Scan Chain Encryption for the Test, Diagnosis and Debug of Secure Circuits

Mathieu da Silva, Giorgio Di Natale, Marie-Lise Flottes, Bruno Rouzeyre

▶ **To cite this version:**

Mathieu da Silva, Giorgio Di Natale, Marie-Lise Flottes, Bruno Rouzeyre. Scan Chain Encryption for the Test, Diagnosis and Debug of Secure Circuits. SETS: South European Test Seminar, Mar 2017, Alpe d'Huez, France. , 2017. lirmm-01892667

HAL Id: lirmm-01892667

https://hal-lirmm.ccsd.cnrs.fr/lirmm-01892667

Submitted on 10 Oct 2018

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Scan Chain Encryption for the Test, Diagnosis and Debug of Secure Circuits

Mathieu Da Silva

PhD Student at LIRMM in Montpellier, France

Thesis advisors:

Giorgio Di Natale

Marie-Lise Flottes

Bruno Rouzeyre

Summary

1) Scan attacks presentation

2) Overview of Scan chain encryption

3) Experimentations on Scan chain encryption

4) Conclusion

Summary

1) **Scan attacks presentation**

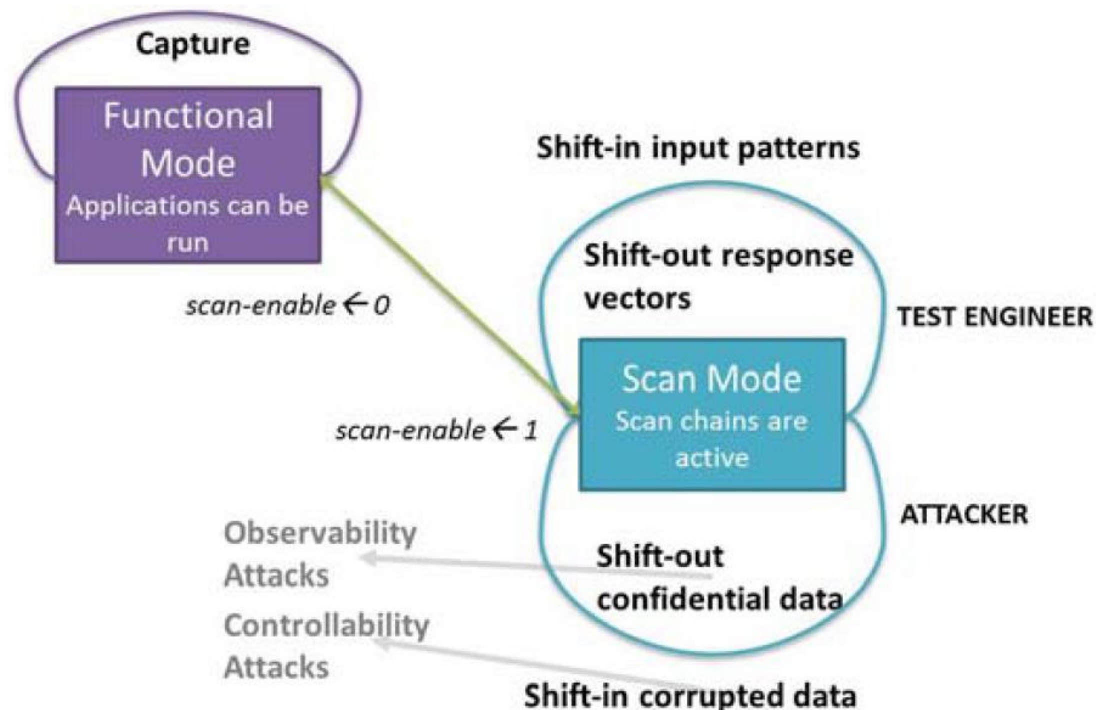
2) Overview of Scan chain encryption

3) Experimentations on Scan chain encryption

4) Conclusion

SCAN ATTACKS PRESENTATION

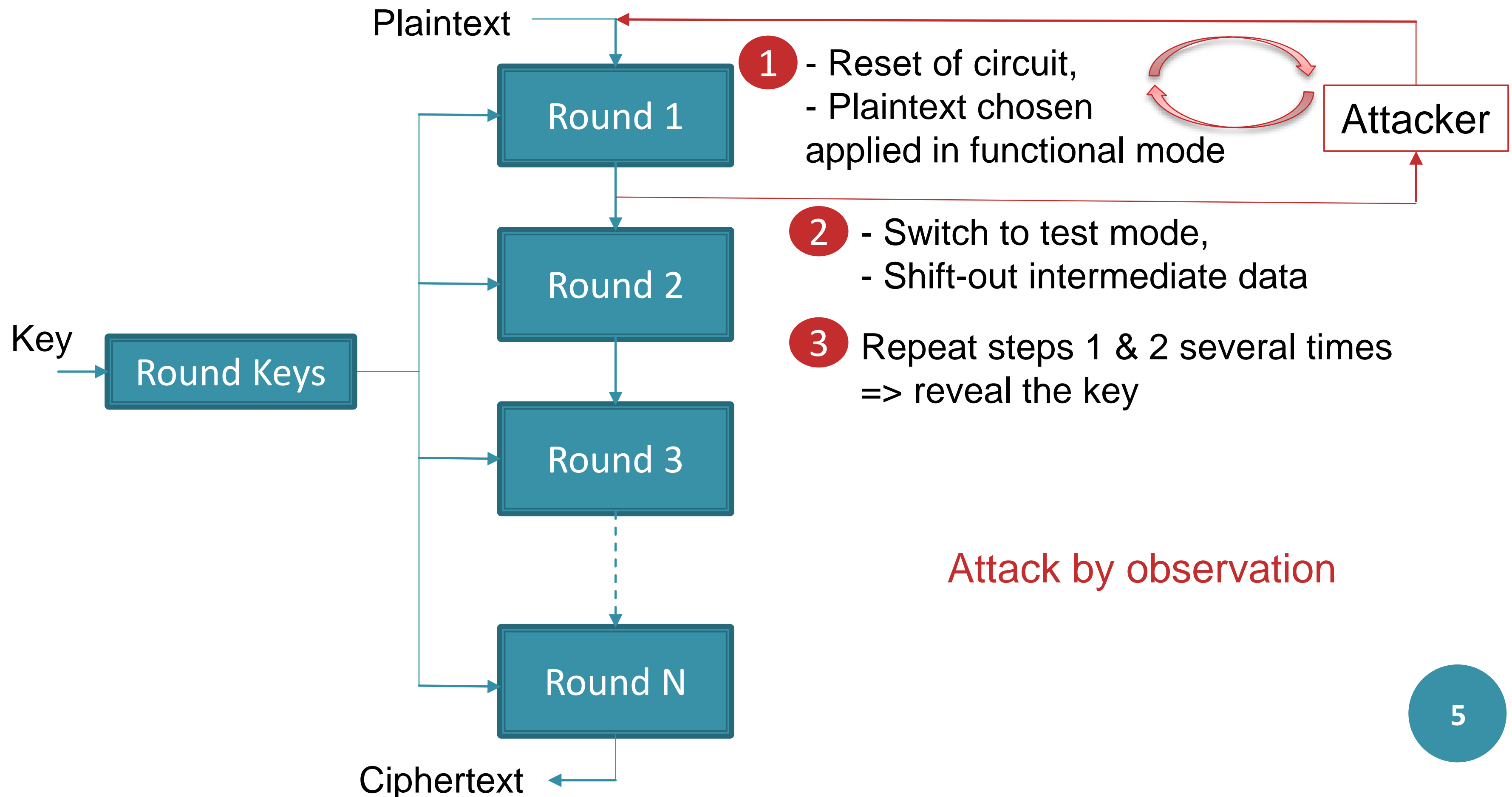
- Scan attacks:
  - Use of observability and controllability offered by scan chains
  - Principle: switch between functional and scan modes
  - Goal: Retrieve embedded secret data



Da Rolt et al., Test Versus Security: Past and Present, IEEE Trans. Emerging Topics Computing 2014

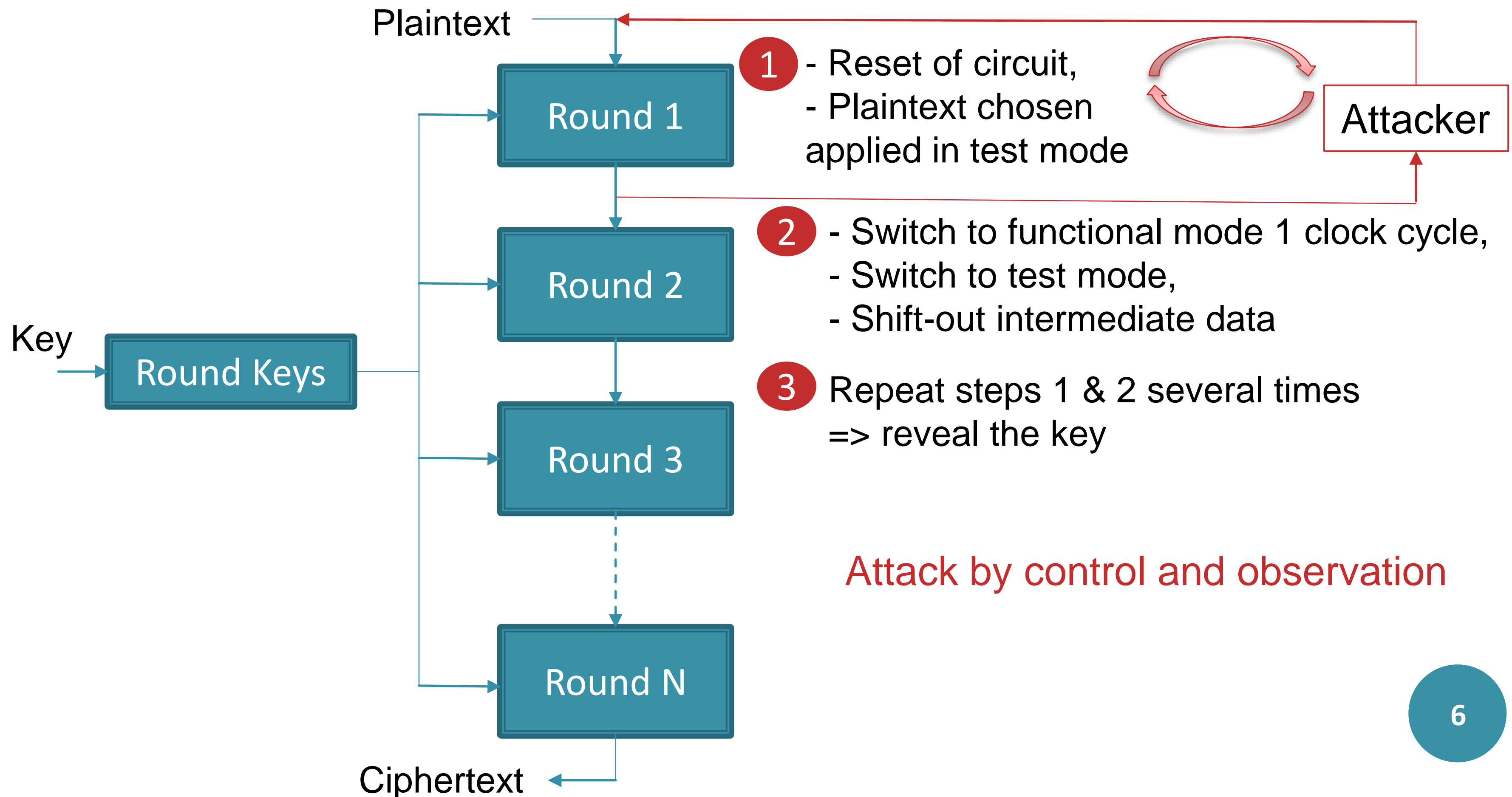
SCAN ATTACKS PRESENTATION

- Scan attacks on crypto-processors:
  - Principle of the attack on Symmetric-Key Cryptography:



SCAN ATTACKS PRESENTATION

- Scan attacks on crypto-processors:
  - Principle of the attack on Symmetric-Key Cryptography:



SCAN ATTACKS PRESENTATION

- Scan attacks on crypto-processors:
  - In literature:
    - On DES [1], AES [2][3][4] (Symmetric-Key Cryptography)
    - On RSA, ECC [5] (Public-Key Cryptography)
    - Also on stream cipher: scan attacks on LFSR [6]

[1] B. Yang, K. Wu and R. Karri, "Scan Based Side Channel Attack on Dedicated Hardware Implementations of Data Encryption Standard," Proceedings ITC International Test Conference, pp. 339-344, 2004.

