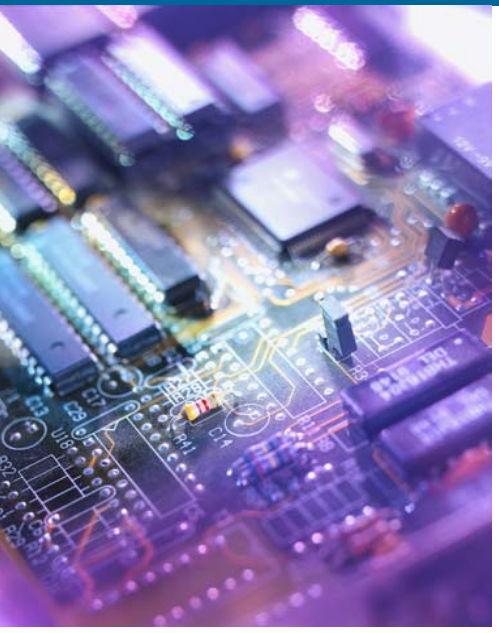


Test and Security

Giorgio Di Natale, Marion Doulcier, Marie-Lise Flottes, Bruno Rouzeyre

{dinatale,doulcier,flottes,rouzeyre}@lirmm.fr

Laboratoire
d'Informatique
de Robotique
et de Microélectronique
de Montpellier
LIRMM

Outline

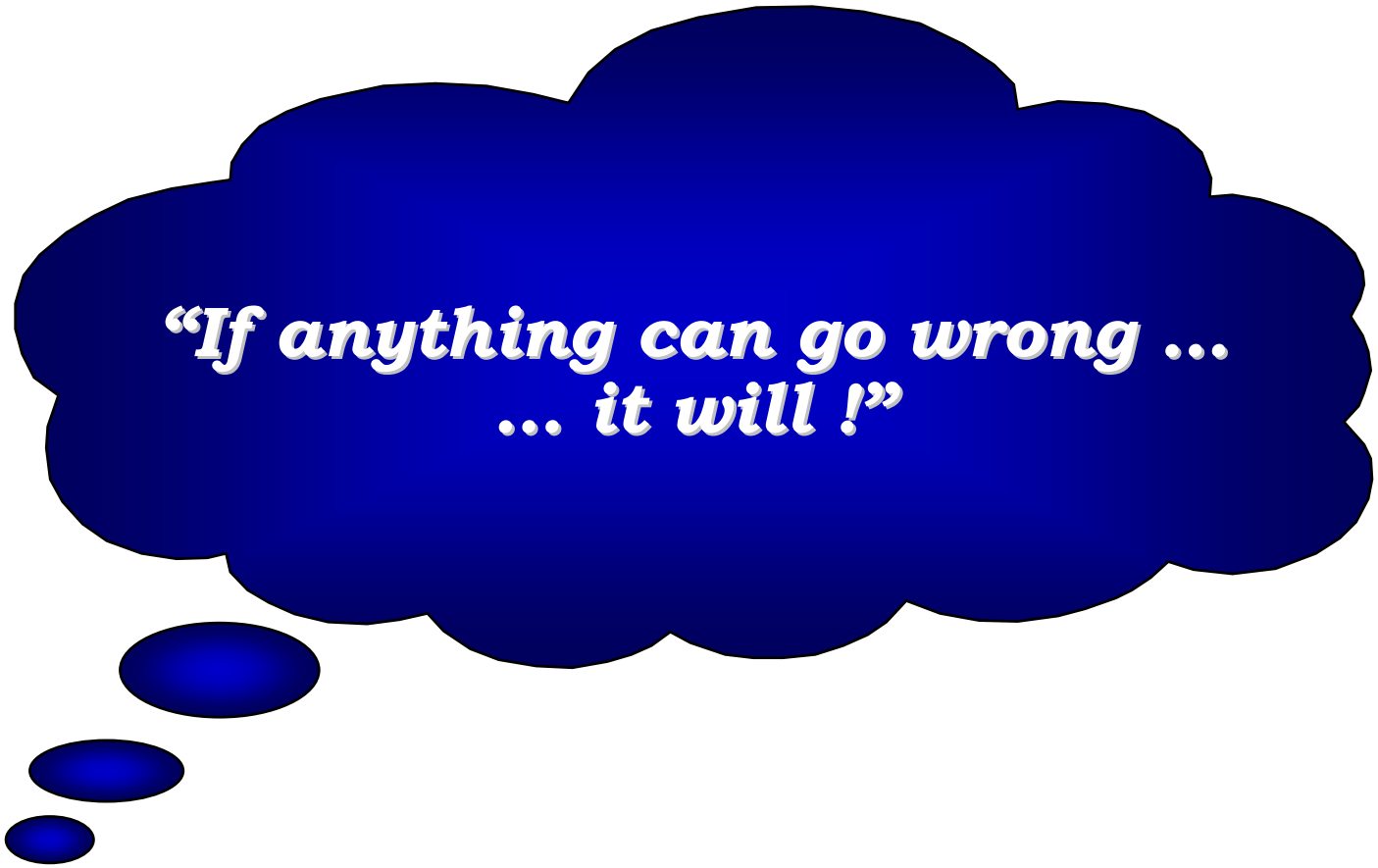
- Test
- Security vs Test
  - Scan-based attacks
  - Securing the scan chains
- AES BIST
- Conclusion

Outline

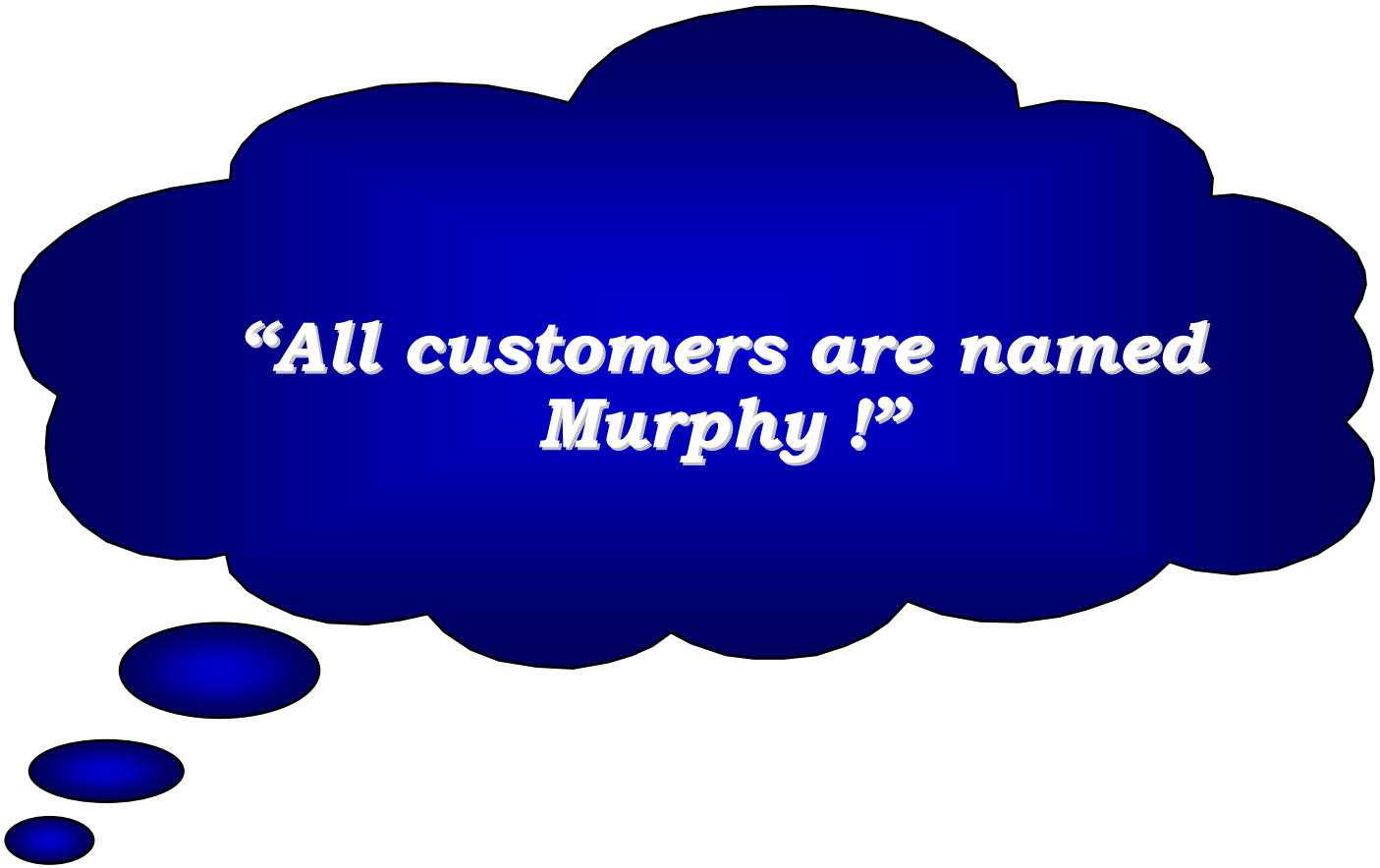
- **Test**
- Security vs Test
  - Scan-based attacks
  - Securing the scan chains
- AES BIST
- Conclusion

Test

- **Test**: set of operations aiming at checking whether a manufactured unit properly works w.r.t. its specifications or not
- Test cost: very high (~30% of the whole IC cost)

