Laboratoire
d'Informatique
de Robotique
et de Microélectronique
de Montpellier

On-Line Self-Test of AES Hardware Implementations

G. Di Natale, M. L. Flottes, B. Rouzeyre

LIRMM, France

{dinatale,flottes,rouzeyre}@lirmm.fr

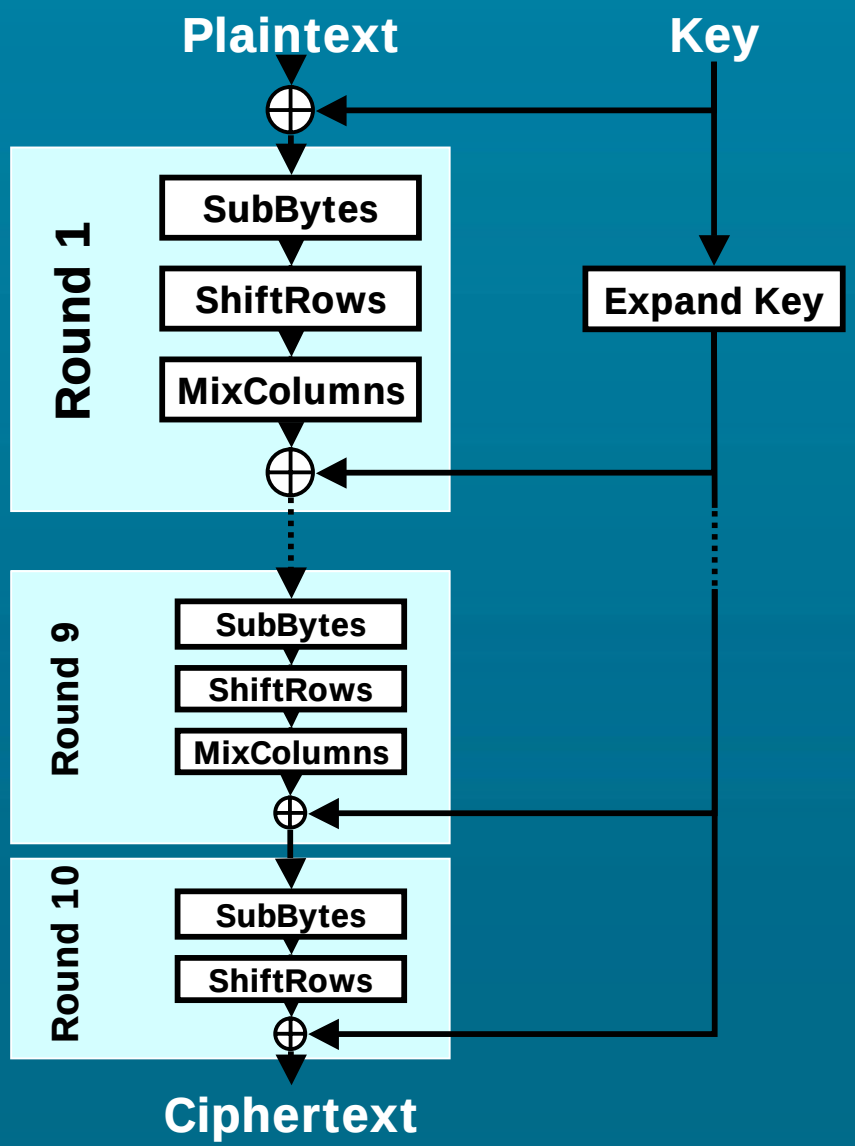
Introduction

- Scenario
  - Consumer electronics
  - Production defects
  - Secure device
- Possible attacks
  - DPA: easy to perform, cheap
- Goal
  - Dependable architecture
  - DPA resistant

