Securing CPSs, new challenge or solved problem?

Francesco Regazzoni

Contents

What is a CPS?

- Yet another definition....
- Cyber-Physical System

Cyber-

- Computational Element
- Some “intelligence”
- Network Connected

-Physical

- Sensors
- Actuators

Cyber-Physical Systems Schema

Applications of CPSs

- Medical
- Critical Infrastructure
- You mention...

Contents

Confidentiality

Attempt to gain access to **data stored/handled** or to the **IP**

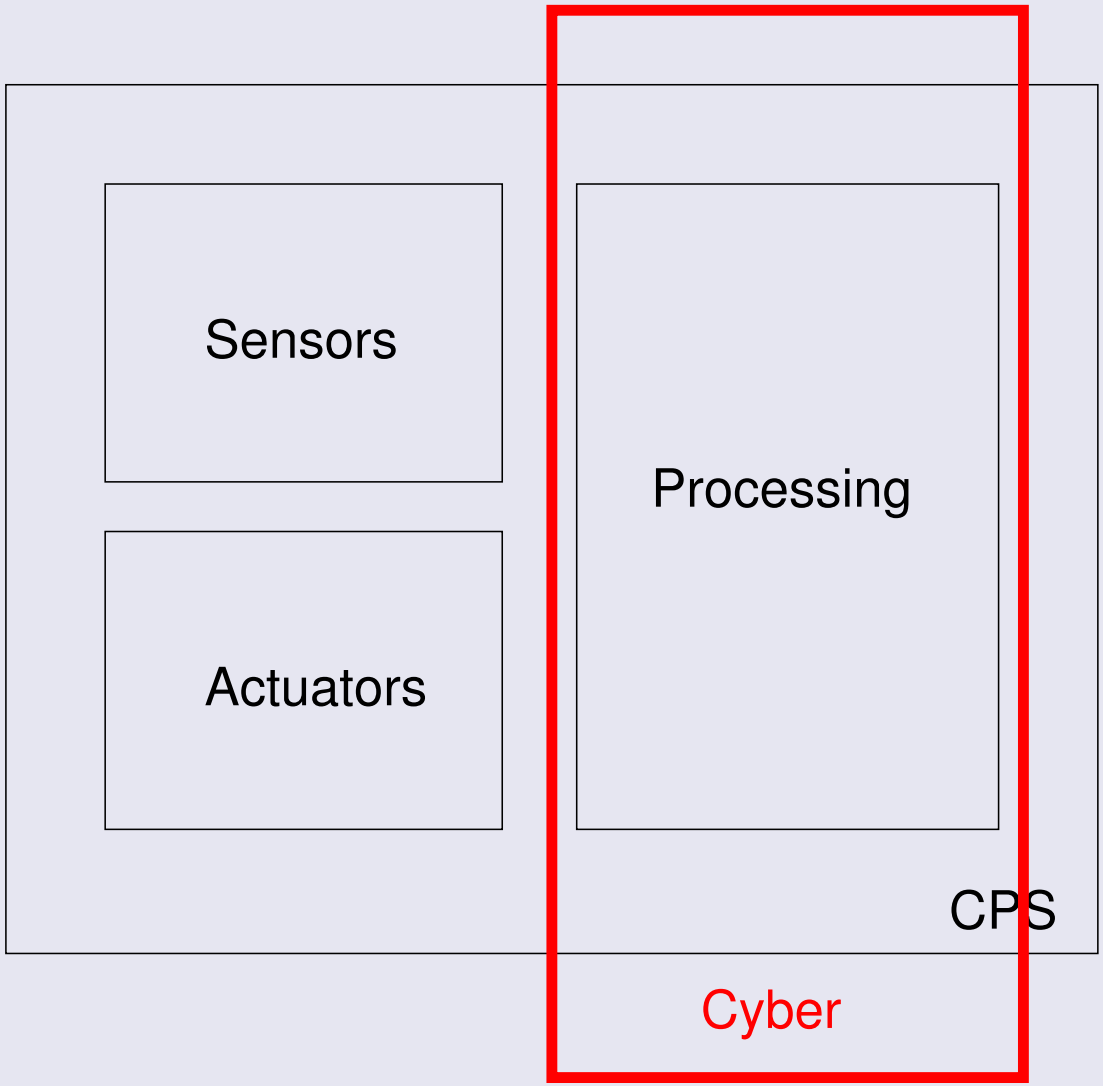
Integrity

It is related to the absence of **undesired malicious modifications**

Authenticity

It is related to the authenticity of **components** and **data**

Cyber-Physical Systems Schema



Cyber-Physical Risk

Let's start from the Cyber-

- Virus-Malware
- Network attacks
- You mention...

Malware

Network Attacks

Hardware Trojans

Contents

Let's stay on the Cyber-

Ops.... something unexpected...

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 6469)

Cyber-Physical Risk

Power Analysis Attacks

Power Analysis Attacks exploit the relation between the power consumed and the processed data.

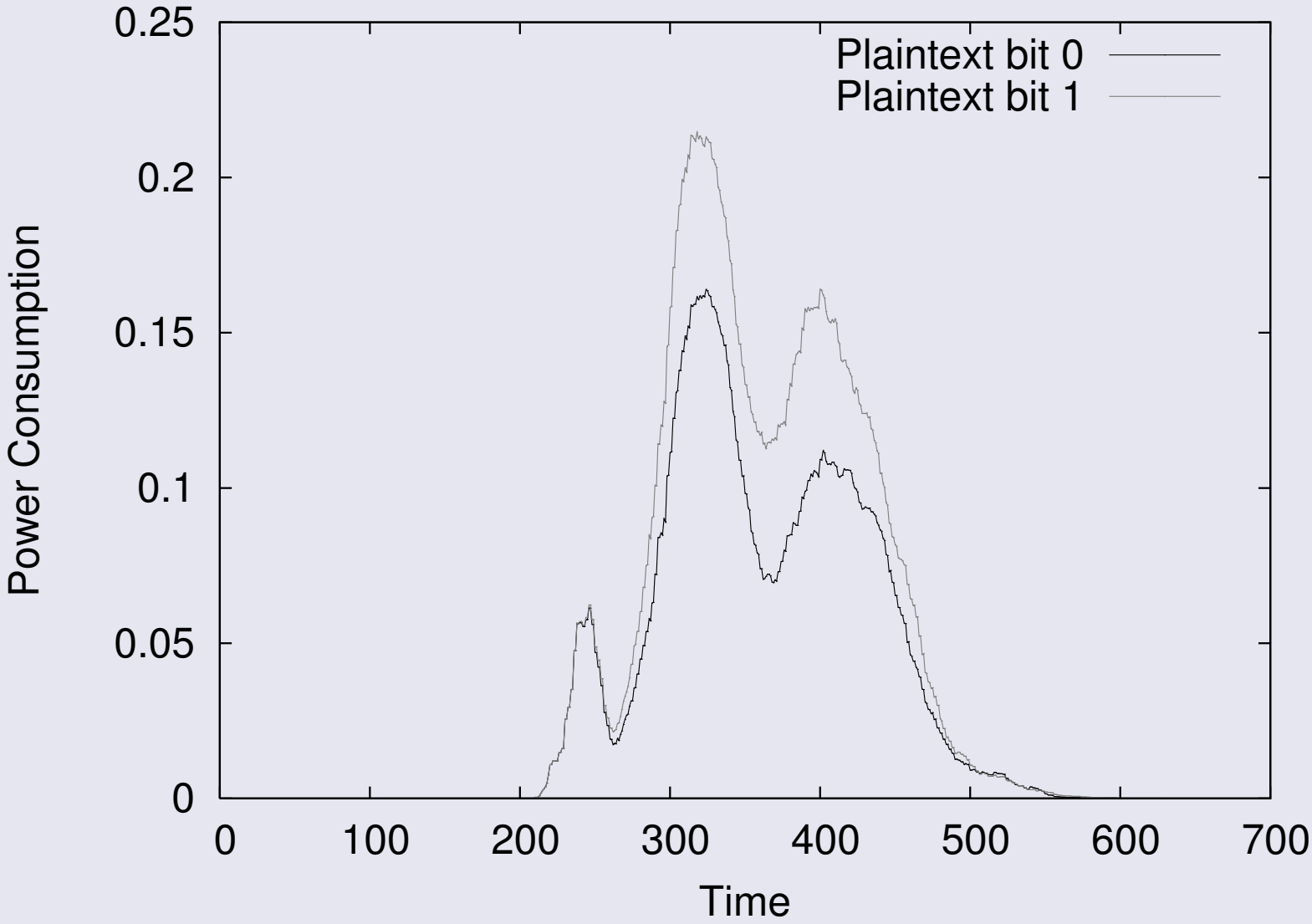
- Cheap
- Powerful

Simple Power Analysis (SPA)

- **Goals**: The adversary attempt to recovery the secret key using a small set of power traces
- **Requirements**: Knowledge about the implementation

- Visual Inspection
- Template Attacks
- Collision Attacks

Visual Inspection



Differential Power Analysis (DPA)

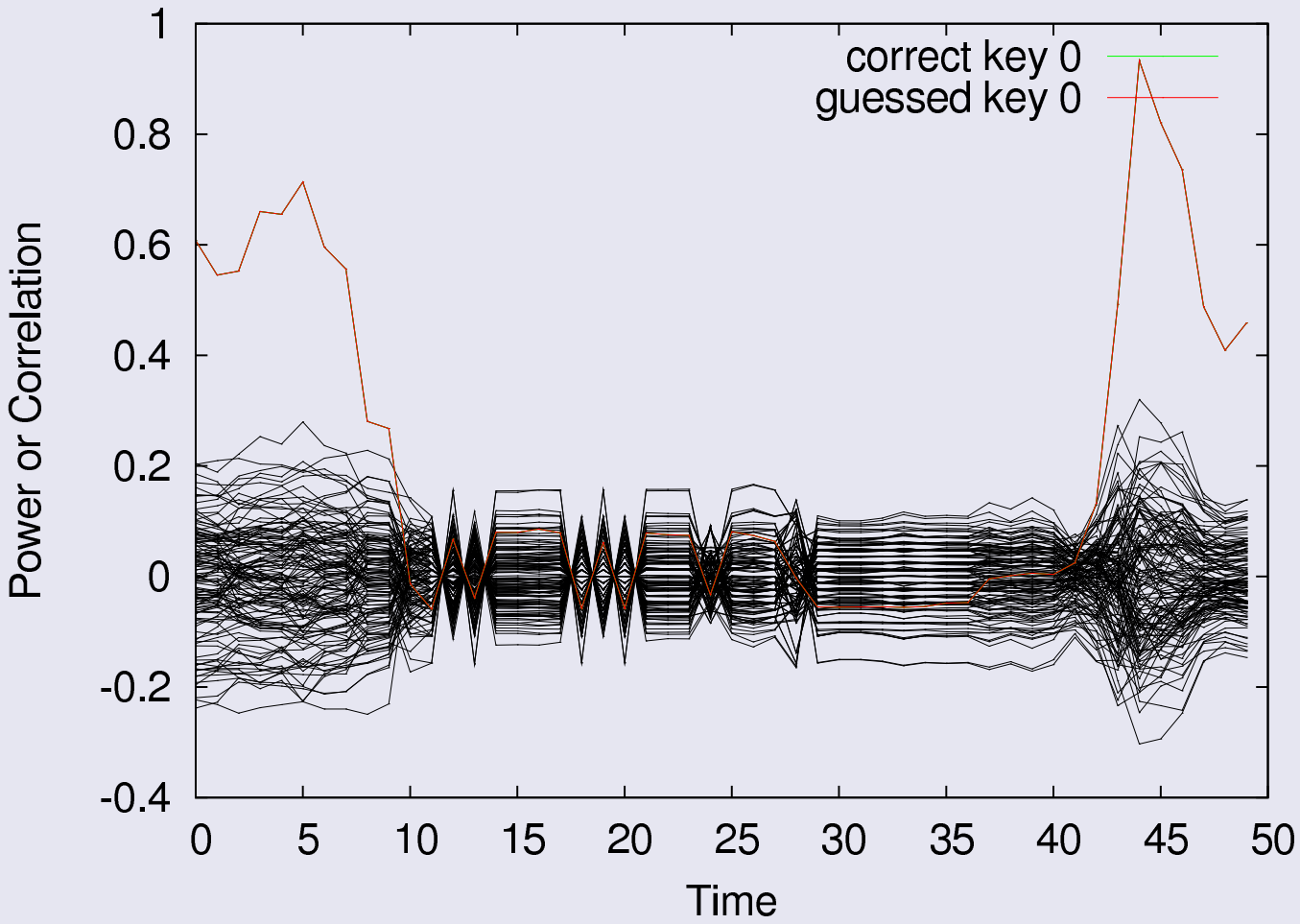
- **Goals**: The adversary make hypotheses on smaller portion of the keys and verify it on the power traces
- **Requirements**: Knowledge about the implemented algorithm

