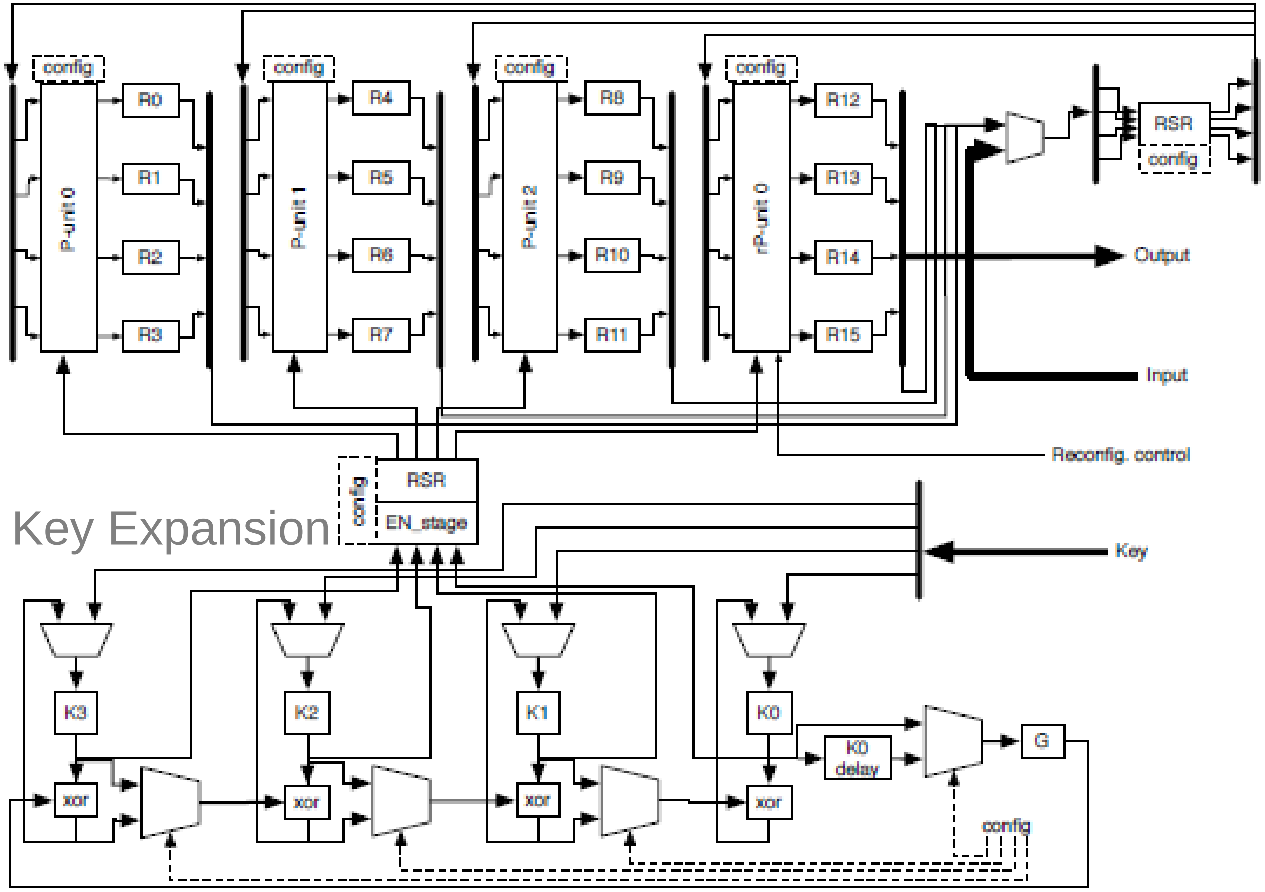
- Change dynamically the degree of in-parallel operating SBox units
- Execute SBox operation on different unit designs
- Merge round operations into one clock cycle
- Manipulate the word-width being processed during one clock cycle