[2] B. Yang, K. Wu and R. Karri, "Secure Scan: A Design-for-Test Architecture for Crypto Chips," IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, vol. 25, pp. 2287-2293, 2006.

[3] J. Da Rolt, G. Di Natale, M.-L. Flottes and B. Rouzeyre, "New Security Threats Against Chips Containing Scan Chain Structures," IEEE International Symposium on Hardware-Oriented Security and Trust (HOST), 2011.

[4] S. S. Ali, O. Sinanoglu, S. M. Saeed and R. Karri, "New scan-based attack using only the test mode," IFIP/IEEE 21st International Conference on Very Large Scale Integration (VLSI-SoC), pp. 234-239, 2013.

[5] J. Da Rolt, B. Rouzeyre, M.-L. Flottes, G. Di Natale, A. Das and I. Verbauwhede, "A scan-based attack on Elliptic Curve Cryptosystems in presence of industrial Design-for-Testability structures," IEEE International Symposium on Defect and Fault Tolerance in VLSI and Nanotechnology Systems (DFT), pp. 43-48, 2012.

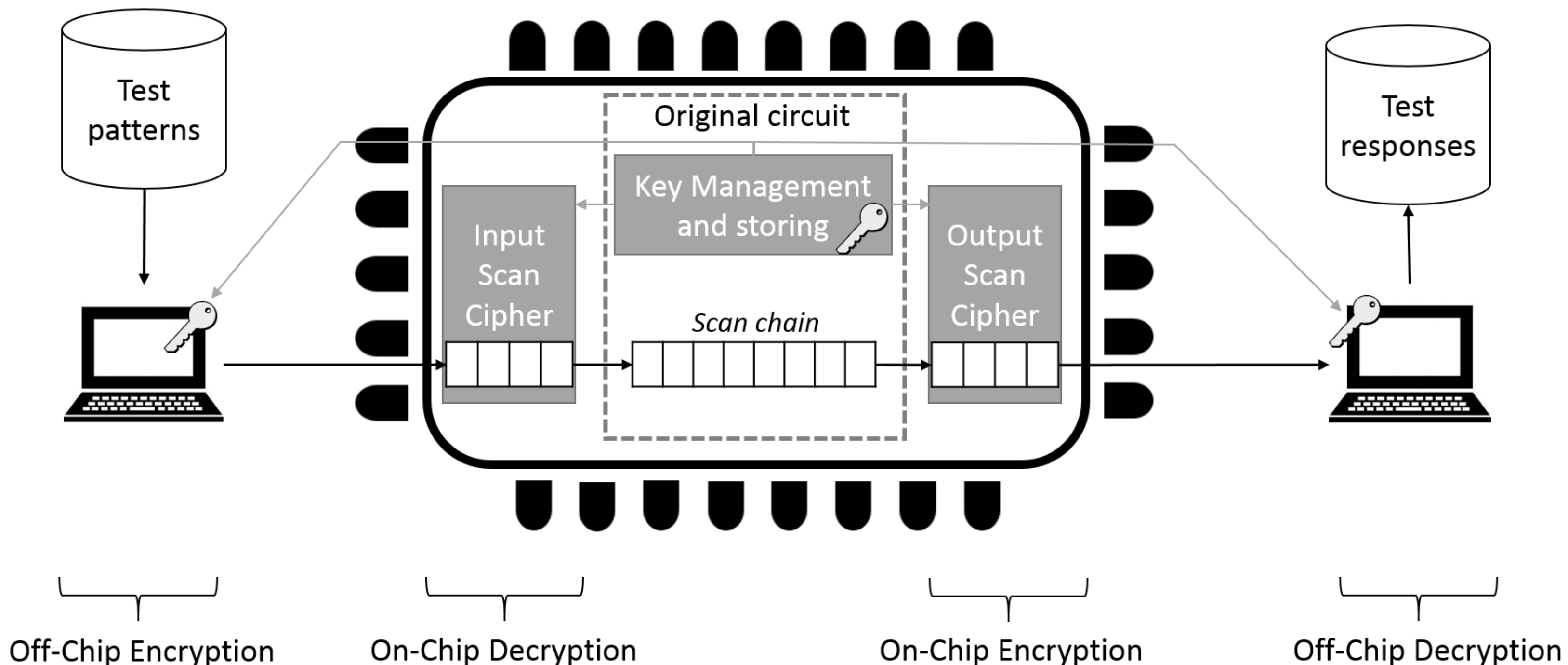
[6] Y. Liu, K. Wu and R. Karri, "Scan-based Attacks on Linear Feedback Shift Register Based Stream Ciphers," ACM Transactions on Design Automation of Electronic Systems (TODAES), vol. 16, 2011.

Summary

1) Scan attacks presentation
2) **Overview of Scan chain encryption**
3) Experimentations on Scan chain encryption
4) Conclusion

OVERVIEW OF SCAN CHAIN ENCRYPTION

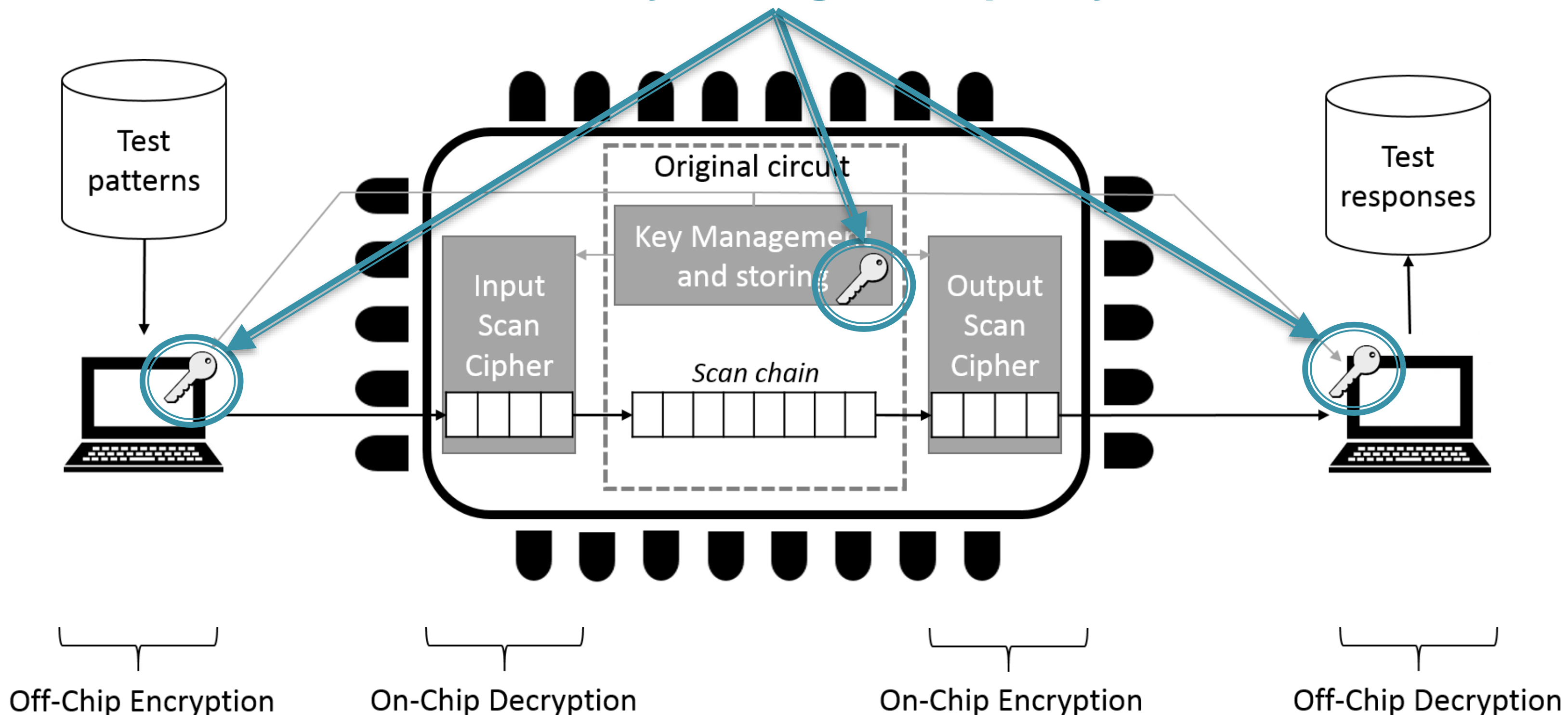
- A new secure scan design on crypto-processor
- Presentation
  - Principle: use the secret key already stored in the circuit under test in order to encrypt test pattern by adding extra scan ciphers



Overview of Scan chain encryption

- A new secure scan design on crypto-processor
- Presentation

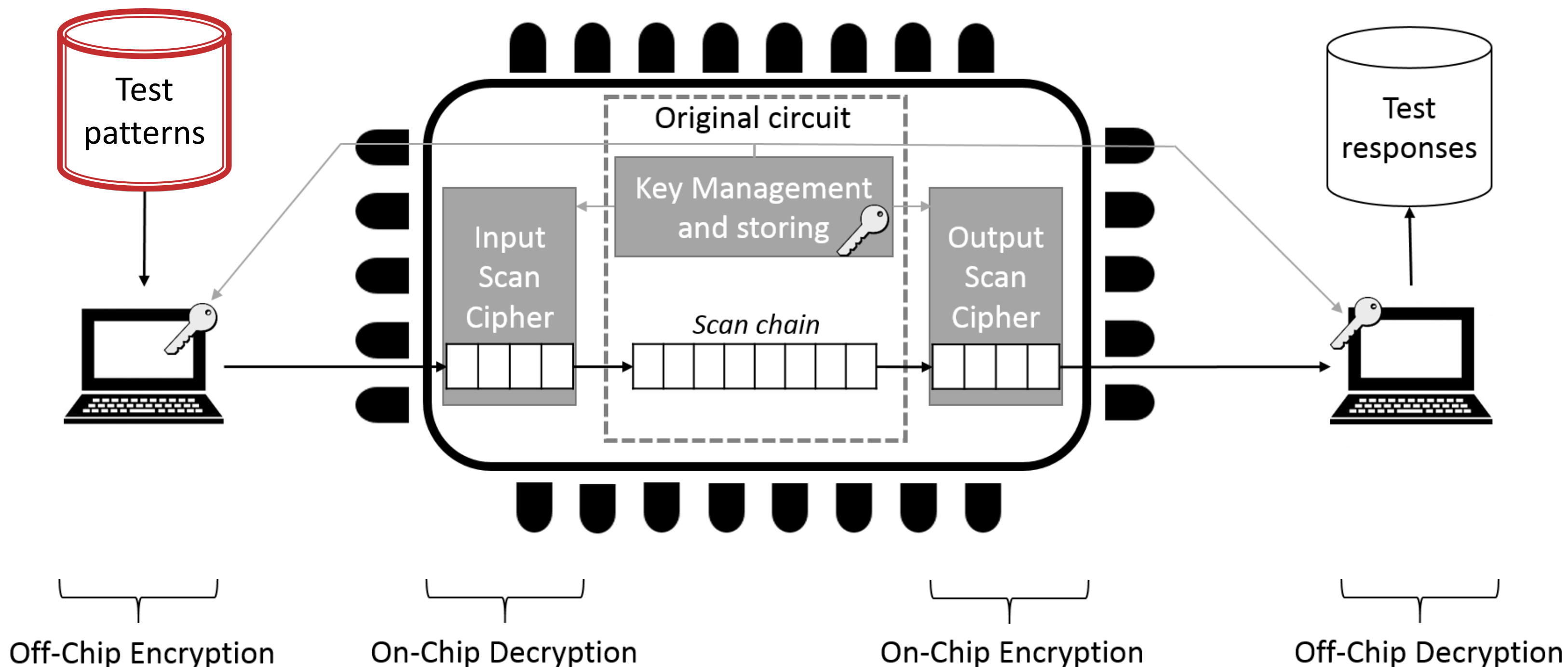
Reuse of key already present in original circuit (crypto-core)
=> no additional key management policy