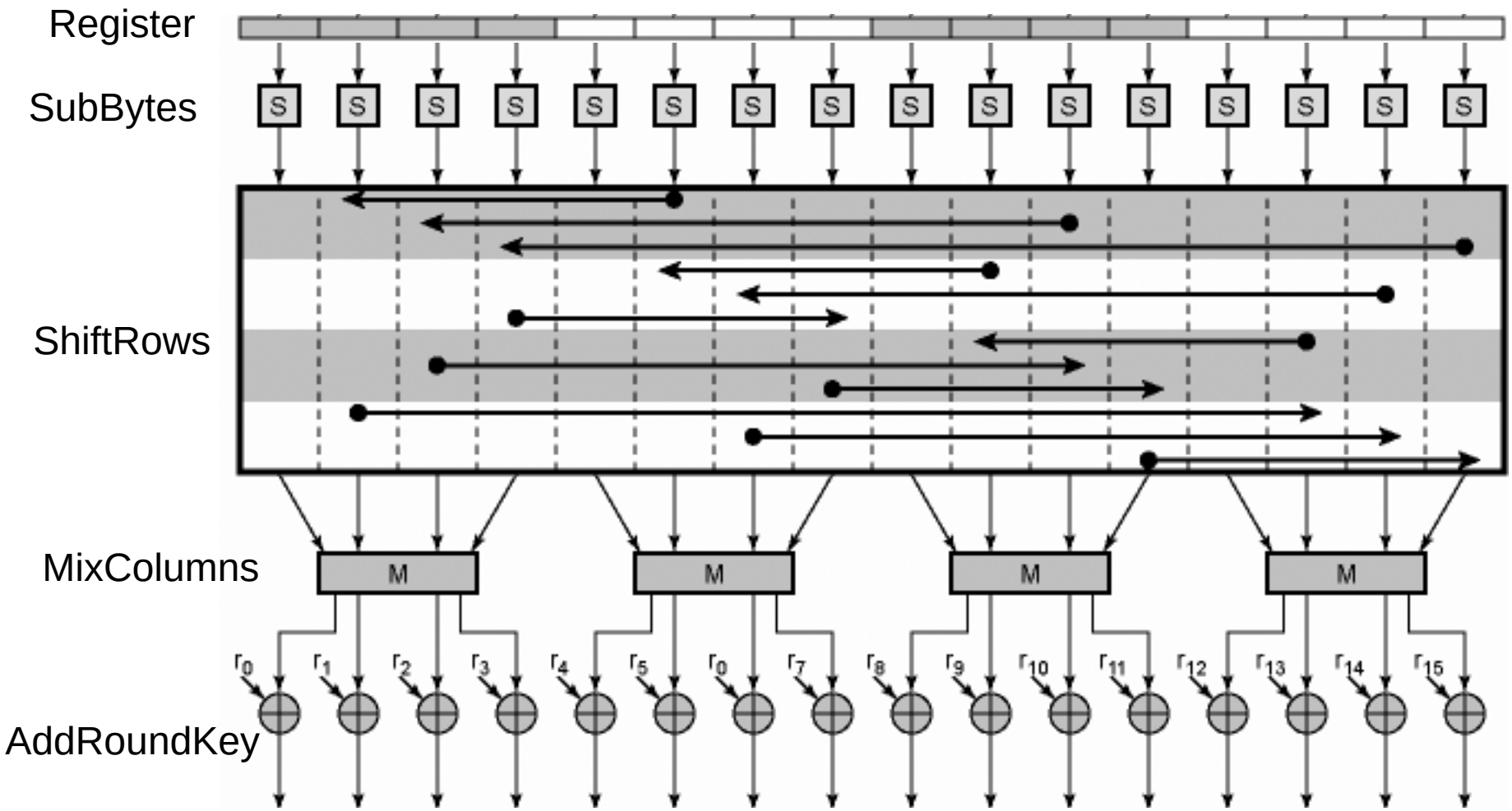
Outline

- AES
- Architecture description
- Experimental results