Distinguishers

- Difference of means
- Correlation
- Multivariate statistic

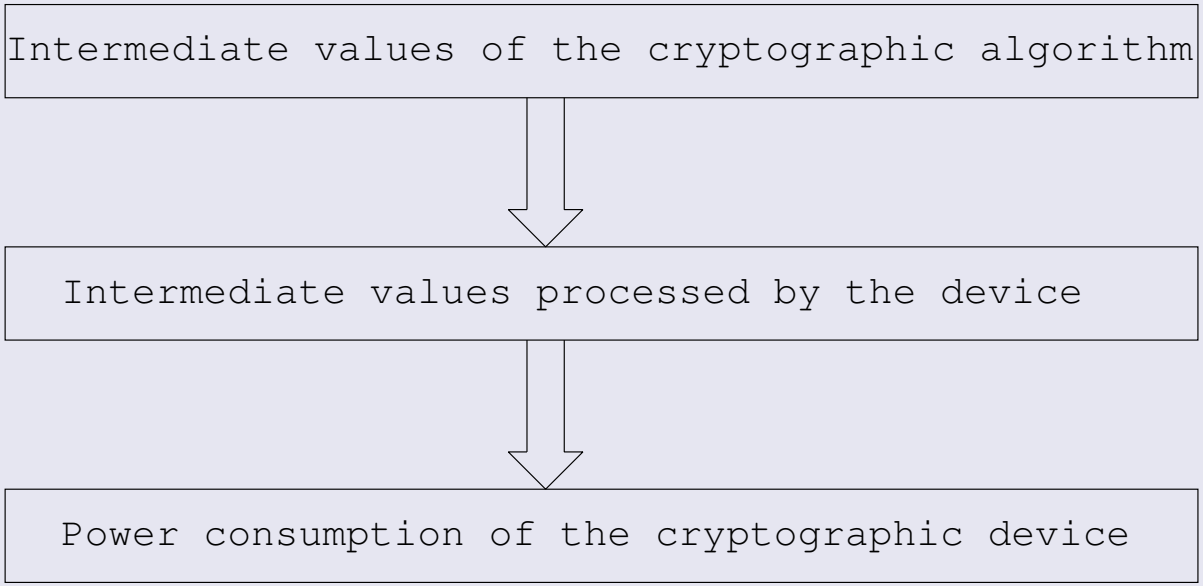
Example of Differential Power Attacks

Simulate whole embedded processor at SPICE



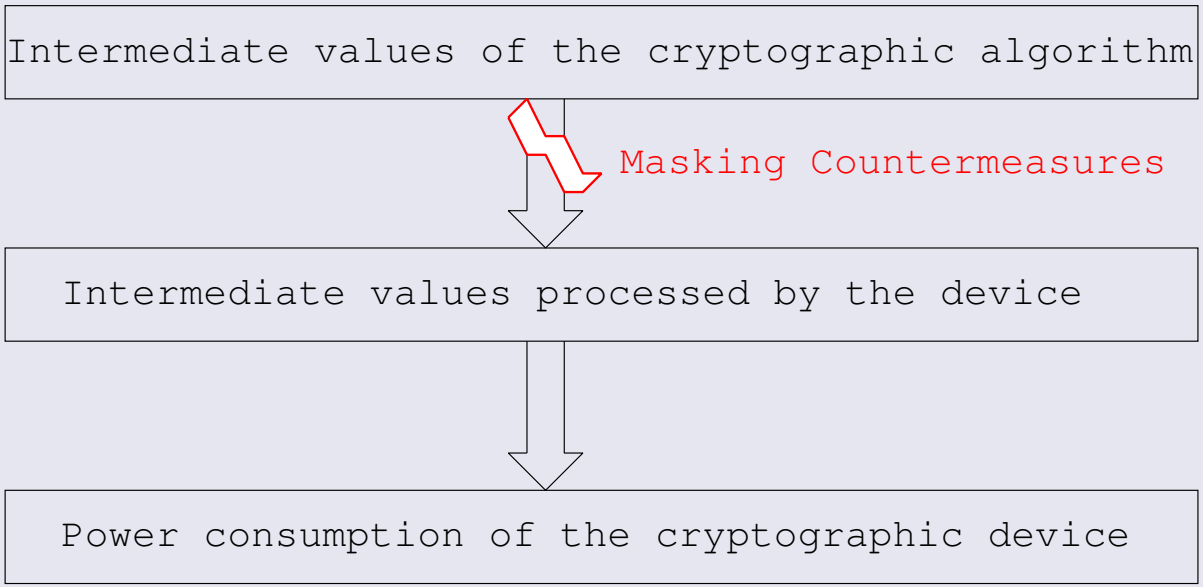
Countermeasures

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



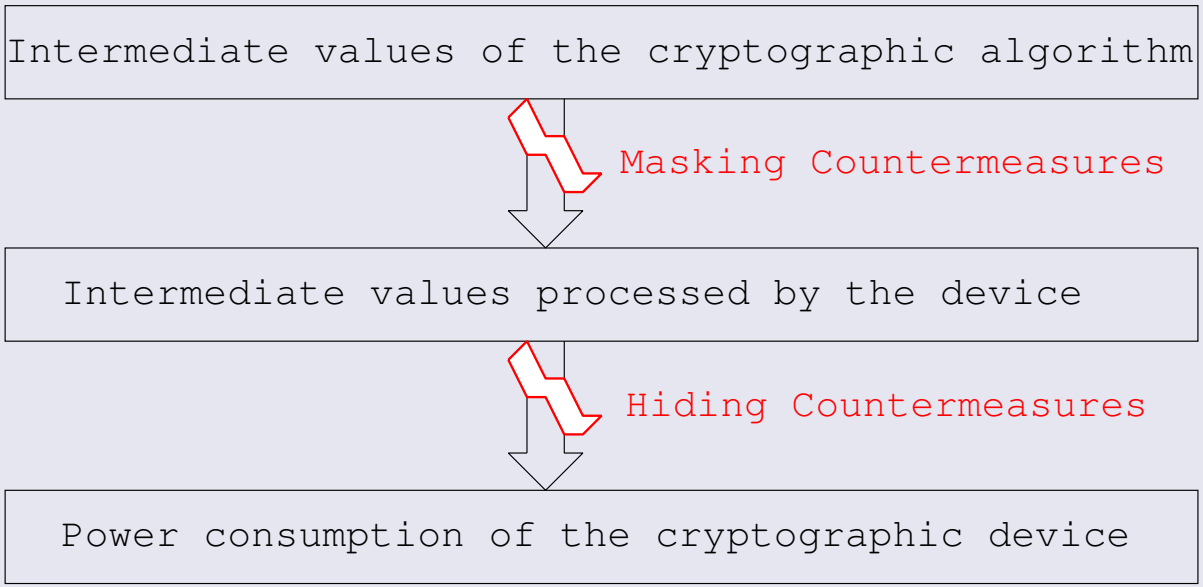
Countermeasures

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



Countermeasures

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



Timing Attacks

- **Goals**: The adversary attempt to recovery the secret key exploiting the time difference of of the instructions
- **Requirements**: Knowledge about the algorithm

- Spy process
- Hardware performance registers
- Visual inspection

Timing Attacks

- Cache increase the time dependency
- Conditional Branch depending on the secret key

Countermeasures

- Avoid branches dependent from secret data
- Compute secret data always in constant time

Fault Attacks

- **Goals**: The adversary attempt to recovery the secret key exploiting the relation between a faulty output and the correct one
- **Requirements**: Fault in the right position

- Laser or equivalent
- Control of the power supply

Fault Attacks

- Single byte fault per column before the last MixColumn
- Single byte fault in the earlier round
- Inject a fault to generate a number not random
- Inject a fault to skip a security check

Countermeasures

- Add space redundancy
- Add time redundancy

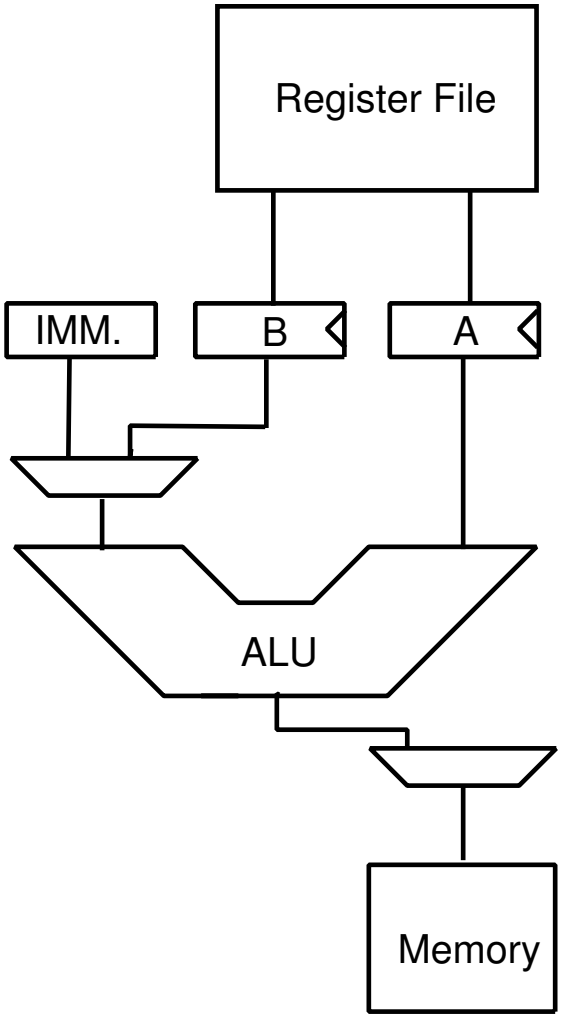
An Interesting Design Challenge (Motivating Example)

```
void maskedARK() {
  unsigned char i;
  for (i=0;i<16;i++){
    st[i] = pt[i] ^
      (key[i] ^ mask[i]);
  }
}
```

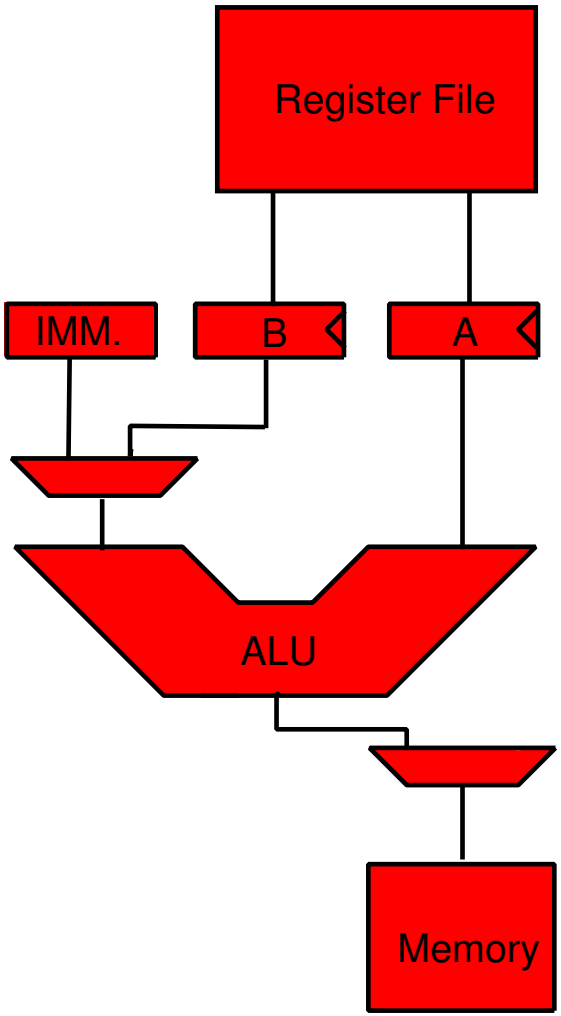
avr-gcc-4.5.3 -O3

```
        .text
.global ARK
        .type   ARK, @function
ARK:
/* prologue: function */
/* frame size = 0 */
/* stack size = 0 */
.L__stack_usage = 0
        lds r24,key
        lds r25,pt
        eor r24,r25
        lds r25,mask
        eor r24,r25
        sts st,r24
        lds r24,key+1
        lds r25,pt+1
        eor r24,r25
        ...
```