Overview of Scan chain encryption

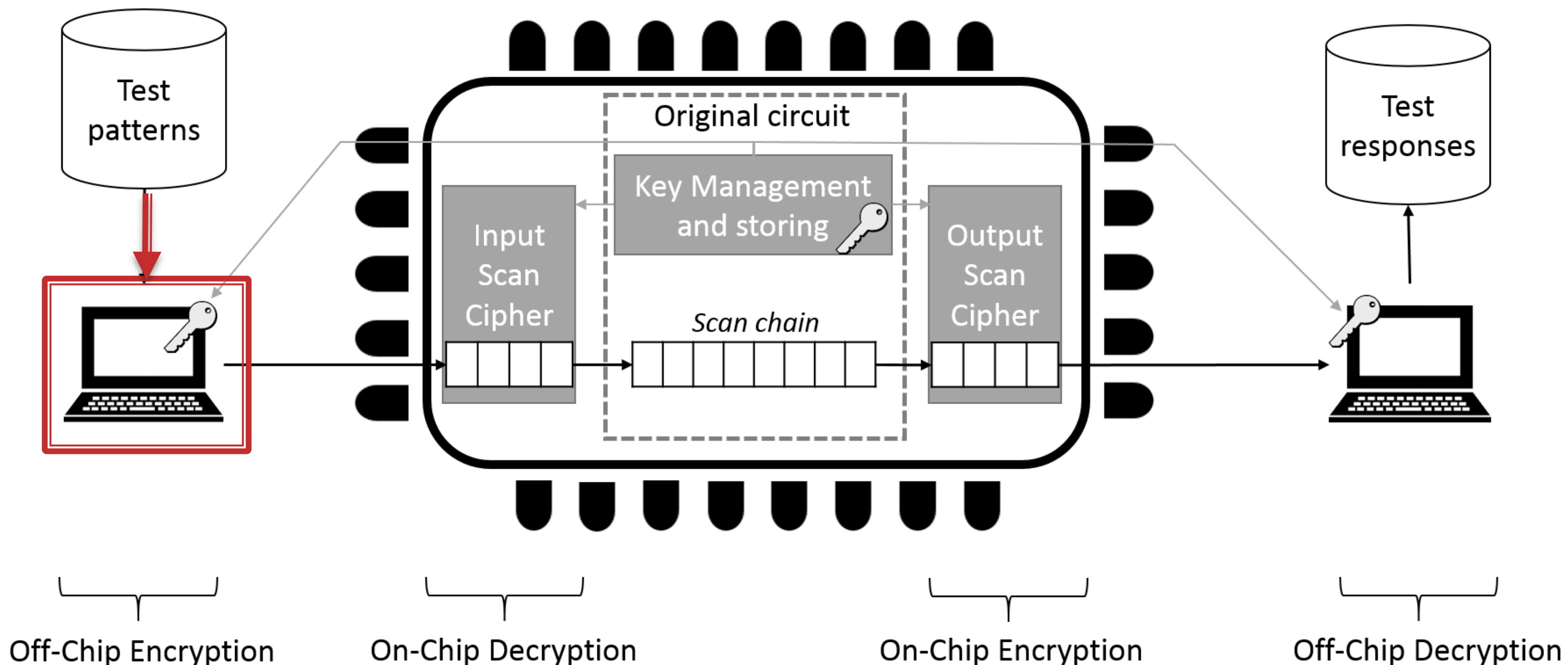
- A new secure scan design on crypto-processor
- Presentation
  - Proposed test procedure:

    1) Generating test patterns for the original circuit and collecting expected test responses



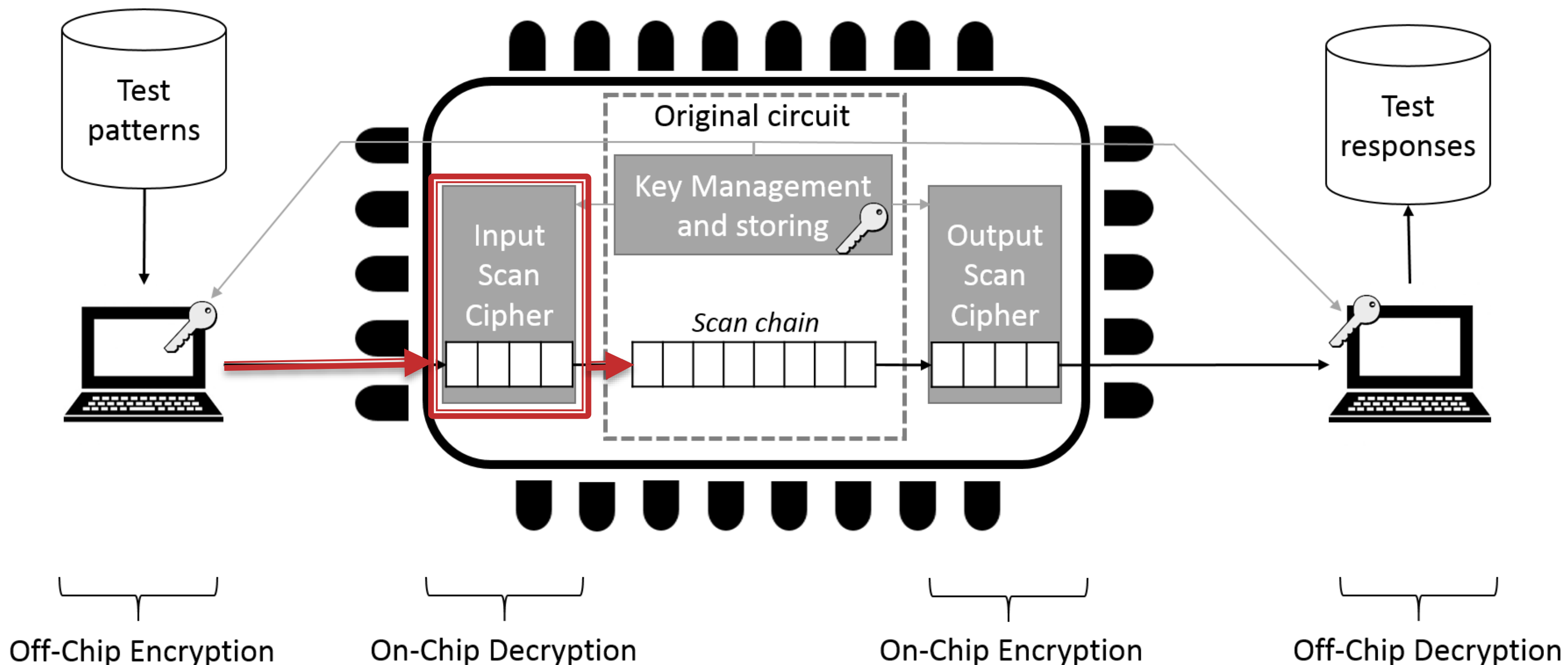
Overview of Scan chain encryption

- A new secure scan design on crypto-processor
- Presentation
  - Proposed test procedure:
    2) Off-chip encrypting test patterns



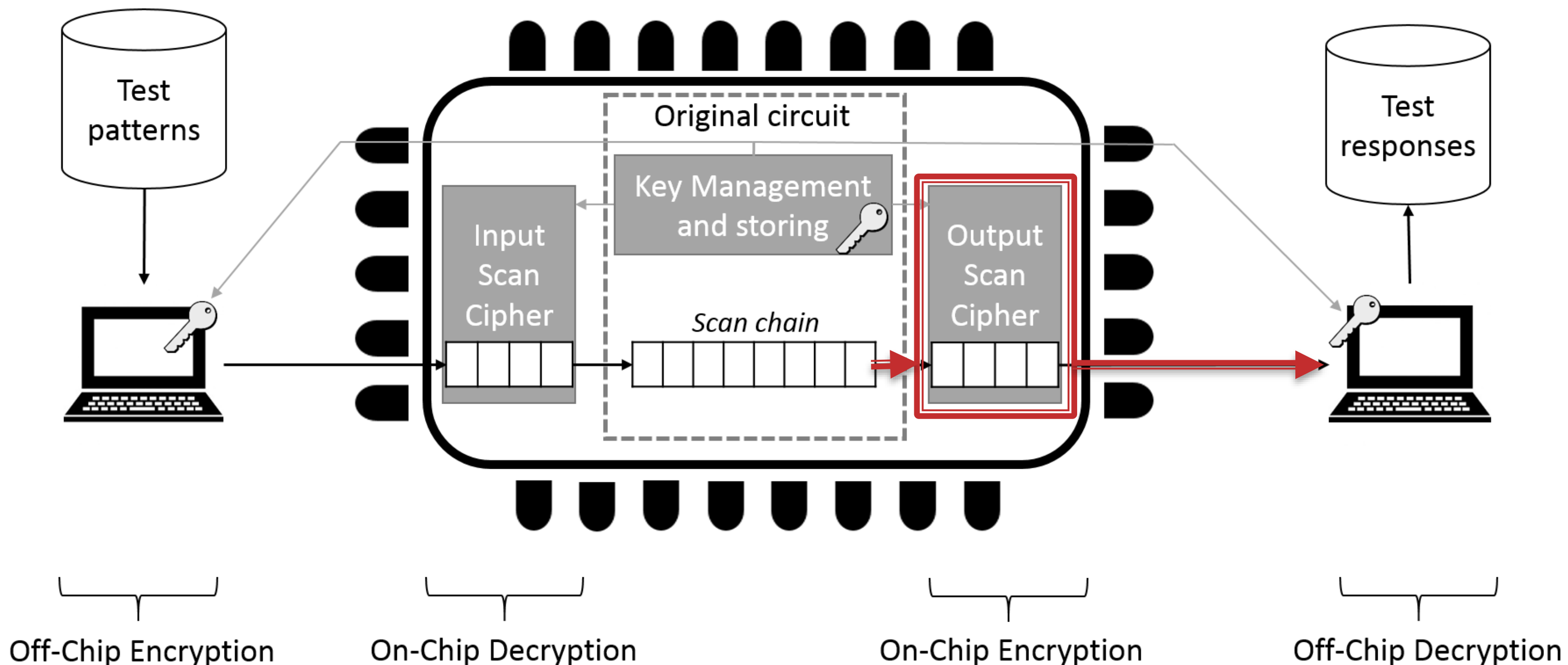
Overview of Scan chain encryption

- A new secure scan design on crypto-processor
- Presentation
  - Proposed test procedure:
    - 3) Test patterns decrypted and shifted in scan chain



