Fraunhofer
AISEC

# A Cost-Effective FPGA-based Fault Simulation Environment

Angelika Janning, Johann Heyszl, Frederic Stumpf and Georg Sigl

28th September 2011

# Outline

Fraunhofer AISEC

1. Motivation
2. FPGA-Based Fault Simulation Environment
3. ECC Case Study

# Outline

Fraunhofer AISEC

1. Motivation
2. FPGA-Based Fault Simulation Environment
3. ECC Case Study

Fraunhofer AISEC

**Fault attacks** - Attackers inject faults to recover secrets.

- Glitches in power or clock supply.
- Optical attacks (e.g., laser).

**Powerful threat for cryptographic implementations**.

Fraunhofer AISEC

**Cryptographic implementations must be protected.**

Fraunhofer AISEC

**Cryptographic implementations must be protected**.

- Physical level.
  Voltage, light sensors.

Fraunhofer AISEC

**Cryptographic implementations must be protected**.

- Physical level.
  Voltage, light sensors.
- General, algorithmic error detection methods.
  Duplication or redundancy.

Fraunhofer AISEC

**Cryptographic implementations must be protected**.

- Physical level.
  Voltage, light sensors.
- General, algorithmic error detection methods.
  Duplication or redundancy.
- Dedicated, algorithmic detection or prevention.
  E.g. point validity check for ECC.

Fraunhofer AISEC

**Cryptographic implementations must be protected**.

- Physical level.
  Voltage, light sensors.
- General, algorithmic error detection methods.
  Duplication or redundancy.
- Dedicated, algorithmic detection or prevention.
  E.g. point validity check for ECC.

**Countermeasures must be verified**.

Fraunhofer AISEC

**Laboratory.**

- Late in design flow.
- Highly complicated.
- Difficult to reach high coverage.

Fraunhofer AISEC

**Laboratory.**

- Late in design flow.
- Highly complicated.
- Difficult to reach high coverage.

**Simulation.**

- Earlier in design flow.
- Fault models for abstraction.
- High performance and coverage possible.

Fraunhofer AISEC

Two choices for hardware simulation.

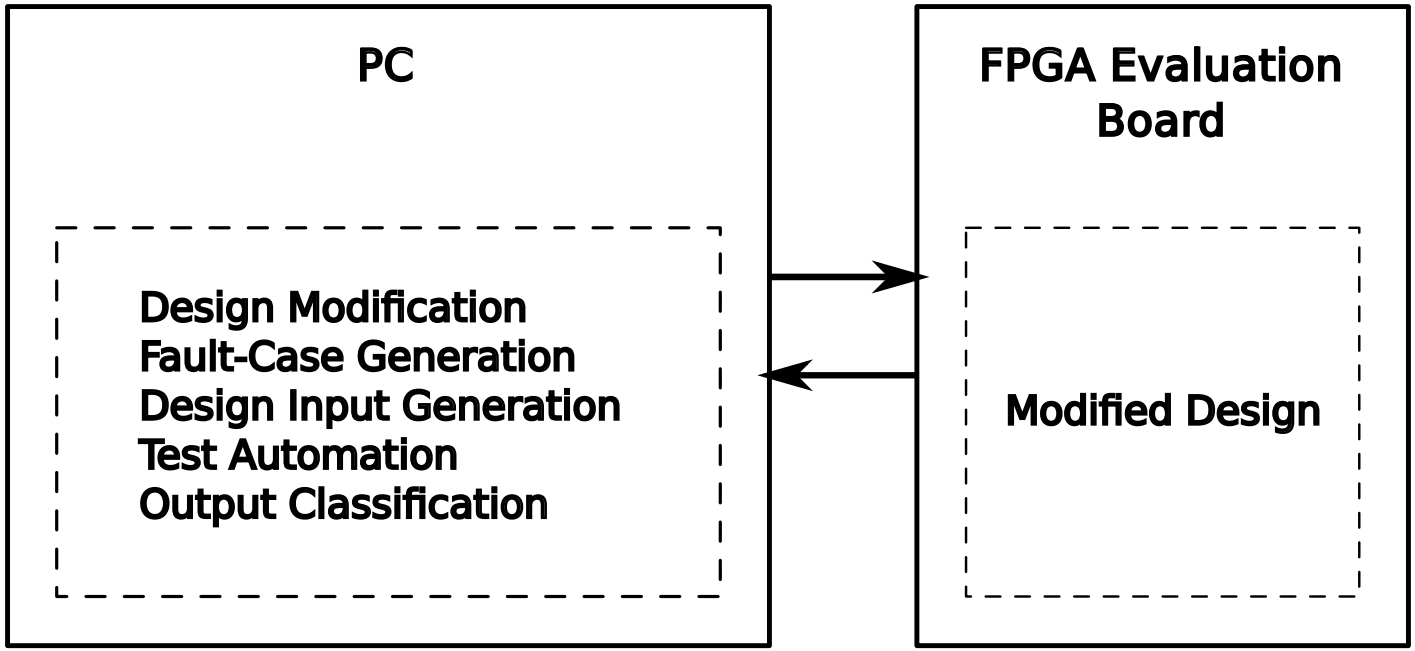
1. **Software-based simulation.**
   - Performance low for large designs.
2. **FPGA-based simulation.**
   - Performance high.