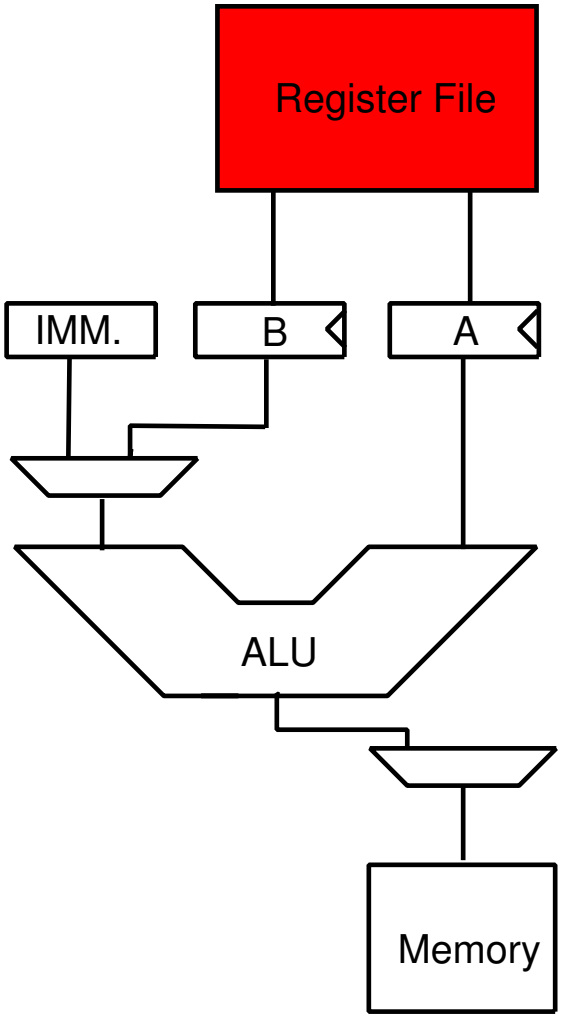
What can I do?



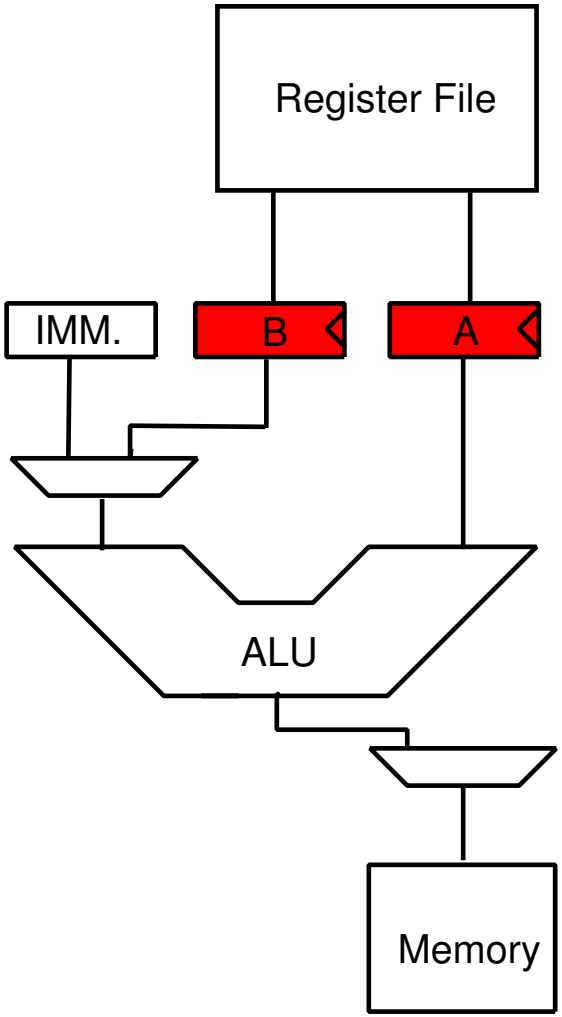
What can I do?



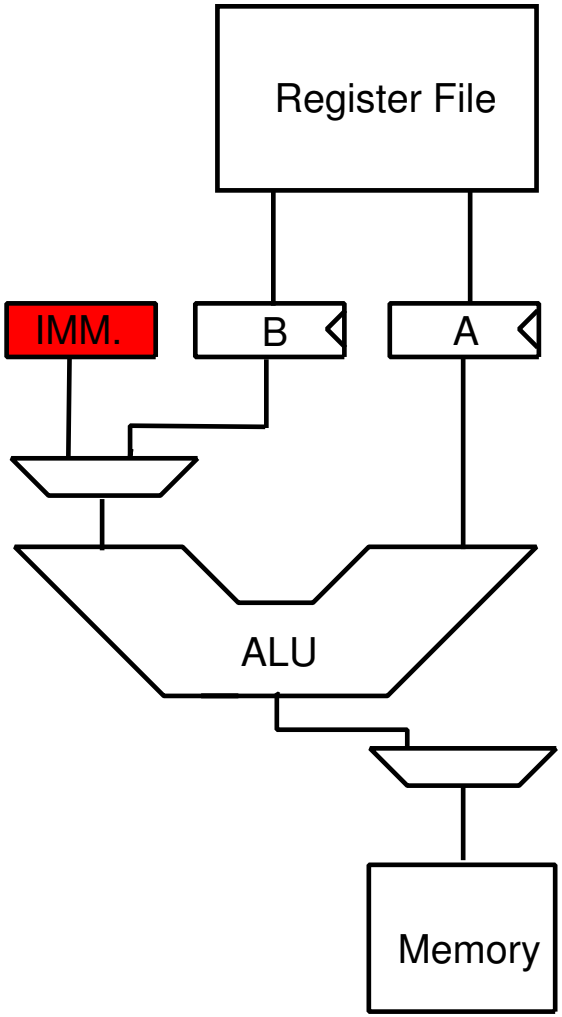
What can I do?



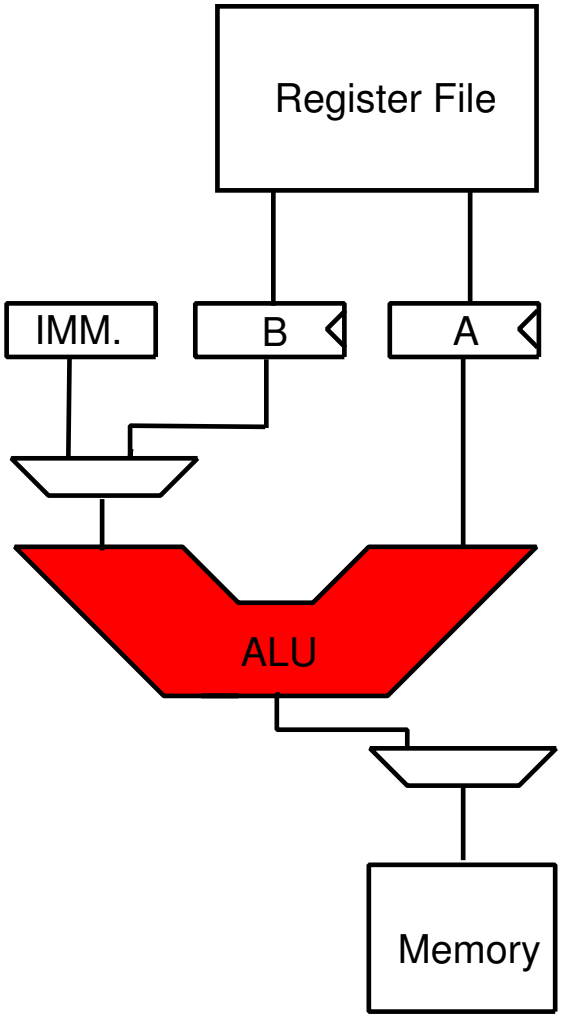
What can I do?



What can I do?



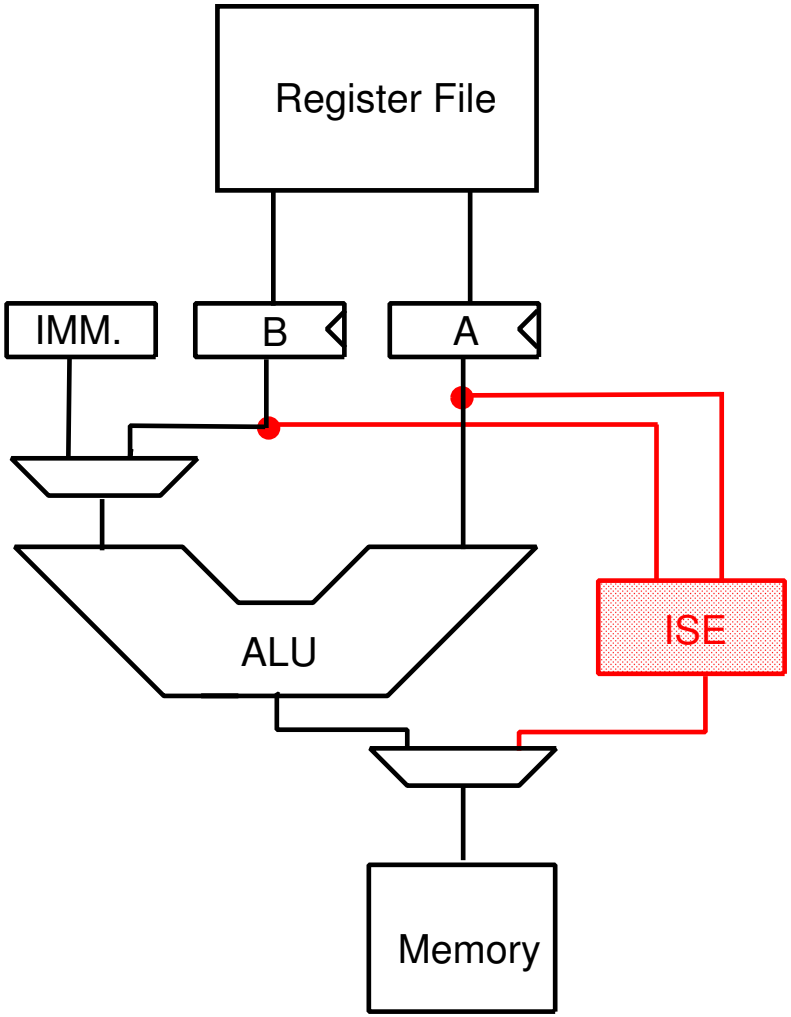
What can I do?



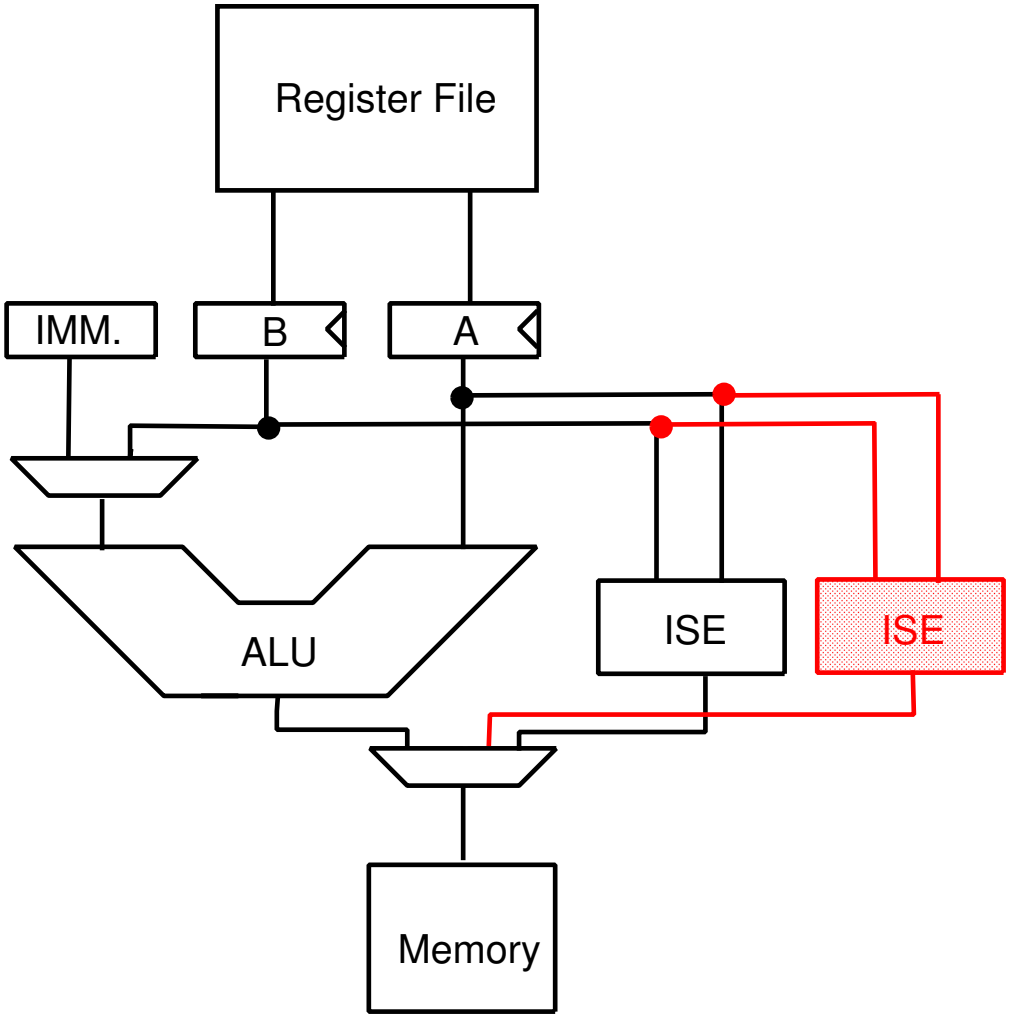
What can I do?

