Towards the Automatic Application of Countermeasures Against Physical Attacks

Francesco Regazzoni

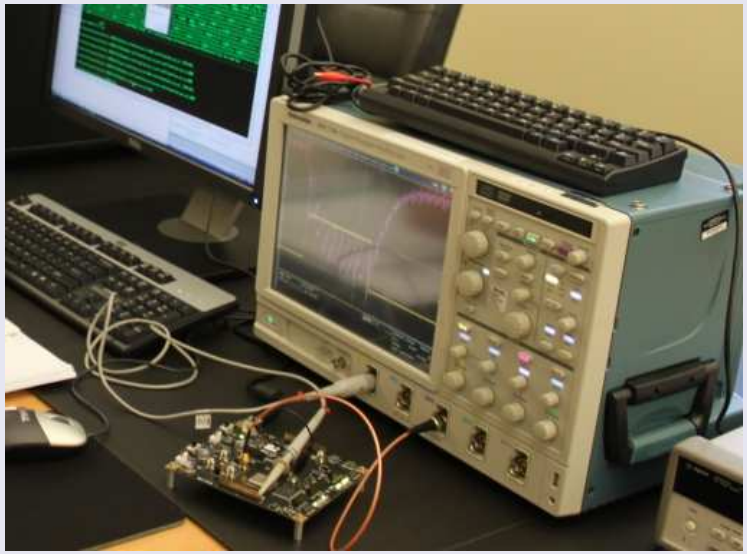
Acknowledgments

Work in collaboration with:

- Paolo Ienne, Ali Galip Bayrak, Alessandro Cevrero, Yusuf Leblebici, Stéphane Badel, Johann Großschädl, Axel Poschmann, Zeynep Toprak, Marco Macchetti, Laura Pozzi, Christof Paar, Frank Gurkaynak, François-Xavier Standaert, Theo Kluter, Philip Brisk, Michael Schwander, Thomas Eisenbarth

What are Physical Attacks

- Physical attacks recover secrets by exploiting the implementation

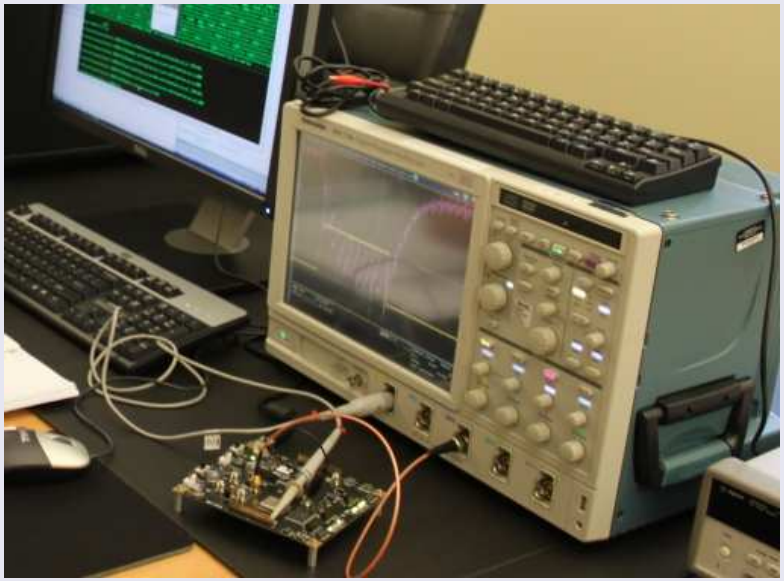


Physical Attacks: the Weakest Point

Active

Fault Injection

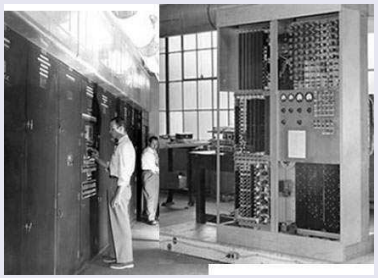
Passive



Power Analysis
Timing Analysis

Why Physical Security is so Important Today?

Long Time Ago



Past

Present

Mainframes

Personal Computer

Pervasive

From Axel Poschmann

Power Analysis Attacks

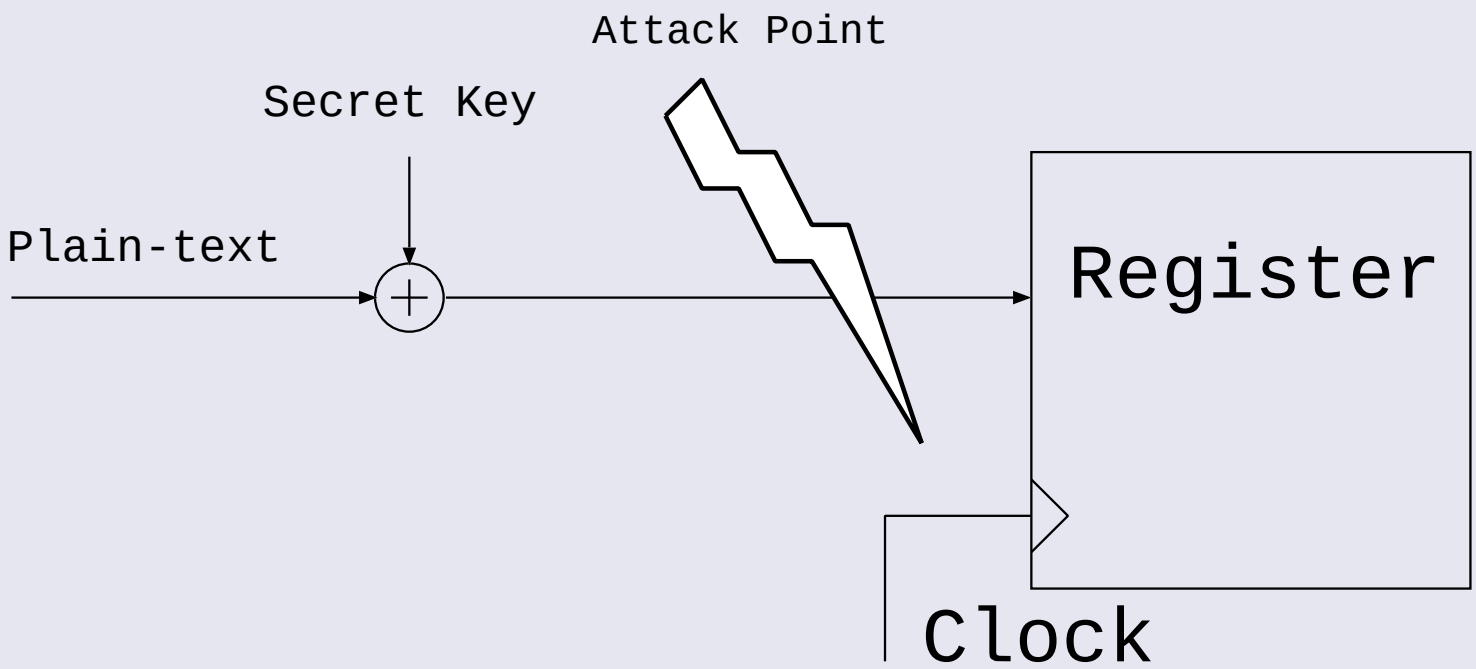
Paul Kocher, Joshua Jaffe, and Benjamin Jun, "**Differential Power Analysis**", in Proceedings of *Advances in Cryptology-CRYPTO'99*, Santa Barbara, California, USA, August 15-19, 1999. (Cited by 3169)

- Cheap
- Powerful

Examples

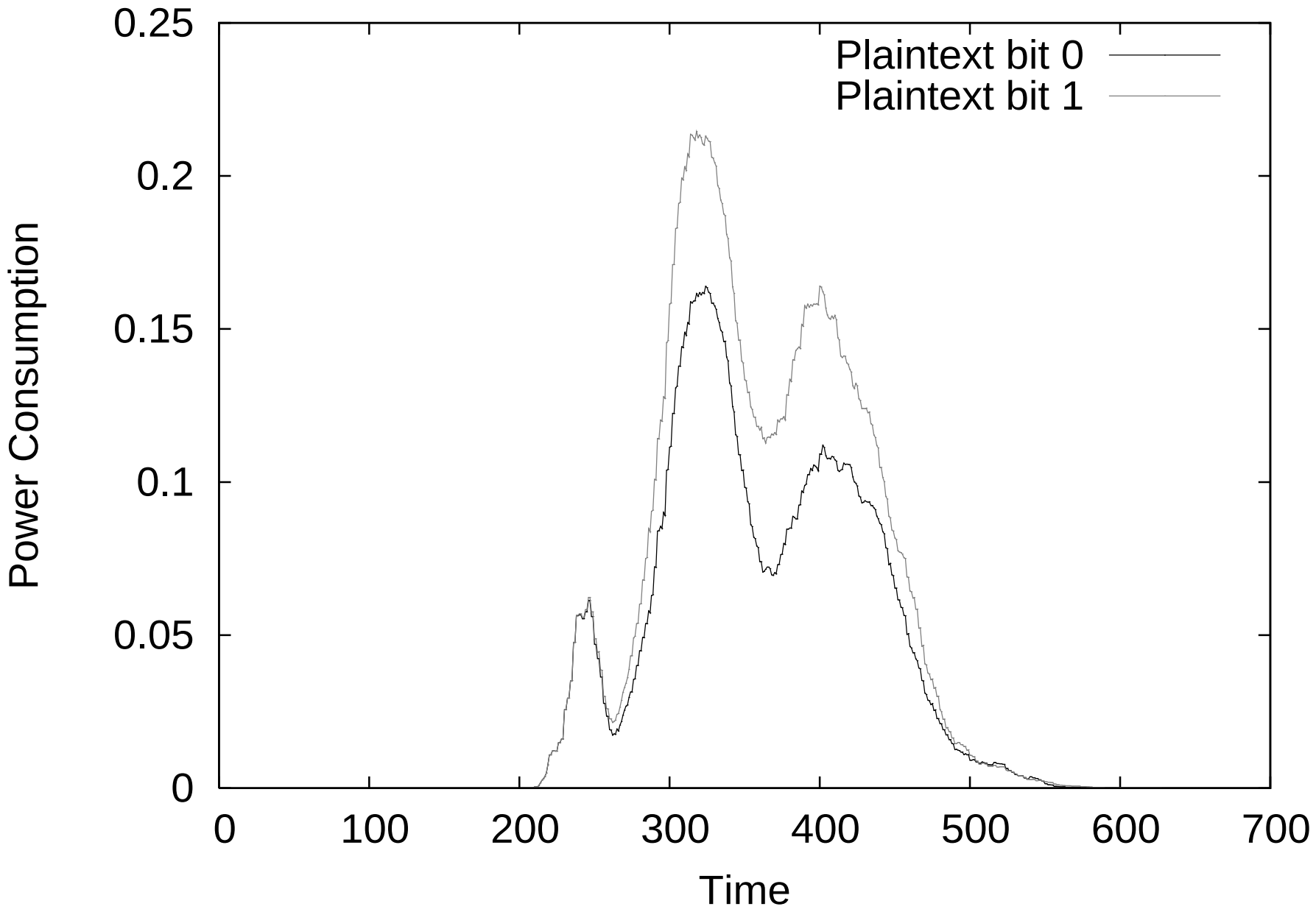
- Simple Power Analysis
- Differential Power Analysis

Simple Power Analysis 1/2

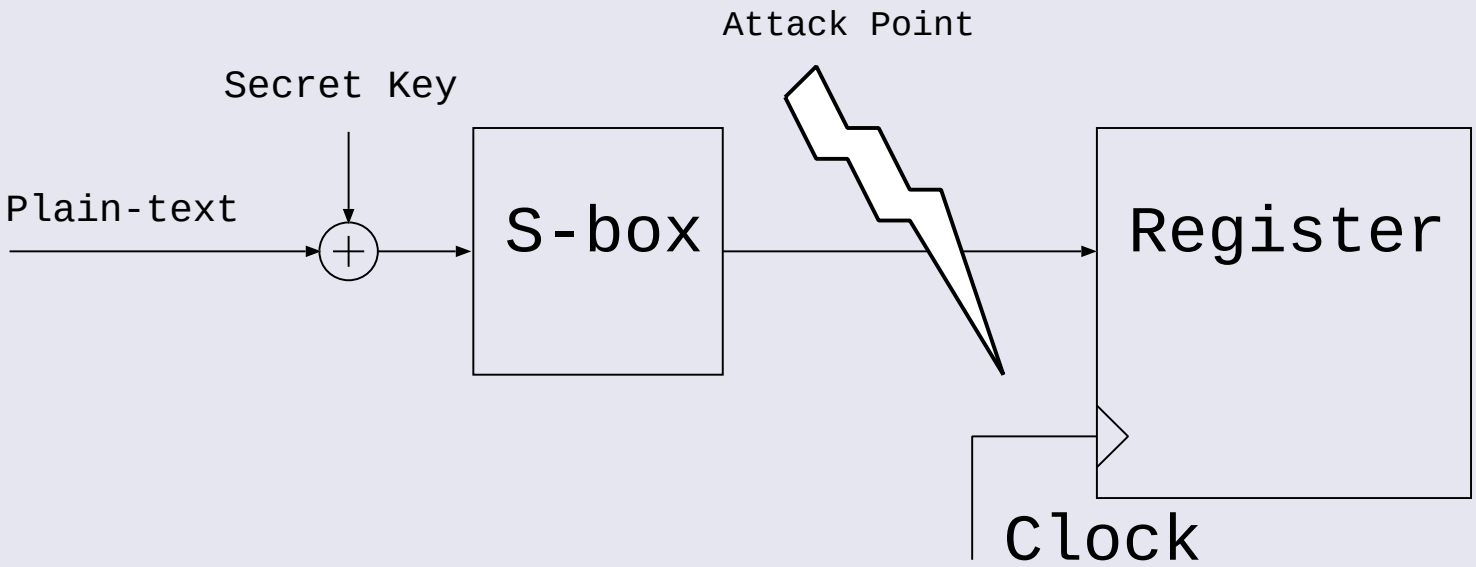


- Details of the implementation are needed
- The key is directly inferred from the power traces