- Conclusions

AES Encryption



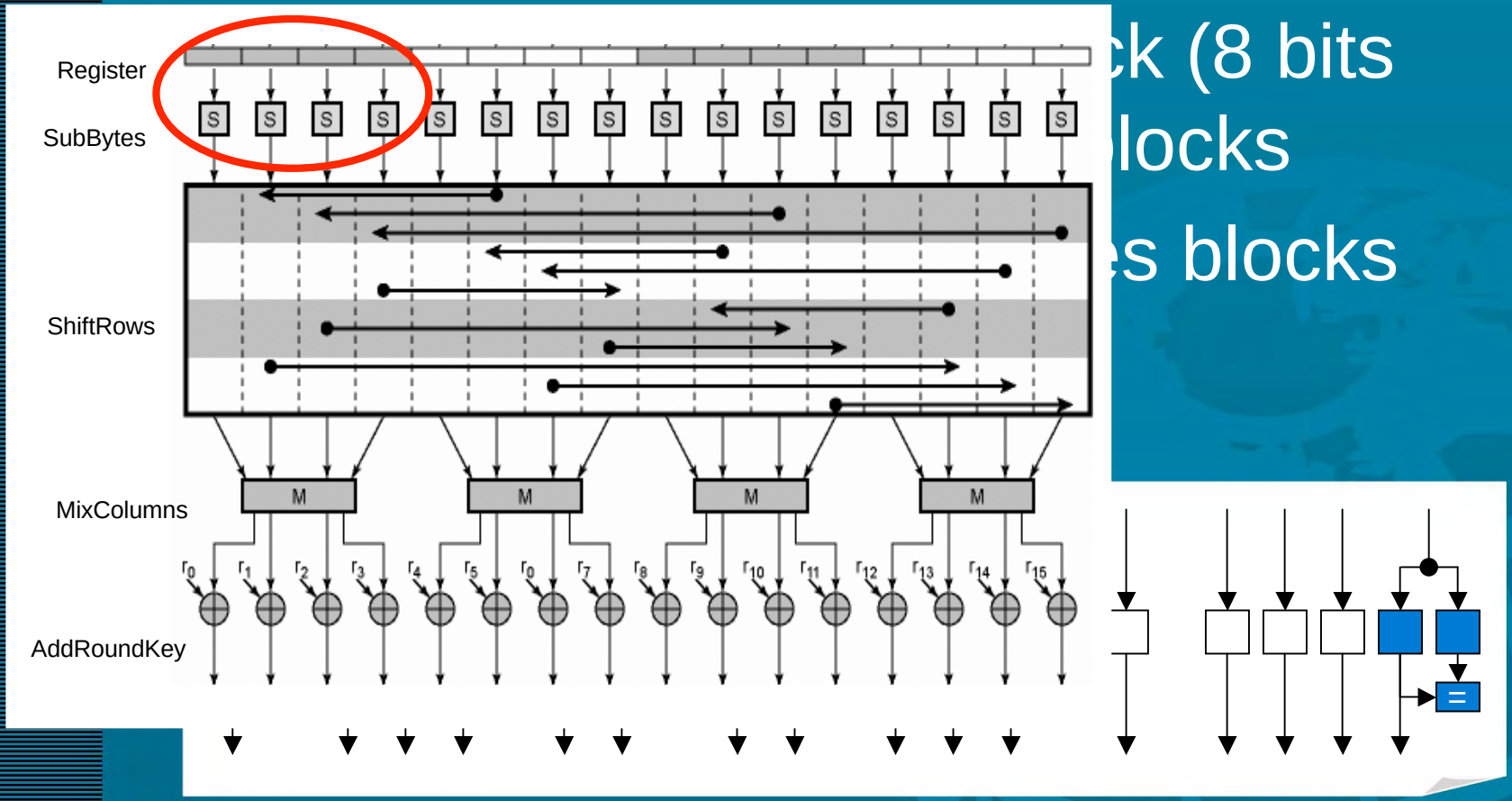
AES Round Details



Outline