Something easier?

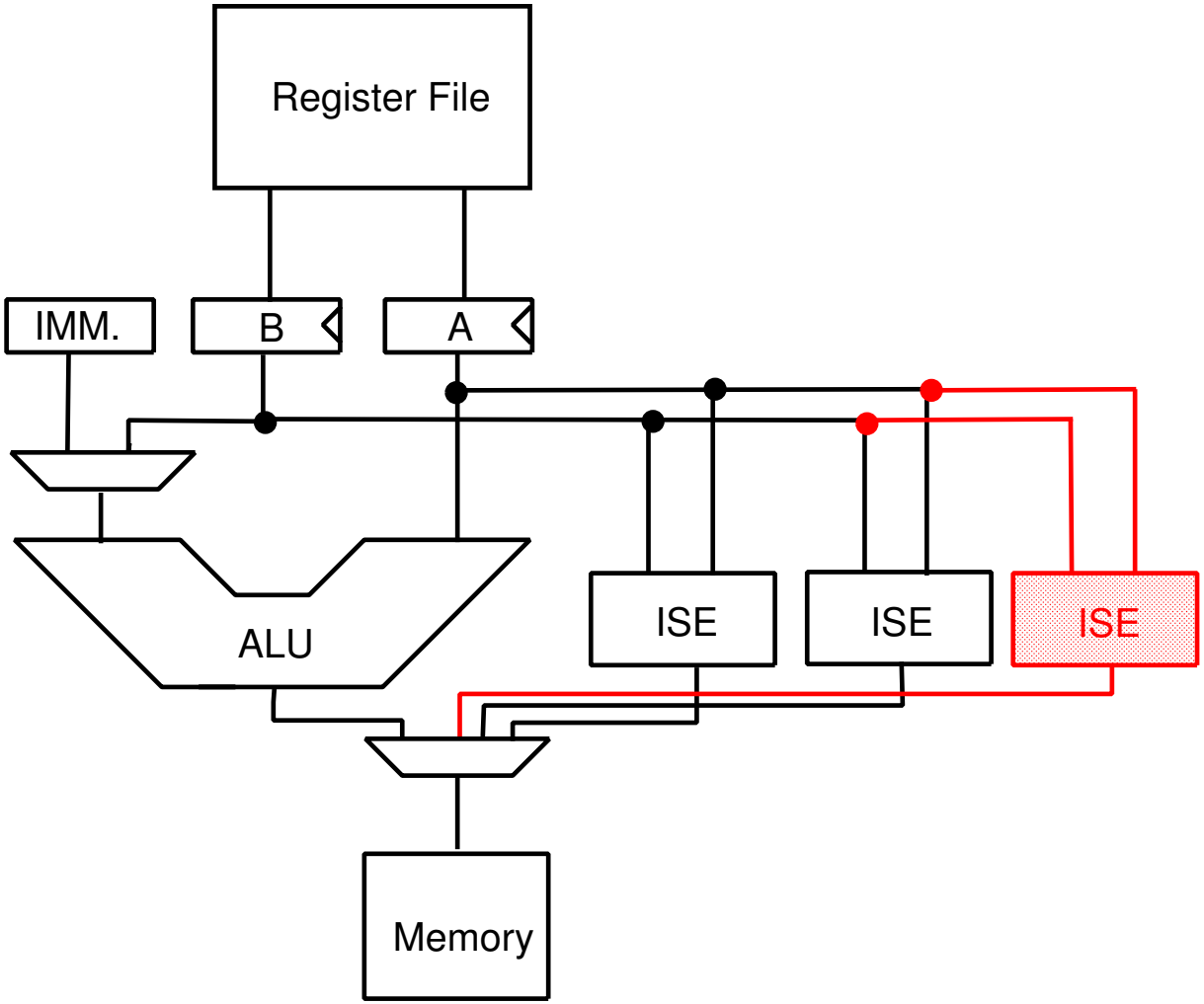
Protected / Non Protected CO-Design!



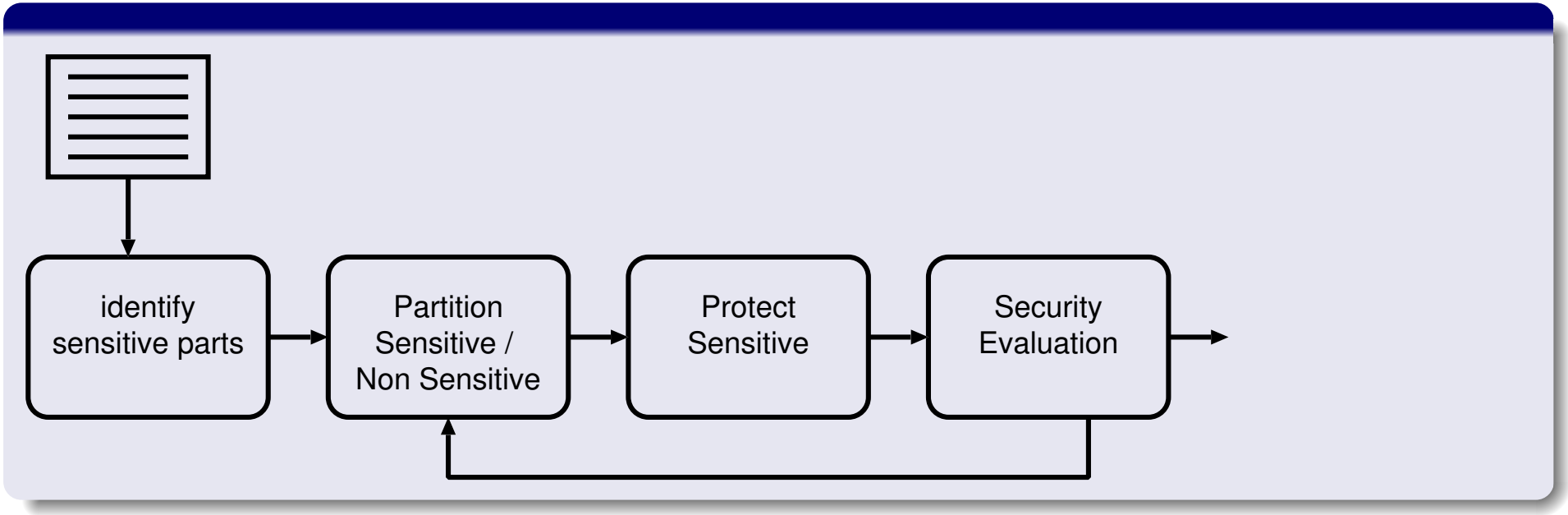
Protected / Non Protected CO-Design!



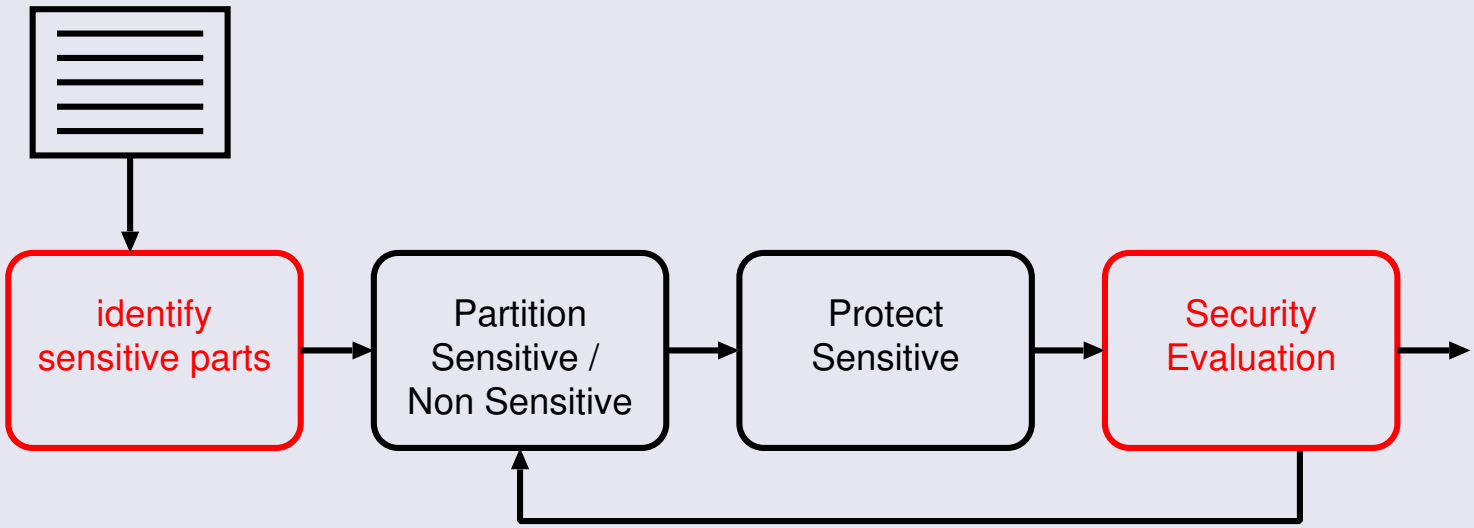
Protected / Non Protected CO-Design!



Automatic design of DPA resistant ISE

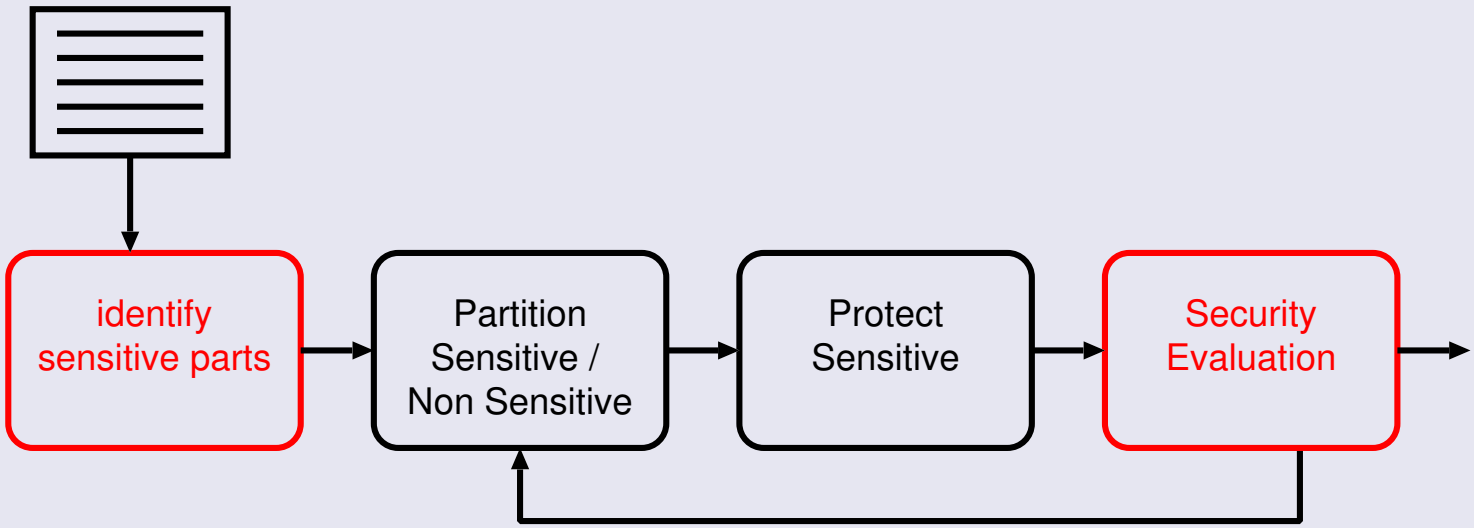


Needed "Basic Blocks"