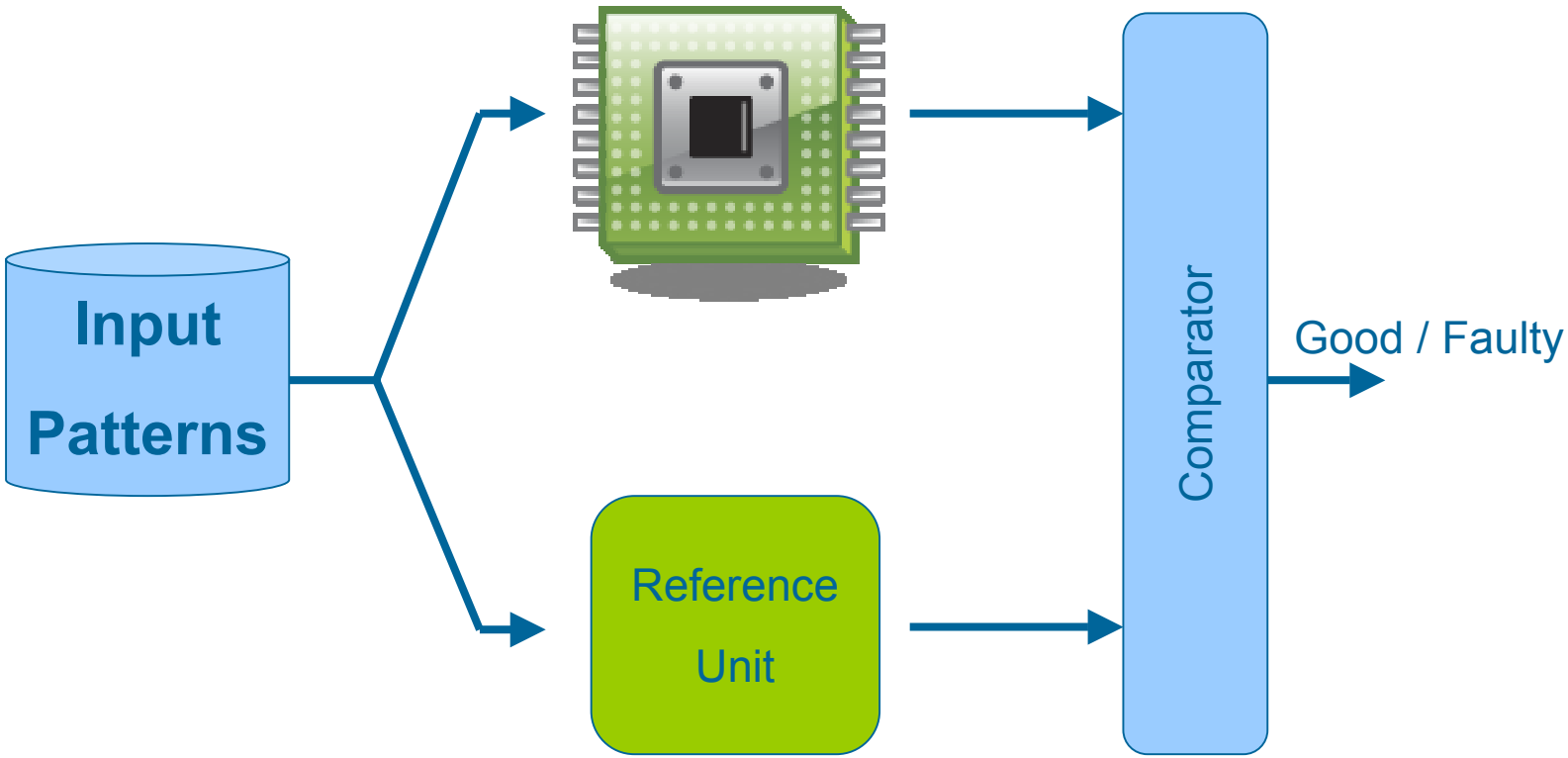


[Murphy]

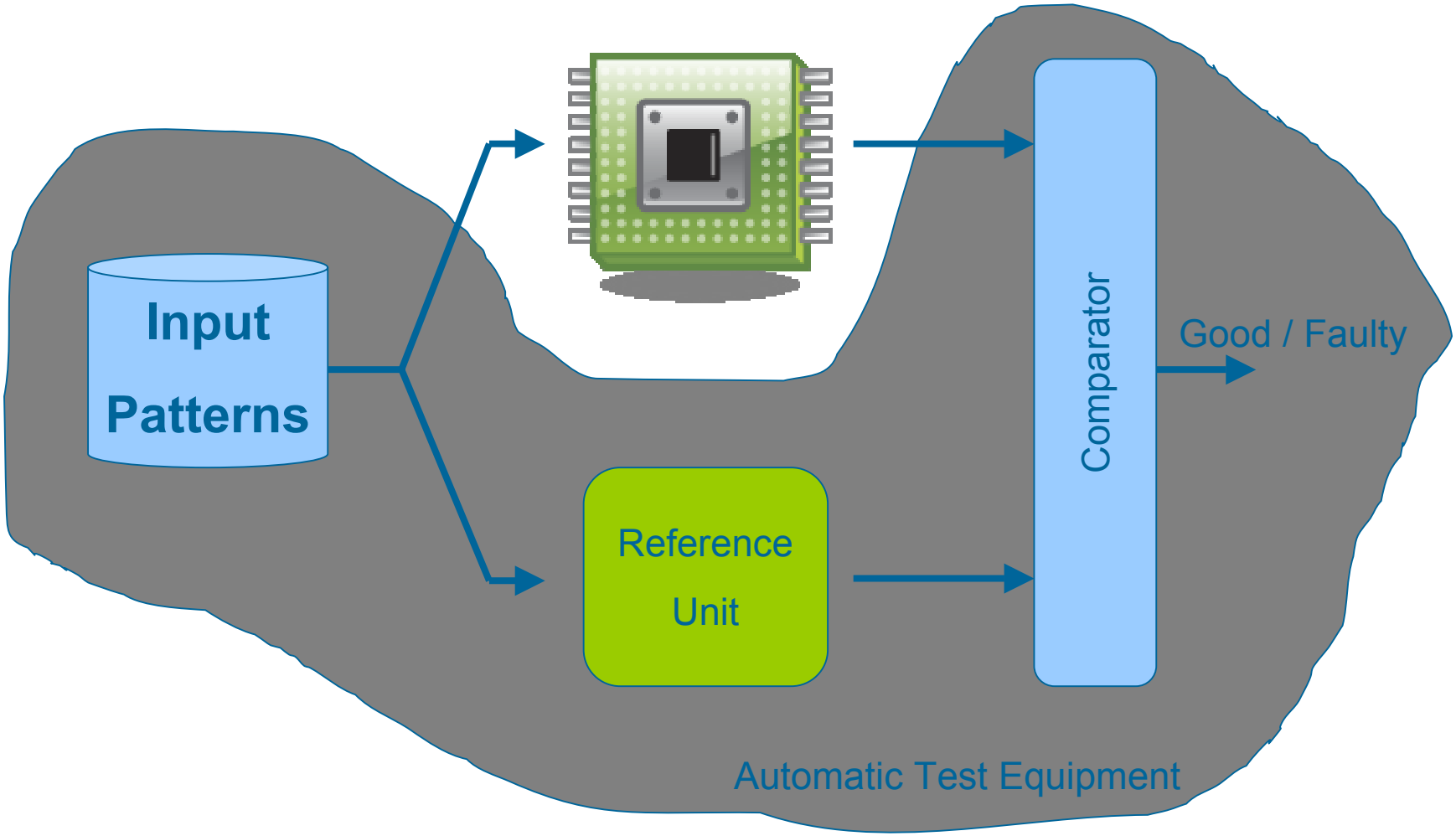


[Any test engineer]