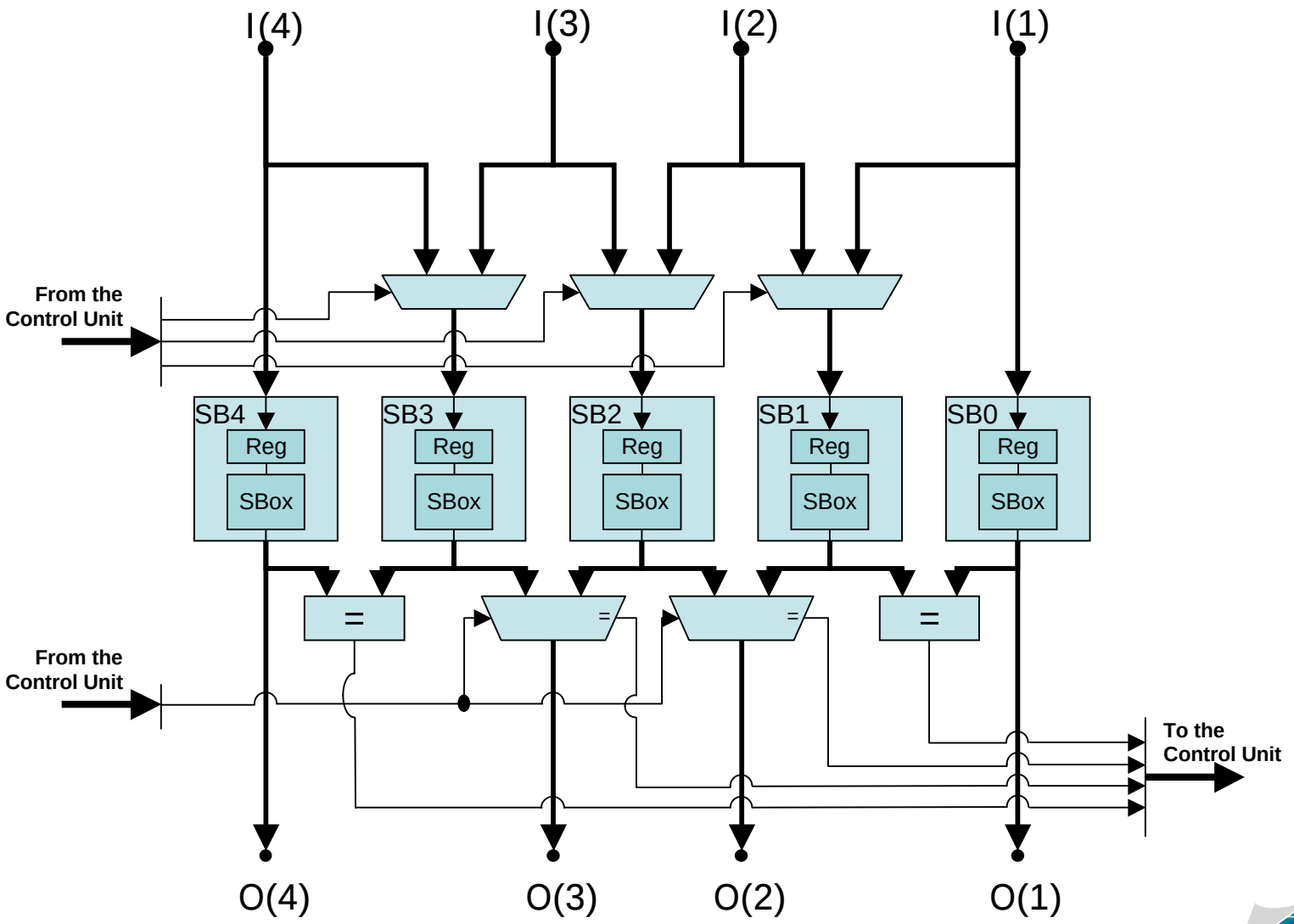
- AES
- Architecture description
- Experimental results
- Conclusions