Simple Power Analysis 2/2

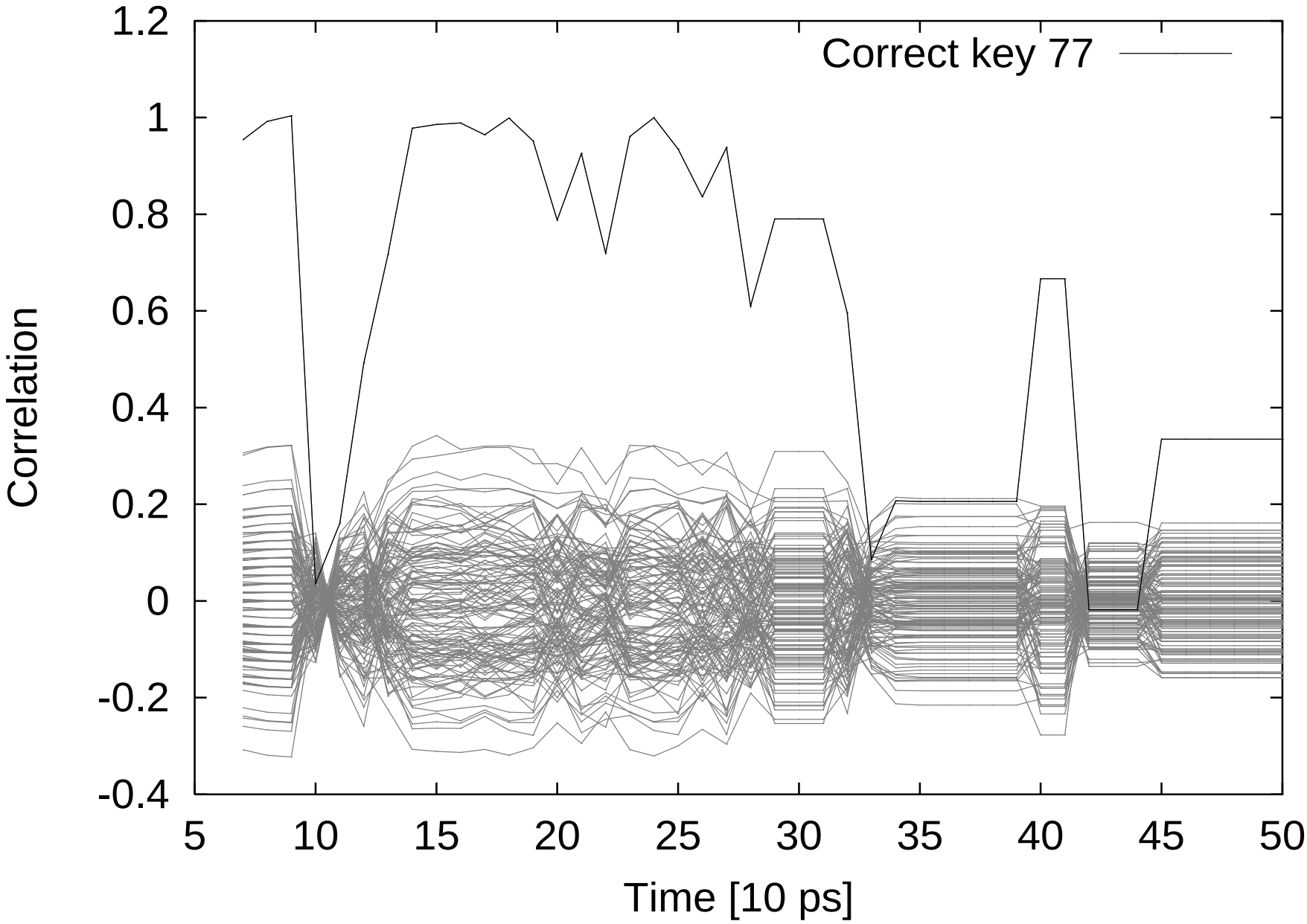


Differential Power Analysis 1/2



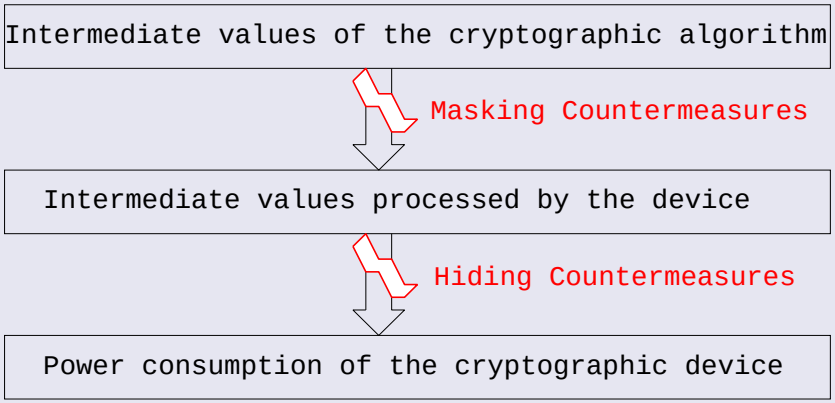
1. Choose an intermediate result of the executed algorithm
2. Measure the power consumption of several encryption
3. Calculate hypothetical intermediate values based on a key guess
4. Map intermediate values to hypothetical power consumption values
5. Compare hypothetical power consumption values with power traces

Correlation with Hamming weight



Countermeasures

Power consumption **independent** from processed key dependent data



Inspired from: Power analysis attacks: Revealing the secrets of smart cards (Stefan Mangard, Elisabeth Oswald, Thomas Popp)

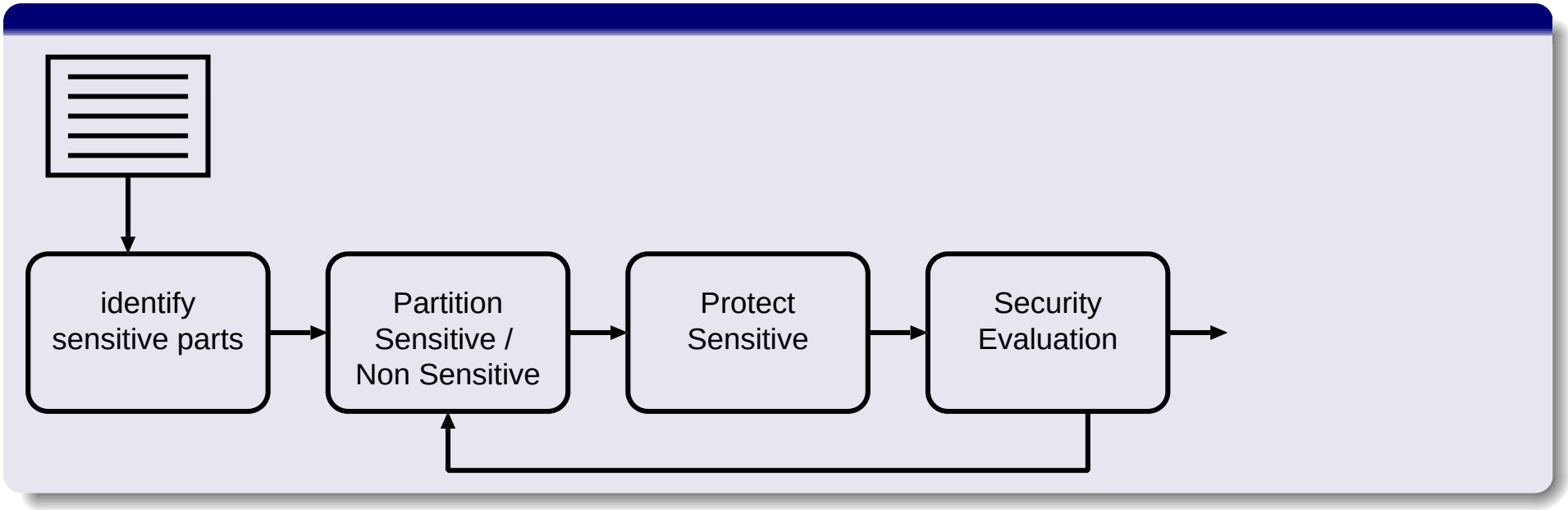
They can be implemented in **Software** or in **Hardware**

Missing tools supporting physical security

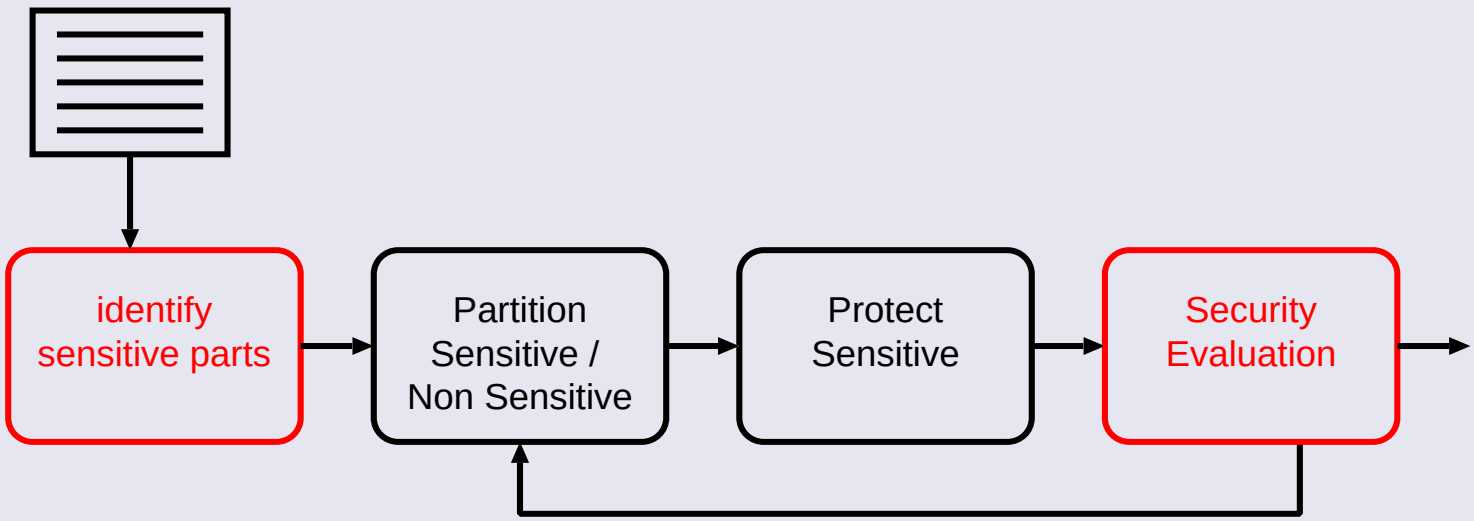
- Embedded systems are **already** used for sensitive applications

- Security is very often considered at later stages of design
- Cost and Time to Market
- Possible Security pitfalls

Enabling the automatic design for DPA resistance

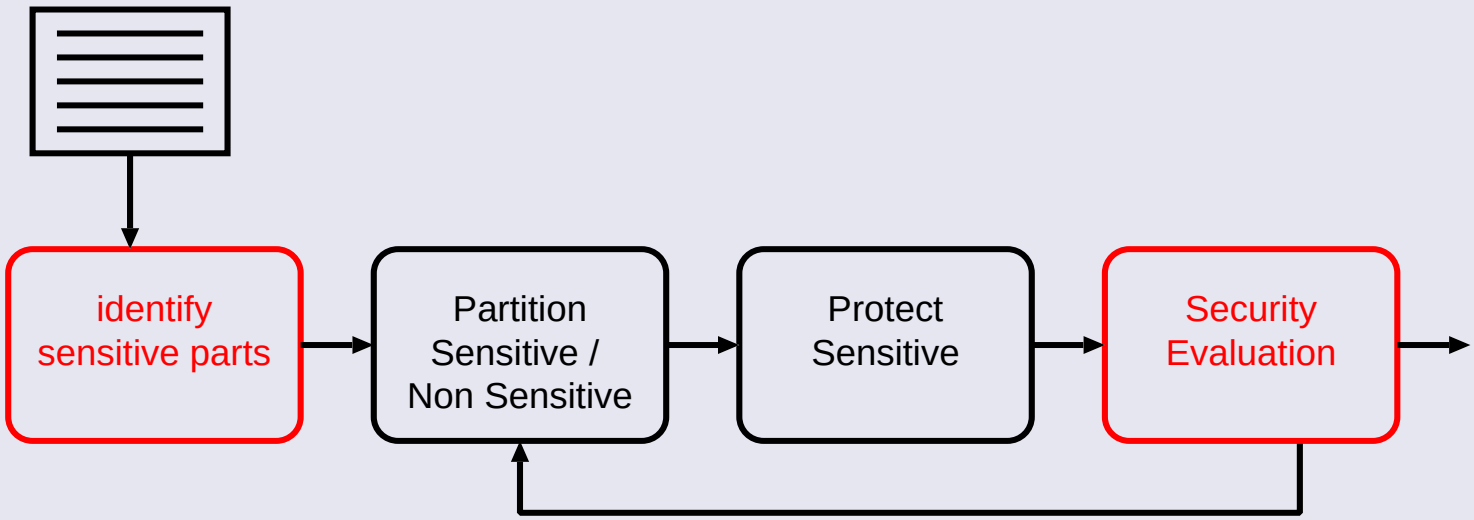


Needed "Basic Blocks"