OVERVIEW OF SCAN CHAIN ENCRYPTION

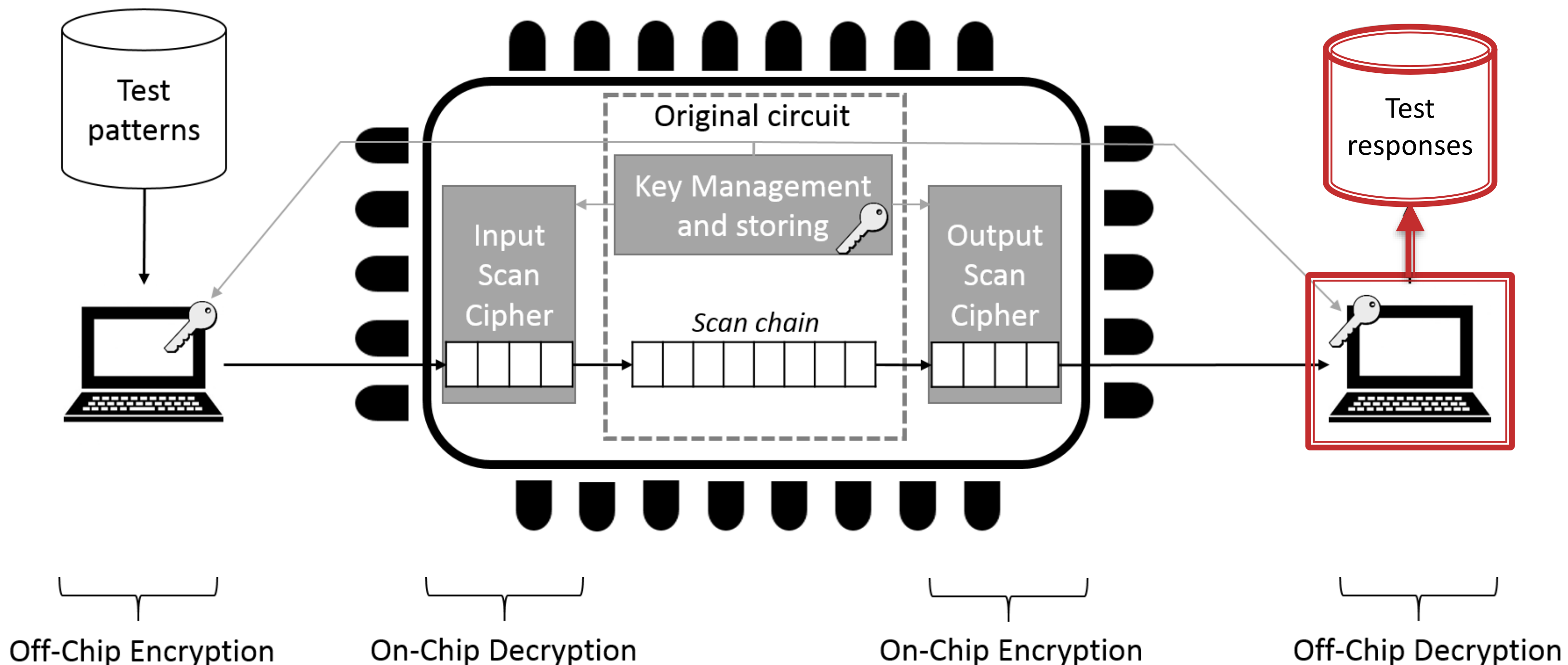
- A new secure scan design on crypto-processor
- Presentation
  - Proposed test procedure:
    4) Test responses encrypted and shifted out



Overview of Scan chain encryption

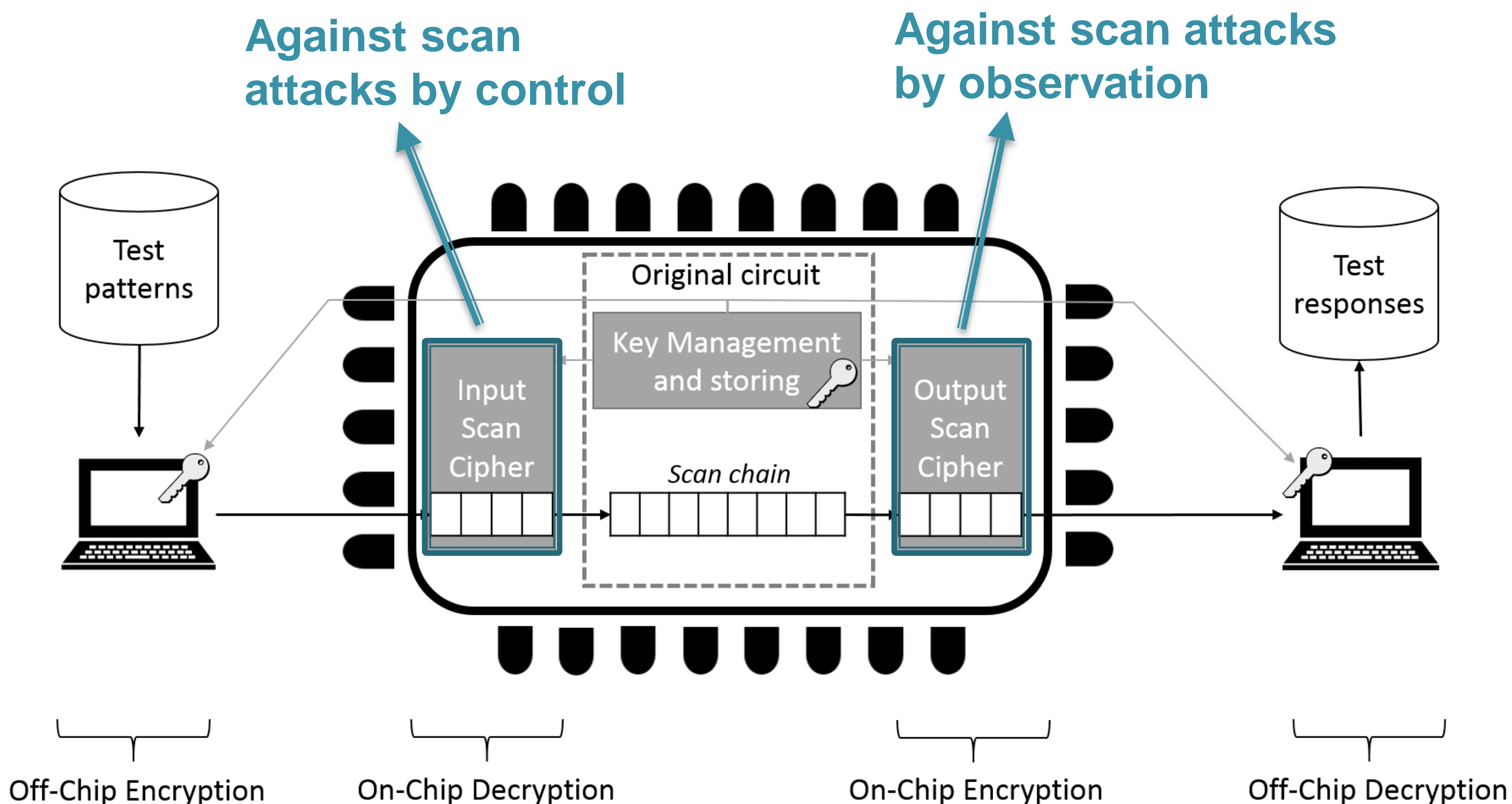
- A new secure scan design on crypto-processor
- Presentation
  - Proposed test procedure:

    5) Test responses decrypted and compared with expected ones



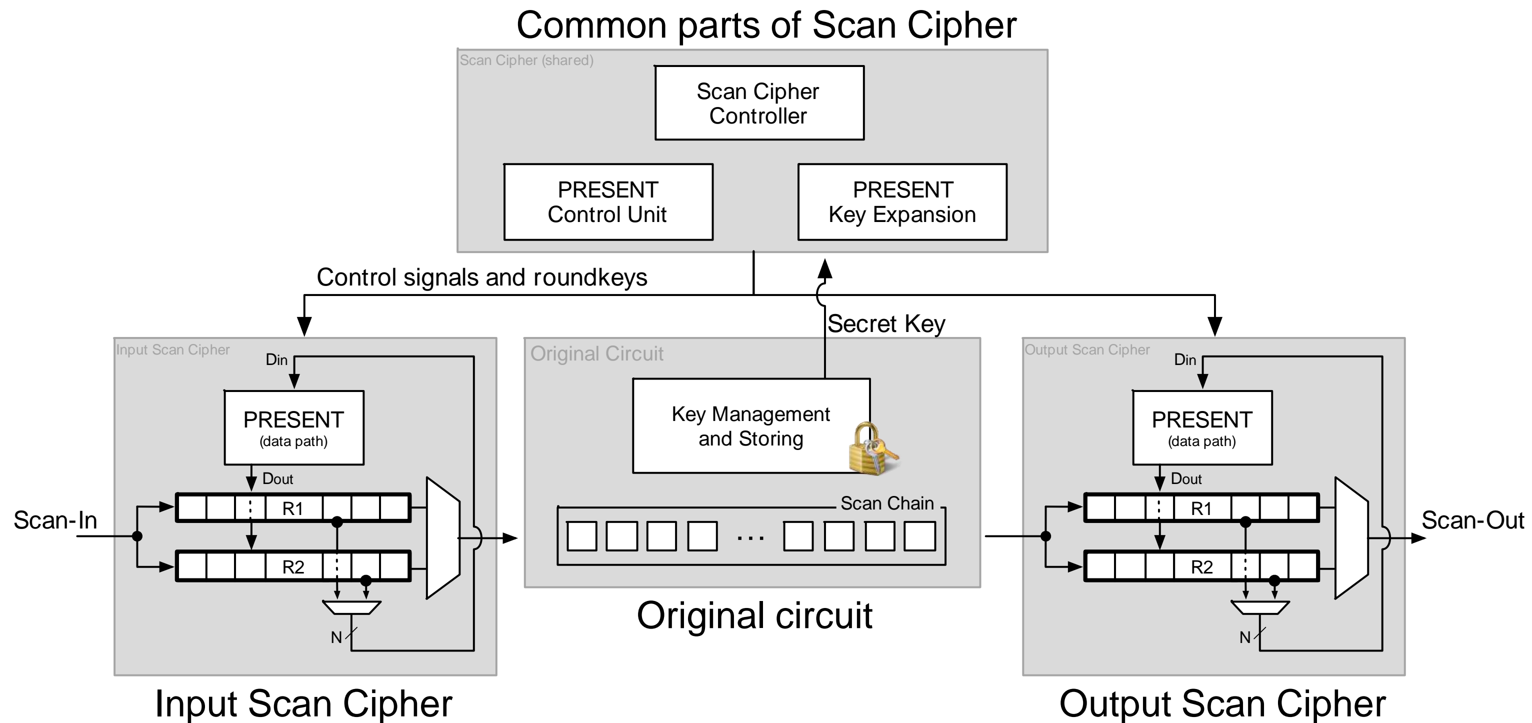
Overview of Scan chain encryption

- A new secure scan design on crypto-processor
- Presentation



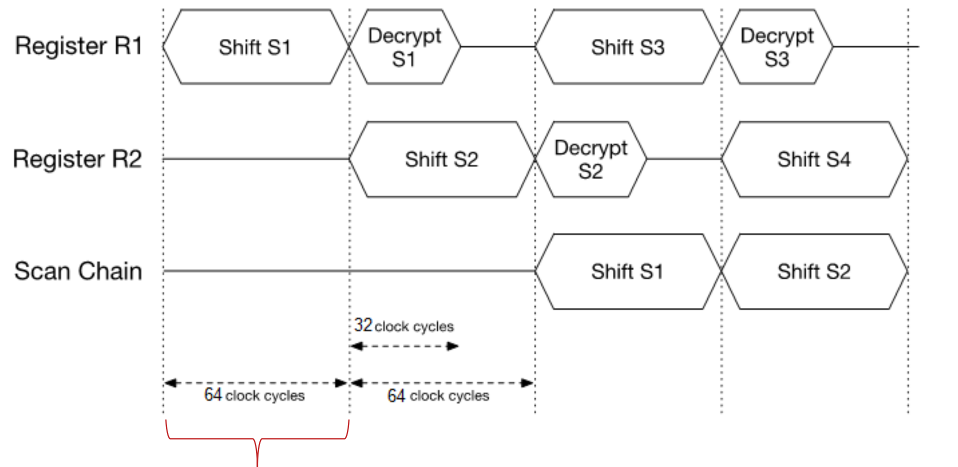
Overview of Scan chain encryption

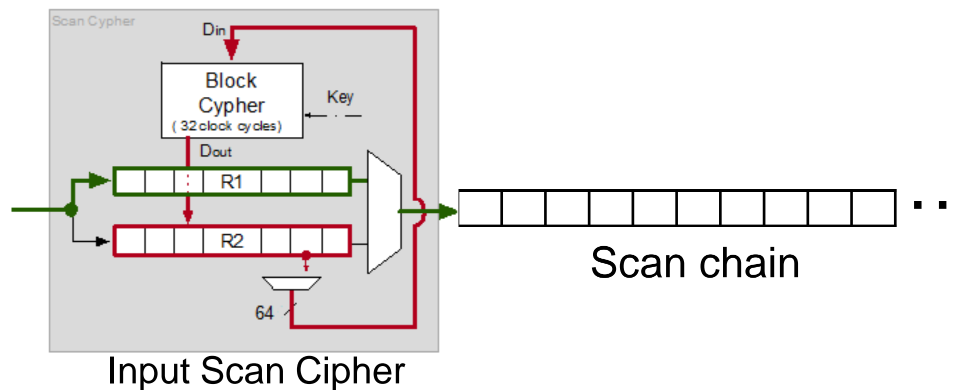
- Implementation
  - Choice of PRESENT Block cipher
    - Key size: 80 bits / Block size: 64 bits / Rounds: 32



Overview of Scan chain encryption

- Mode of operations
  - Two registers to gain test time

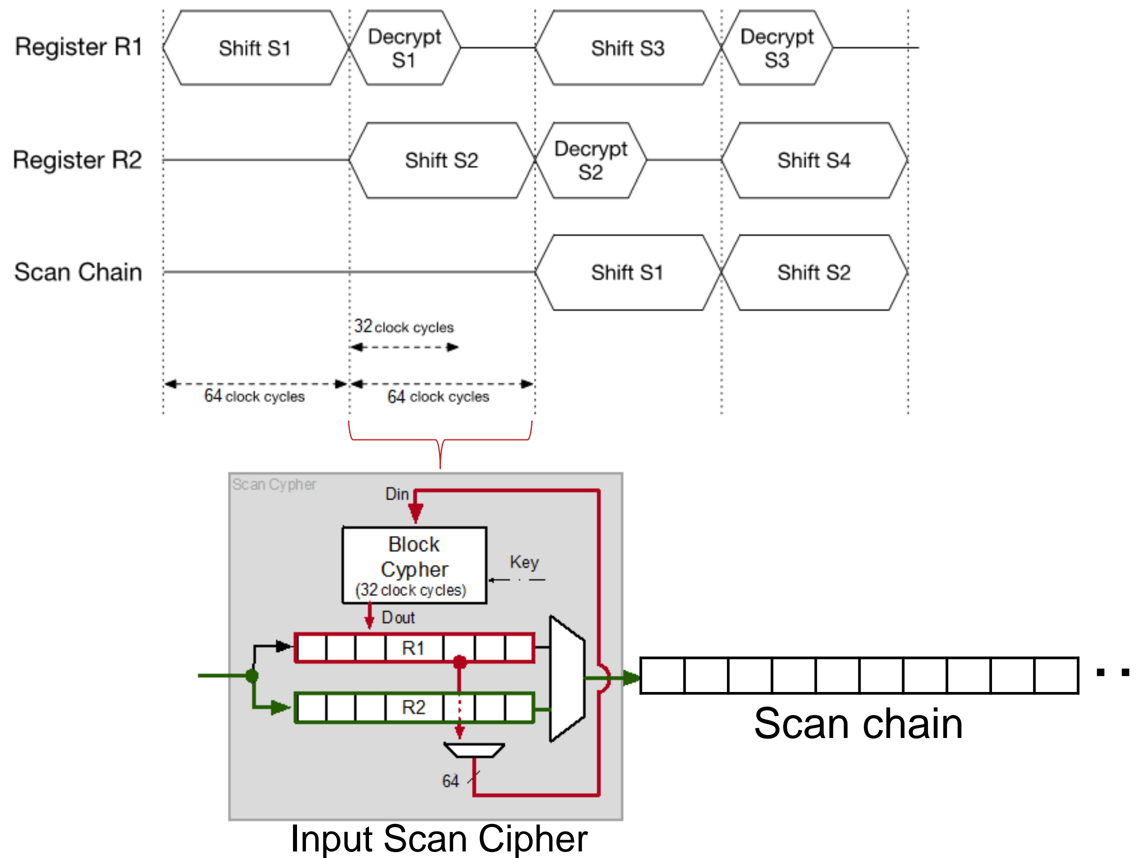




Input Scan Cipher

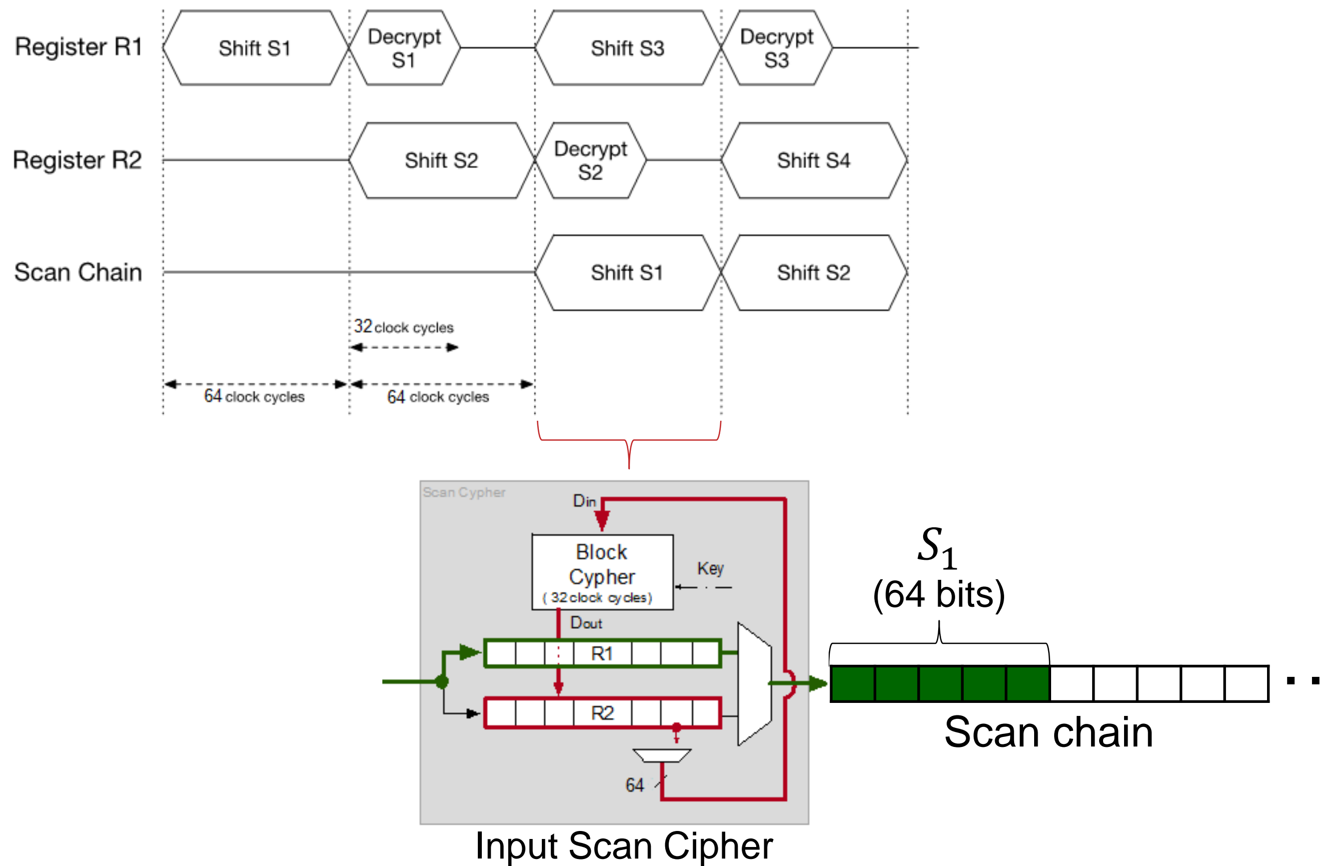
Overview of Scan chain encryption

- Mode of operations
  - Two registers to gain test time



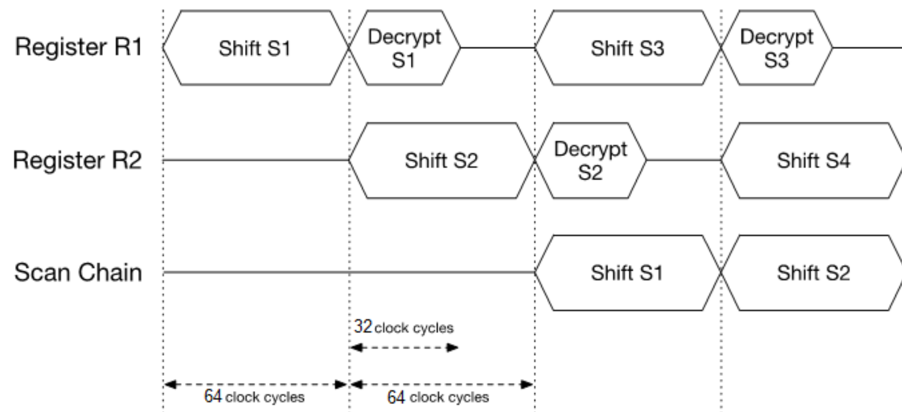
Overview of Scan chain encryption

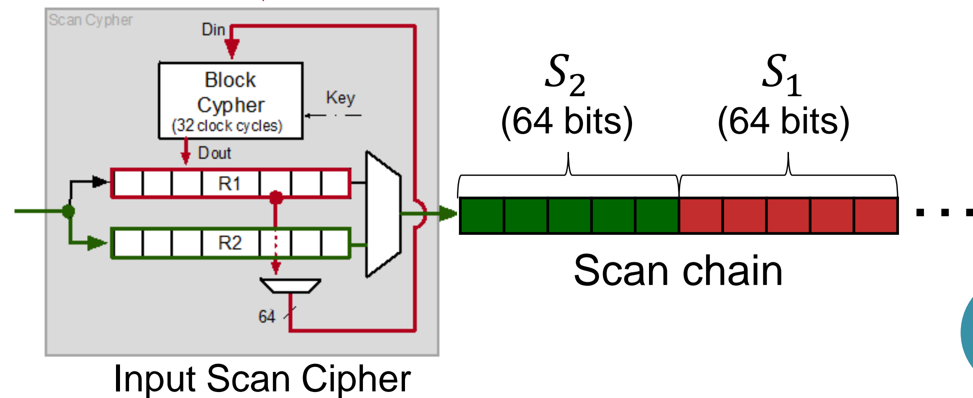
- Mode of operations
  - Two registers to gain test time