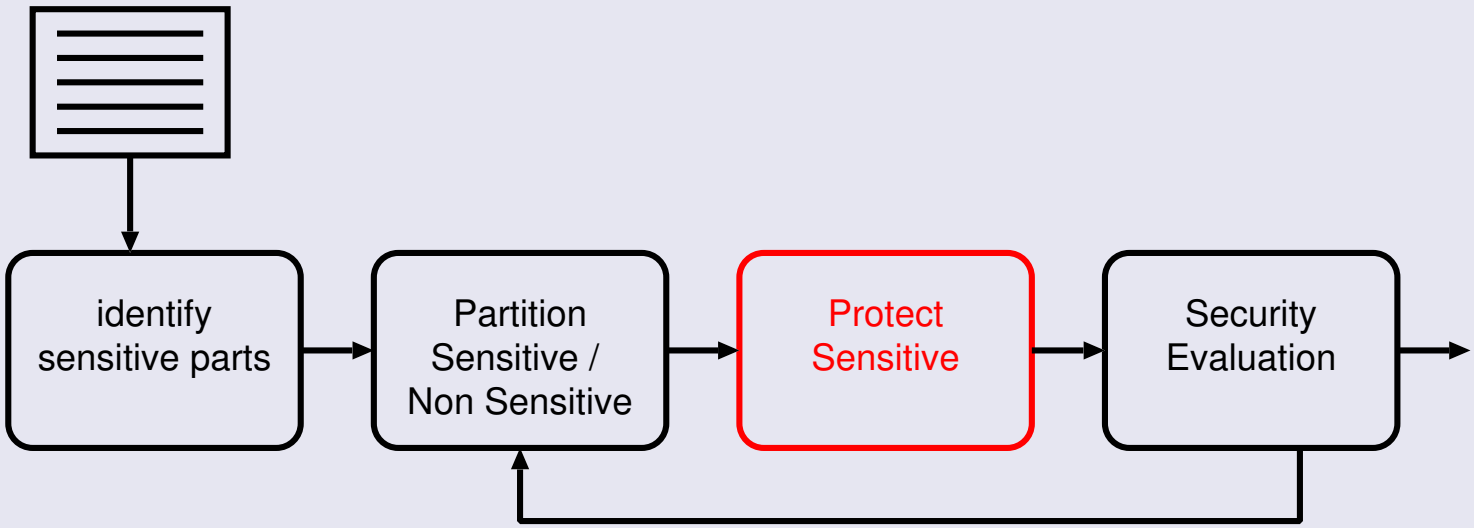
- Generate useful power traces?

Needed "Basic Blocks"



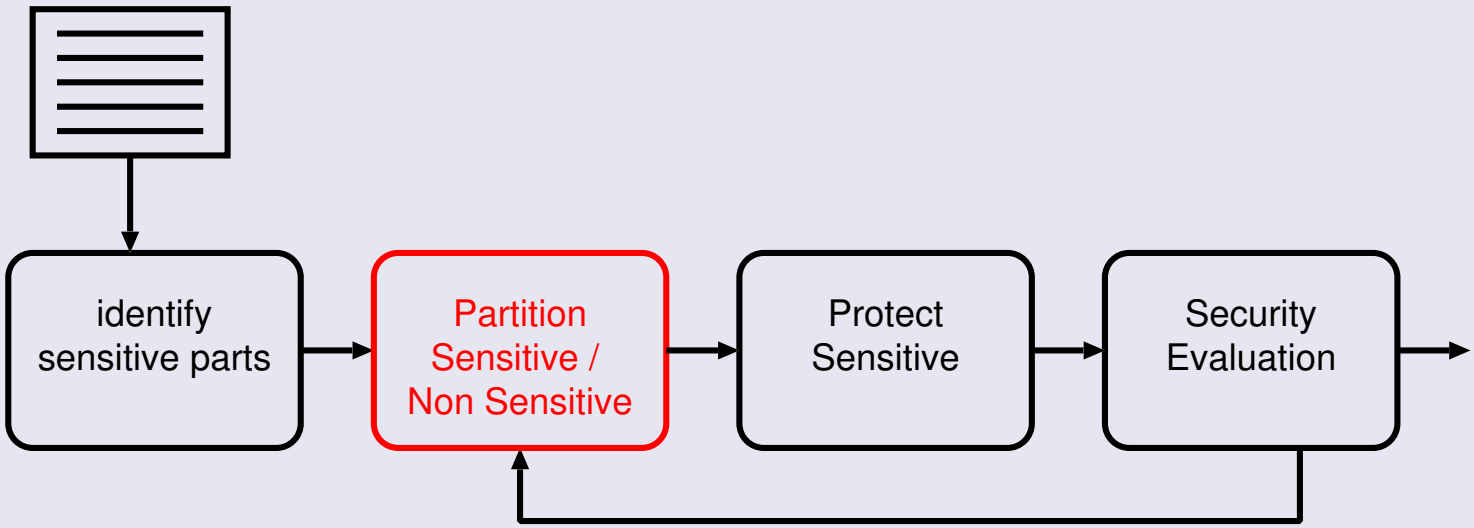
- Generate useful power traces?
- Measure the DPA resistance?

Needed "Basic Blocks"



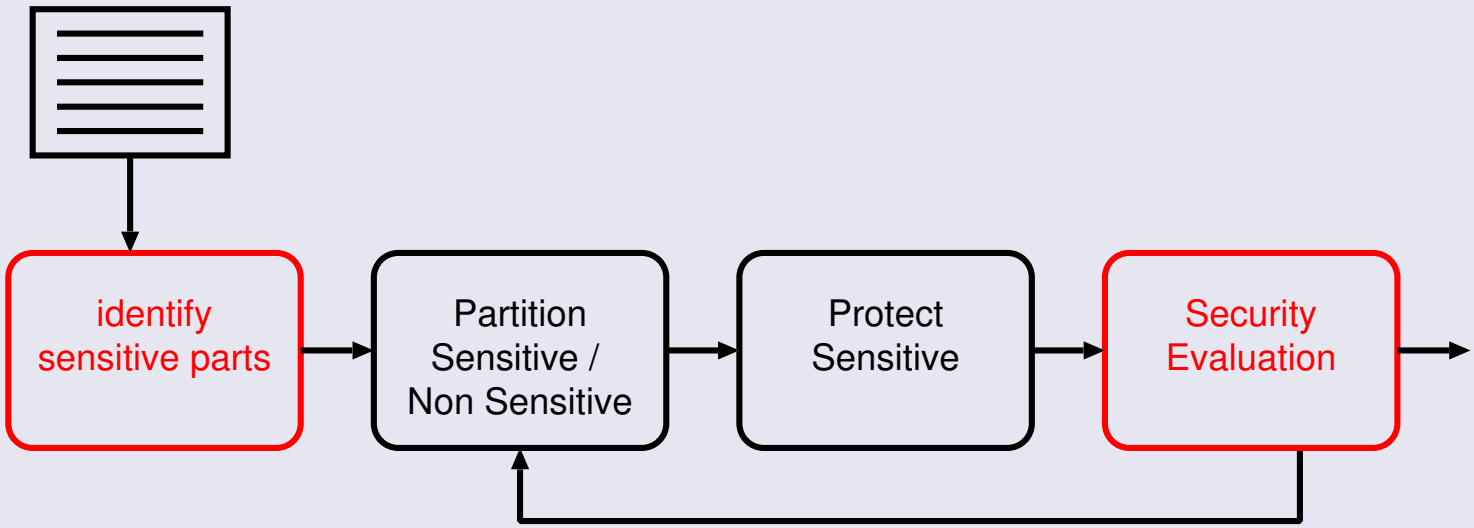
- Generate useful power traces?
- Measure the DPA resistance?
- Countermeasure and its design flow?

Needed "Basic Blocks"



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

Needed "Basic Blocks"



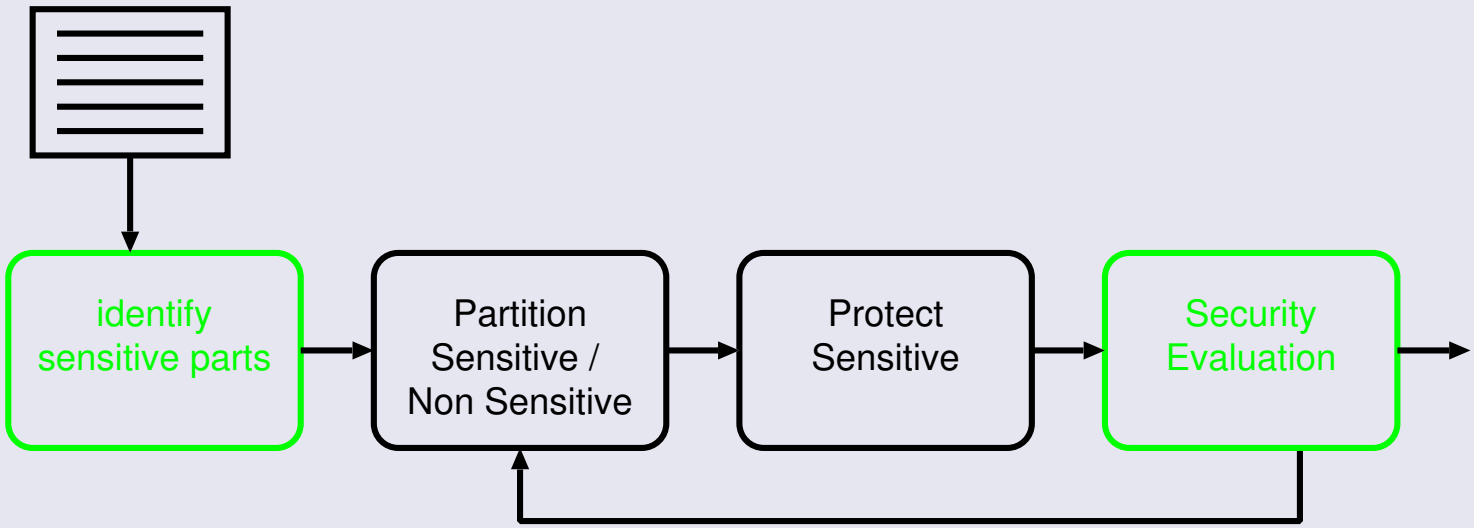
- Generate useful power traces?
- Measure the DPA resistance?
- Countermeasure and its design flow?
- Partition the algorithm?