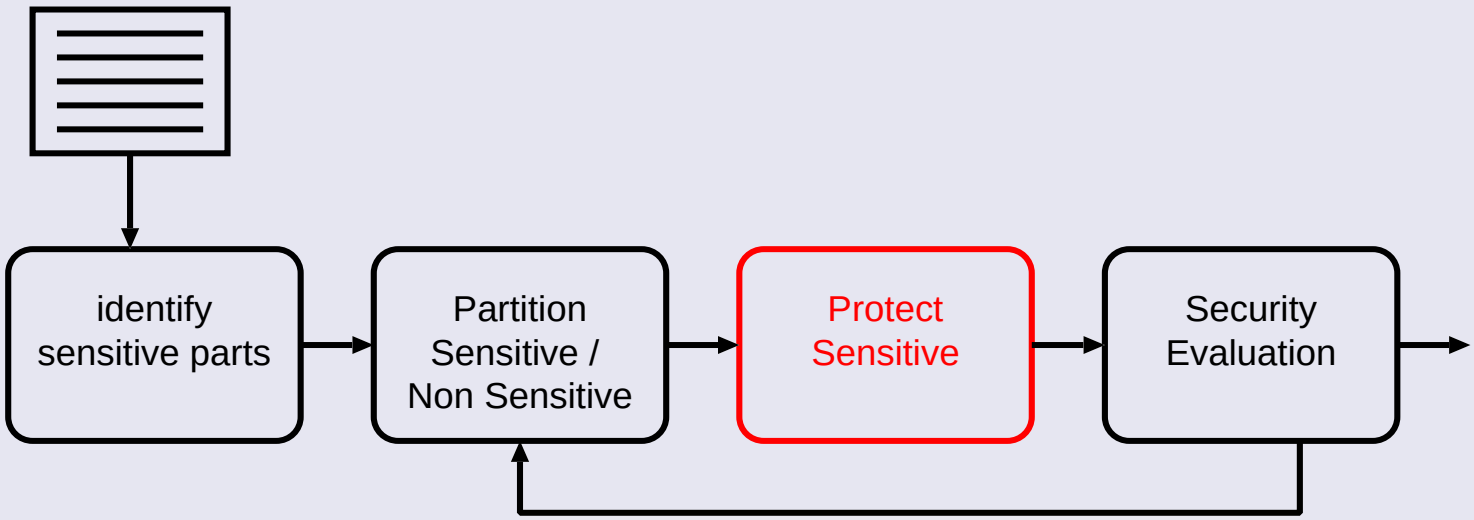
- Generate useful power traces?

Needed "Basic Blocks"



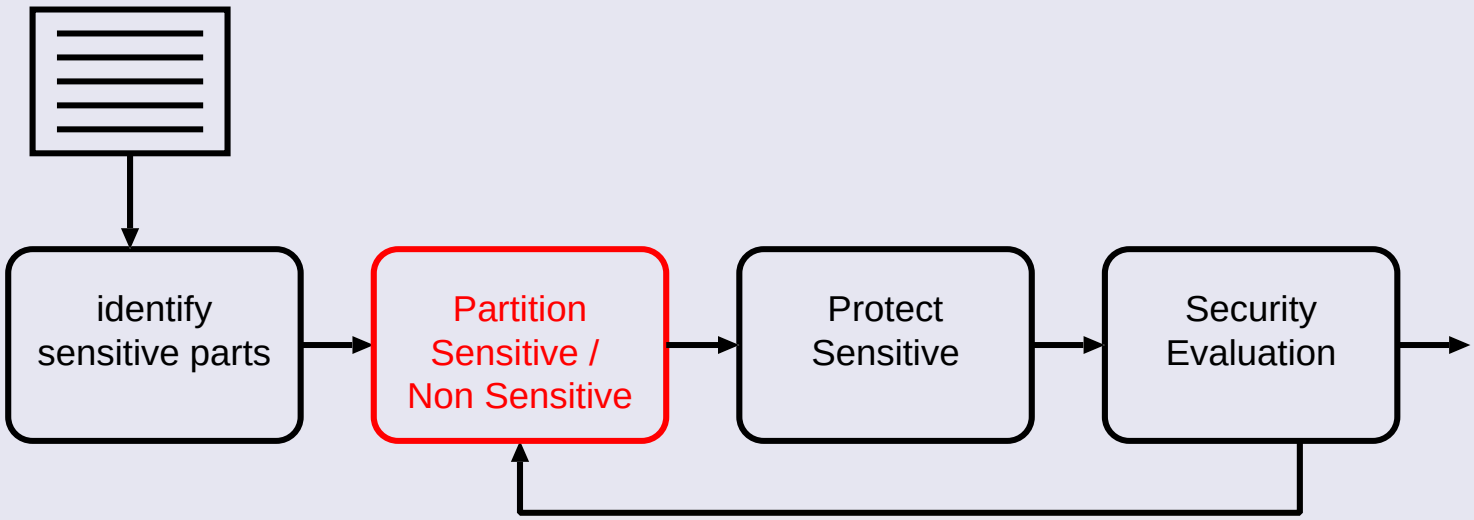
- Generate useful power traces?
- Measure the DPA resistance?

Needed "Basic Blocks"



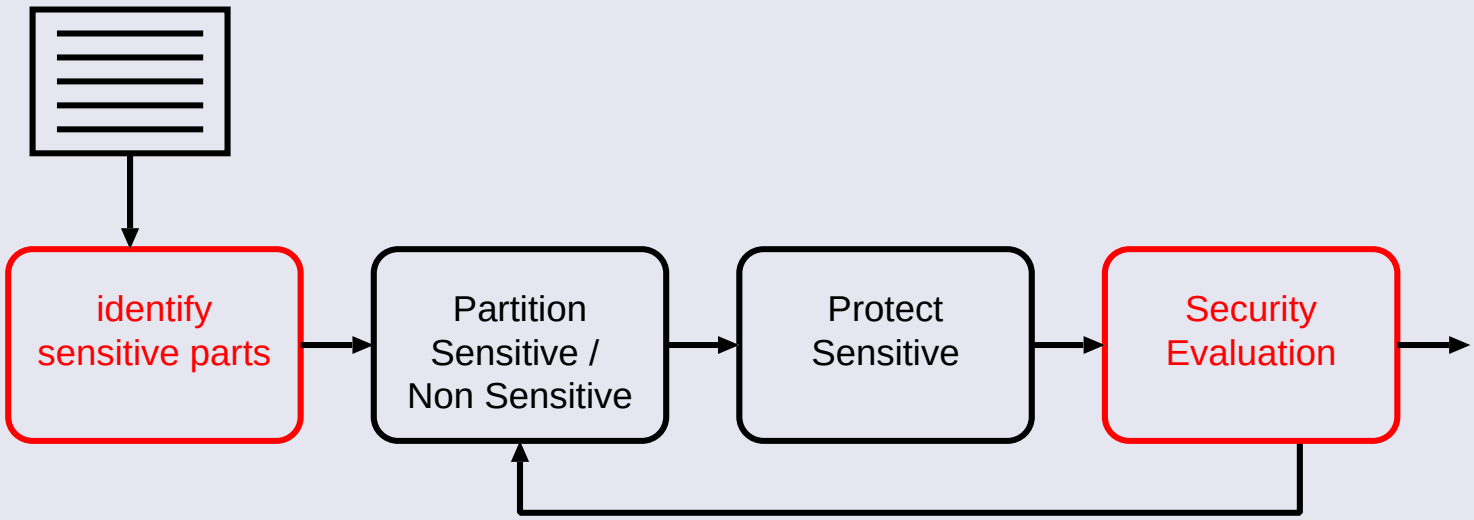
- Generate useful power traces?
- Measure the DPA resistance?
- Countermeasure and its design flow?

Needed "Basic Blocks"



- Generate useful power traces?
- Measure the DPA resistance?
- Countermeasure and its design flow?
- Partition the algorithm?

Needed "Basic Blocks"

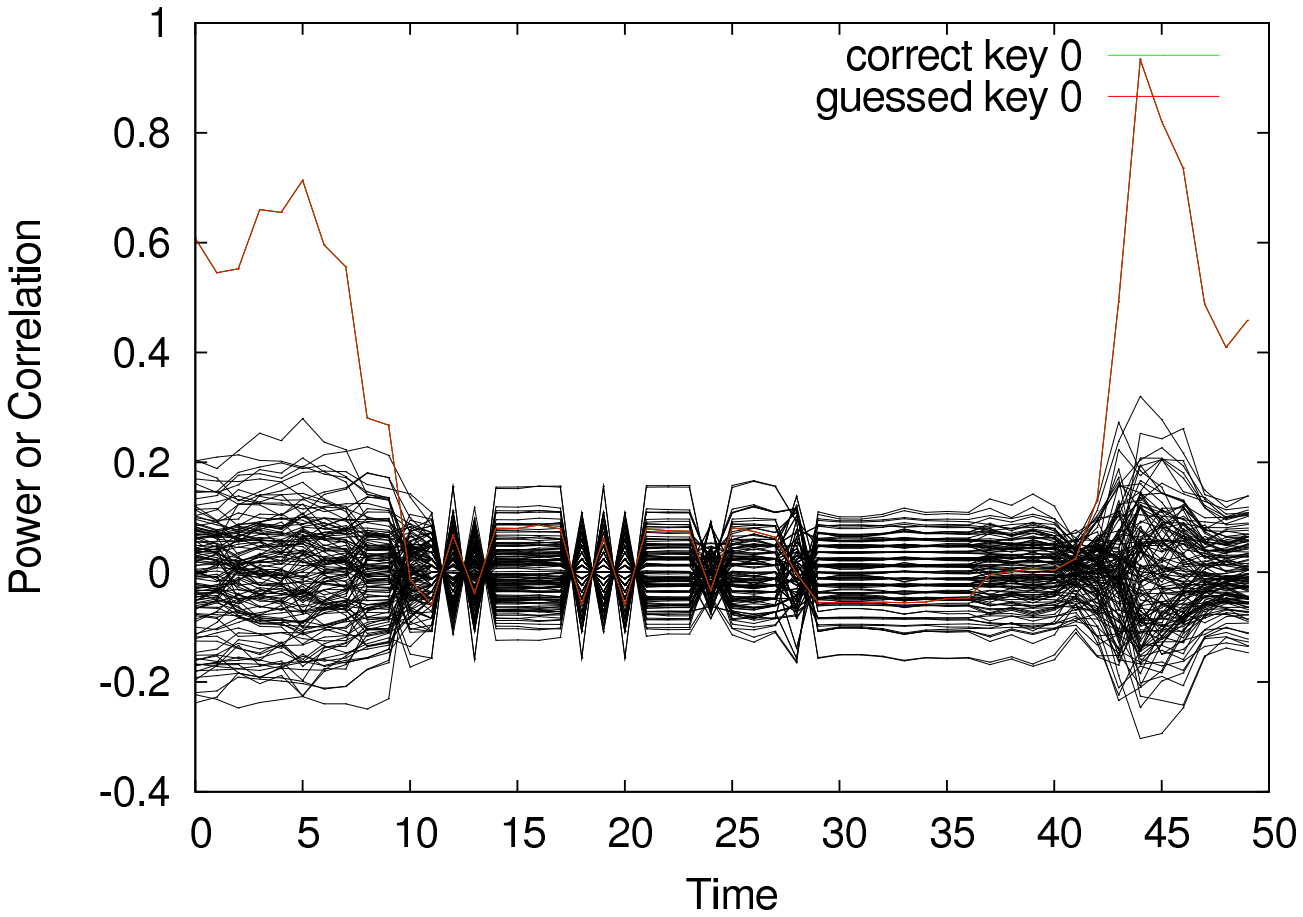


- Generate useful power traces?
- Measure the DPA resistance?
- Countermeasure and its design flow?
- Partition the algorithm?