Test: basic principles

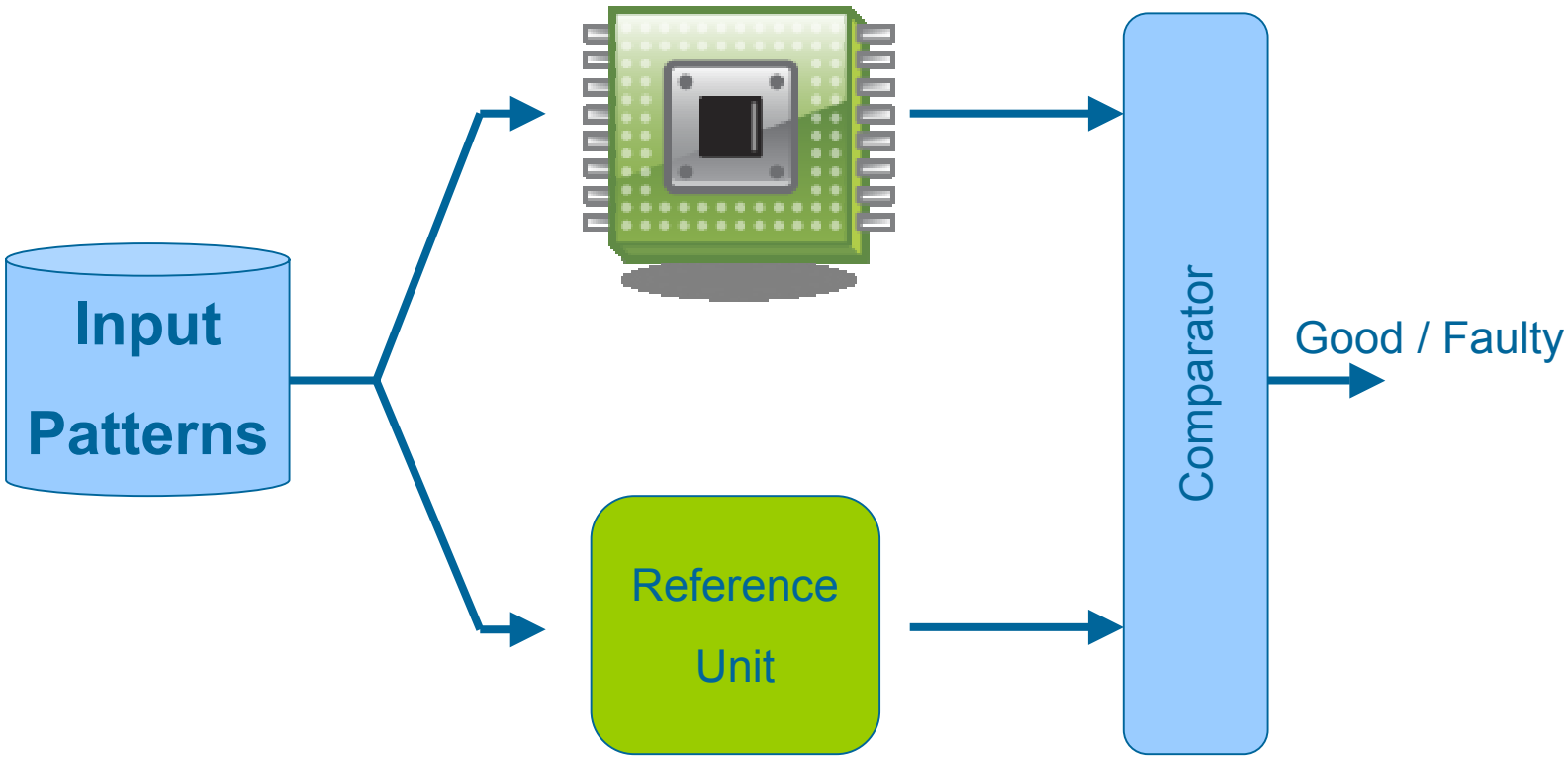


How to test? 1: Tester




V93000 SOC
VERIGY
V93000

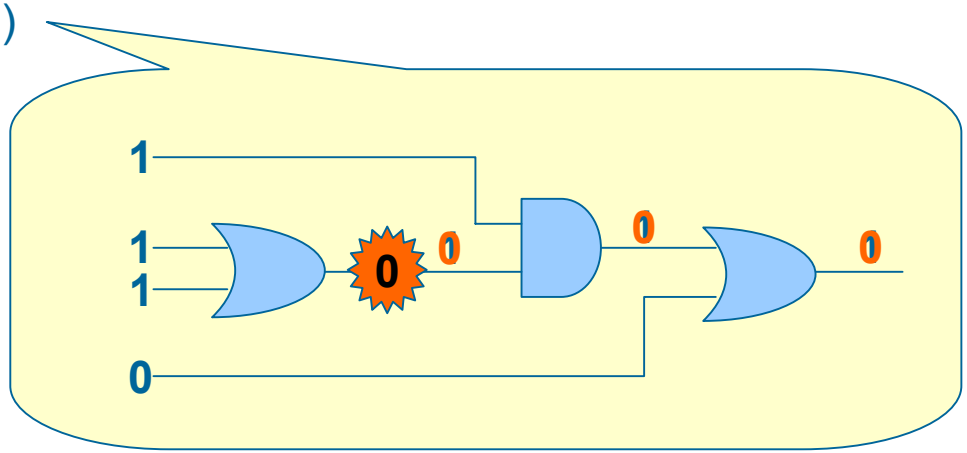
How to test? 2: Built In Self-Test



The increased densities of ICs makes it possible to include additional hardware to improve the test

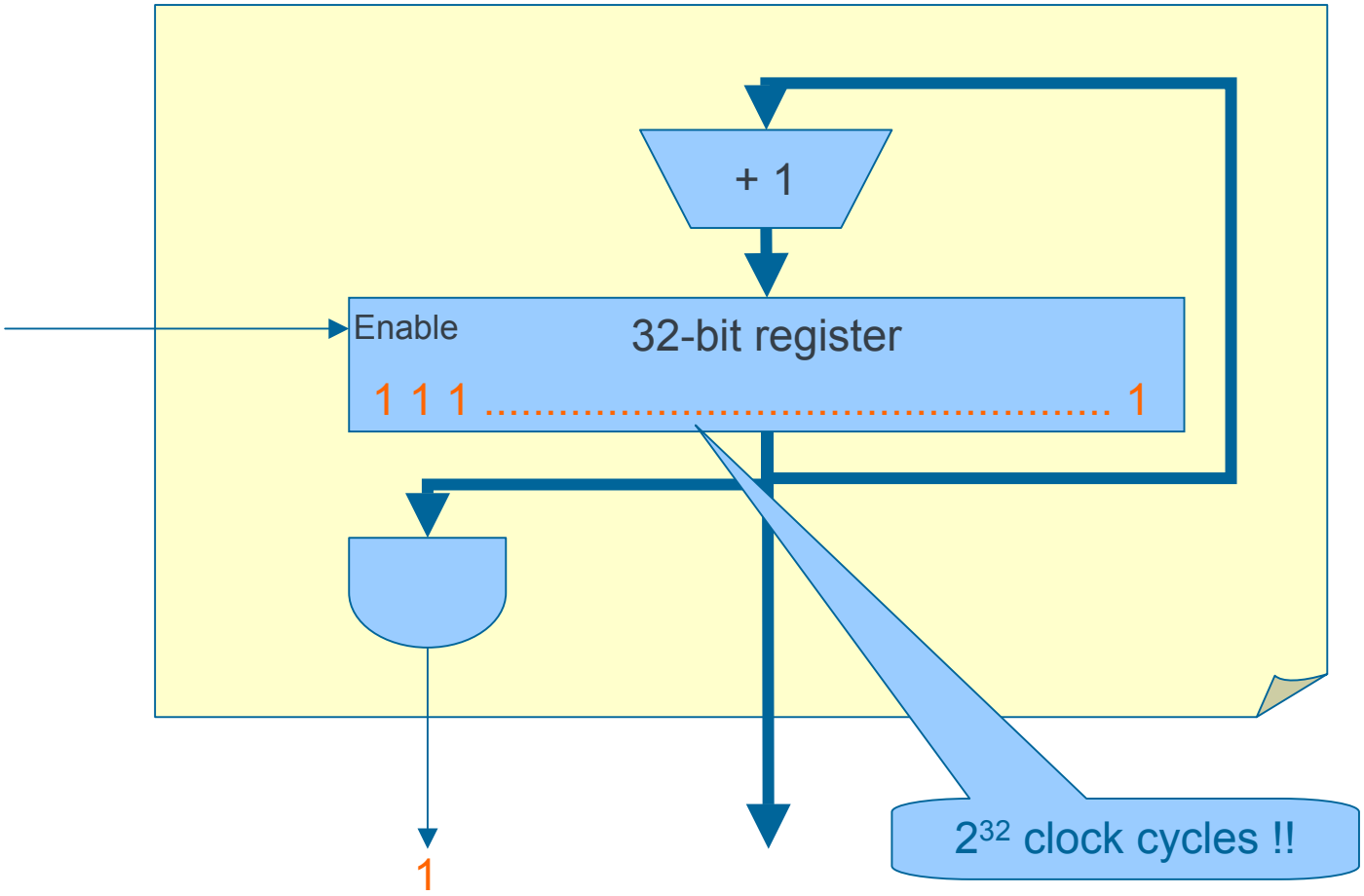
How to generate input patterns?

- Functional Test
- Structural Test
  - Netlist
  - Fault model (stuck-at, ...)
  - Generation:
    - Exhaustive
    - Deterministic (ATPG)
    - Pseudo-random



Sequential circuits

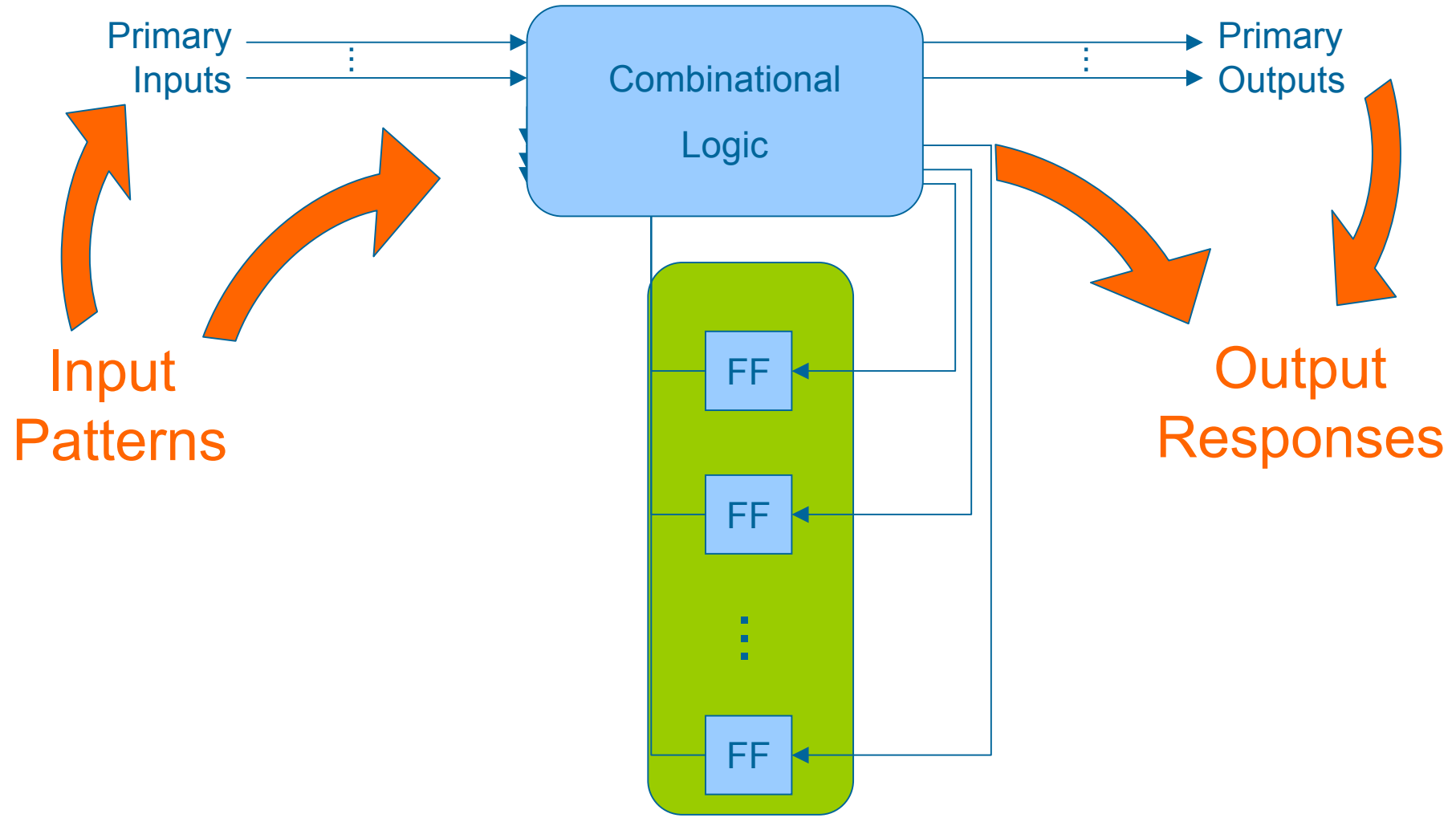
- Example: terminal counter in a 32-bit counter