Architecture Description

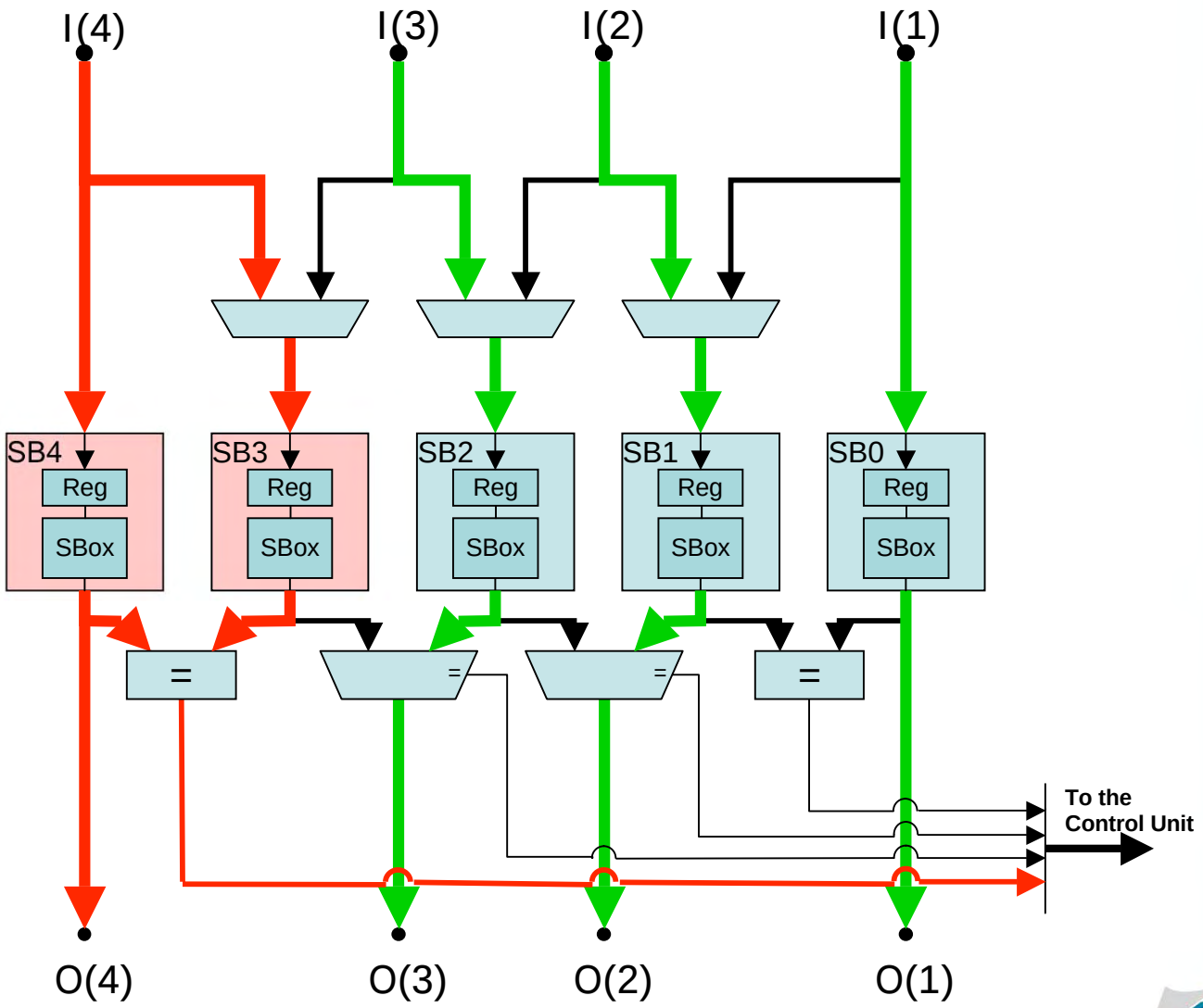


ck (8 bits
locks
es blocks

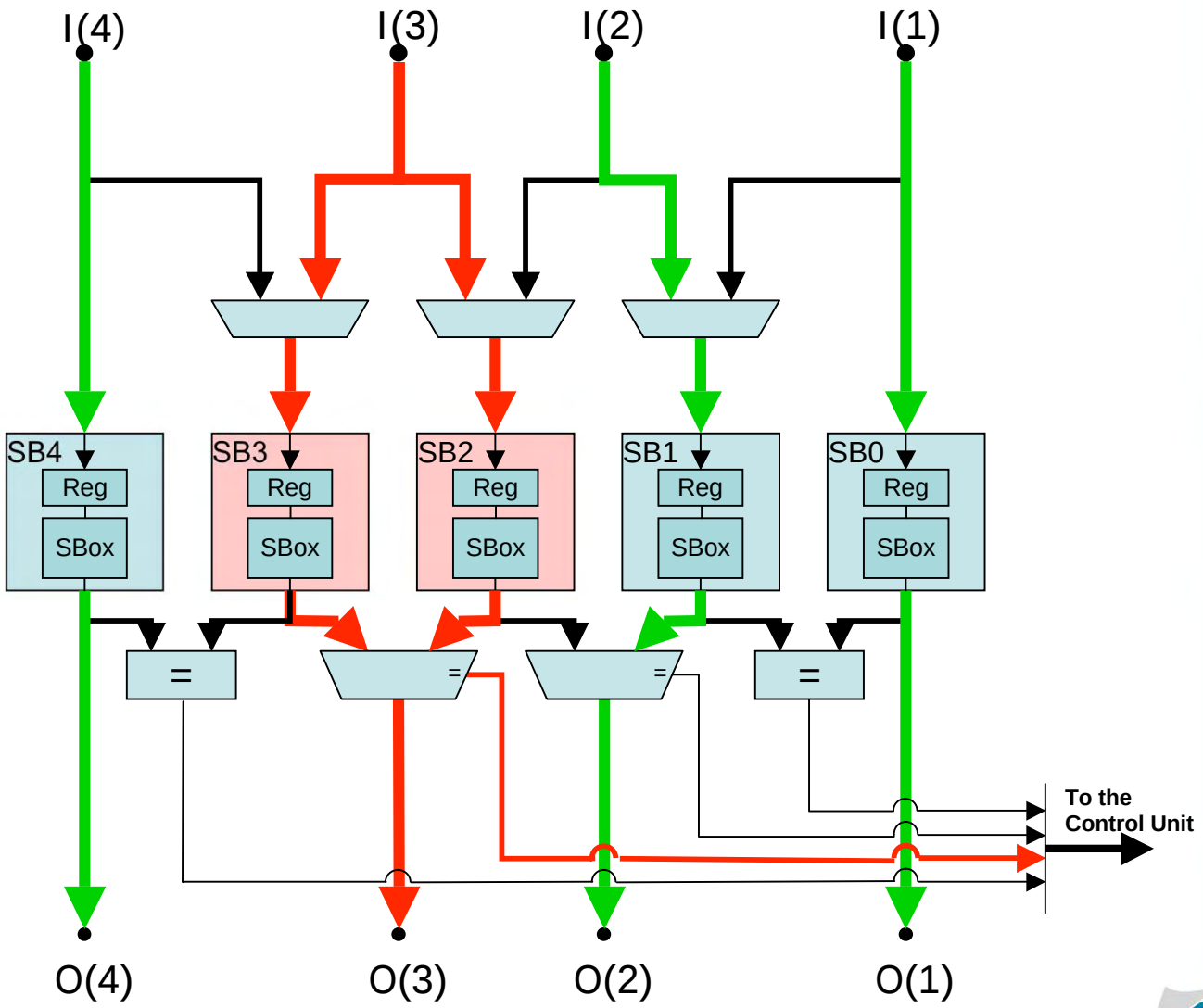
Architecture details



Architecture details



Architecture details



Outline

- AES
- Architecture description
- Experimental results
- Conclusions

Experimental Results

- Synthesis: VHDL + Cadence RTL Compiler
- Technology: 0.35µm CMOS library provided by Austria Micro Systems