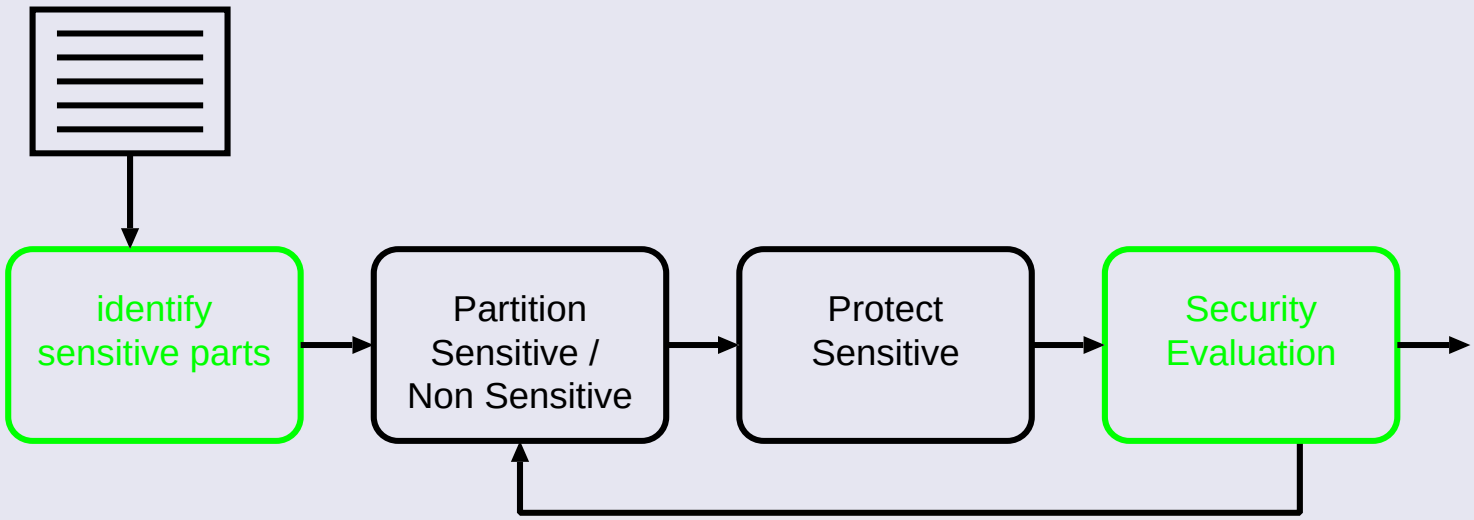
Fast Simulation SPICE level

Simulate Complex Design at SPICE level (whole processor)

Simulated about 400 traces: approximately 20 hours!

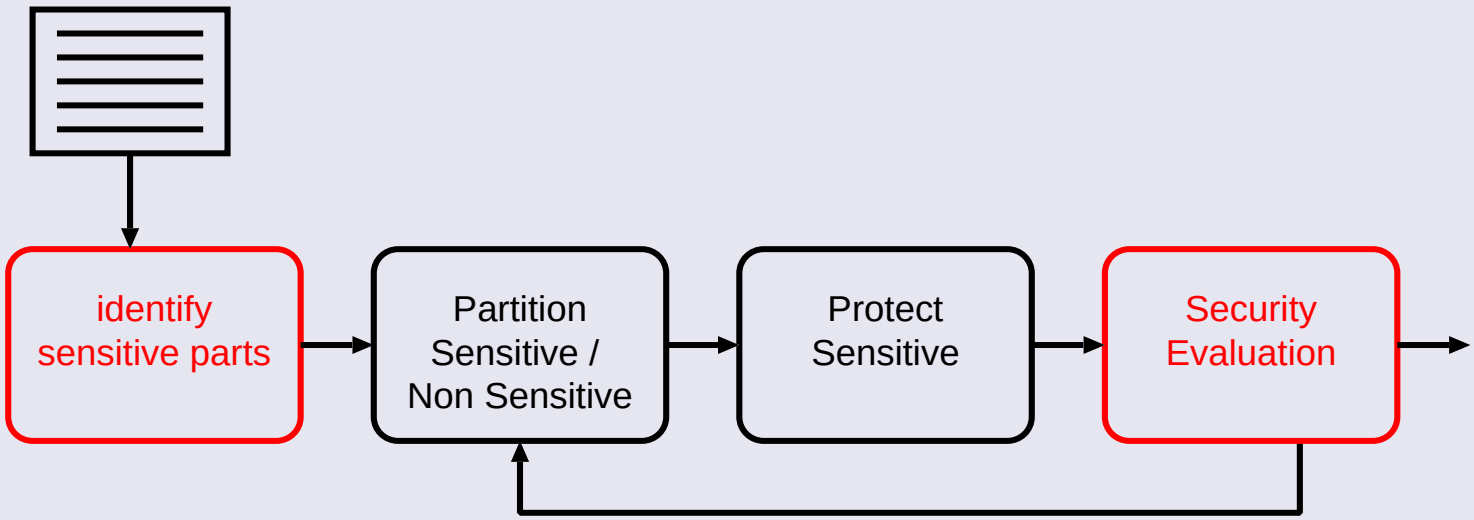


Needed "Basic Blocks"



- Generate useful power traces? ✓
- Measure the DPA resistance?
- Countermeasure and its design flow?
- Partition the algorithm?

Needed "Basic Blocks"



- Generate useful power traces? ✓
- Measure the DPA resistance?
- Countermeasure and its design flow?
- Partition the algorithm?

Metric

- **Number of Samples** Easy but based on specific attack scenario
- **Success Rate** Based on specific attack scenario

$$\mathrm{Succ}^{K}_{\mathrm{attack}} = \Pr[f = 1]$$

- **Information Theory** Complex but independent from the attack scenario

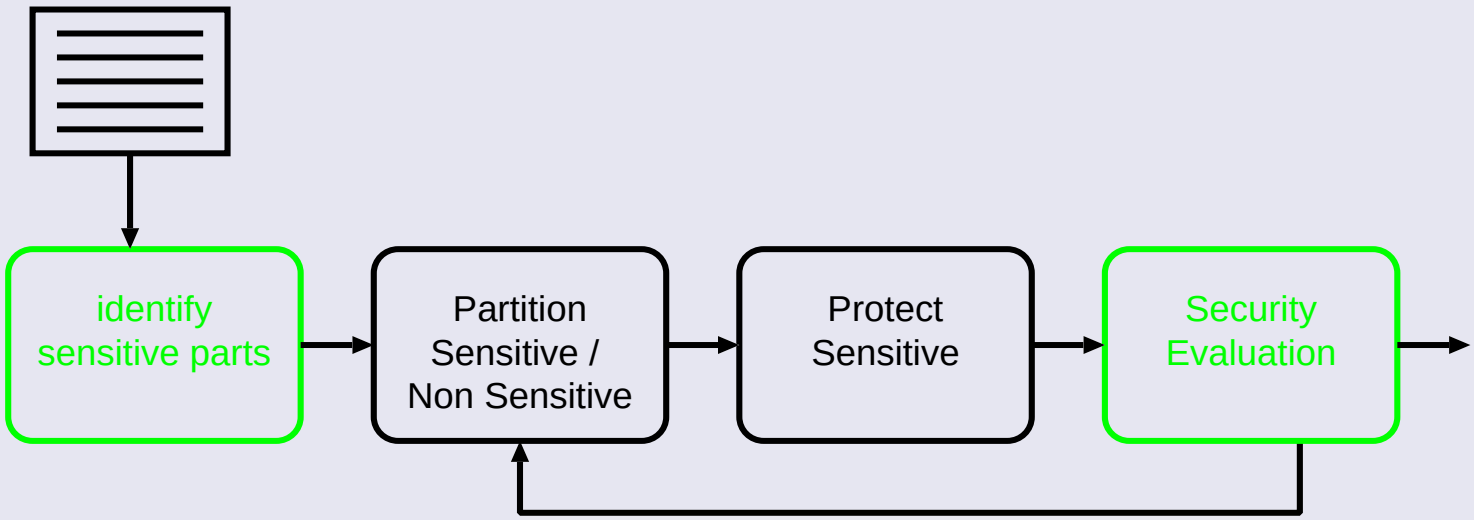
Details on Information Theory (and Compression Technique)

- Maximum extraction
- Integration
- PCA

$$\mathrm{H}[K|L] = -\sum_{k} \Pr[k] \cdot \sum_{x} \Pr[x] \int \Pr[l|k,x] \cdot \log_2 \Pr[k|l,x] \; dl.$$

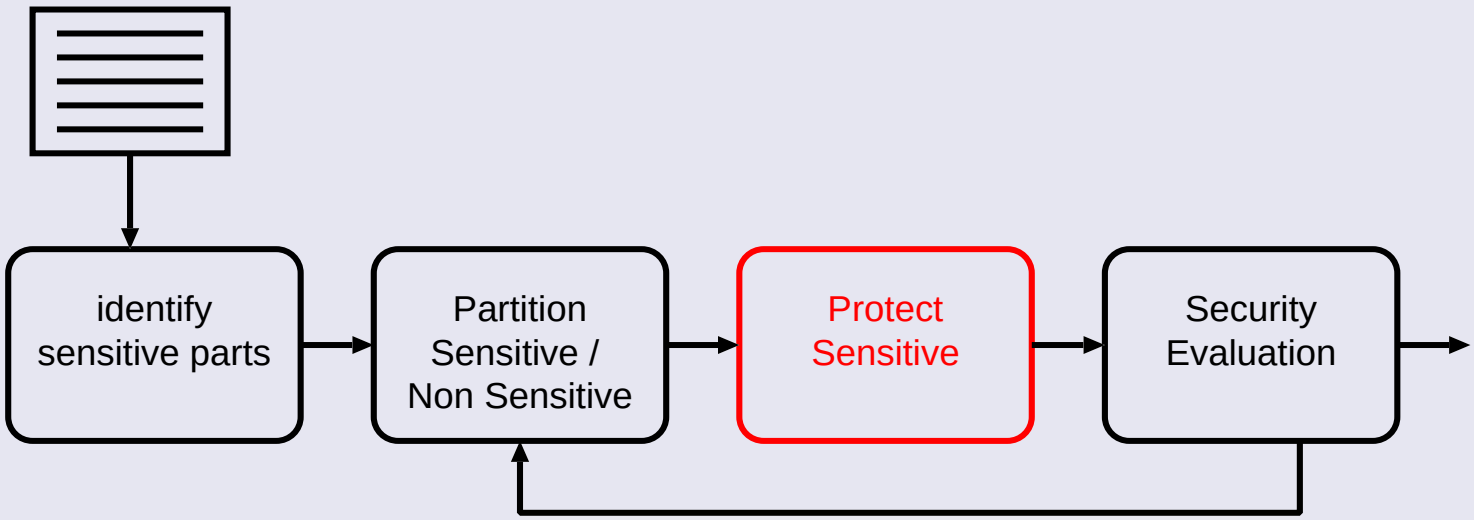
- Add white noise
- Reduce the dimension using compression
- Compute the mutual information

Needed "Basic Blocks"



- Generate useful power traces? ✓
- Measure the DPA resistance? ✓
- Countermeasure and its design flow?
- Partition the algorithm?

Needed "Basic Blocks"



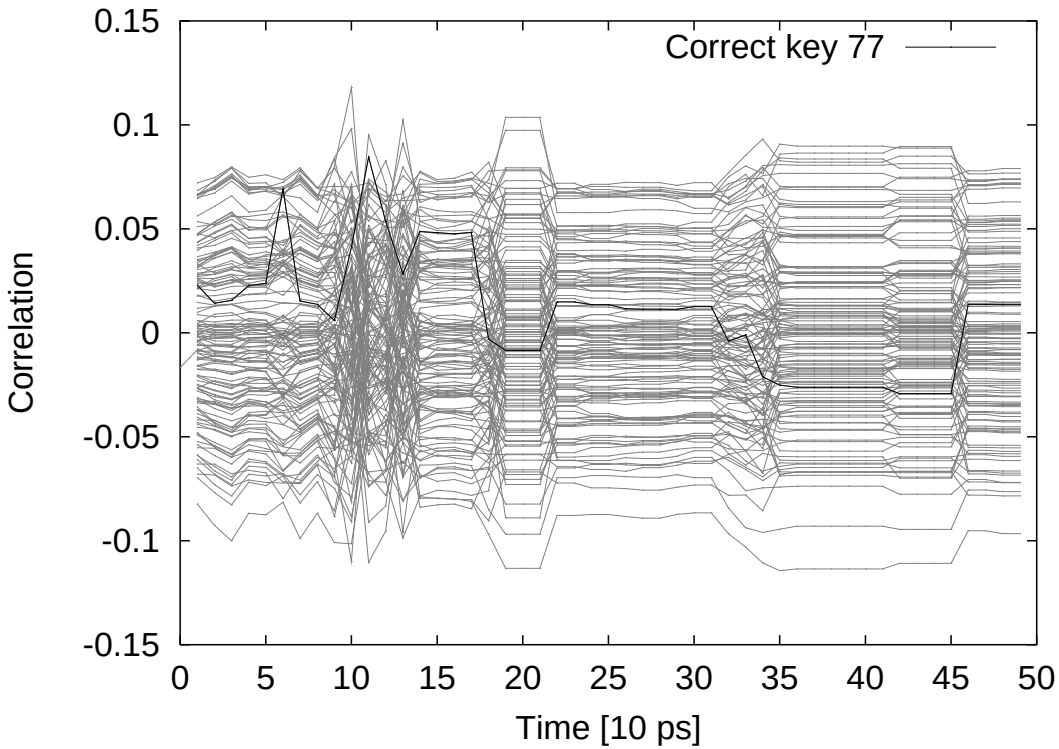
- Generate useful power traces? ✓
- Measure the DPA resistance? ✓
- Countermeasure and its design flow?
- Partition the algorithm?