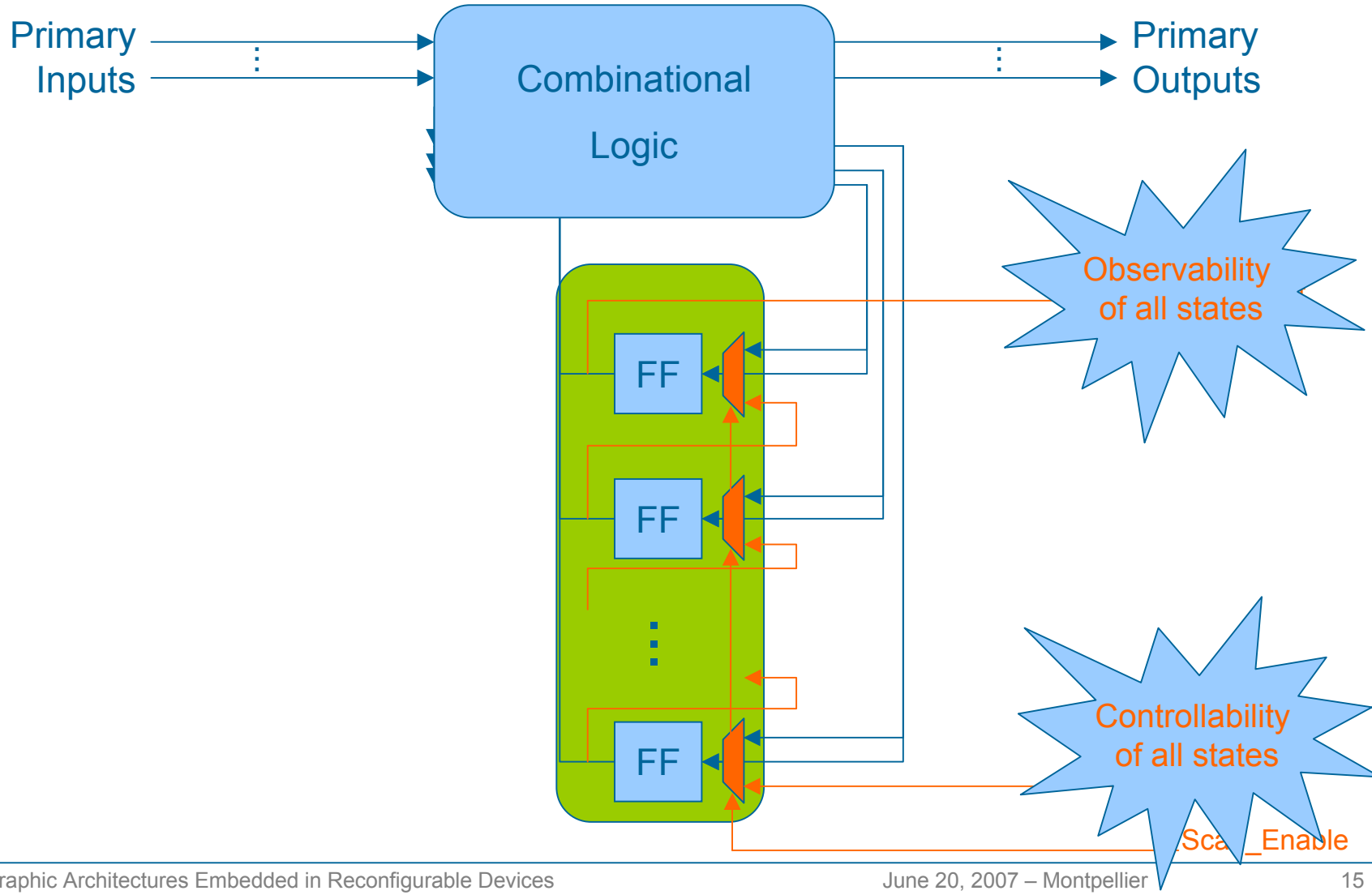
Design for Testability (DfT)

- Design techniques that add testability features to a device
- Goal: to increase controllability and observability
- Techniques:
  - Built-In Self-Test
  - Scan chains for sequential circuits
  - Insertion of controllability and observability points

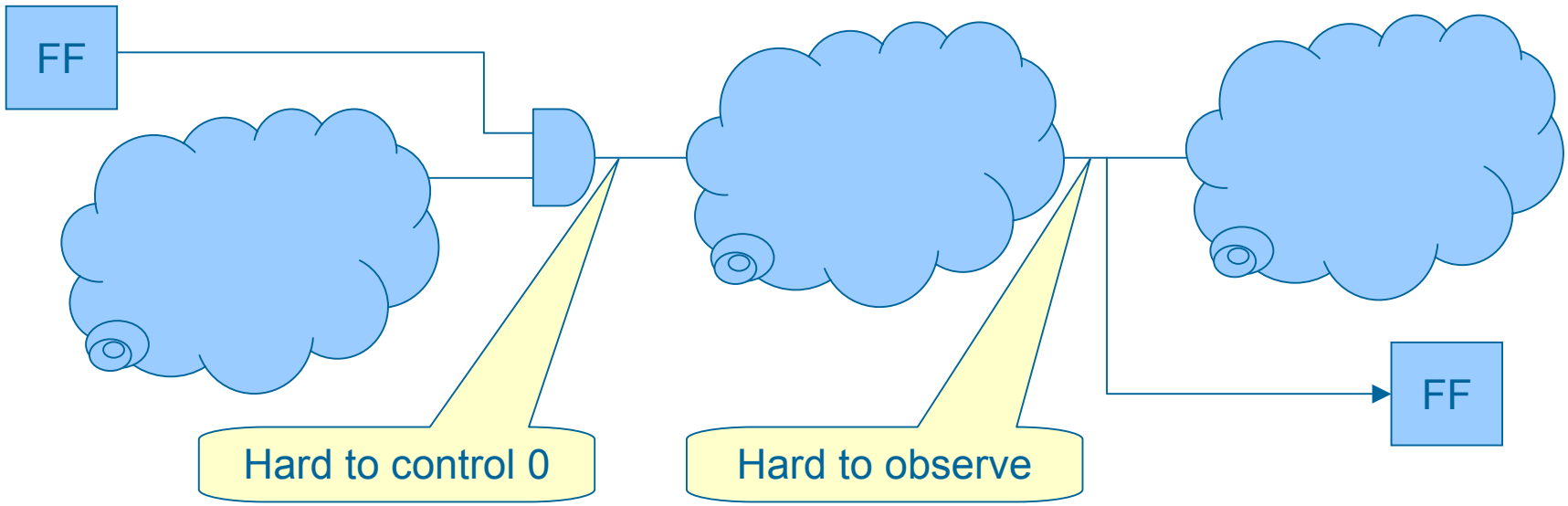
Scan-based Design



Scan-based Design (2)



Controllability and observability points



Outline

- Test
- **Security vs Test**
  - Scan-based attacks
  - Securing the scan chains
- AES BIST
- Conclusion

Secure chips

- Functions
  - Secure storage of confidential data
  - Cryptographic capacity (ciphering algorithms)
- Applications
  - Identification
  - Electronic signature
  - Access control for restricted areas or systems
  - Electronic purse…
- Fields
  - Communication
  - Banking
  - E-government
  - Pay-tv…
- Manufacturing
  - Integrated circuits
  - Must be tested
    - Because it's an integrated circuit
    - Primordial to insure high level of security

Security vs Test

- But ... Security fears testability !
  - Security reduces controllability and observability
  - Testability induces more controllability and observability
    - Create new attacks