# Outline

Fraunhofer AISEC

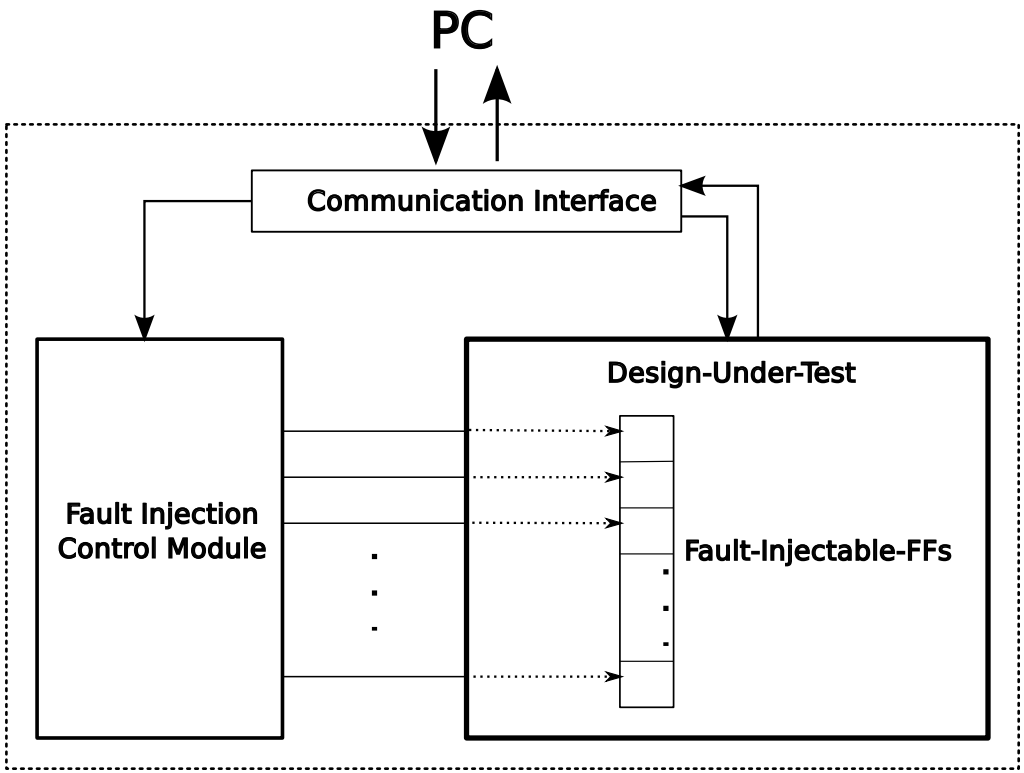
1. Motivation
2. FPGA-Based Fault Simulation Environment
3. ECC Case Study

For digital hardware designs of cryptographic algorithms.