Overview of Scan chain encryption

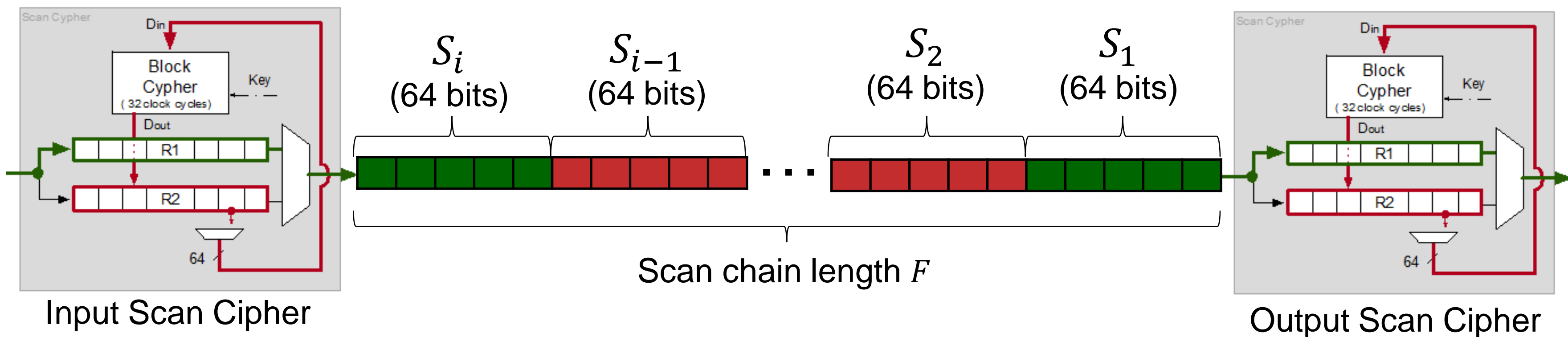
- Mode of operations
  - Two registers to gain test time





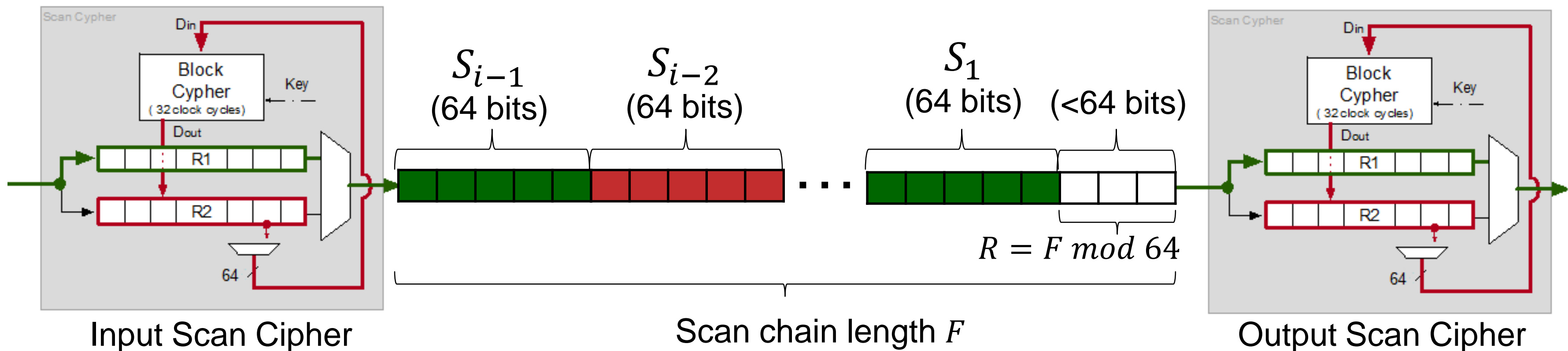
Overview of Scan chain encryption

- Mode of operations
  - Encryption/Decryption of 64-bits block size
  - In the case where scan chain length F is a multiple of 64



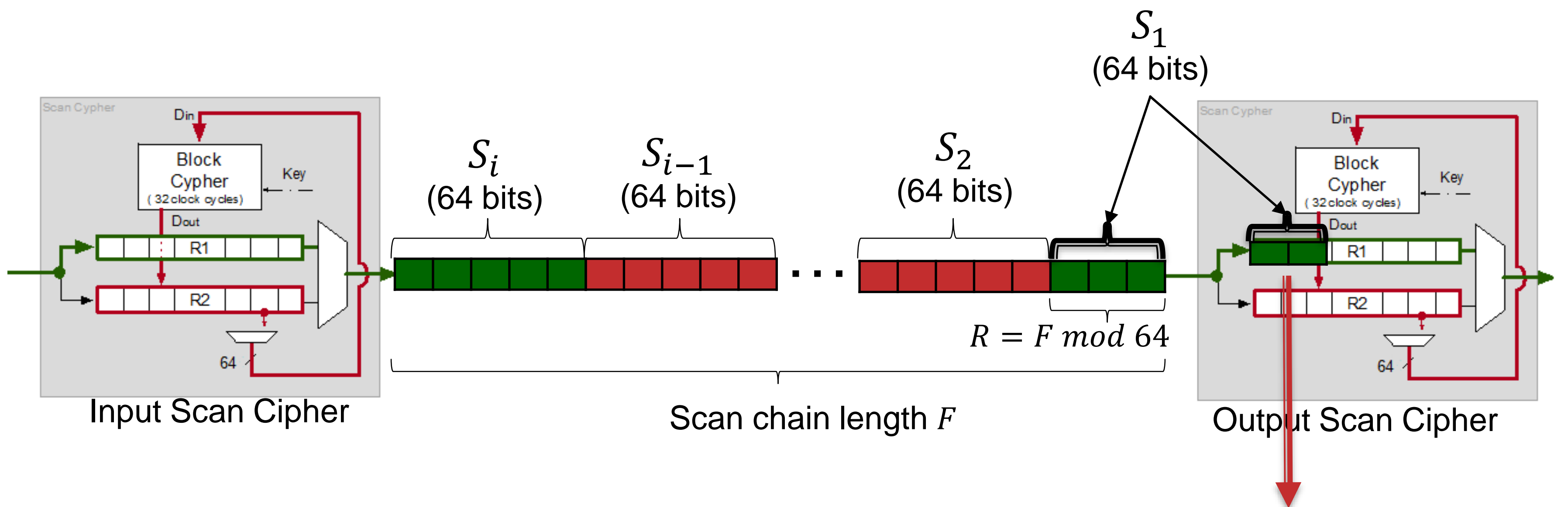
Overview of Scan chain encryption

- Mode of operations
  - Encryption/Decryption of 64-bits block size
  - In the case where scan chain length F isn't a multiple of 64



Overview of Scan chain encryption

- Mode of operations
  - Encryption/Decryption of 64-bits block size
  - In the case where scan chain length F isn't multiple of 64



Impact on test time: additional shift on each pattern $(64 - R)$, where $\mathrm{R} = F \ mod \ 64$

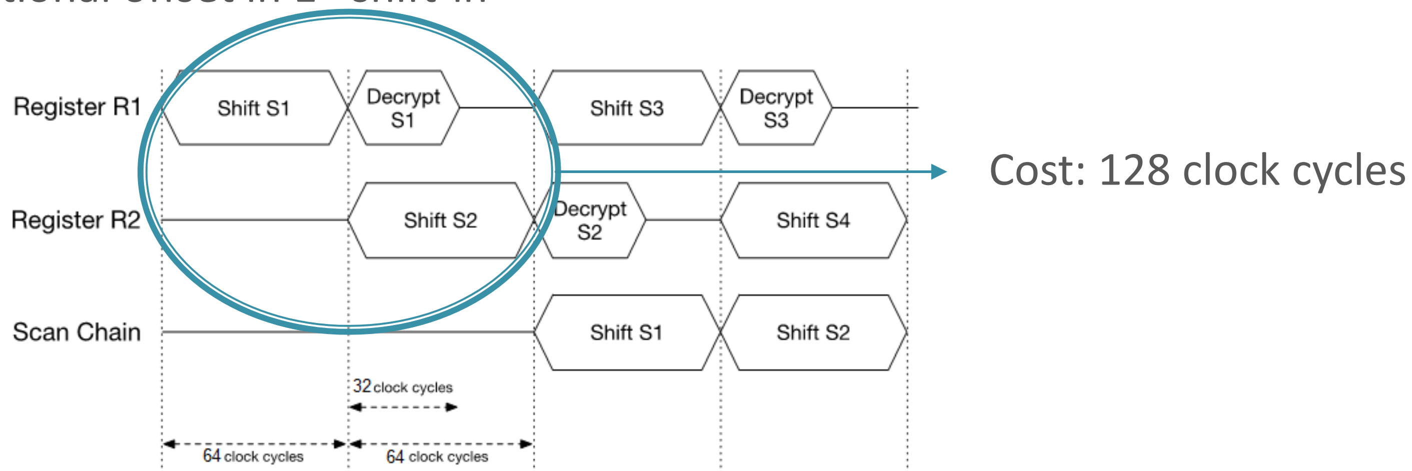
Overview of Scan chain encryption

- Cost on test time:

Test time with simple scan chain:
- K number of patterns - F number of SFF in the scan chain - T test clock cycle

$$\boldsymbol{T = K(F + 1) + F}$$

Test time with scan chain encryption:
- Additional offset in 1st shift-in



Cost: 128 clock cycles

- Additional offset in last shift-out => Cost: 128 clock cycles

Overview of Scan chain encryption

- Cost on test time:

Test time with simple scan chain:

- K number of patterns - F number of SFF in the scan chain - T test clock cycle

$$\boldsymbol{T = K(F+1) + F}$$

Test time with scan chain encryption:

- $R = F \ mod \ 64$
- T_f test clock cycle with PRESENT Scan chain Encryption

Case of number SFF multiple of 64:

If $R = 0$, $\boldsymbol{T_f = T + 2 \times 128}$

Case of number SFF not multiple of 64:

If $R \neq 0$, $\boldsymbol{T_f = T + 2 \times 128 + (64 - R)(K+1)}$

2×128: 1st shift-in & Last shift-out

$(64 - R)(K+1)$: Additional shift on each pattern

Summary

1) Scan attacks presentation

2) Overview of Scan chain encryption

3) **Experimentations on Scan chain encryption**

4) Conclusion

Experimentations on Scan chain encryption

- Test time cost for an example: Pipelined AES 128
  - $F = 7873 = 123 \times 64 + 1 \implies 64 - R = 63$ additional shift on each pattern (worst case)

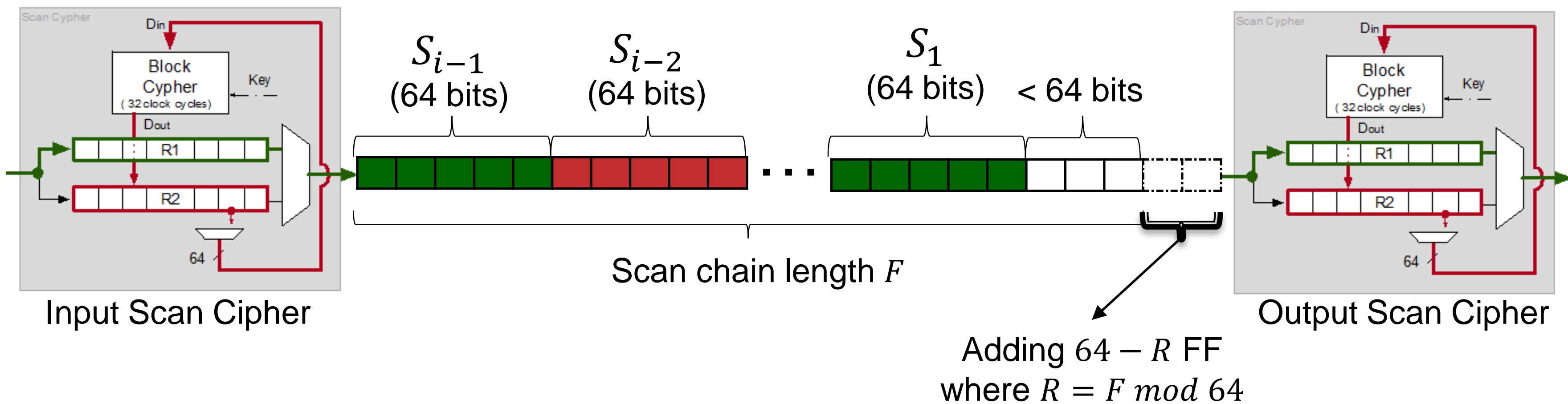
Pipelined AES 128	#SFF	#Patterns	Test time (clock cycles)	Test time overhead
Scanned circuit	7 873	246	1 944 877	Ref
+ Scan Encryption	7 873	246	1 960 694	+0,81%