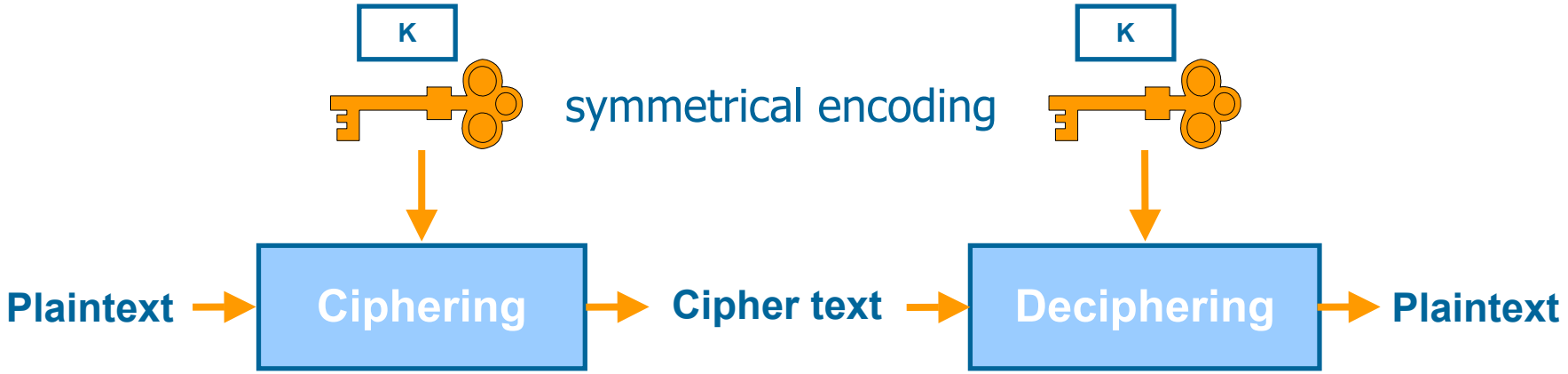
Security vs Test (2)

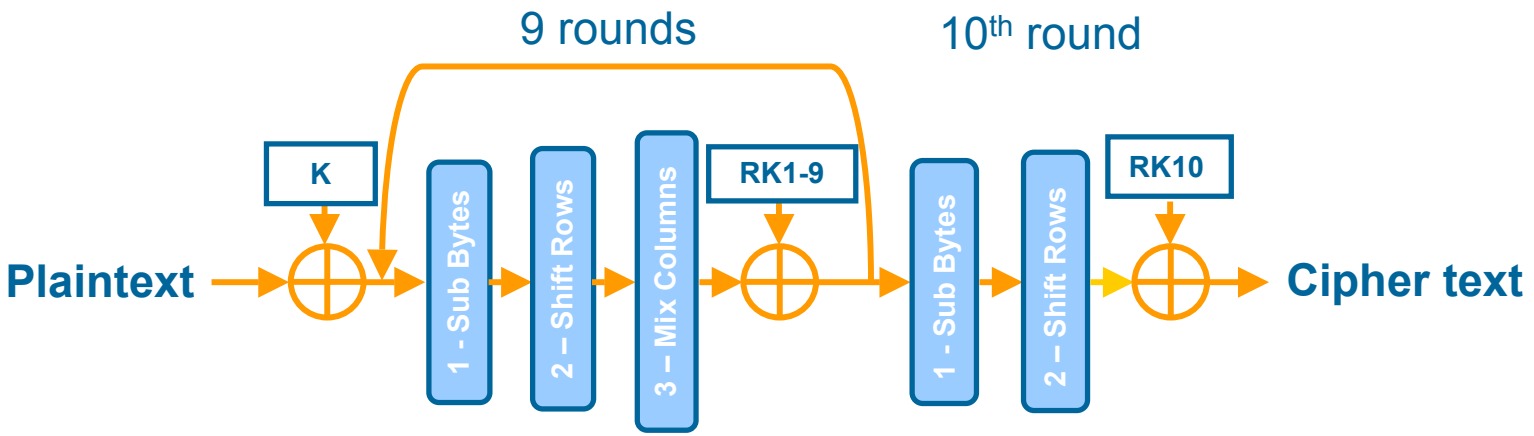
- Problem to solve
  - Choose an appropriate DfT strategy
  - Imagine the possible hazards induced by the DfT technique
  - Adapt the DfT technique to security constraints

Outline

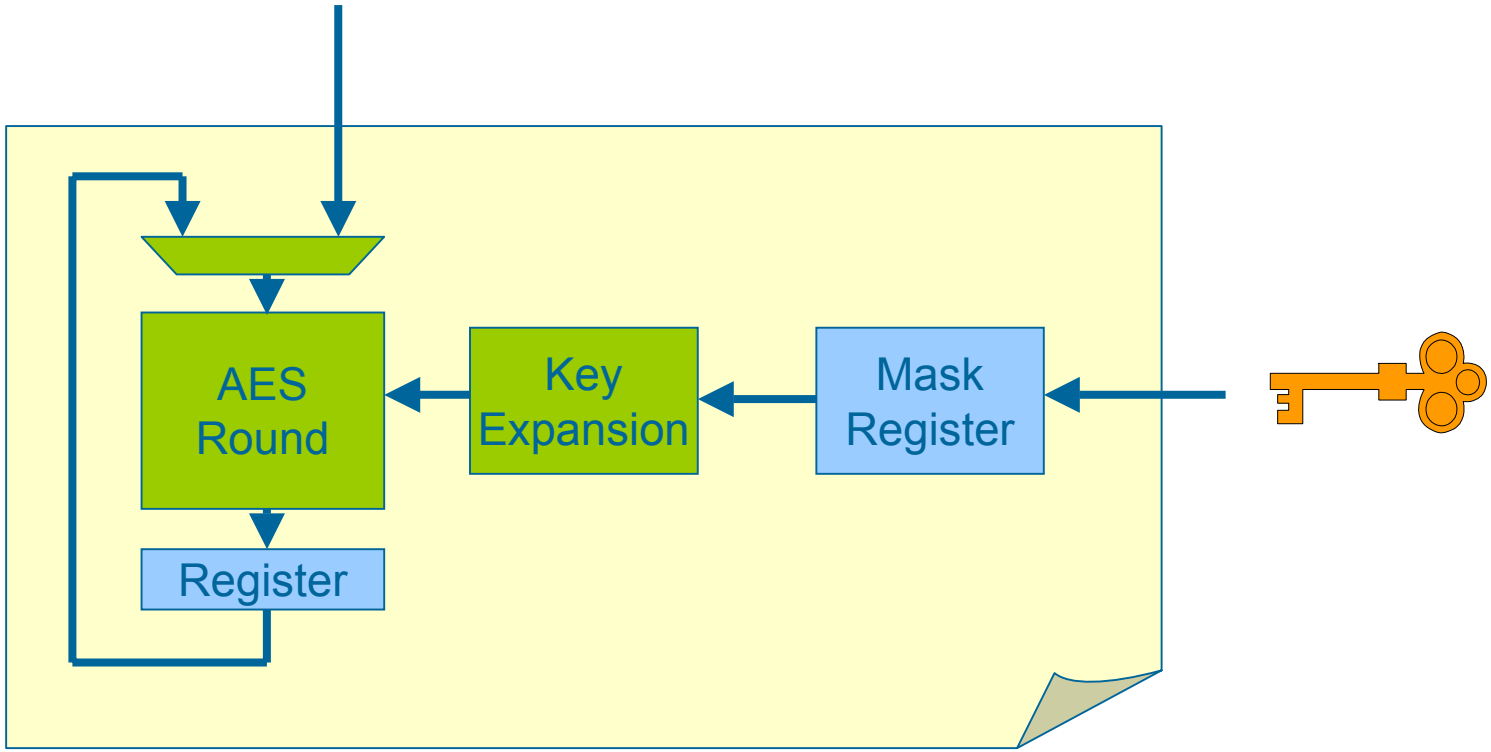
- Test
- Security vs Test
  - **Scan-based attacks**
  - Securing the scan chains
- AES BIST
- Conclusion