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

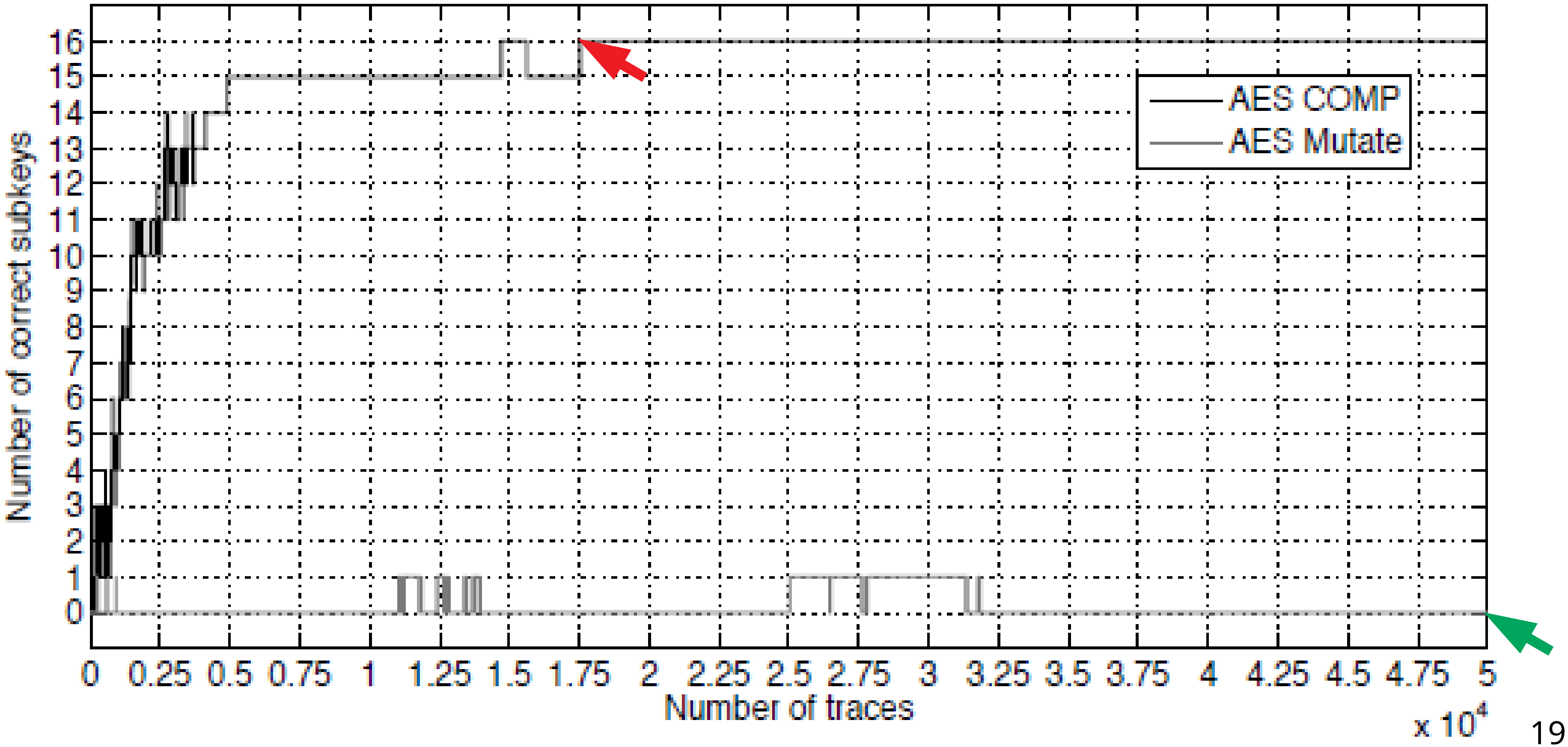
Plaintext to Ciphertext



Key Expansion

SCA Results

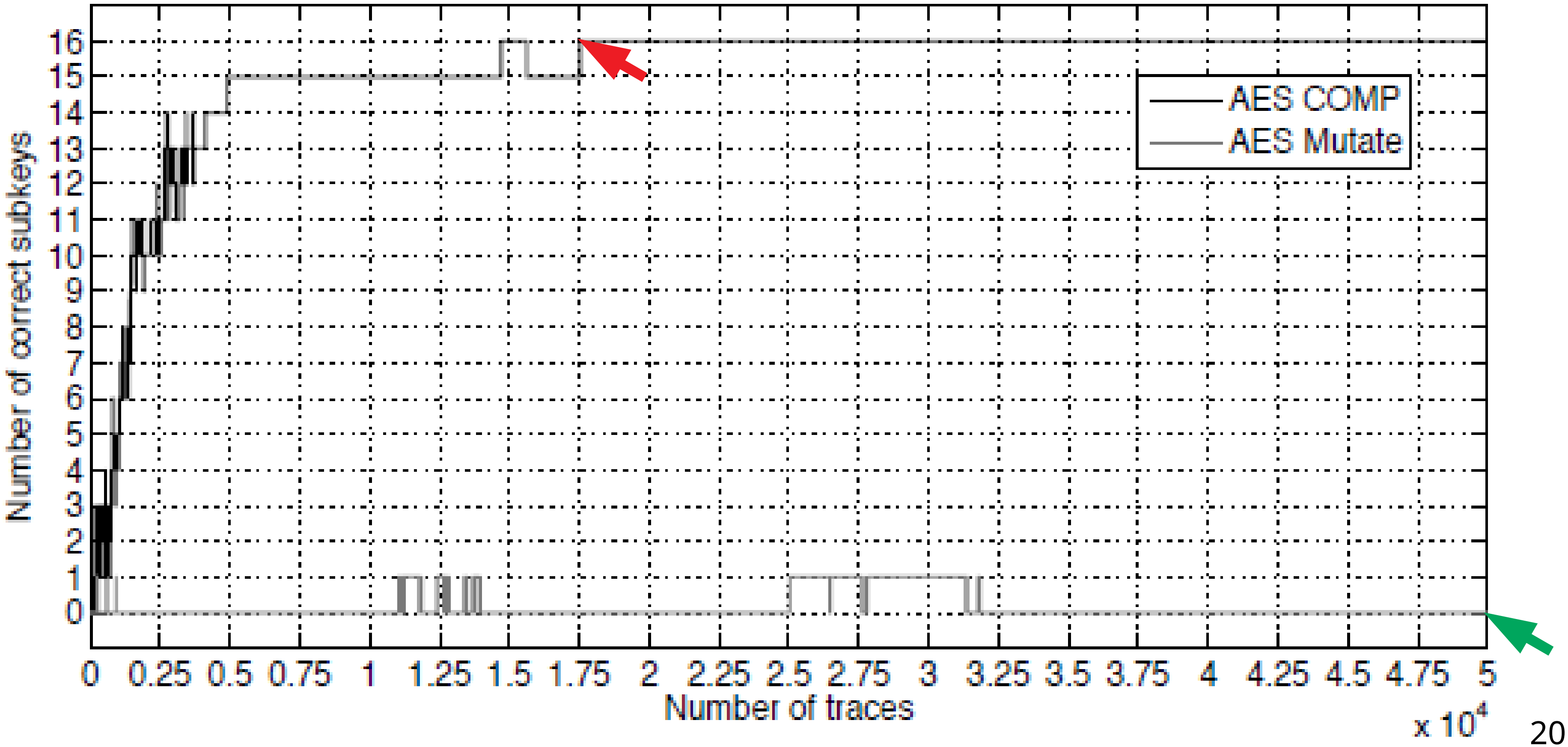
- SASEBO-GII board
- 450k traces in profiling phase of Stochastic Approach
- 50k traces in attack phase



SCA Results

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

N. Belleville, D. Courousé, K. Heydemann, H.-P. Charles, „Automated Software Protection for the Masses against Side-Channel Attacks“, ACM Trans. on Arch. and Code Opt., 1, 1, 2017.



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

- **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

- **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

- **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!