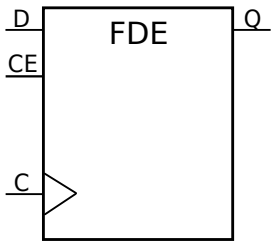
## Design-Under-Test (DUT) is modified through script.

- Replace flip-flops.
- Netlist.
- New top-level.
- Additional fault injection control and communication module.



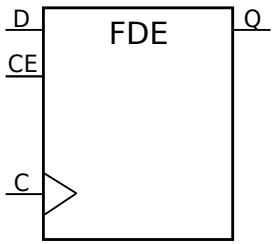
Fraunhofer AISEC

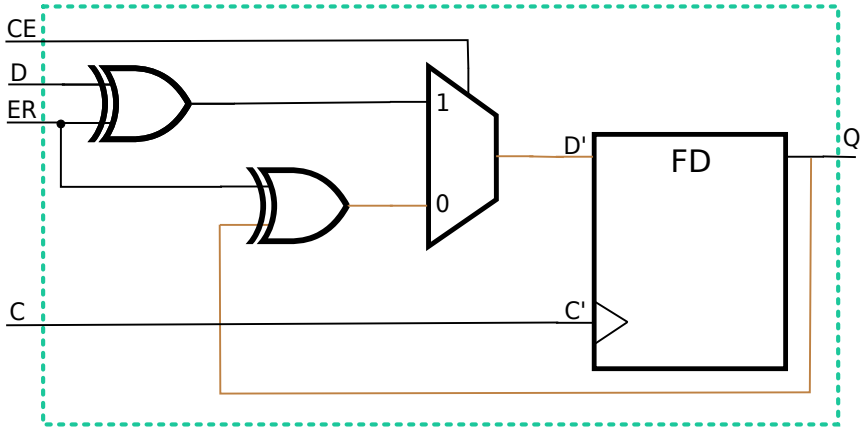
## Flip-flop cell replacement.



Fraunhofer AISEC

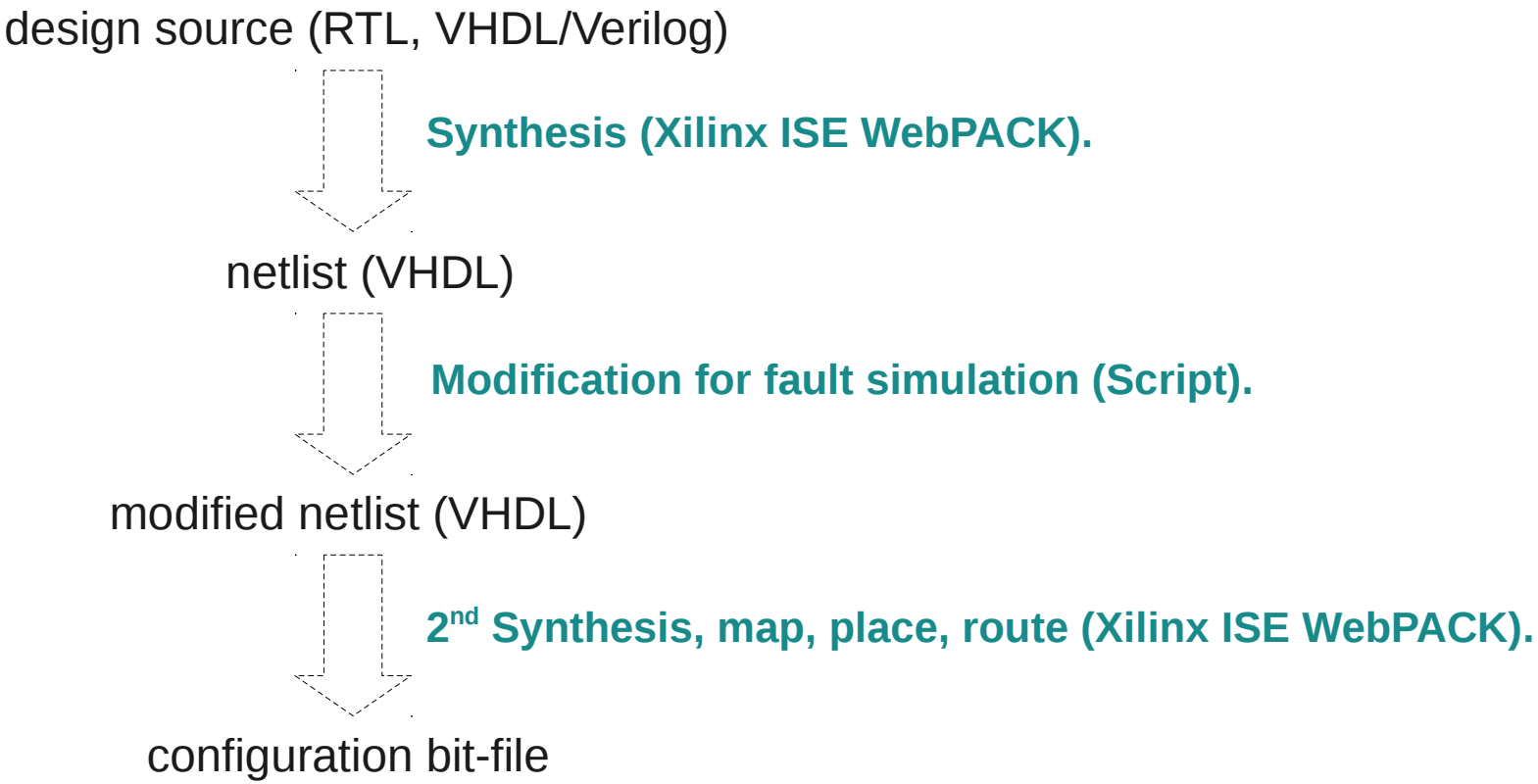
## Flip-flop cell replacement.