AES 128 bit ciphering

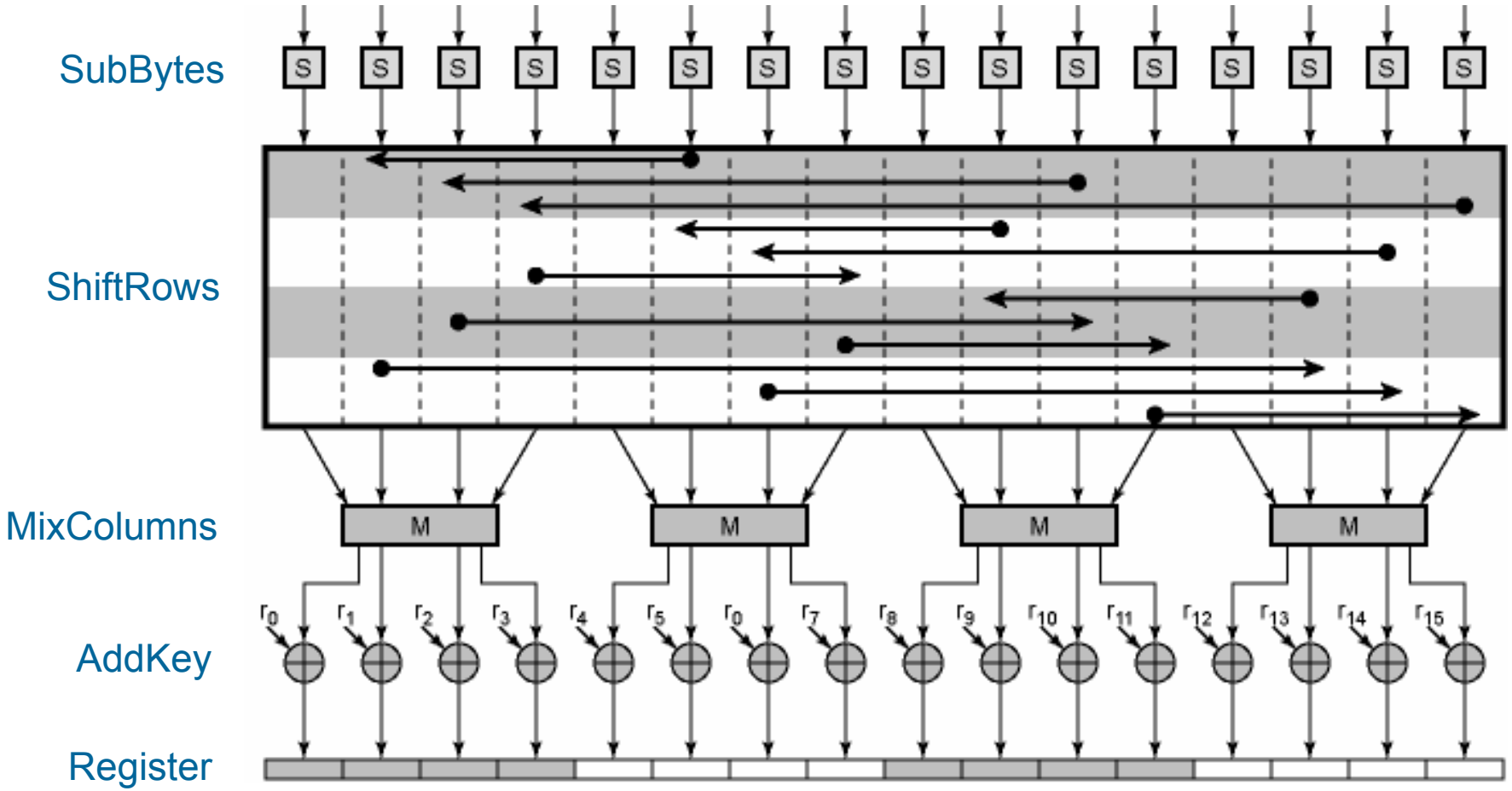




AES Architecture



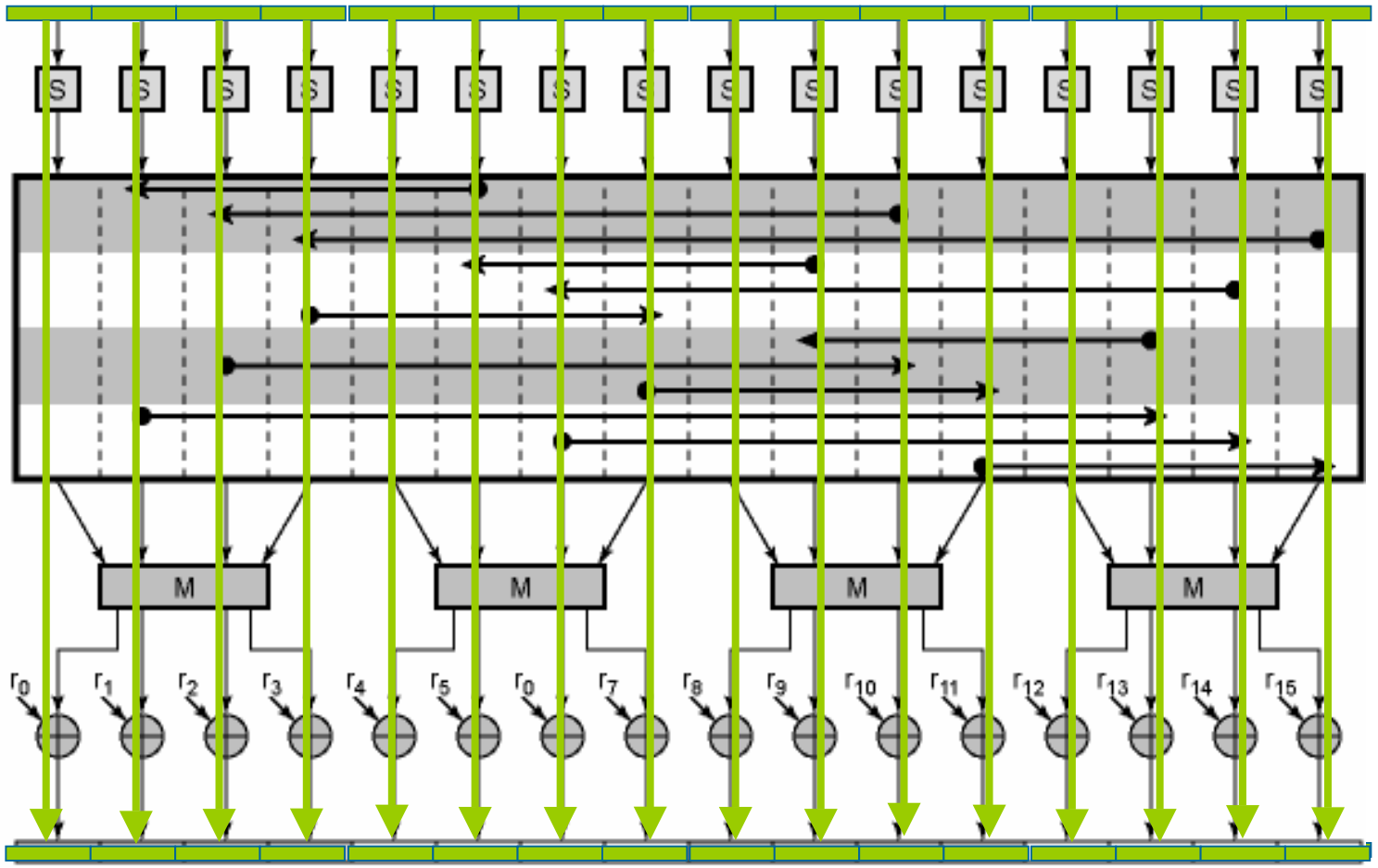
AES Round Architecture



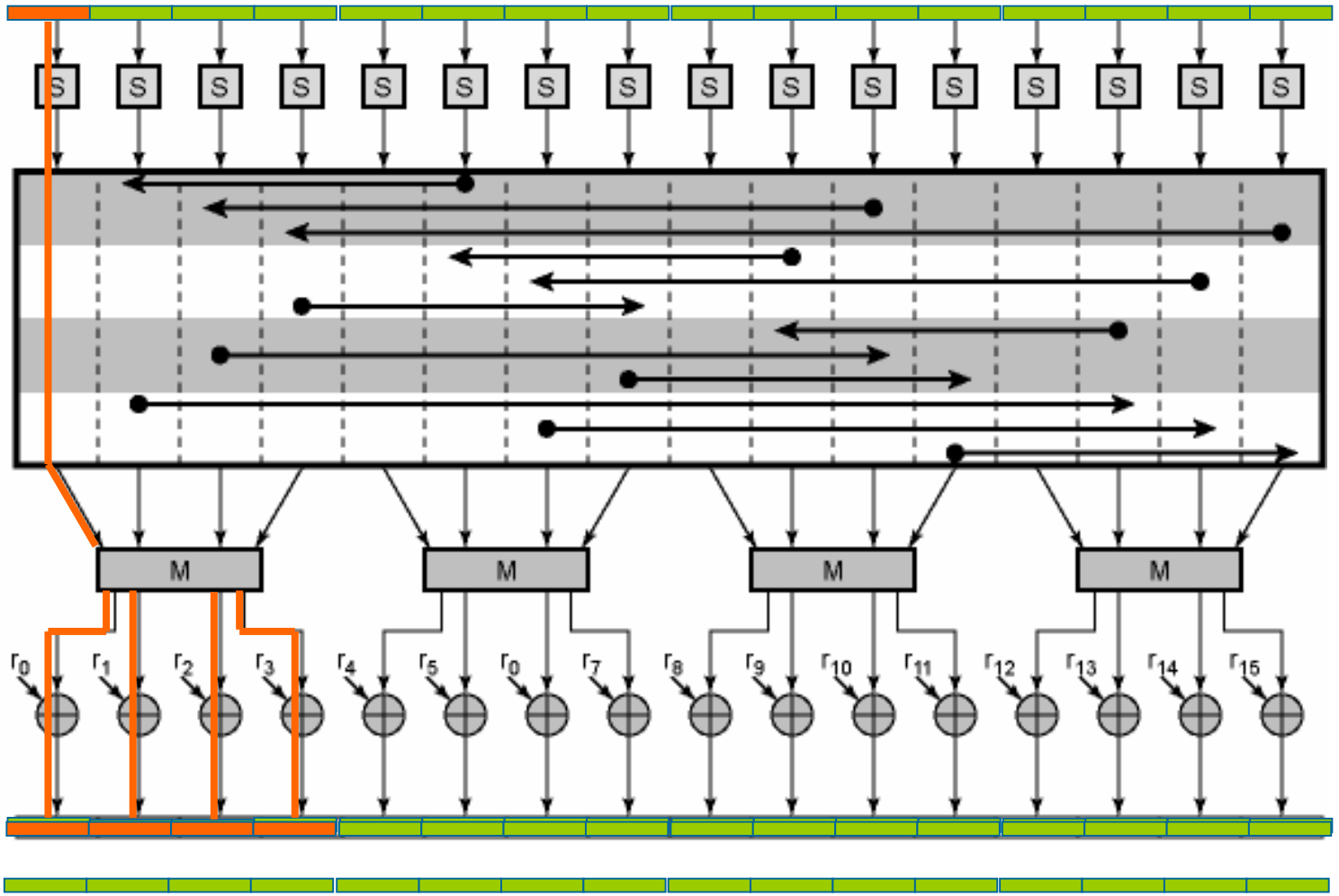
Scan based attack [Yang, DAC05]

- Goal
  - Retrieve the User key (K)
- Principle
  - Use the scan chain to observe the data processed by the circuit at various moments
- Method
  1. Retrieve the FFs storing the cipher text
  2. Read the FFs content after 1 encryption round
  3. Mathematically compute the key