Results obtained by ATPG Tool: TetraMAX (Synopsys)

  - 63 additional clock cycles wasted => another solution to use this test time

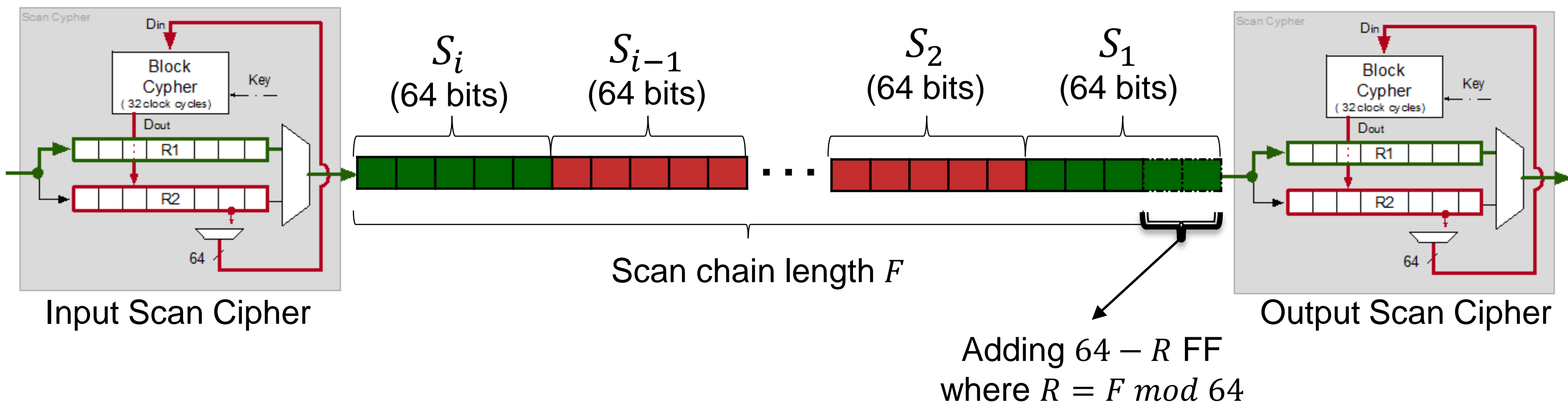
Experimentations on Scan chain encryption

- Optimization of the solution to improve test time
  - Add dummy FF in the scan chain



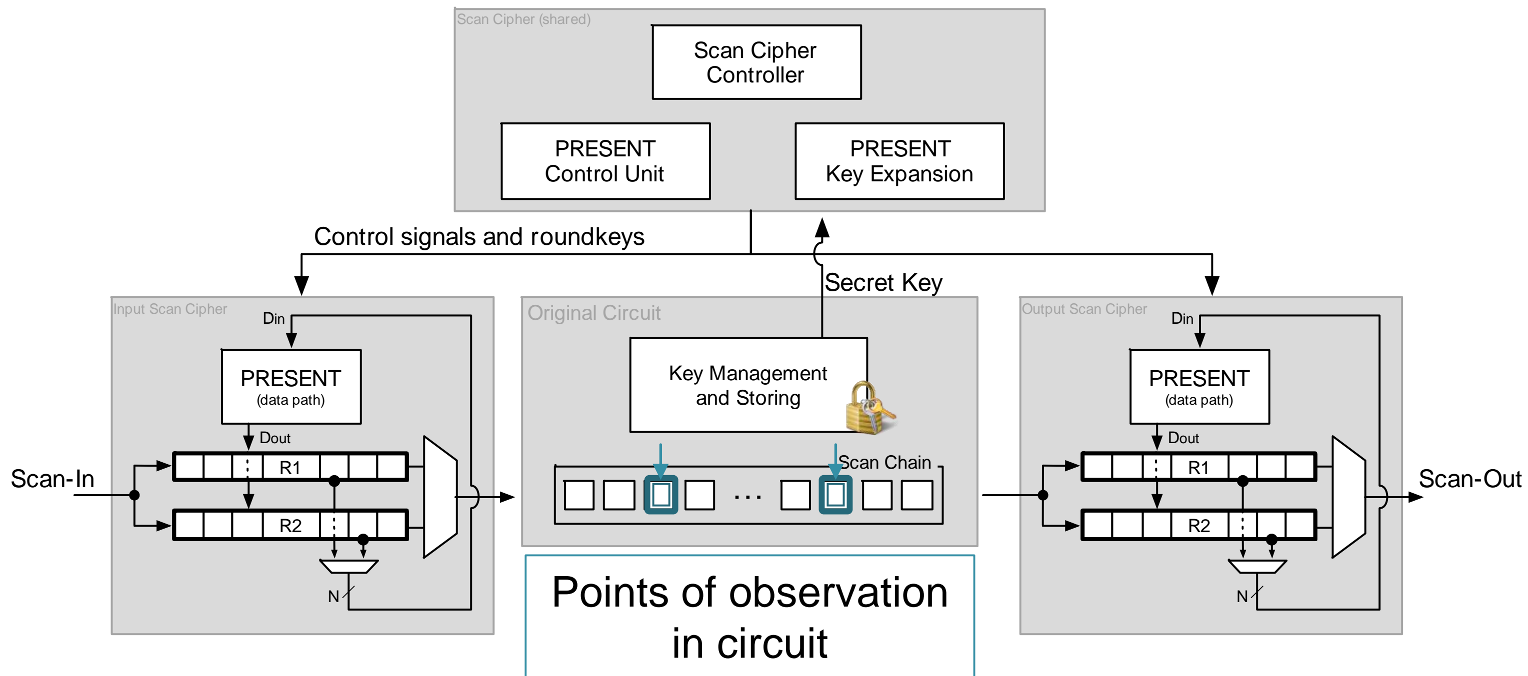
Experimentations on Scan chain encryption

- Optimization of the solution to improve test time
  - Add dummy FF in the scan chain



Experimentations on Scan chain encryption

- Optimization of the solution to improve test time
  - Use additional FF as test points
  - Observation points in the circuit



  - Goal: reduce number of patterns

Experimentations on Scan chain encryption

- Test time cost for an example: Pipelined AES 128
  - $F = 7873 = 123 \times 64 + 1 \implies 64 - R = 63$ additional shift on each pattern (worst case)

Pipelined AES 128	**#SFF**	**#Patterns**	**Test time (clock cycles)**	**Test time overhead**
Scanned circuit	7 873	246	1 944 877	Ref
+ Scan Encryption	7 873	246	1 960 694	+0,81%
Optimized version: + 63 FF as observation points	7873+63 = **8 332**	235 (**-11**)	1 873 387	**-3,68%**

EXPERIMENTATIONS ON SCAN CHAIN ENCRYPTION

- Area cost for adding Scan chain encryption with PRESENT

Cells	Combinational	Sequential	Total cell area (Estimation by Design Compiler)
Scan chain encryption	2081	396	10 760

- Area cost for an example: Pipelined AES 128

Pipelined AES 128	Combinational	Sequential	Total cell area	Area overhead
Scanned circuit	96 722	7 873	367 926	Ref
+ Scan Encryption	98 803	7 873	378 686	+**2,92**%
Optimized version: + 63 FF as observation points	98 998	8 332	380 563	+**3,43**%

Results obtained by synthesis tool: Design Compiler (Synopsys)

Experimentations on Scan chain encryption

- Test time cost & Area cost for several circuits

Circuit		#SFF	#Patt	Test time (clock cycles)	Area (Cell area)
Triple-DES	Circuit	**8 808** = 137×64+40	77	687 101	187 494
	Encrypt	**8 808**	77	+0.31%	+5.74%
	Optimized	8808+24 = **8 832**	74	-3.55%	+5.87%
Pipelined AES 128	Circuit	**7 873** = 123×64+1	246	1 944 877	367 926
	Encrypt	**7 873**	246	+0.81%	+2.92%
	Optimized	7873+63 = **7 936**	235	-3.68%	+3.43%
Pipelined AES 256	Circuit	**12 736** = 199×64	357	4 559 84	669 193
	Encrypt	**12 736**	357	+0,01%	+1,61%
RSA 1024	Circuit	**16 459** = 257×64+11	2 393	39405239	468 415
	Encrypt	**16 459**	2 393	+0.33%	+2.30%
	Optimized	16459+53 = **16 512**	2 393	+0.33%	+2.51%
LEON3*	Circuit	**107 518** = 1679×64+62	107	11 612 051	1 902 095
	Encrypt	**107 518**	107	+0.004%	+0.57%
	Optimized	107518+2 = **107 520**	102	-4.63%	+0.57%

*: for LEON3, test time and number of patterns are evaluated to obtain a test coverage of 70% due to limits of ATPG tools TetraMAX (patterns memory allocation)

EXPERIMENTATIONS ON SCAN CHAIN ENCRYPTION

- **Test time cost** & Area cost for several circuits

Circuit		#SFF	#Patt	Test time (clock cycles)	Area (Cell area)
Triple-DES	Circuit	**8 808** = 137×64+40	77	687 101	187 494
	Encrypt	**8 808**	77	**+0.31%**	+5.74%
	Optimized	8808+24 = **8 832**	74	**-3.55%**	+5.87%
Pipelined AES 128	Circuit	**7 873** = 123×64+1	246	1 944 877	367 926
	Encrypt	**7 873**	246	**+0.81%**	+2.92%
	Optimized	7873+63 = **7 936**	235	**-3.68%**	+3.43%
Pipelined AES 256	Circuit	**12 736** = 199×64	357	4 559 84	669 193
	Encrypt	**12 736**	357	**+0,01%**	+1,61%
RSA 1024	Circuit	**16 459** = 257×64+11	2 393	39405239	468 415
	Encrypt	**16 459**	2 393	**+0.33%**	+2.30%
	Optimized	16459+53 = **16 512**	2 393	**+0.33%**	+2.51%
LEON3*	Circuit	**107 518** = 1679×64+62	107	11 612 051	1 902 095
	Encrypt	**107 518**	107	**+0.004%**	+0.57%
	Optimized	107518+2 = **107 520**	102	**-4.63%**	+0.57%

*: for LEON3, test time and number of patterns are evaluated to obtain a test coverage of 70% due to limits of ATPG tools TetraMAX (patterns memory allocation)