- S-Boxes synthesized as combinational logic
- Number of Sboxes:
  - 16 data + 4 spares
  - 4 key generation + 1 spare

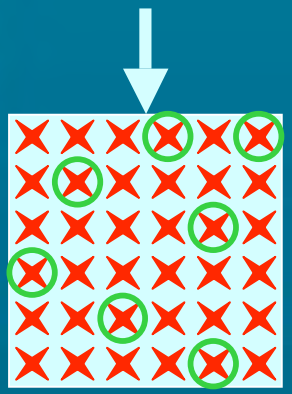
Area

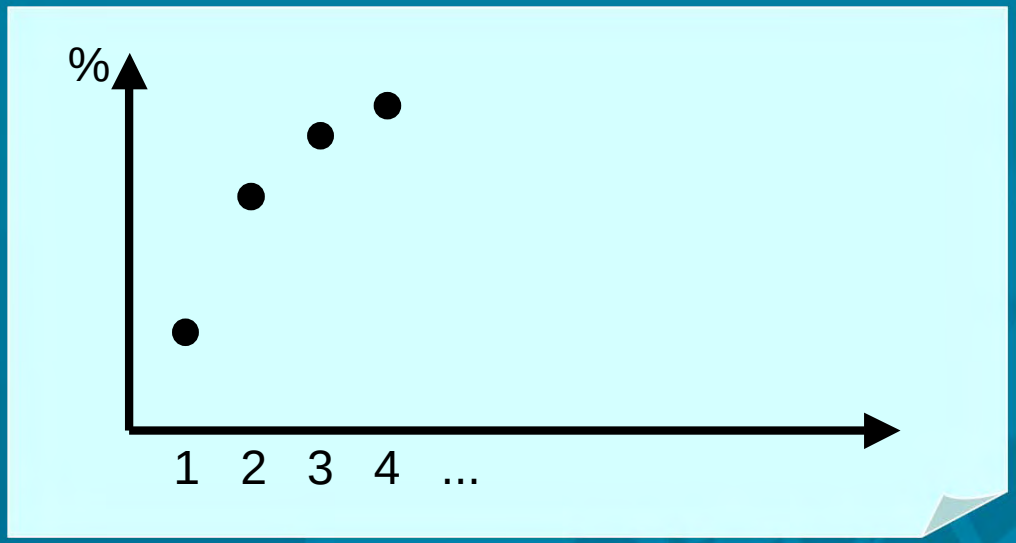
	Base	Redundant
Registers S-Boxes	9590	2397
MixColumns ShiftRows AddKey	552	0
Control Unit	55	275
Key Generator	2805	746
Total	**13002**	**3418**