1. Retrieve the FFs



1. Retrieve the FFs



Outline

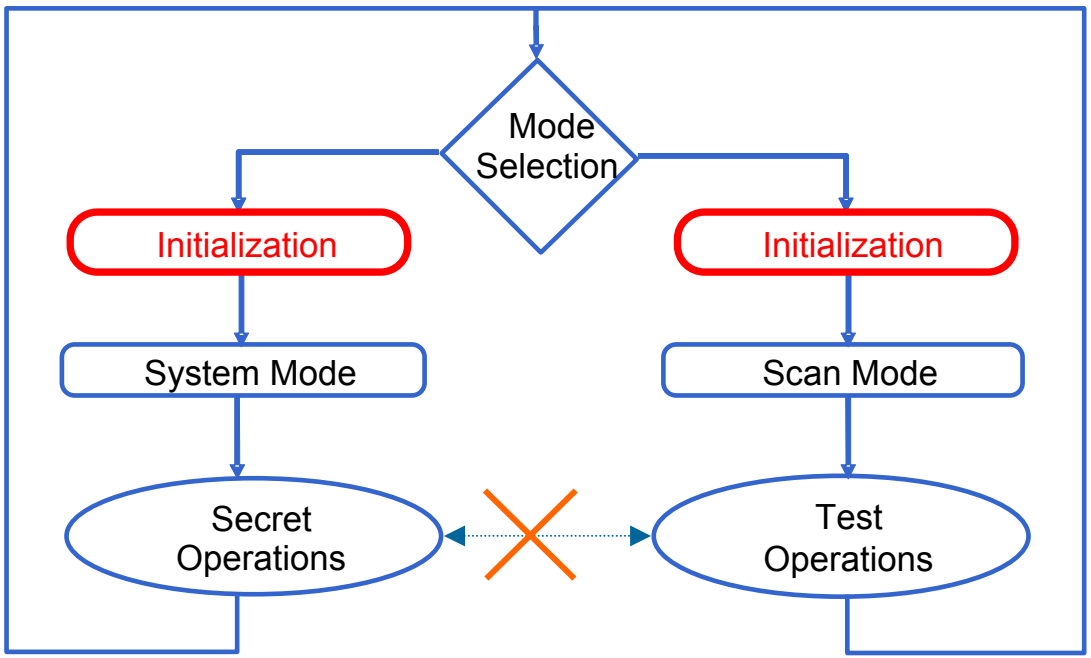
- Test
- Security vs Test
  - Scan-based attacks
  - **Securing the scan chains**
- AES BIST
- Conclusion

Securing the scan chain

- Goal
  - No observation nor control of the functional data processed by the secure system during mission time
- Principle
  - Prevent illegal scan shift operations
- Solutions
  - Test mode protection
    - Scan protocol
    - Test Patterns watermarking
  - System mode protection
    - Scan chain scrambling
    - Scan enable tree protection
    - Spy FFs

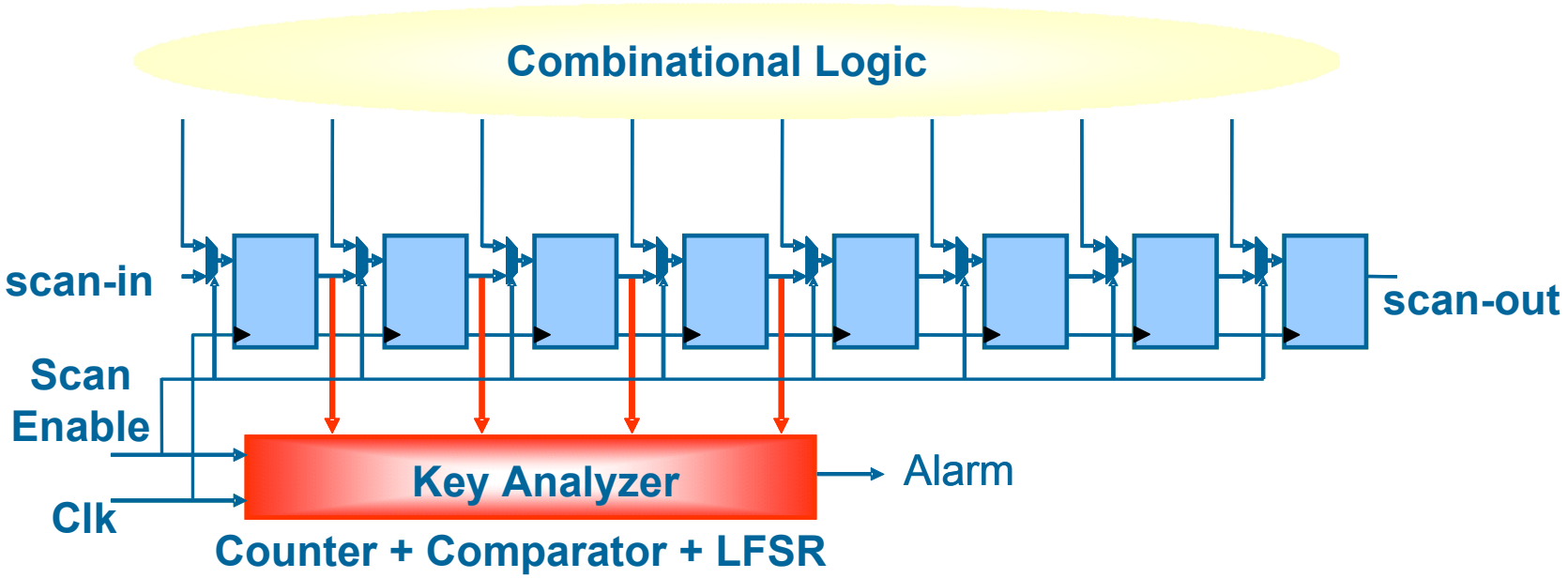
Test mode protection

- Scan protocol
  - The circuit is initialized (reset) before and after test mode
  - Initialization is checked before switching to another mode
  - Switch between the 2 modes, bypassing the initialization, is detected



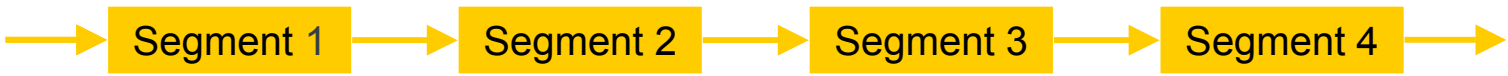
Test mode protection

- Test pattern watermarking
  - Test patterns embed authentication keys
  - Keys are dynamically changed (LFSR-based)

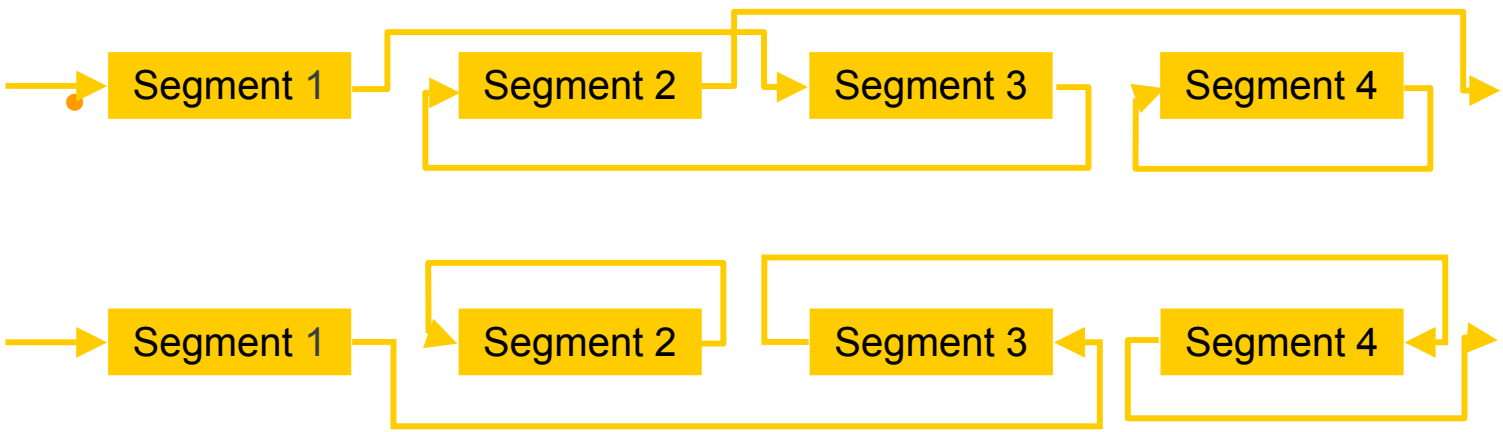


System mode protection

- Scrambling method
  - Scan path with a prefixed segment organization during test mode