Protected Logic styles

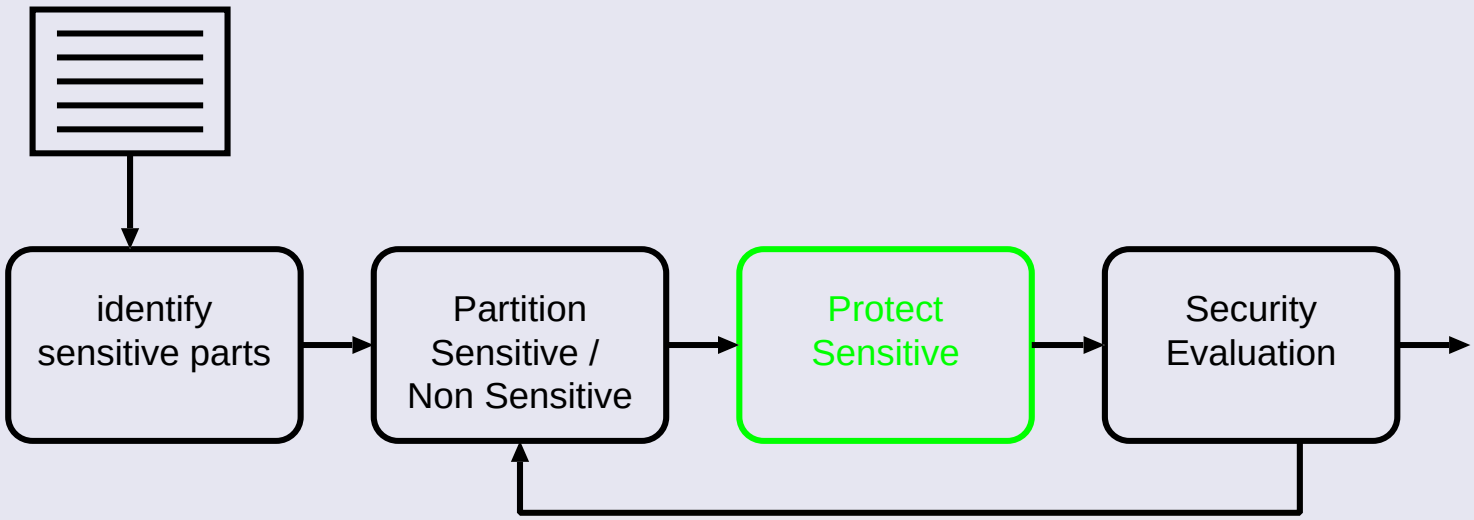
- **WDDL** attacks exist but easy to implement
- **MDPL** attacks exist and complex to P&R
- **MCML** robust but high power consumption

More details on MCML

- Power consumption independent from switching activity and fan-out conditions
- Power consumption can be reduced using power gating

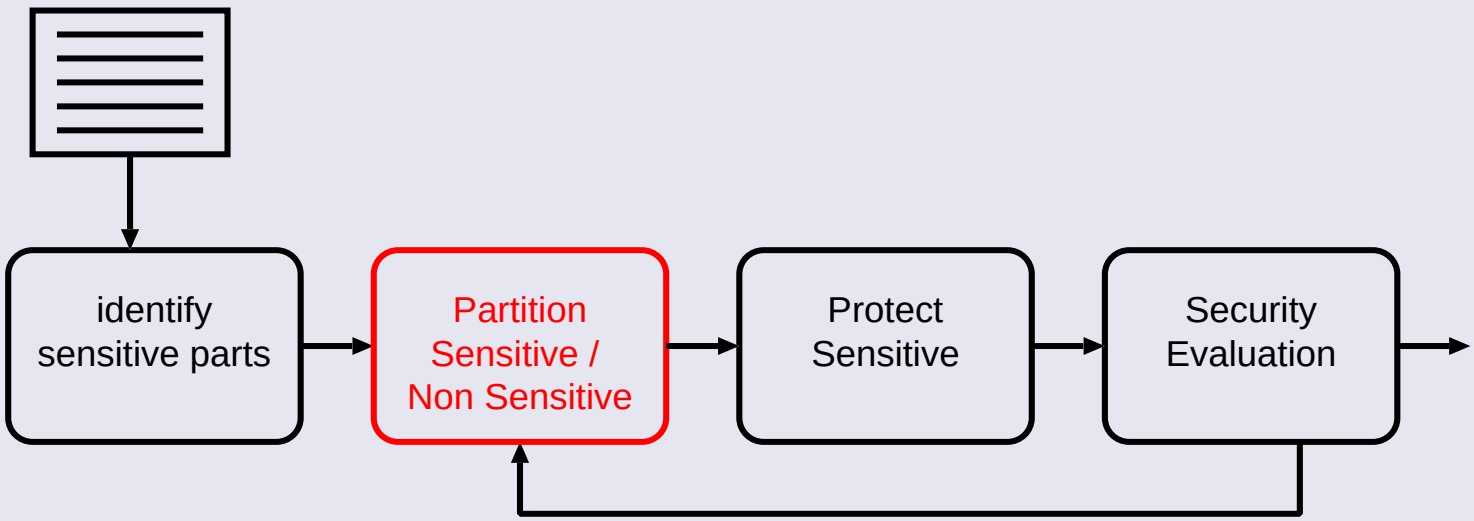


Needed "Basic Blocks"



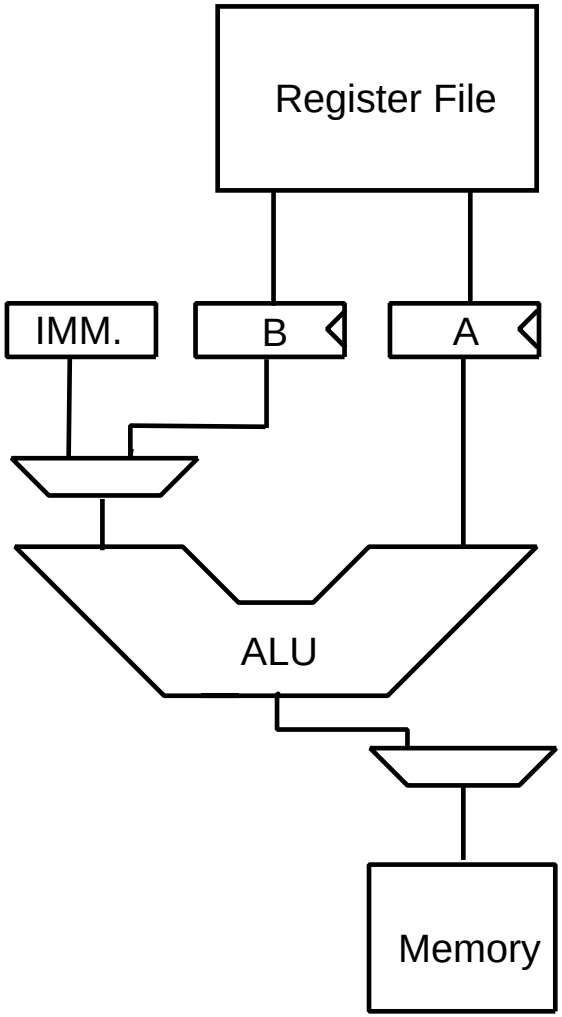
- Generate useful power traces? ✓
- Measure the DPA resistance? ✓
- Countermeasure and its design flow? ✓
- Partition the algorithm?

Needed "Basic Blocks"

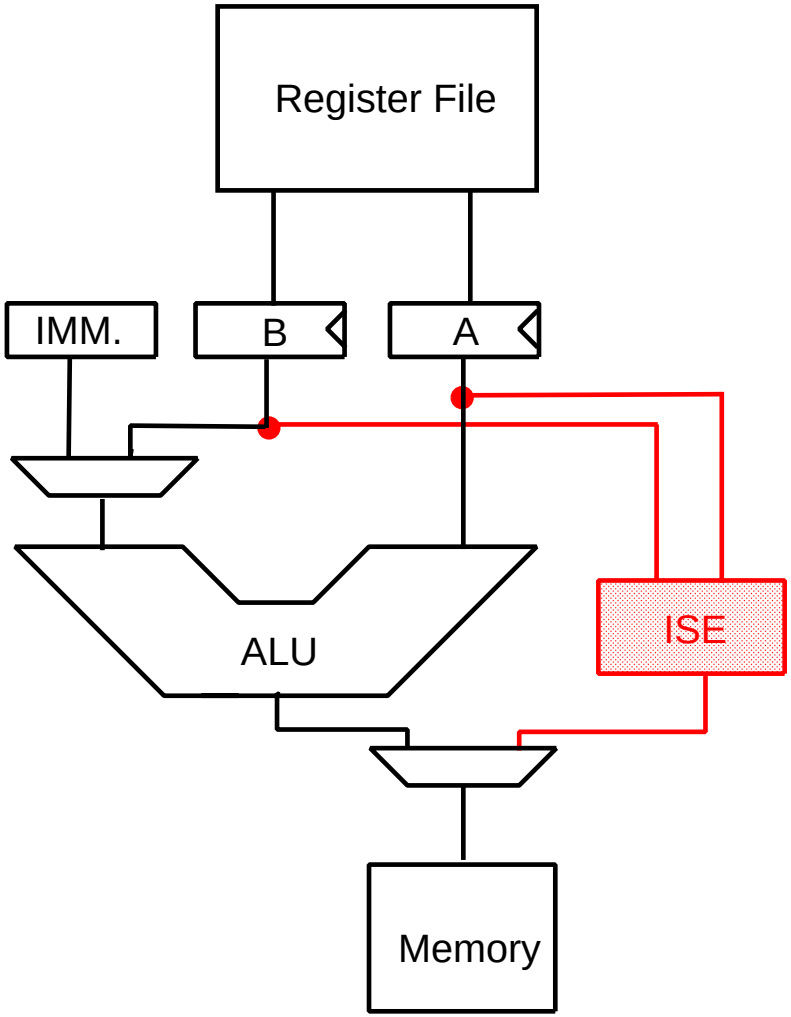


- Generate useful power traces? ✓
- Measure the DPA resistance? ✓
- Countermeasure and its design flow? ✓
- Partition the algorithm?