Information Theory Metric

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

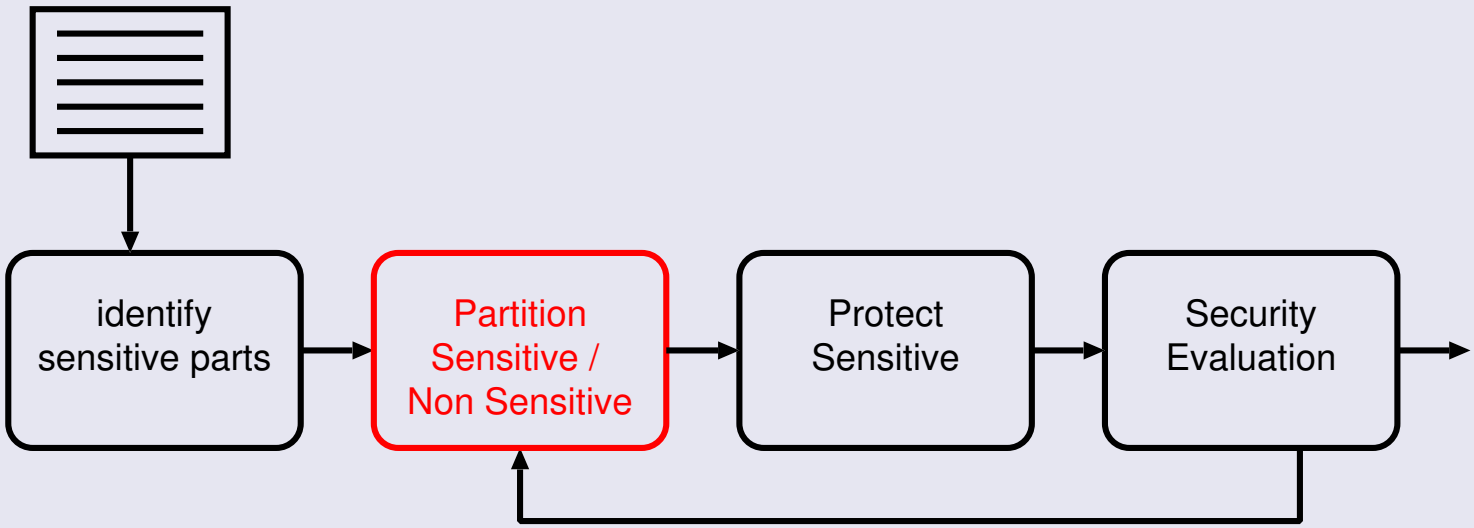
- Add white noise
- Reduce the dimension using compression
- Compute the mutual information

Needed "Basic Blocks"



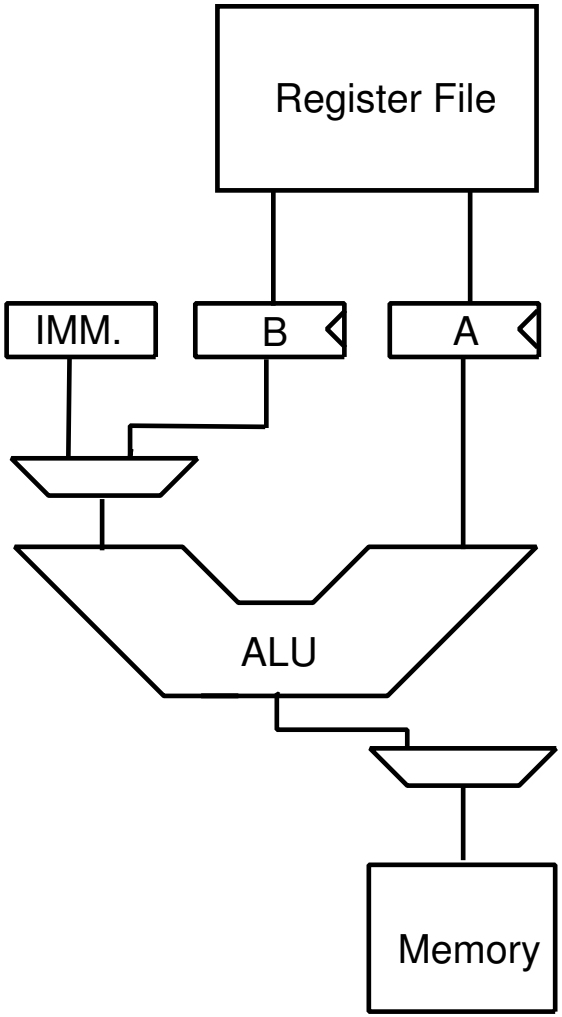
- Generate useful power traces? ✓
- Measure the DPA resistance? ✓
- Countermeasure and its design flow?
- Partition the algorithm?

Needed "Basic Blocks"

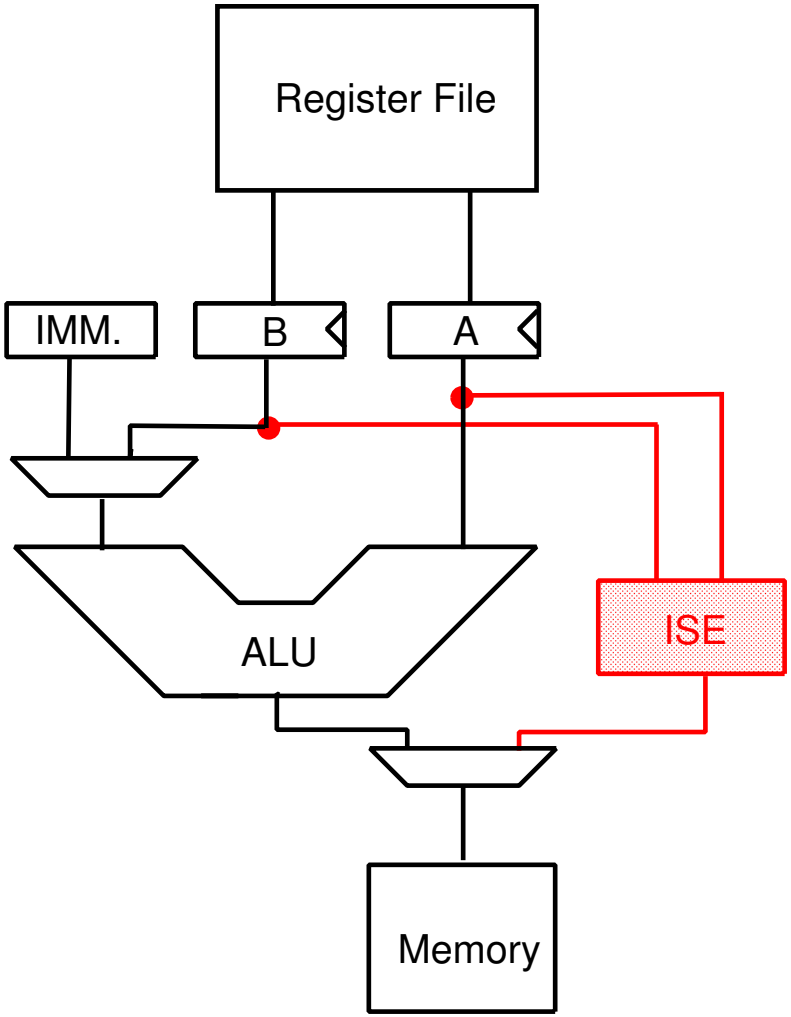


- Generate useful power traces? ✓
- Measure the DPA resistance? ✓
- Countermeasure and its design flow? ✓
- Partition the algorithm?