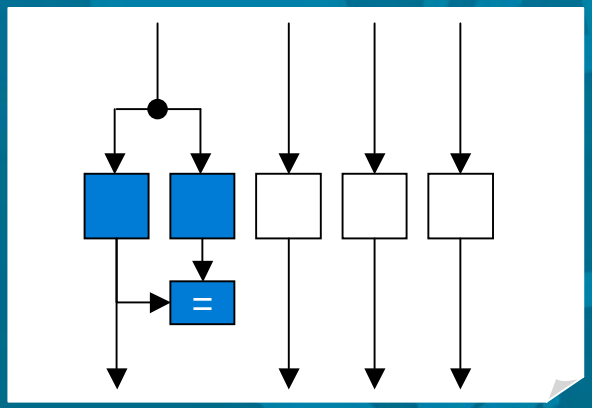
Overhead = ~25%

Fault Latency

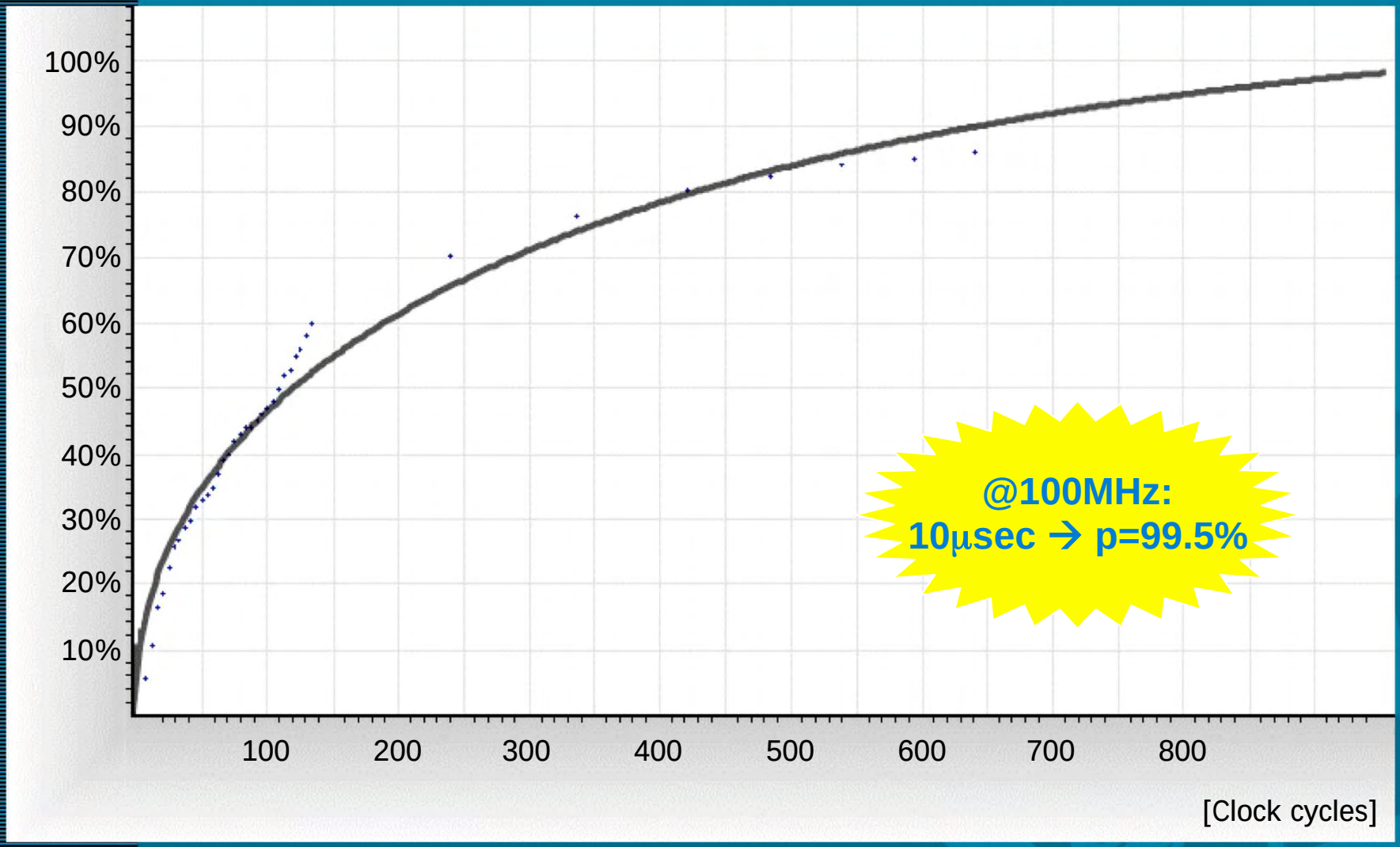
00110011
01010000
11000011
00000000
01010111