# Design Flow Integration

## FPGA-Based Fault Simulation Environment



Fraunhofer AISEC

**Fault model specific for fault attacks**.

**Fault model specific for fault attacks**.

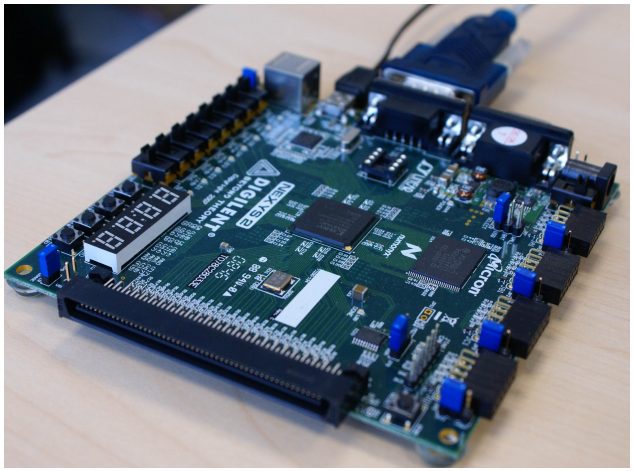
- Complete timing control.
- Complete location control.
  All single or multi-bit faults.
- Bit flip effect.
- Transient (one cycle) fault duration.

Fault model can be further restricted.

**Fault-case generation automated**.

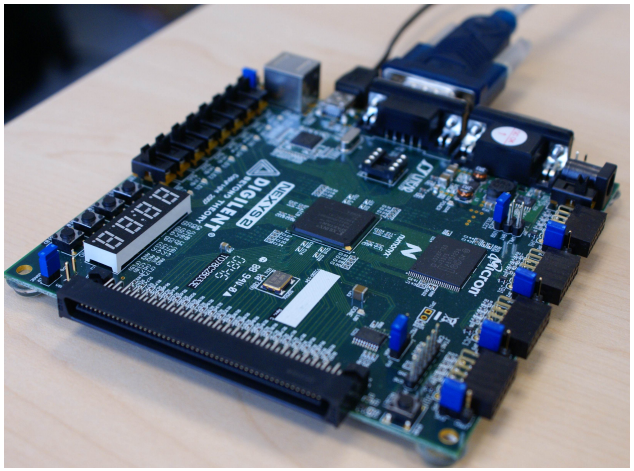
- Requires list of fault-injectable flip-flops.
- Requires fault configuration.
- Outputs list of fault test cases.
  If space to large, random choice of subset.