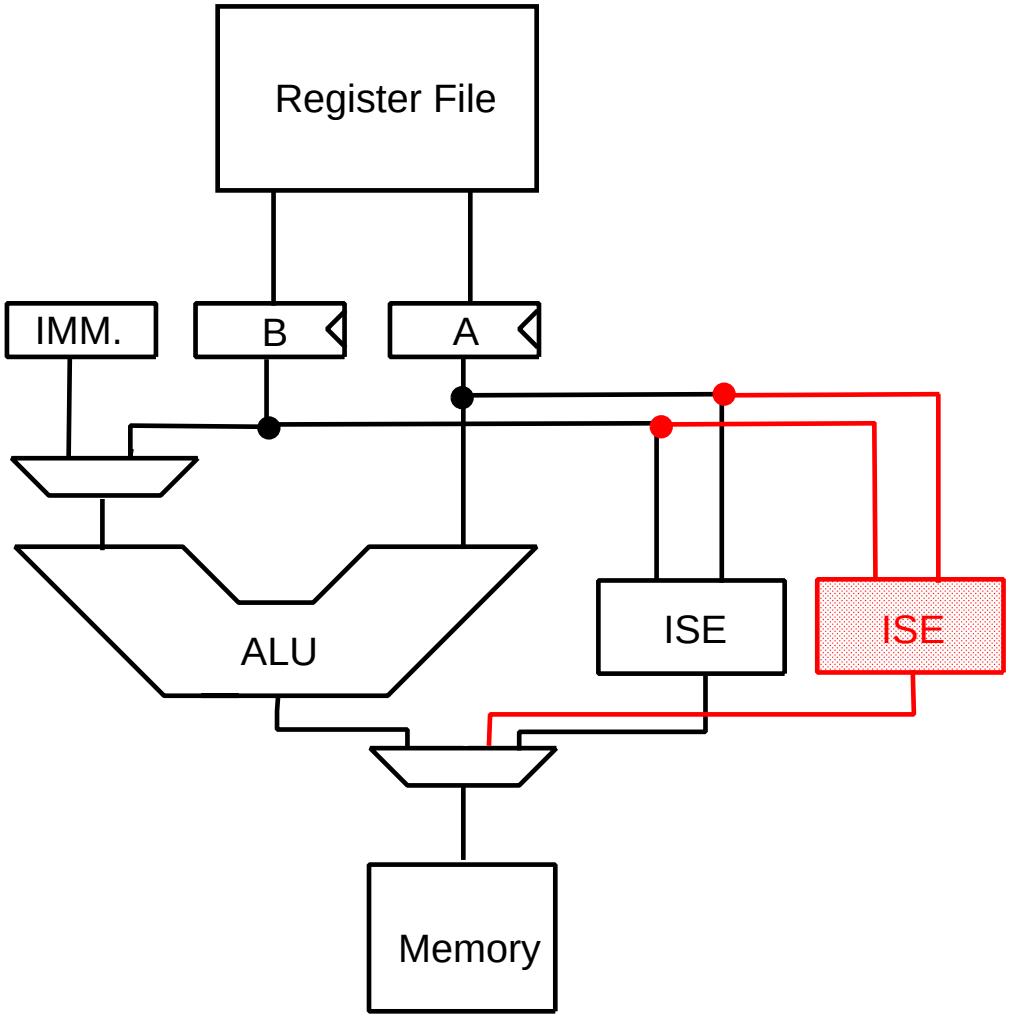
Algorithm partitioning tool



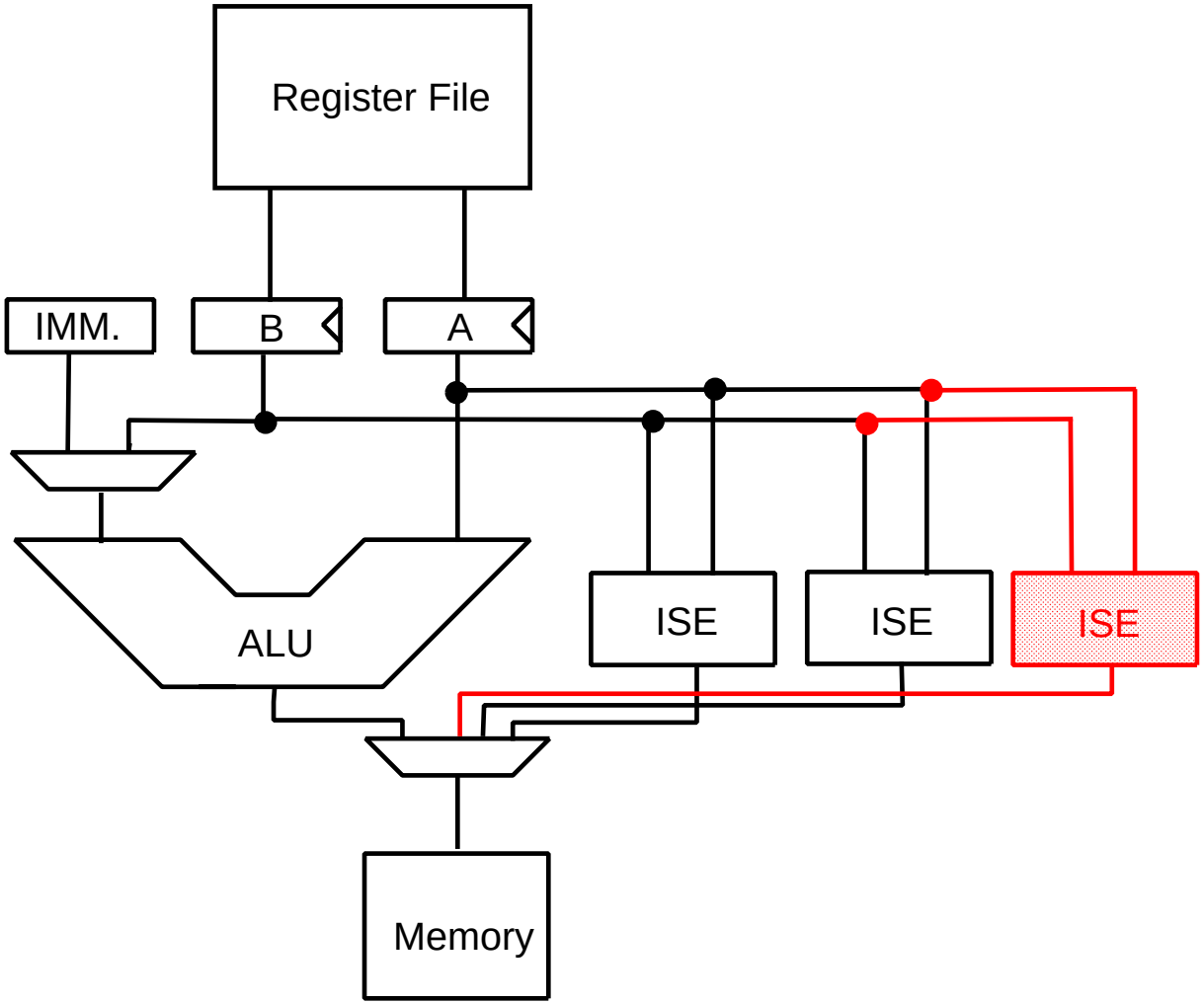
Algorithm partitioning tool



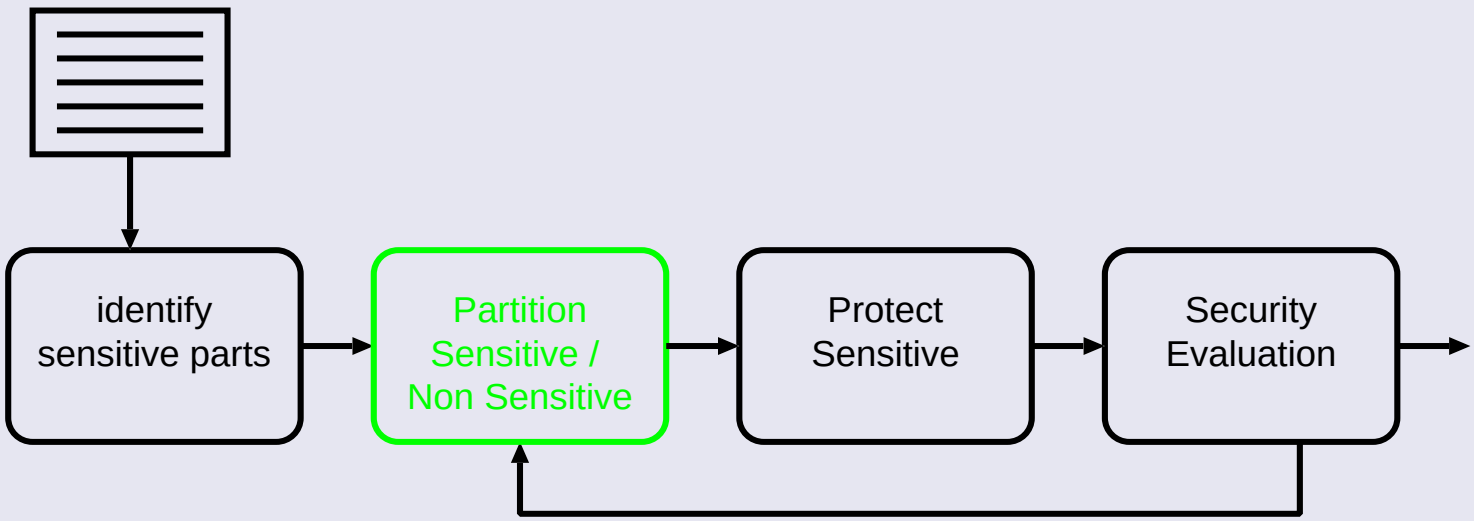
Algorithm partitioning tool



Algorithm partitioning tool

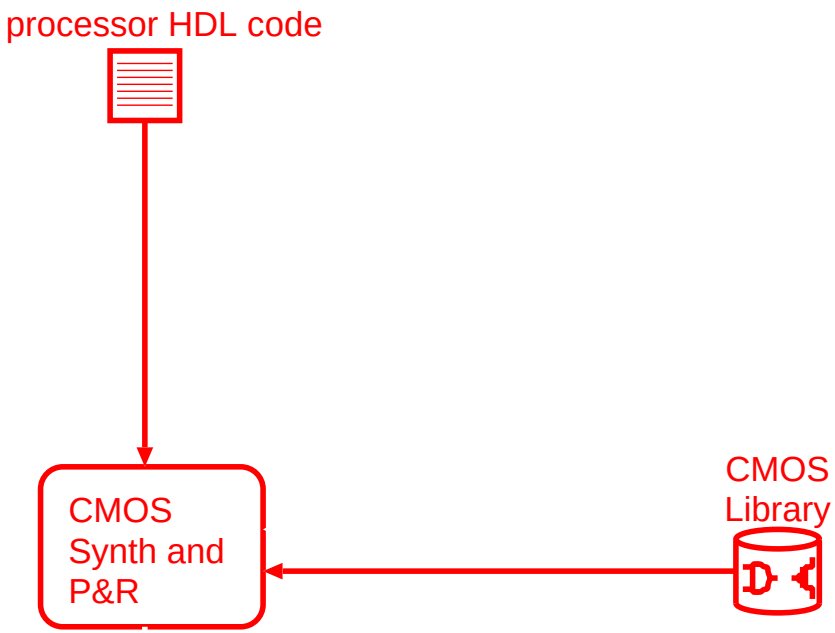


Needed "Basic Blocks"

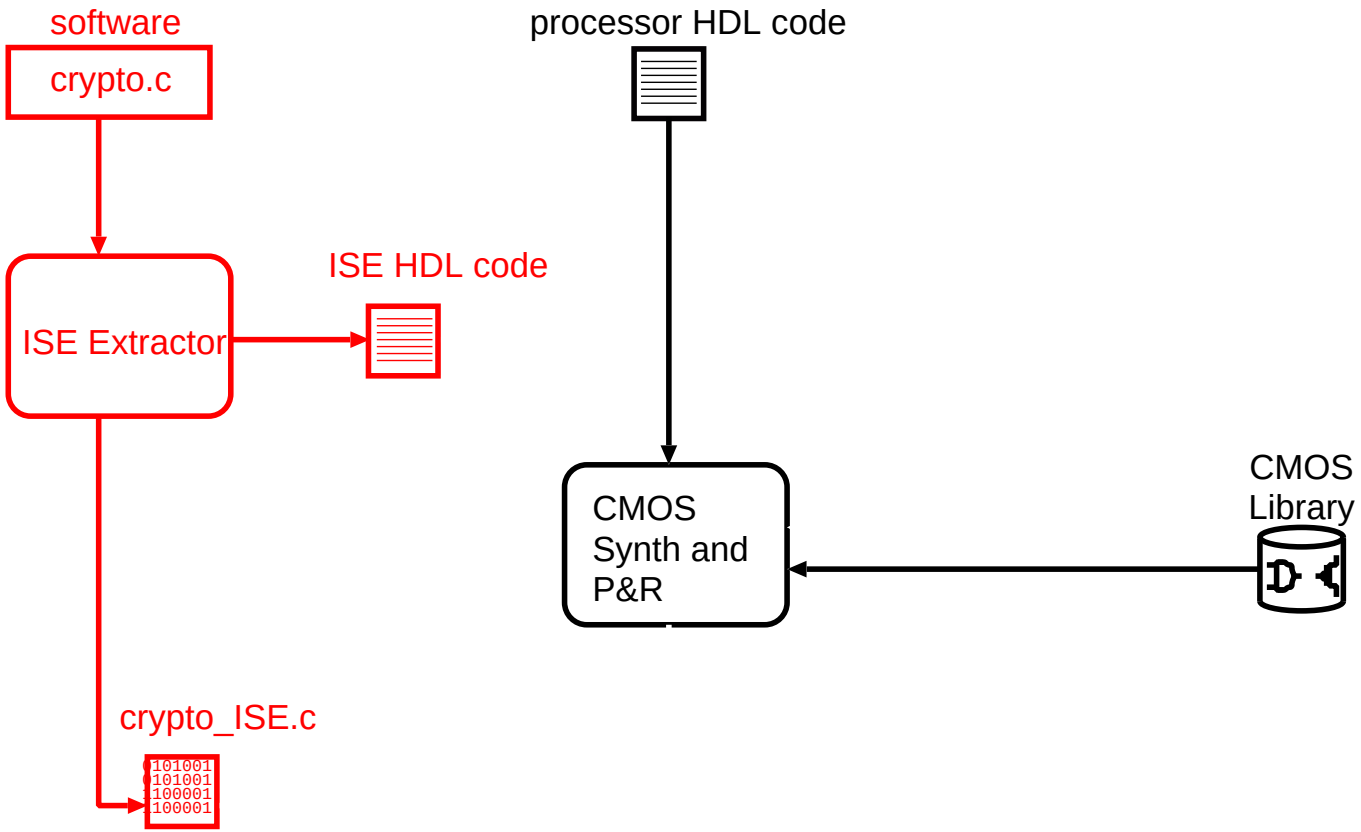


- Generate useful power traces? ✓
- Measure the DPA resistance? ✓
- Countermeasure and its design flow? ✓
- Partition the algorithm? ✓