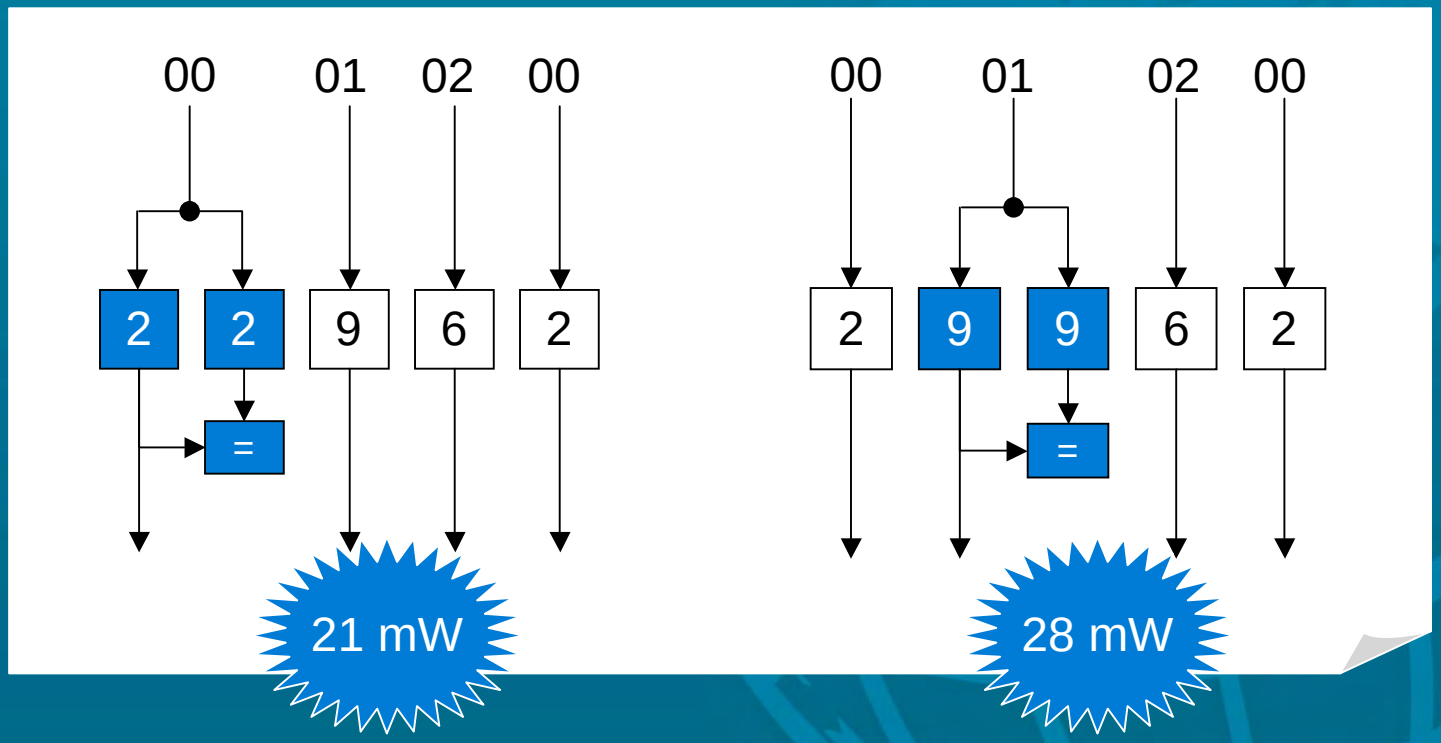


Fault detection probability



Power analysis

Input	Power
00	2 mW
01	9 mW
02	6 mW
...	...



Outline

- AES
- Architecture description
- Experimental results
- Conclusions

Conclusions

- Proposed solution:
  - Low cost concurrent online Self-Test
  - Acceptable fault detection latency
  - DPA Resistant
- Future works:
  - Not concurrent online BIST to decrease fault latency
  - Online Self-Repair

LIRMM

Thank you