## **Simulation is automated**.



1. FPGA configured with modified design.
2. All fault cases are performed. For every case:

## **Simulation is automated**.



1. FPGA configured with modified design.
2. All fault cases are performed. For every case:
   - Fault injection control module re-configuration.
   - Start simulation.
   - Collect output and store testcase outcome.

**Available information.**

- DUT output vs. expected output.
- DUT status indication.
- Timing compliance.

**Available information.**

- DUT output vs. expected output.
- DUT status indication.
- Timing compliance.

**Fault case simulation outcome.**

1. Silent - still correct.
2. Detected - detected fault.
3. Fault - faulty result output.
4. Timeout - No response.

# Simulation Environment Conclusion

Fraunhofer AISEC

- **FPGA-based for high performance.**
- **Supports Verilog and VHDL designs.**
- **Automated modification on netlist - no design effort.**
- **Cost-effective Tooling.**

# Outline

Fraunhofer AISEC

1. Motivation
2. FPGA-Based Fault Simulation Environment
3. ECC Case Study

Fraunhofer AISEC

**DUT** =
Digital hardware design of **Elliptic Curve Scalar Multiplication**.

- **Countermeasure** against fault attacks:
  **point validity check** at the end of computation.
  $\rightarrow$ This countermeasure is evaluated.

Fraunhofer AISEC

**Fault model configuration:**

- Derived from fault attacks on ECC.
- Every clock cycle during ECSM.
  - $95,000$ cycles.
- Transient (one cycle) faults.
- Bit-flip fault effect.
- Single bit (to simplify case study) faults in all registers.
  Split simulation in two parts:
  - $1,600$ data-path flip-flops.
  - $90$ control-path flip-flops.

Fault injection **hardware overhead** for DUT $\sim +25\,\%$.

**Simulation performance** of 16 *ms* per test-case.

- DUT at **50** *MHz*.
- RS232 transmission more than **70%**.

Fraunhofer AISEC

Simulation in two parts:

- **Control-path flip-flops.**
  - $\sim$ 9 million test-cases.
  - 100 % coverage.
- **Data-path flip-flops.**
  - $\sim$ 35 million test-cases.
  - 22 % coverage.

Fraunhofer AISEC

Simulation in two parts:

- **Control-path flip-flops.**
  - $\sim$ 9 million test-cases.
  - 100 % coverage.
- **Data-path flip-flops.**
  - $\sim$ 35 million test-cases.
  - 22 % coverage.

9 **days of simulation** $\sim$ 46 years in software simulation.

Fraunhofer AISEC

**Control-path**.

- 1 % Timeouts.
- 38 % Silent faults.
- 44 % Detected faults.
- 18 % **Faults**.
  In most cases program counter was manipulated and intermediate values output. → **Serious problem.** → **Countermeasure required**.

# Simulation Results, cont'd

ECC Case Study

Fraunhofer AISEC

**Control-path**.

- 1 % Timeouts.
- 38 % Silent faults.
- 44 % Detected faults.
- 18 % **Faults**.
  In most cases program counter was manipulated and intermediate values output. → **Serious problem.** → **Countermeasure required**.

**Data-path**.

- 0 % Timeouts.
- 24 % Silent faults.
- 77 % Detected faults.
- 0.02 % **Faults**.
  Most changed output after point check. → **Useless for attacker**.

# Case Study Conclusion

Fraunhofer AISEC

- **Speed-up of $\sim$ 2000 compared to software simulation.**
- **Point validity check countermeasure proved very effective.**
- **However, weaknesses were successfully exposed.**
  - **Control path needs protection.**
  - **Detected faults can be used for safe-error attacks.**