

Johann Großschädl

University of Bristol, Department of Computer Science

Woodland Road, Bristol BS8 1UB, United Kingdom

<http://www.cs.bris.ac.uk/~johann/>

Micro-Architectural Countermeasures Against Side-Channel Attacks

(joined work with Dan Page and Philipp Grabher)

Rump Session of CHES 2008, Washington, D.C., August 12, 2008

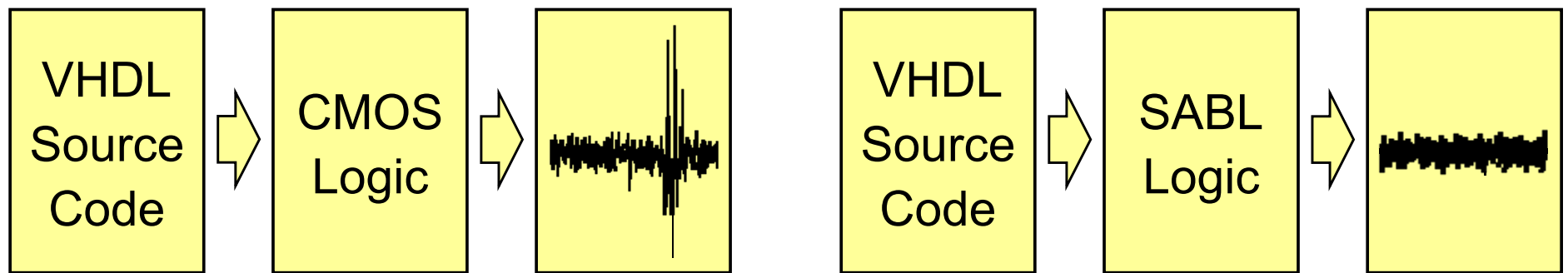


Micro-Architecture

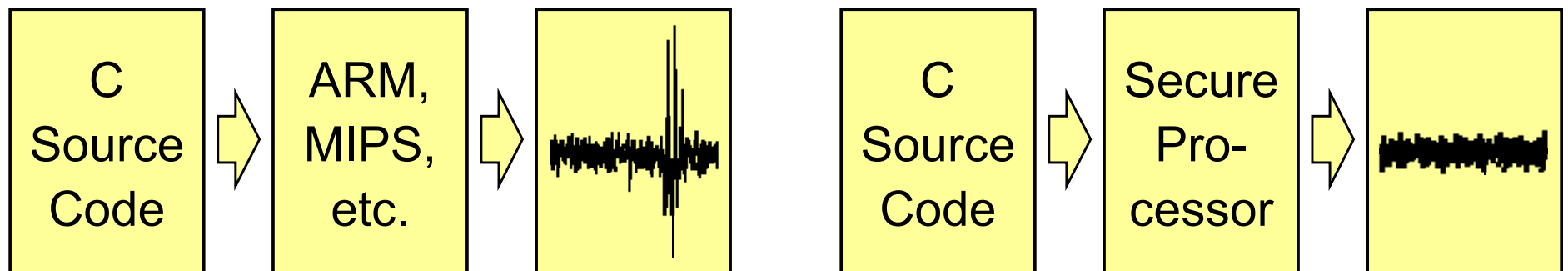
- “Destructive” Use: Side-Channel Attacks
 - Cache-based SCA
 - Branch prediction attacks
- “Constructive” Use: Countermeasures
 - Generic and algorithm-independent
 - Little or no impact on execution time, power, area, etc.
 - Countermeasures against DPA
 - Detection of faults in instruction stream

Generic Countermeasures

- Hardware: SCA-Resistant Logic Style



- Software: SCA-Resistant Micro-Architecture



Examples

- **Randomize Power Consumption of Multiplier**
 - Multiplier = array or tree of carry-save adders
 - Add (and subtract) a random number
 - Makes DPA of RSA/ECC more costly
- **Randomize Instruction Sequence**
 - Sequences of independent instructions can be executed in arbitrary order (or even in parallel)
 - Random re-ordering of instructions
- **“Fingerprinting” of Instruction Stream**
 - Hash all instructions that arrive at the instruction decoder
 - Compare hash values to detect faults in instruction stream

Implementation

- CRISP Project

- Cryptographic RISC Processor
- 32-bit RISC processor with instruction set extensions for crypto processing and built-in countermeasures against side-channel attacks

- Further References

- Presentation tomorrow by Philipp Grabher
- Upcoming paper at IACR eprint archive
- Homepage of CRISP project
<http://www.cs.bris.ac.uk/home/page/research/crisp.html>