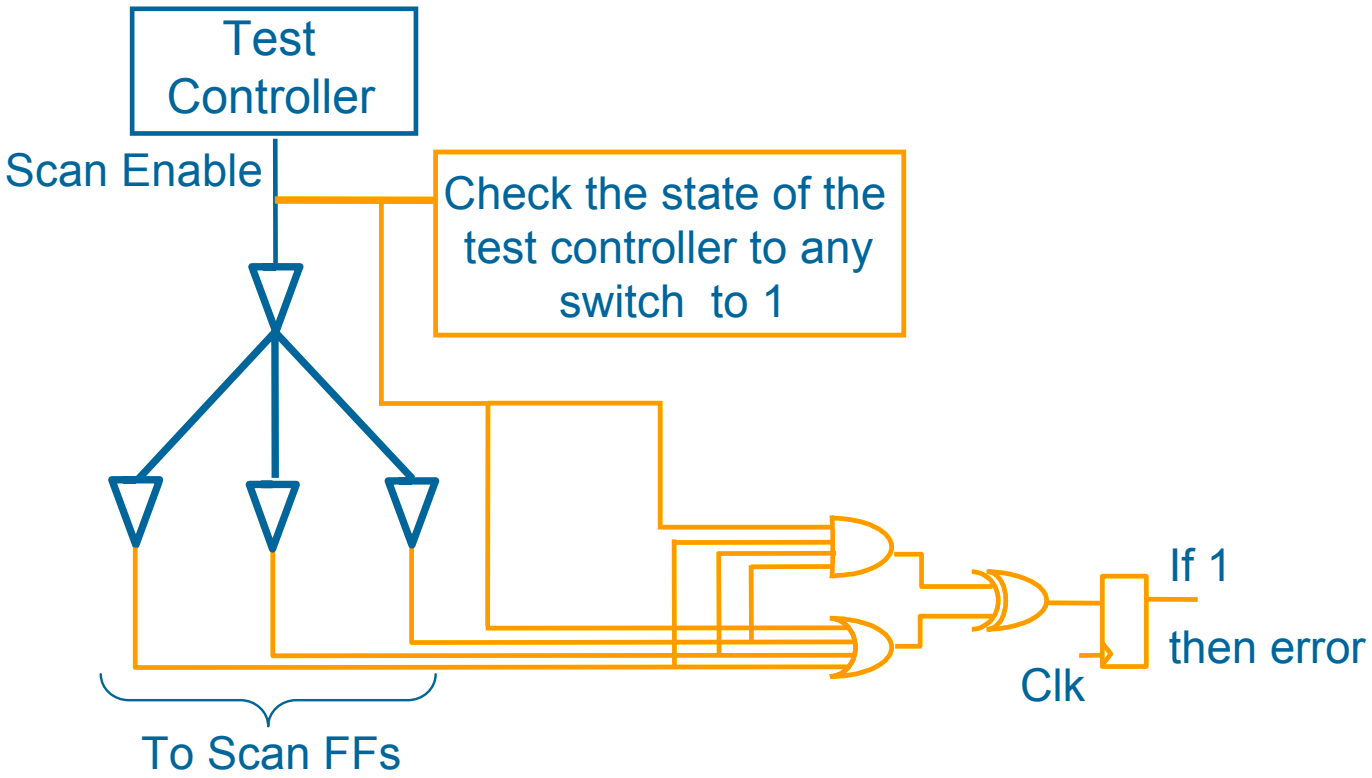


  - Scan path with random segment organization if shift during system mode
    - Time T1



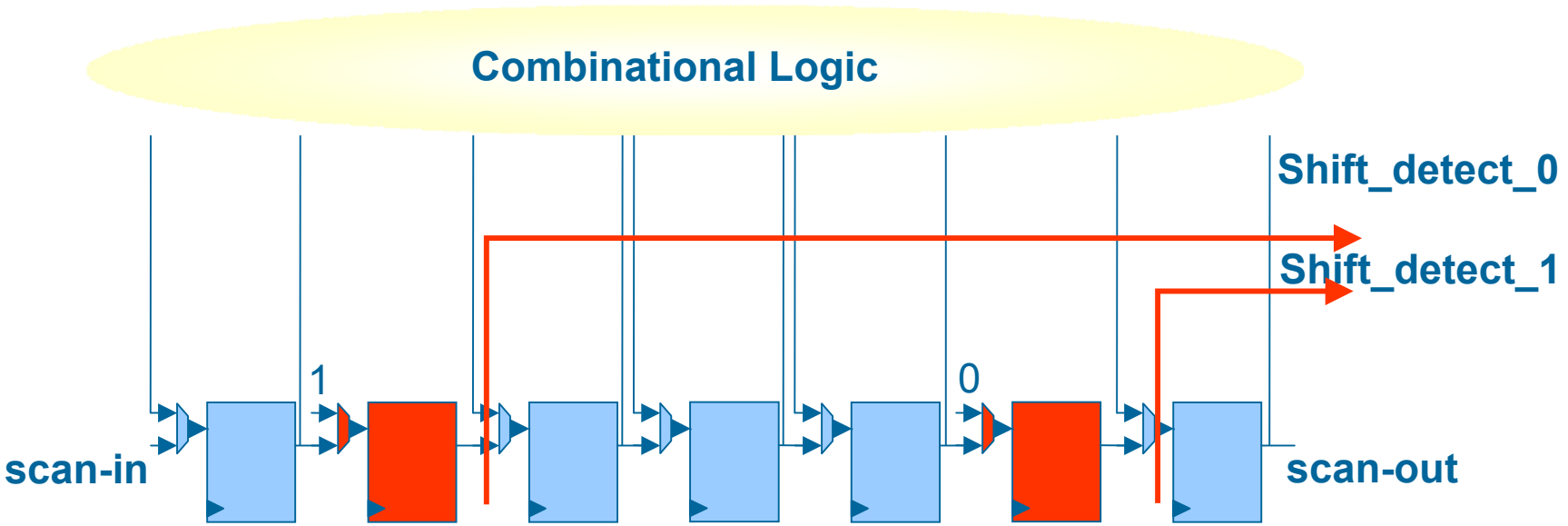
System mode protection

- Scan-Enable Tree Protection
  - Compare the scan enable signals at different locations



System mode protection

- Spy Flip-Flops
  - Include Spy cells in the scan chain
  - Control the spy cells to a constant value
  - Observe the spy cells states



Experimental results

- Design used for comparison
  - DES (198 FFs)
  - 1 buffer on the scan-enable tree leaf drives up to 6 FFs
- Scrambling : 6 segments
- Scan-enable observation : 8 branches
- Spy cells : 6 additional FFs
- Pattern watermarking : 4-bit keys

Experimental results

		Scrambling	Scan enable	Spy cell	Pattern watermarking
Insertion flow		RTL	RTL + place&route	RTL	RTL
Test	Test time	0%	1%	5%	0.4%
Design	Area	0.2%	0.3%	1.8%	~0%
	power c.	7%	0%	0%	0%
Security		+++	++	++	+

Outline

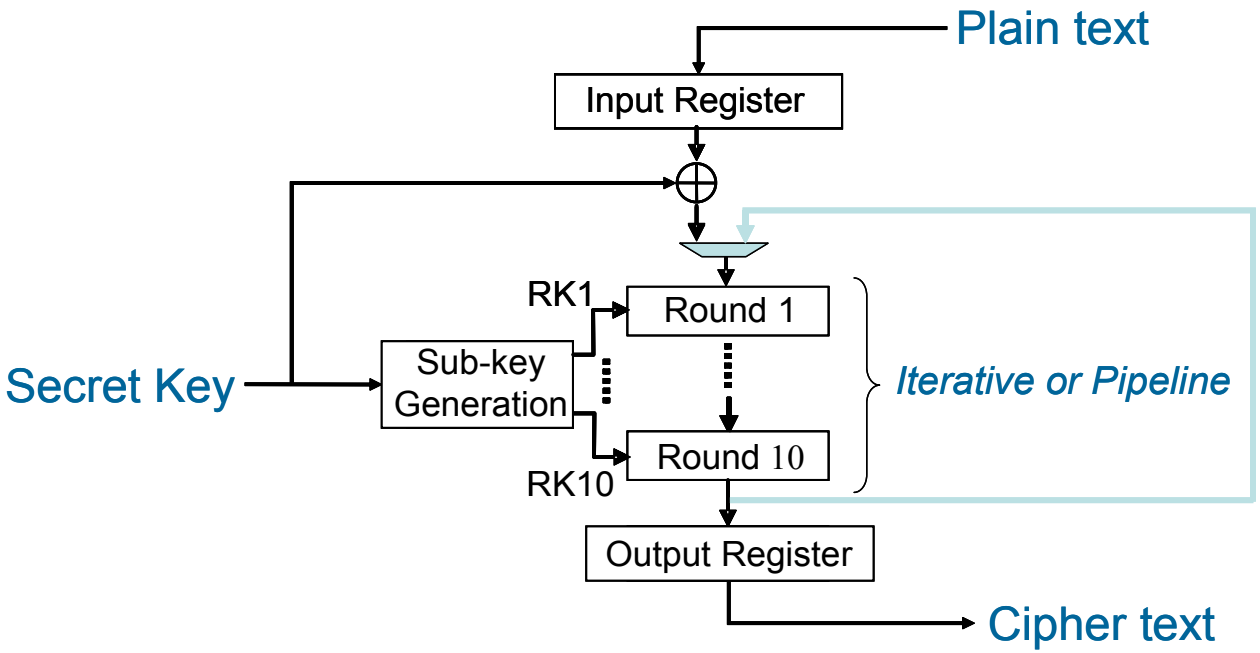
- Test
- Security vs Test
  - Scan-based attacks
  - Securing the scan chains
- **AES BIST**
- Conclusion

Test Solutions for Secure Chips

- Scan path
  - High fault coverage
  - Automatic generation of scan chains
  - Simplified test sequence generation
  - *Full control / observation of internal states !*

- BIST
  - Reduced ATE cost
  - In-situ testing
  - Test at nominal speed
  - Limited control / observation of internal states
  - *FC% & Cost ?*

AES Self-test



- Crypto operation: FC=100% with 1750 patterns

Outline

- Test
- Security vs Test
  - Scan-based attacks
  - Securing the scan chains
- AES BIST
- **Conclusion**

Conclusion

- Security requires new approaches for scan designs
- Countermeasures must address two kinds of attack
  - Legal activation of the test circuitry
    - corruption of the authentication scheme
    - malfunction of the security
    - insider attack
  - Physical access to the chip
    - high knowledge of the circuit
    - very expensive equipment
- The secure scan solutions must be chosen according to the required level of security and the impact on the design