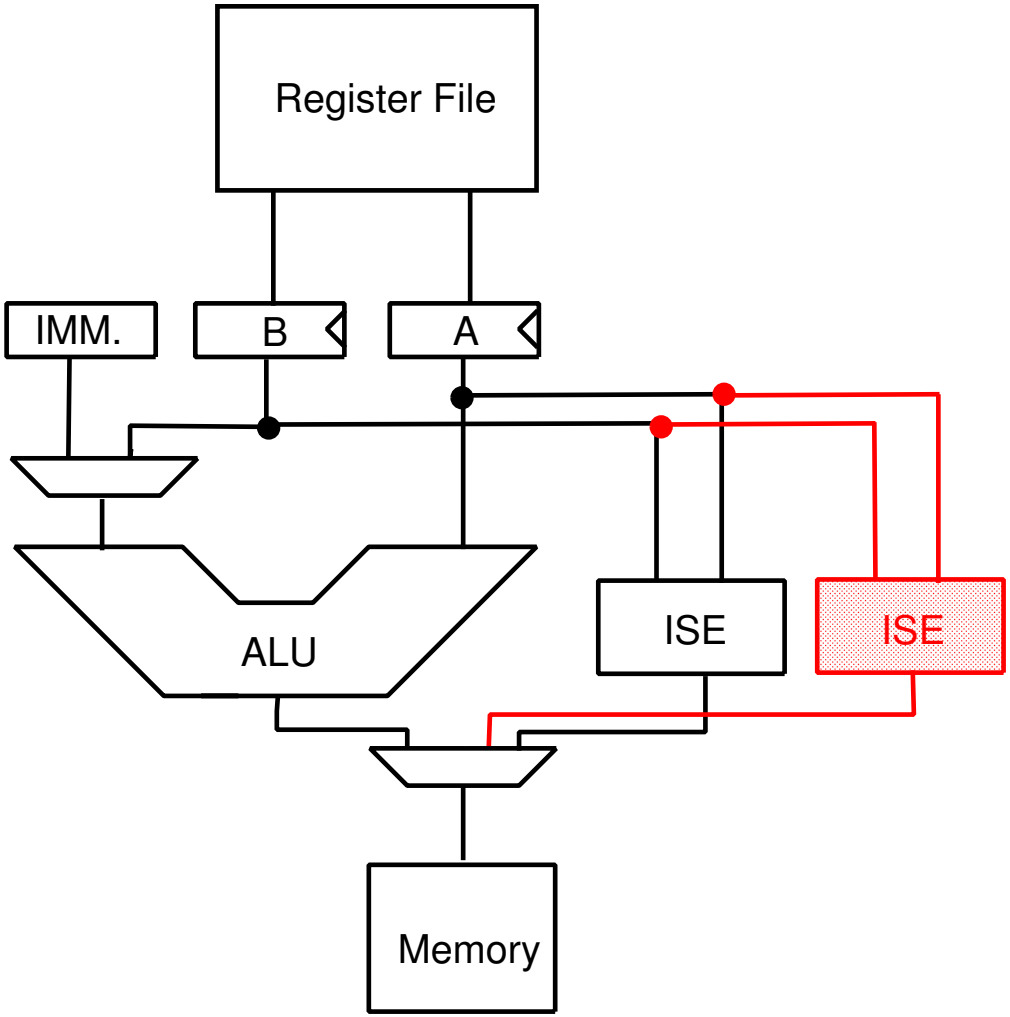
Algorithm partitioning tool



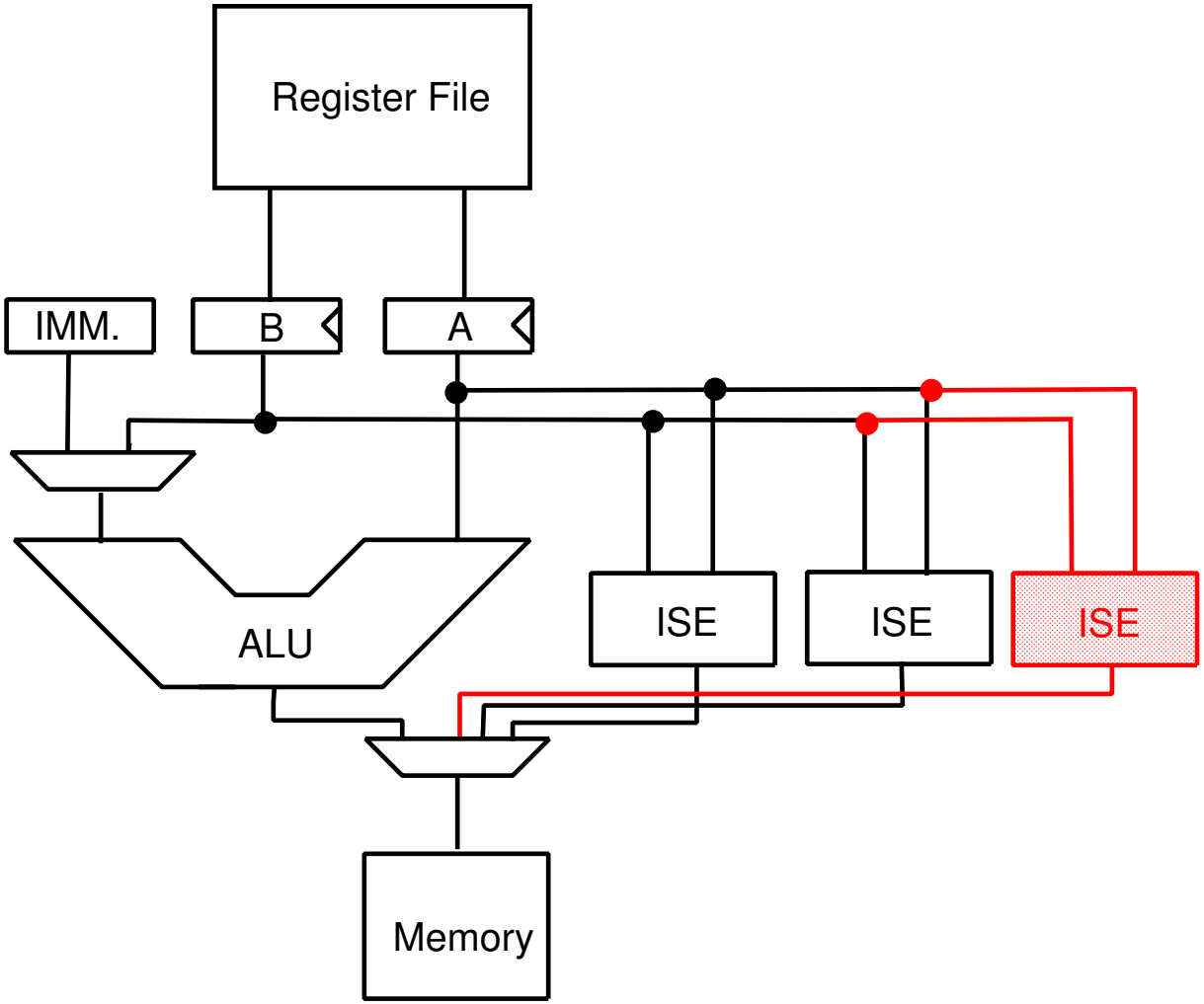
Algorithm partitioning tool



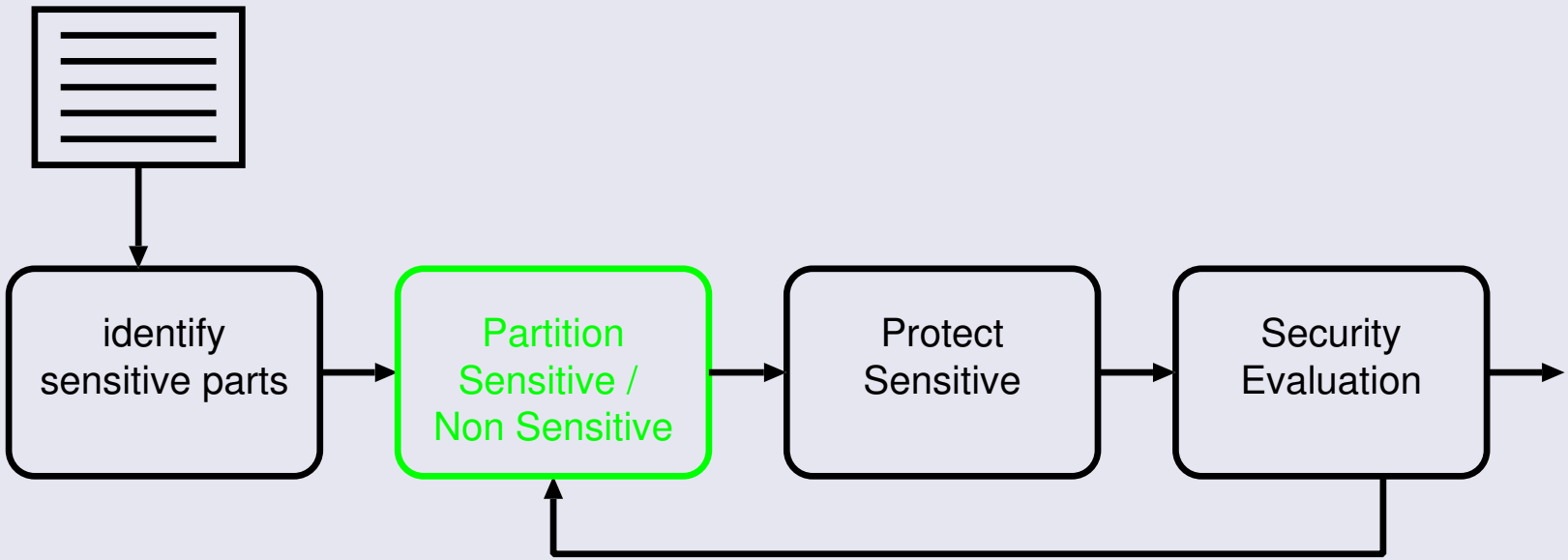
Algorithm partitioning tool



Algorithm partitioning tool

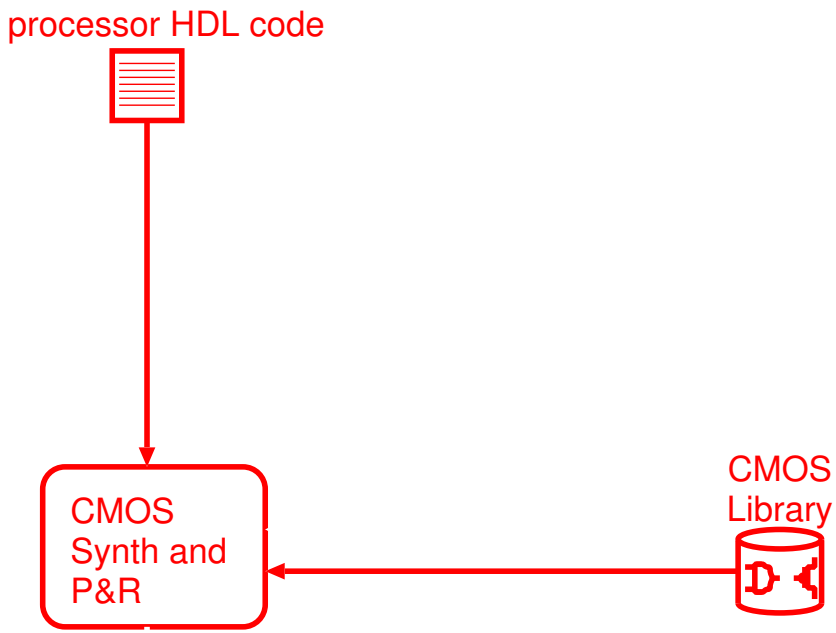


Needed "Basic Blocks"

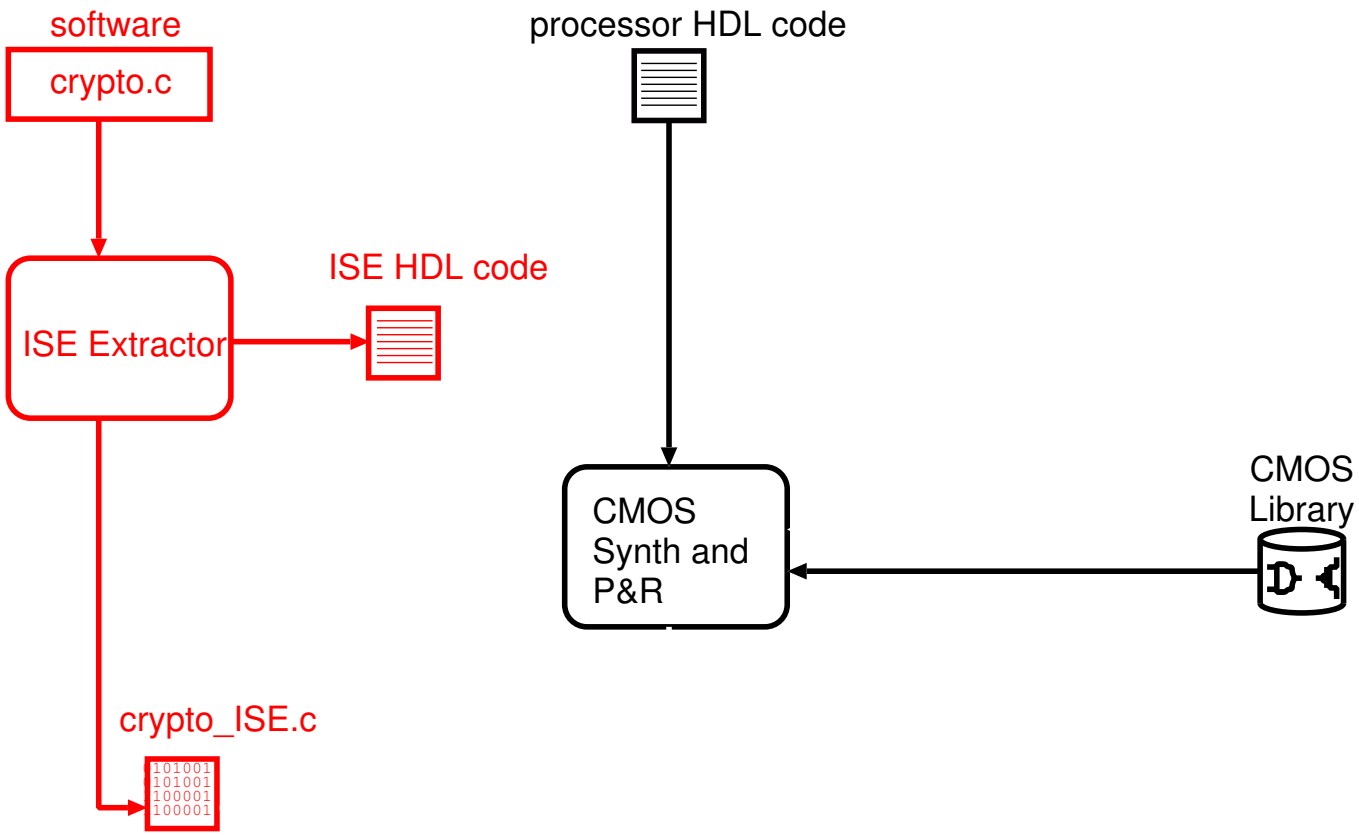


- Generate useful power traces? ✓
- Measure the DPA resistance? ✓
- Countermeasure and its design flow? ✓
- Partition the algorithm? ✓