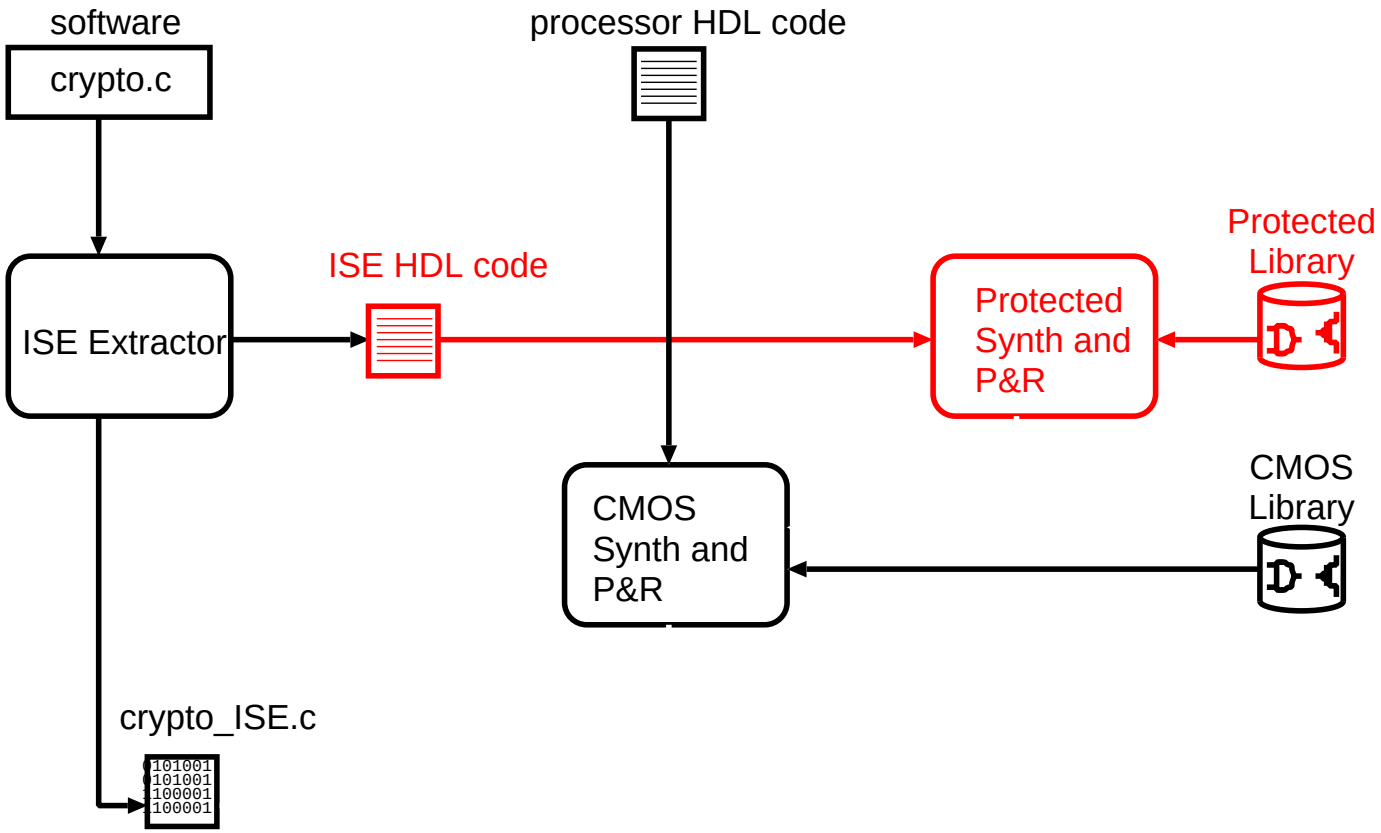
The CMOS Design Flow



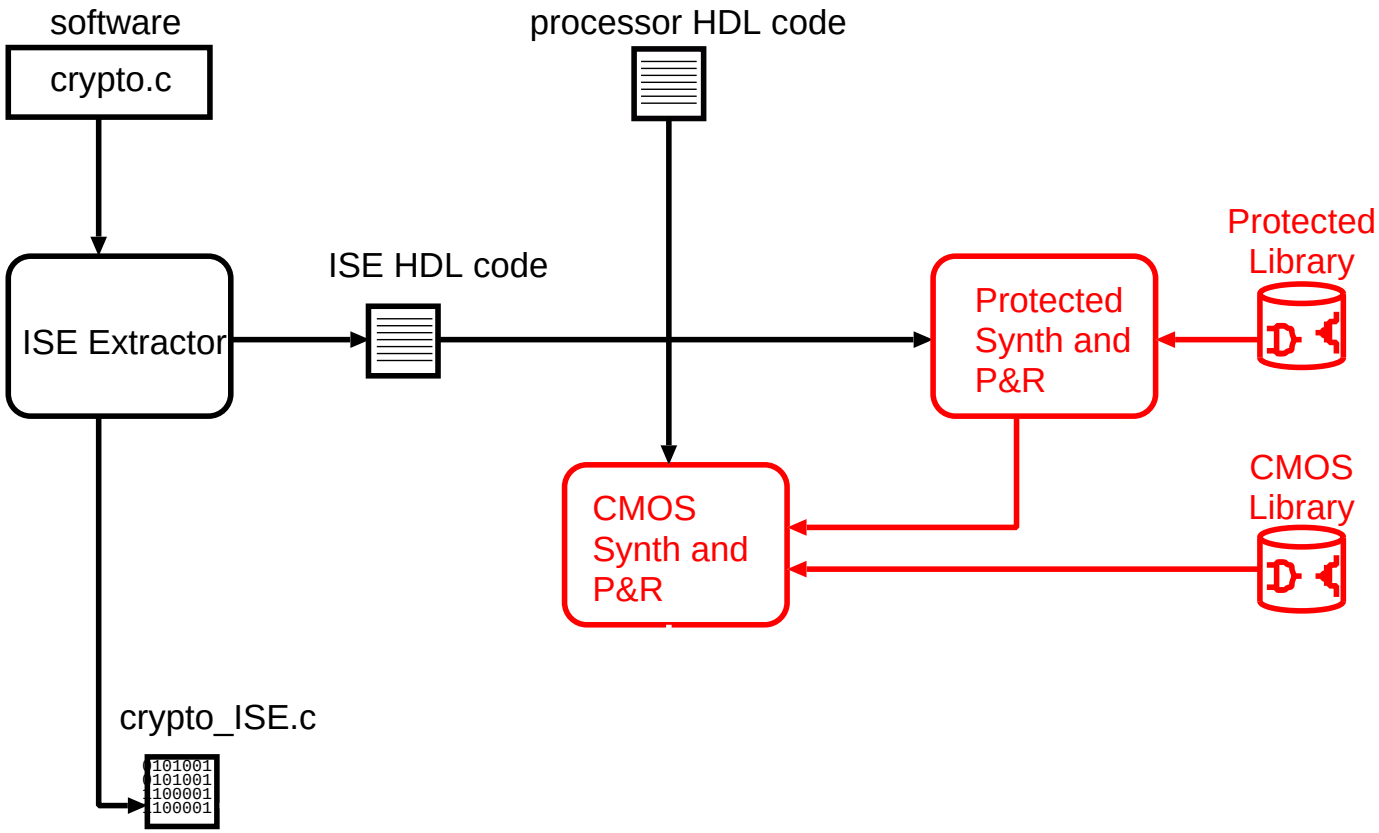
The Processor Customization



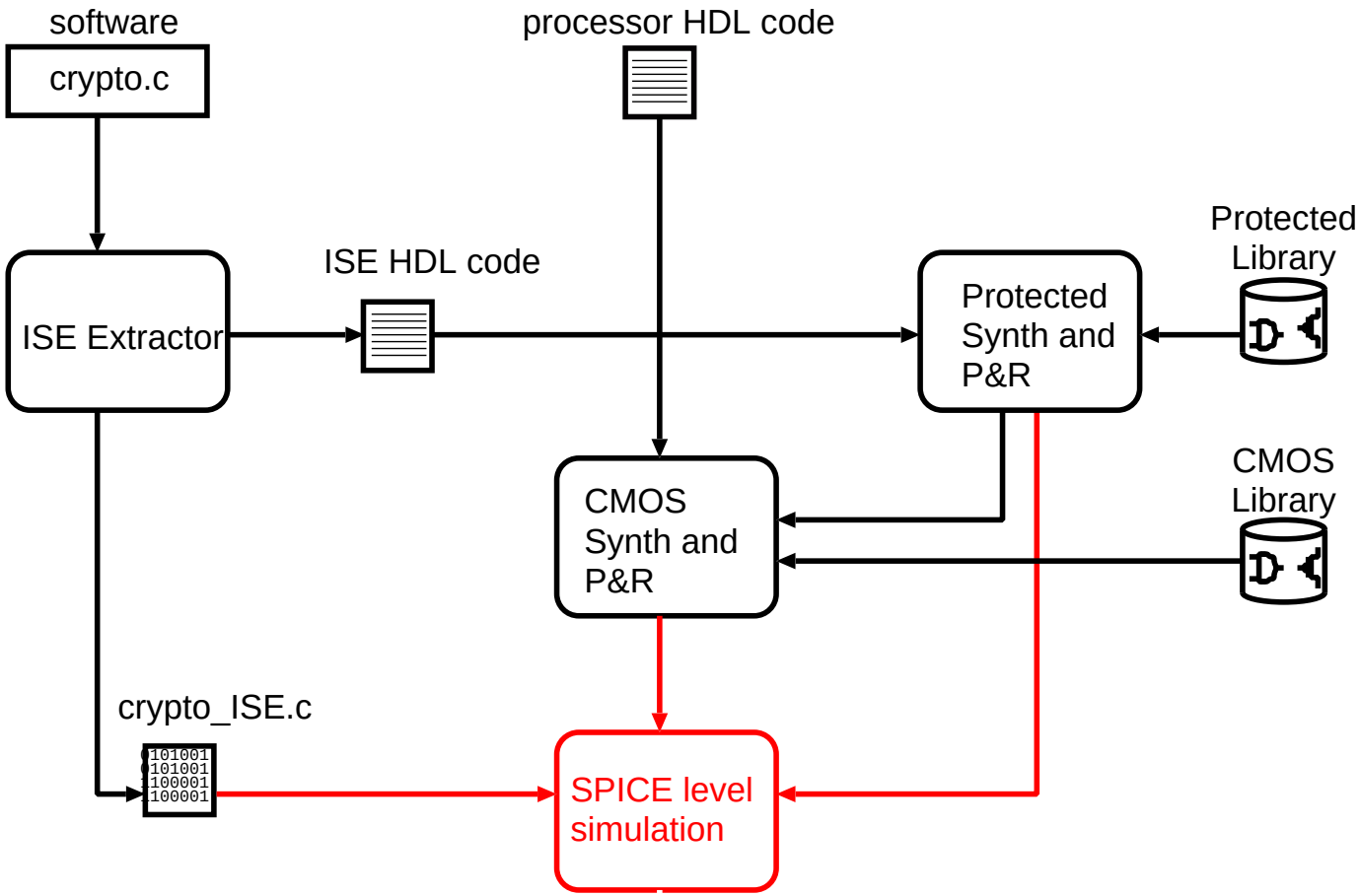
The Protected Design Flow



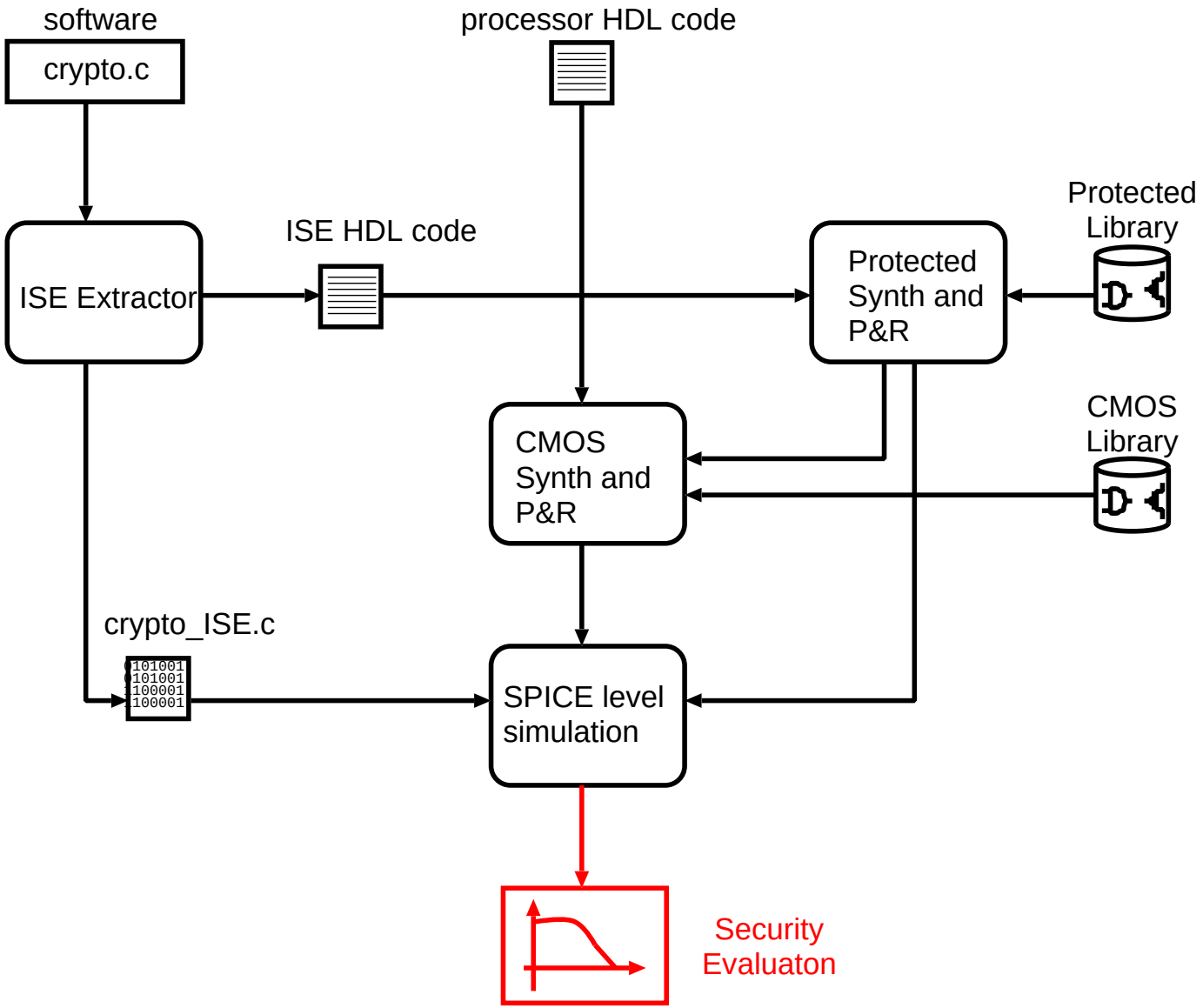
The Hybrid Design Flow



The Simulation Environment



The Overall Design Flow

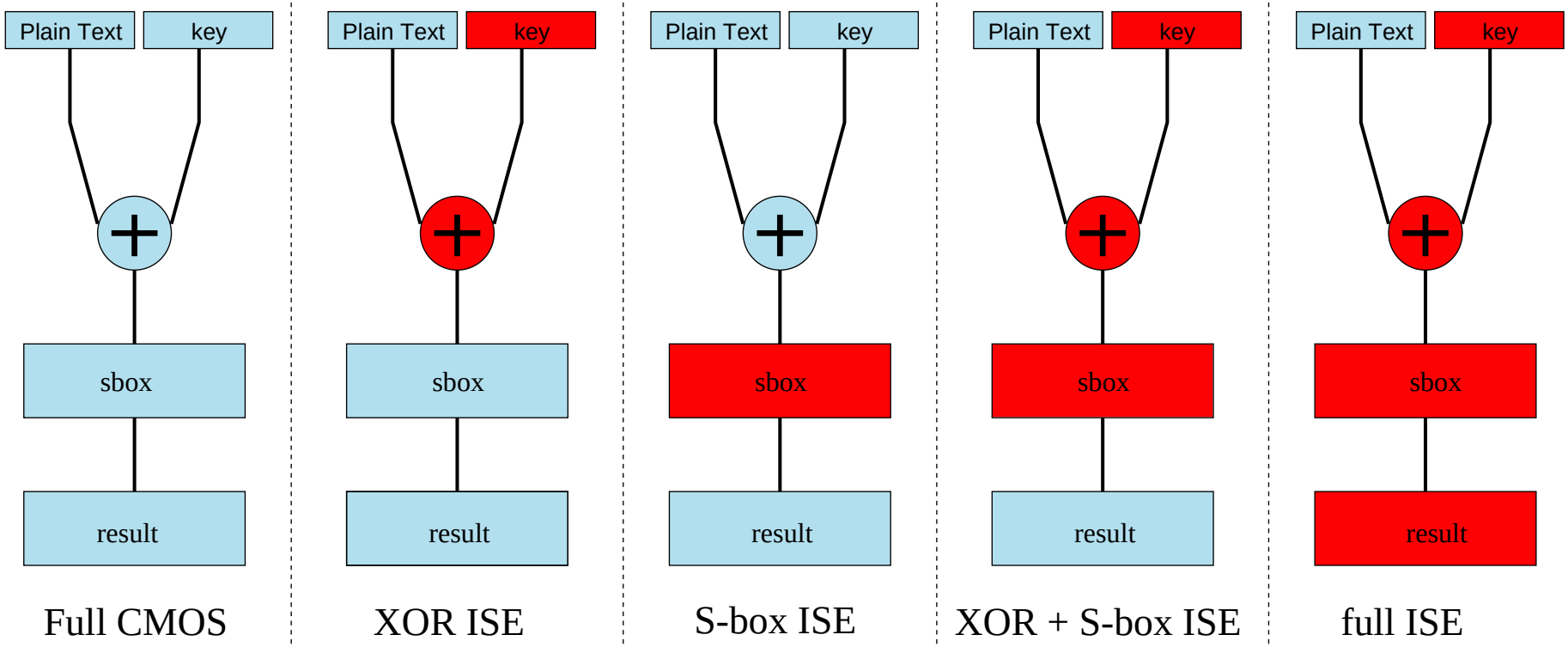


Design flow Example: PRESENT on OpenRISC

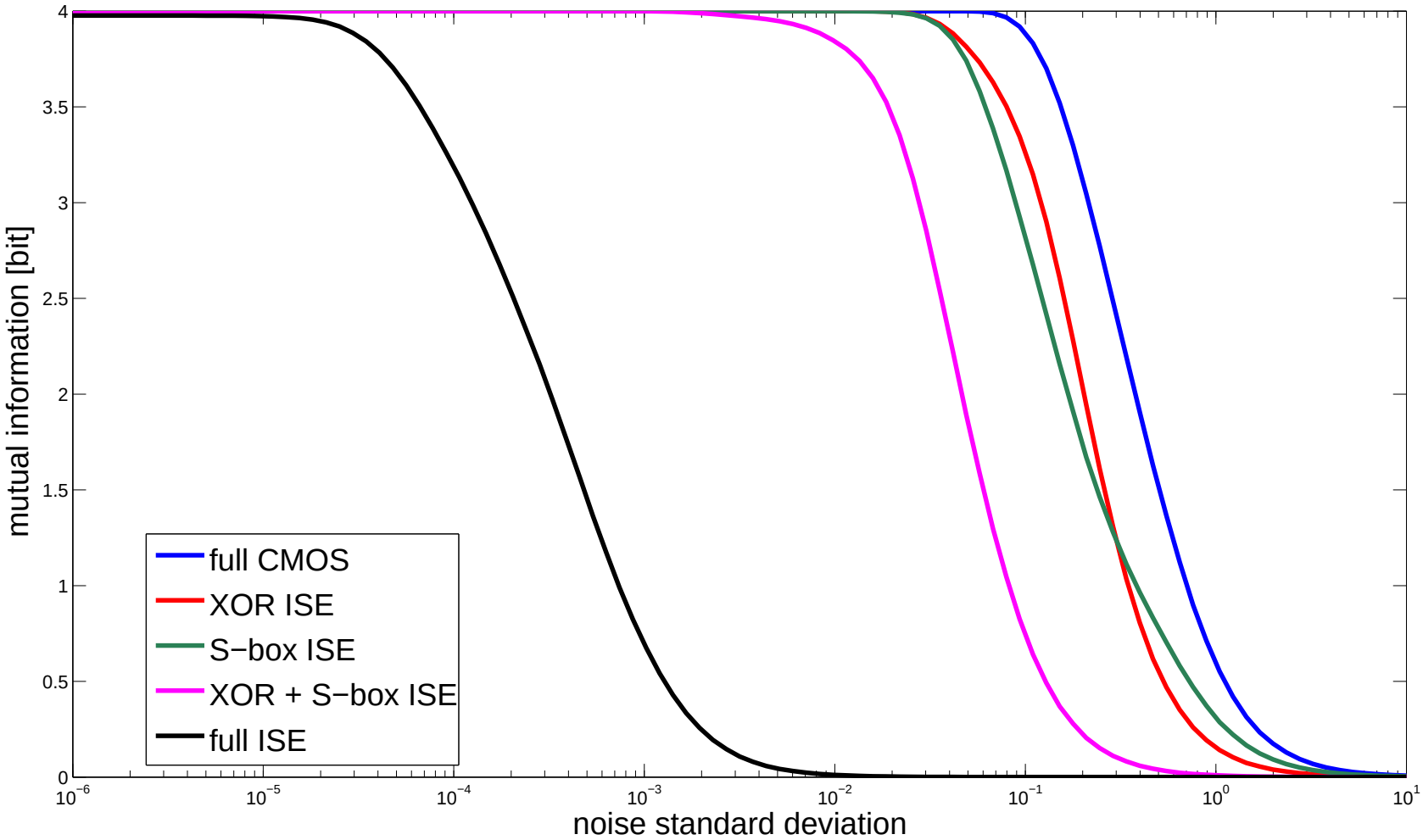
- Lightweight block cipher
- **4 bit** S-box
- *addRoundKey*, *sBoxLayer*

```
// Calculate S-box (plaintext XOR key)
int PRESENT(int plaintext, int key) {
1 int result = 0; // initialize the result
2 plaintext = plaintext ^key; // perform the xor with the key
3 result = S[plaintext]; // perform the S-box
4 return result; }; // return the result
```

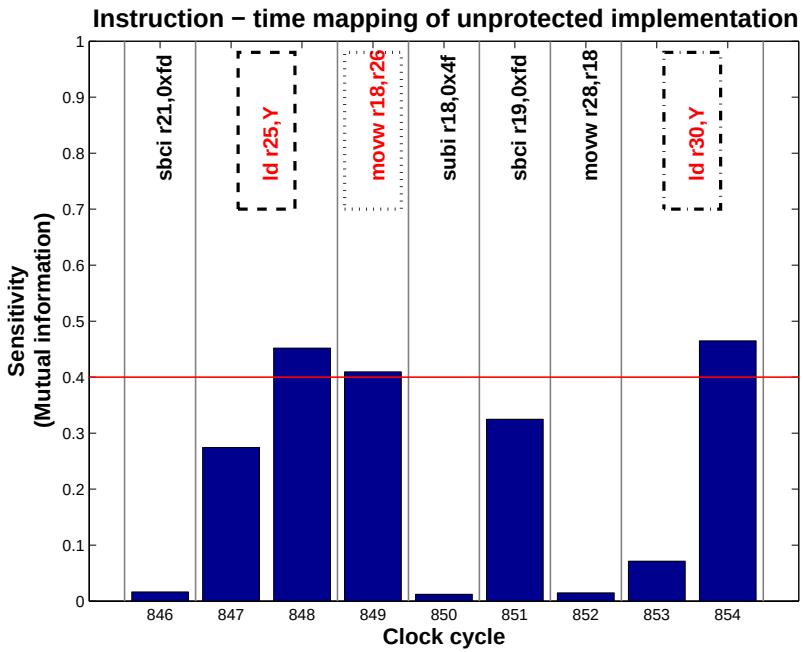
Partitioning of the PRESENT algorithm S-box

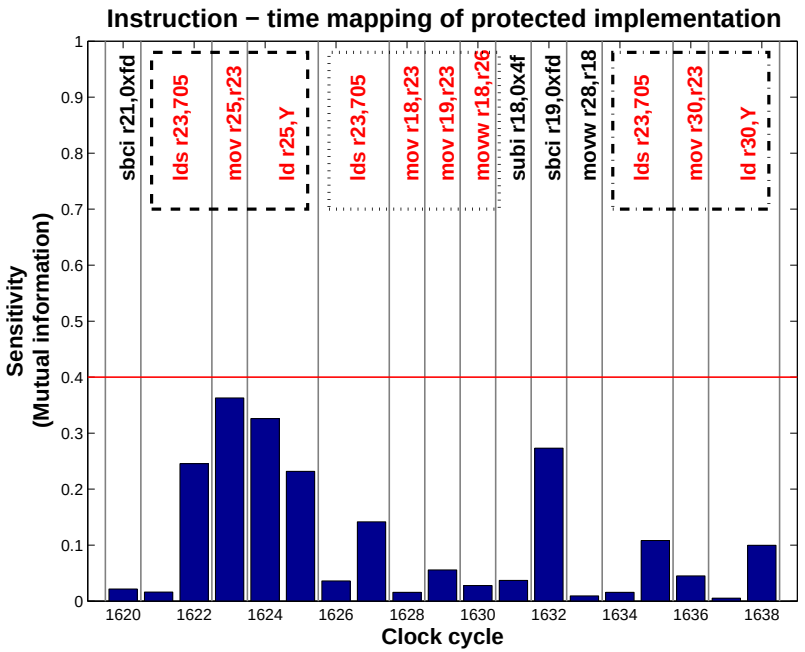


Security Evaluation



Example on Software





Conclusions

- Physical security is a concern
- Design automation for physical security is crucial for Embedded systems
- Initial steps for power analysis are promising
- This is just the beginning...

More details on

Francesco Regazzoni, Stéphane Badel, Thomas Eisenbarth, Johann Großschädl, Axel Poschmann, Zeynep Toprak, Marco Macchetti, Laura Pozzi, Christof Paar, Yusuf Leblebici and Paolo Ienne "**Simulation-based Methodology for Evaluating DPA-Resistance of Cryptographic Functional Units with Application to CMOS and MCML Technologies**", in Proceedings of *International Conference on Embedded Computer Systems: Architectures, Modeling, and Simulation (SAMOS IC 07)*, Samos, Greece, July 16 - 19 2007

Francesco Regazzoni, Thomas Eisenbarth, Johann Großschädl, Axel Poschmann, Frank Gurkaynak, Zeynep Toprak, Marco Macchetti, Laura Pozzi, Christof Paar, Yusuf Leblebici and Paolo Ienne "**Evaluating Resistance of MCML Technology to Power Analysis Attacks Using a Simulation-Based Methodology**", in Transactions on Computational Science 4, 2009

Francesco Regazzoni, Alessandro Cevrero, François-Xavier Standaert, Stéphane Badel, Theo Kluter, Philip Brisk, Yusuf Leblebici and Paolo Ienne "**A Design Flow and Evaluation Framework for DPA-Resistant Instruction Set Extensions**", in Proceedings of *Cryptographic Hardware and Embedded Systems - CHES 2009*, Lausanne, Switzerland, September 2009

More details on

Alessandro Cevrero, *Francesco Regazzoni*, Michael Schwander, Stéphane Badel, Paolo Ienne, and Yusuf Leblebici "**Power-Gated MOS Current Mode Logic (PG-MCML): A Power-Aware DPA-Resistant Standard Cell Library**", in Proceedings of *48th Design Automation Conference (DAC) 2011*, San Diego, Califorina, June 5 - 9 2011

Ali Galip Bayrak, *Francesco Regazzoni*, Philip Brisk, François-Xavier Standaert, and Paolo Ienne and Paolo Ienne "**A First Step Towards Automatic Application of Power Analysis Countermeasures**", in Proceedings of *48th Design Automation Conference (DAC) 2011*, San Diego, Califorina, June 5 - 9 2011

Questions?

Thank you for your attention!