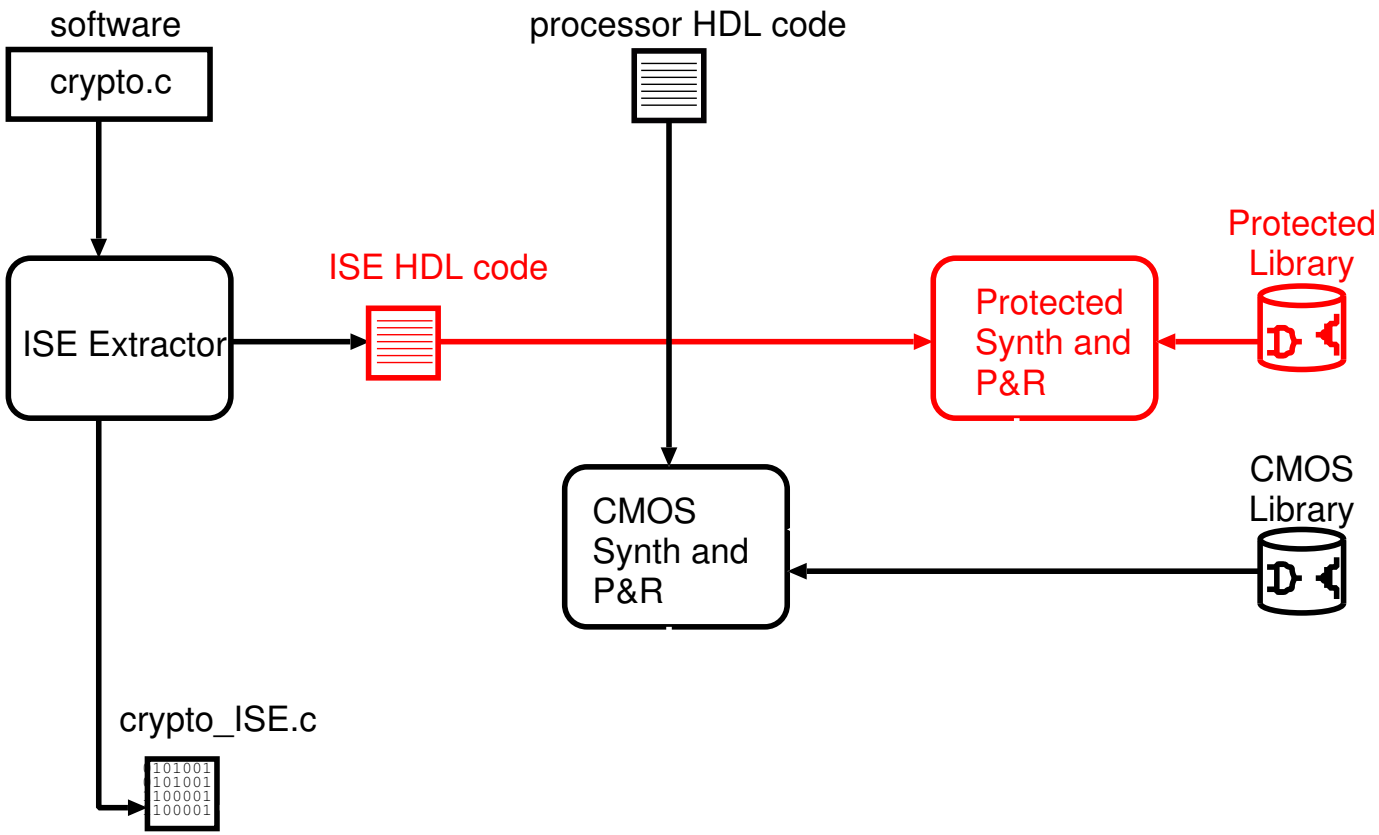
The CMOS Design Flow



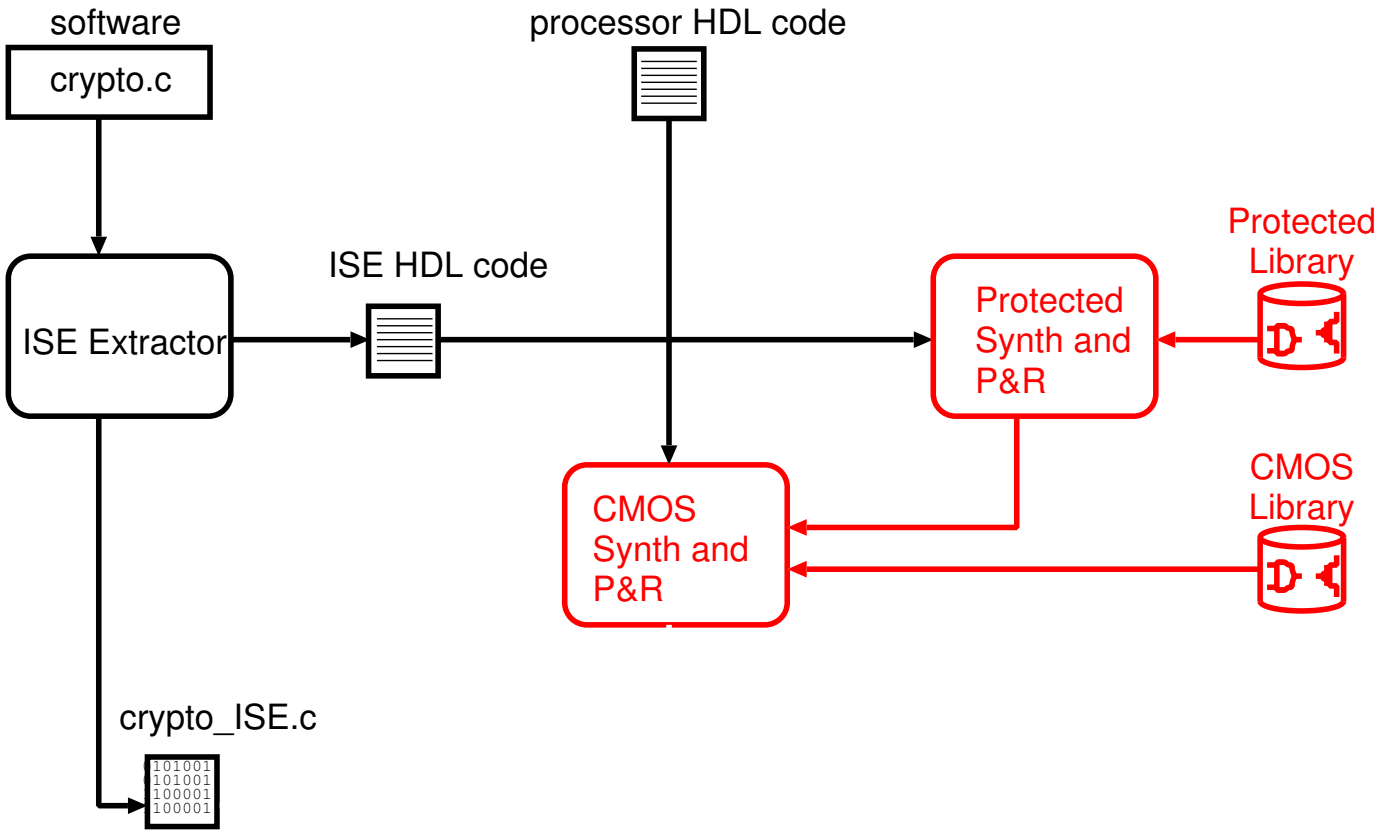
The Processor Customization



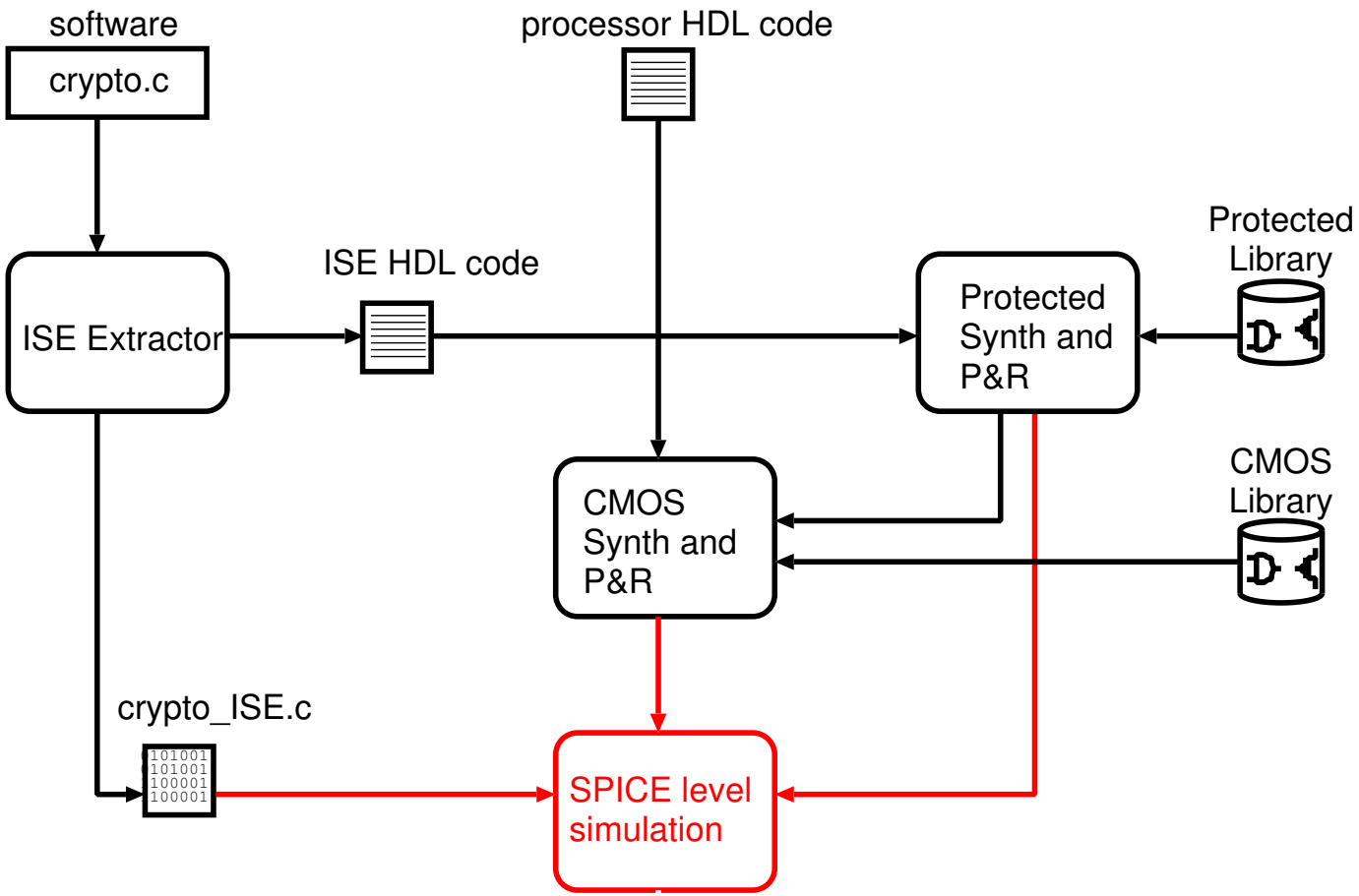
The Protected Design Flow



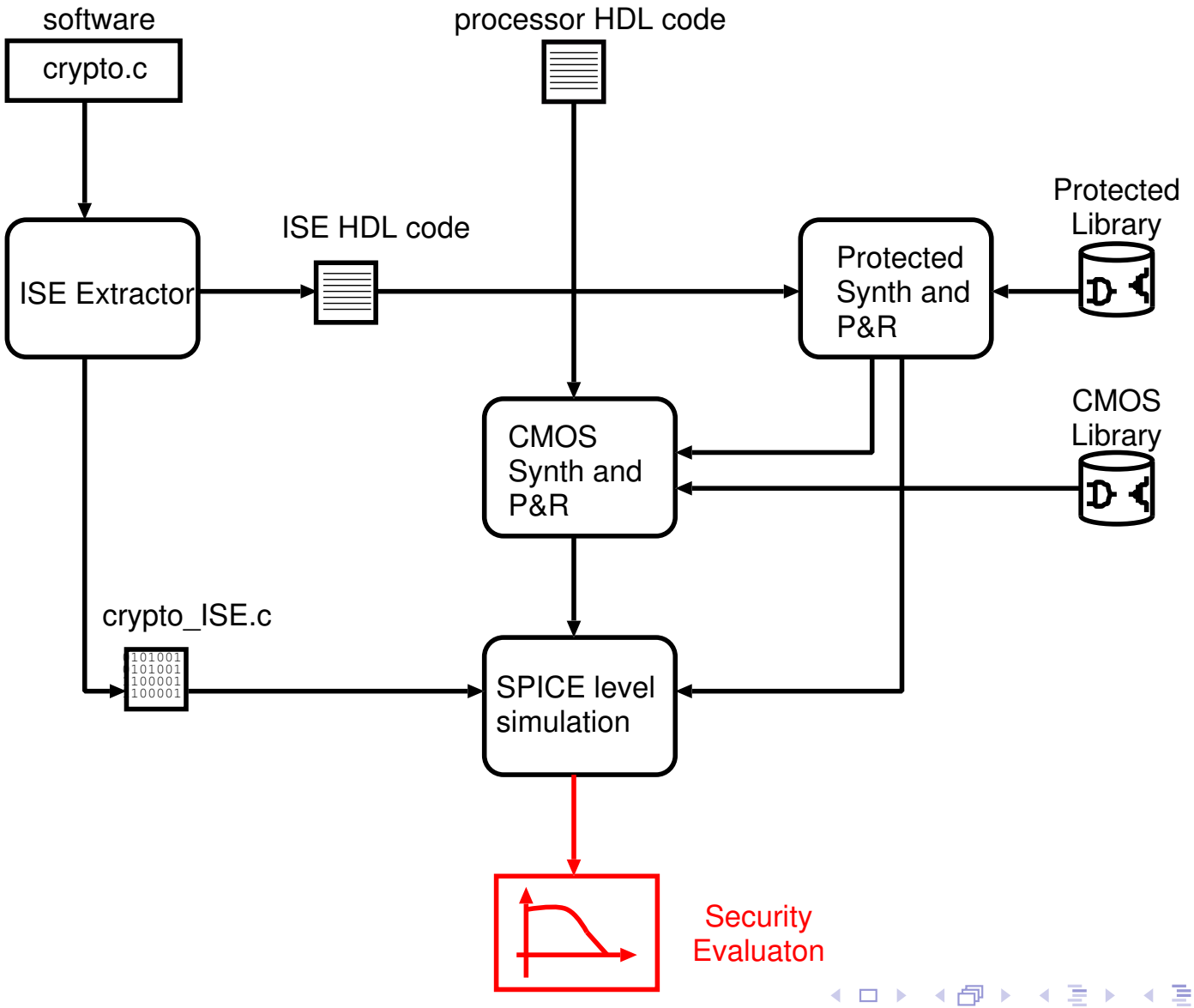
The Hybrid Design Flow



The Simulation Environment



The Design Evaluation



Contents

Cyber-Physical Risk

Physical on Physical the 3D printer

- **Profile a Side Channel**
- **Listen**
- **Reconstruct the printing file**
- **Still the IP**

Cyber on Physical tampering with the printing file

- **Tamper with the printing file**
- **Print the tampered object**
- **The object is too weak!**

Contents

More potential weakest links

- CPS consists of hardware, software, sensors, actuators, and communication infrastructure...
- ...an adversary can attack any of these (or a combination of them)

- Several CPS are expected to operate for many decades...
- ..they will be exposed to threats that are not known today

- A massive number of CPSs will surround us

...and don't forget the complete picture!

- A massive number of CPSs will surround us
- the devices are in the hand of the attacker
- large diffusion would imply catastrophic consequences in case of fail
- large number of deployed systems means an extremely large platform for carry out distributed attacks.

Conclusions

- Security is a crucial property for CPSs
- Some challenges are similar to cyber-systems
- Very little is done to secure the physical part

Questions?