EXPERIMENTATIONS ON SCAN CHAIN ENCRYPTION

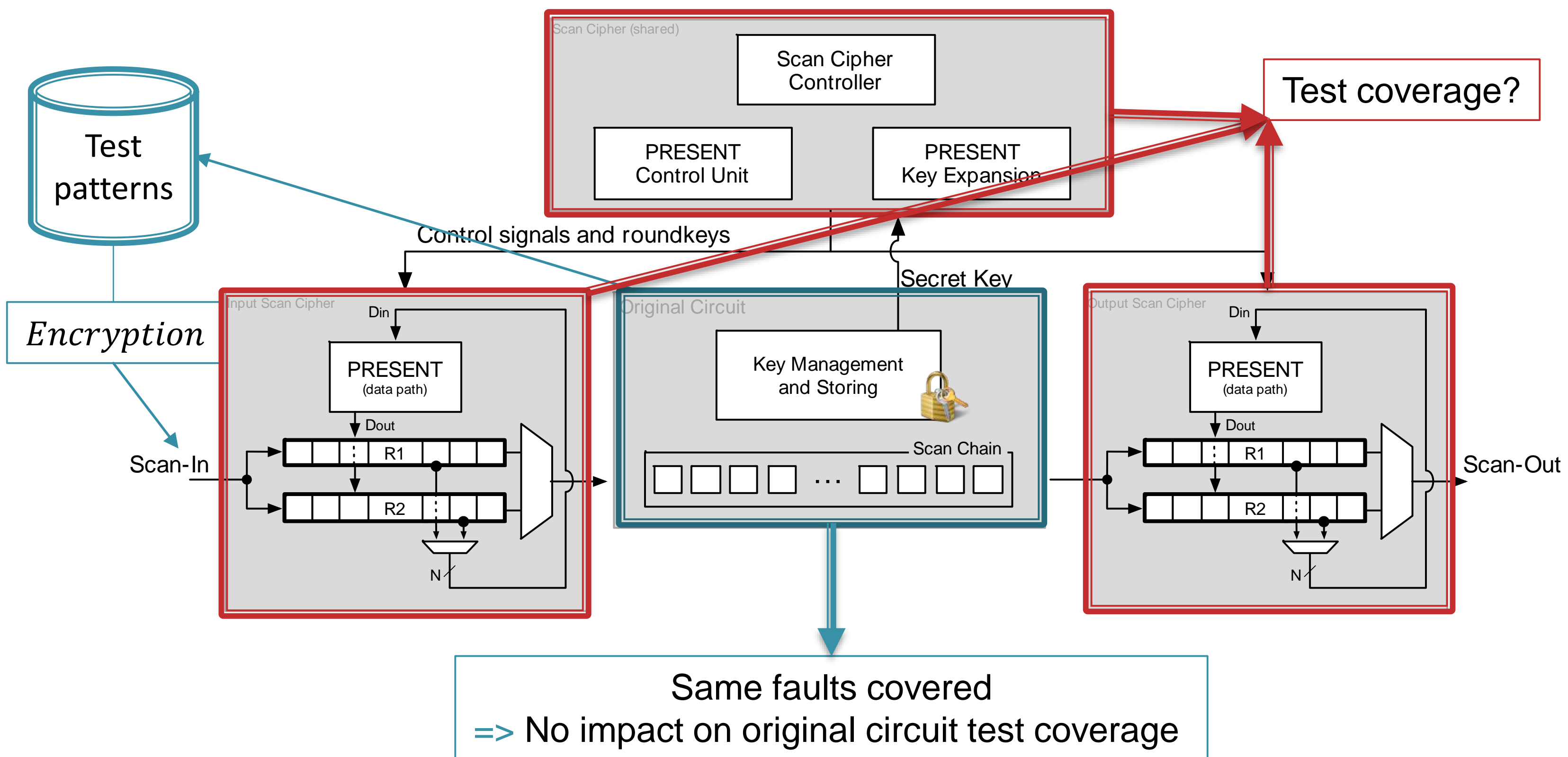
- Test time cost & **Area cost** for several circuits

Circuit		**#SFF**	**#Patt**	**Test time (clock cycles)**	**Area (Cell area)**
Triple-DES	Circuit	**8 808** = 137×64+40	77	687 101	187 494
	Encrypt	**8 808**	77	+0.31%	**+5.74%**
	Optimized	8808+24 = **8 832**	74	-3.55%	**+5.87%**
Pipelined AES 128	Circuit	**7 873** = 123×64+1	246	1 944 877	367 926
	Encrypt	**7 873**	246	+0.81%	**+2.92%**
	Optimized	7873+63 = **7 936**	235	-3.68%	**+3.43%**
Pipelined AES 256	Circuit	**12 736** = 199×64	357	4 559 84	669 193
	Encrypt	**12 736**	357	+0,01%	**+1,61%**
RSA 1024	Circuit	**16 459** = 257×64+11	2 393	39405239	468 415
	Encrypt	**16 459**	2 393	+0.33%	**+2.30%**
	Optimized	16459+53 = **16 512**	2 393	+0.33%	**+2.51%**
LEON3*	Circuit	**107 518** = 1679×64+62	107	11 612 051	1 902 095
	Encrypt	**107 518**	107	+0.004%	**+0.57%**
	Optimized	107518+2 = **107 520**	102	-4.63%	**+0.57%**

*: for LEON3, test time and number of patterns are evaluated to obtain a test coverage of 70% due to limits of ATPG tools TetraMAX (patterns memory allocation)

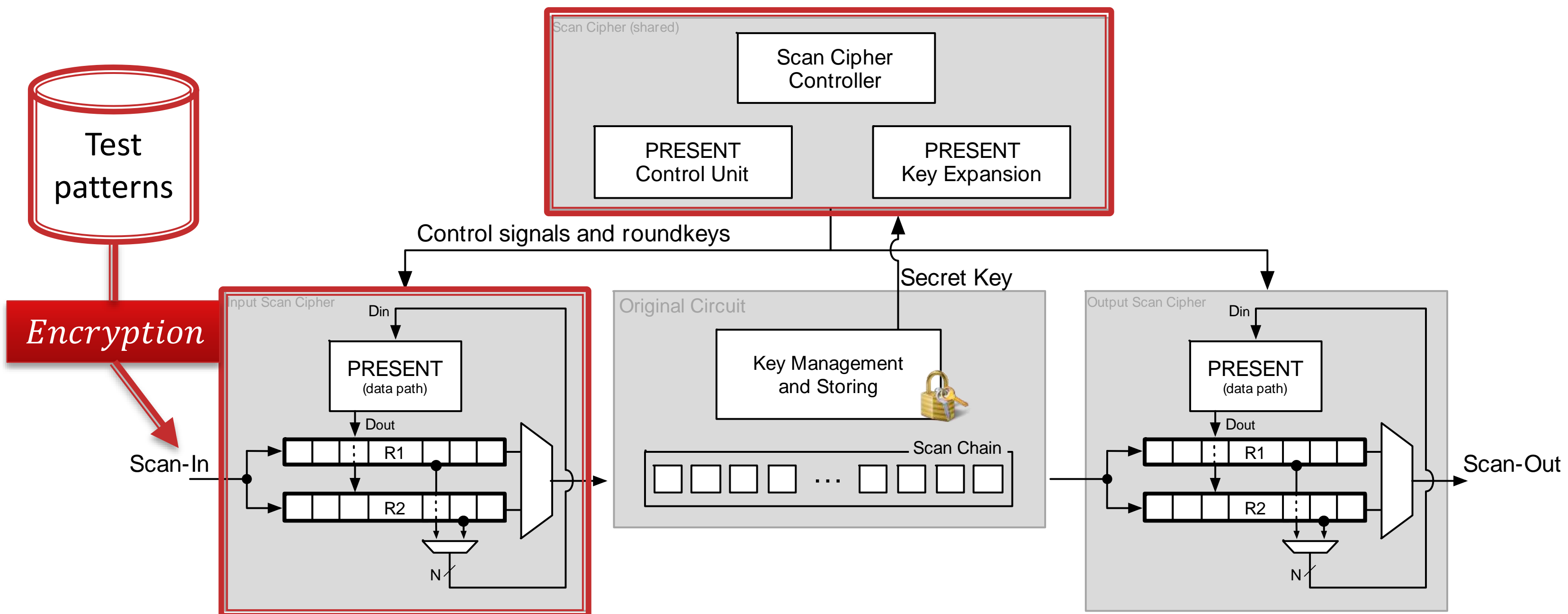
EXPERIMENTATIONS ON SCAN CHAIN ENCRYPTION

- Test coverage
  - Test of the scan chain encryption?



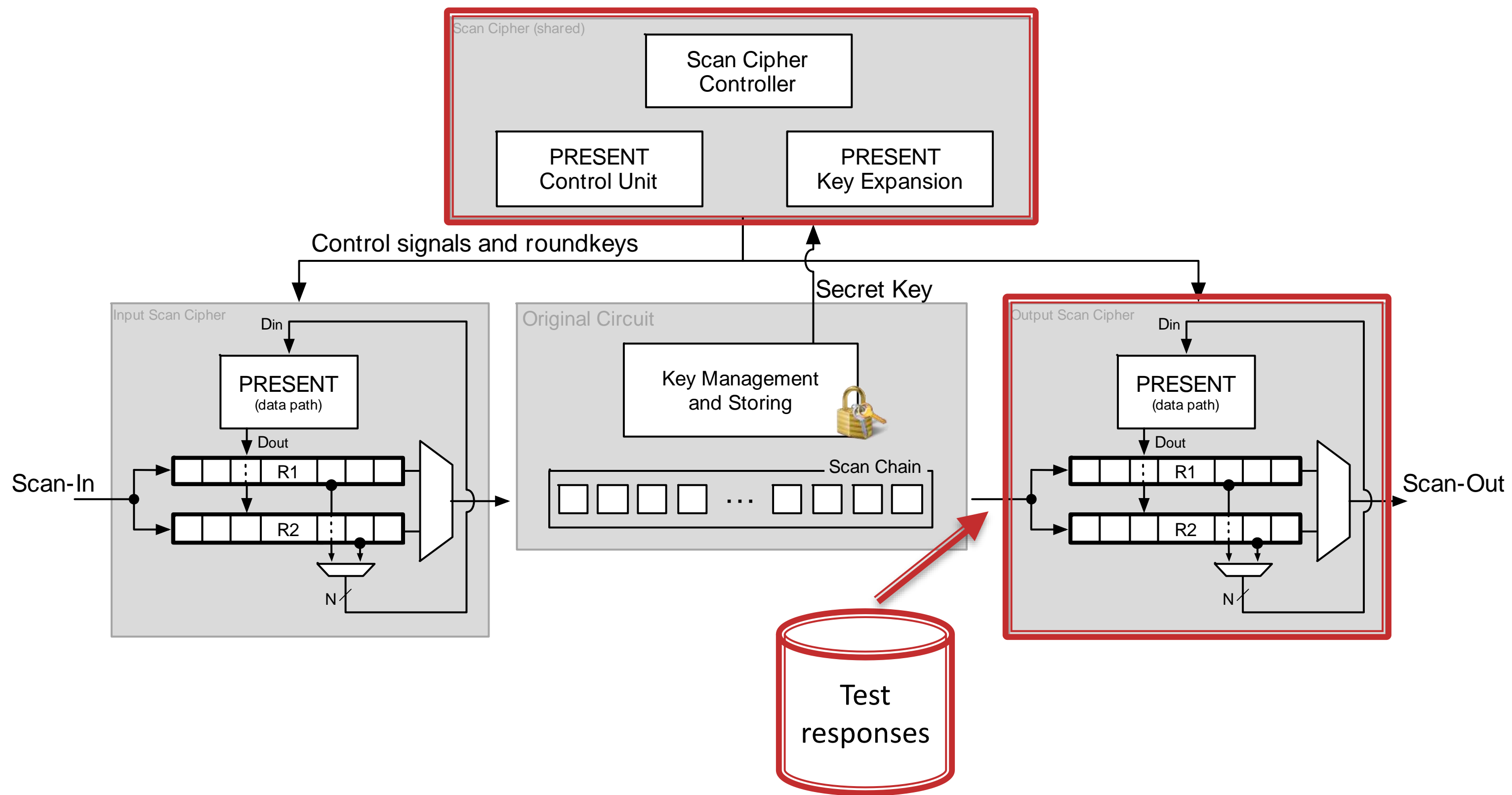
EXPERIMENTATIONS ON SCAN CHAIN ENCRYPTION

- Test coverage
  - Test patterns propagated and processed by Input Scan Cipher



Experimentations on Scan chain encryption

- Test coverage
  - Test responses propagated and processed by Output Scan Cipher



LIGHT SCAN CHAIN ENCRYPTION WITH PRESENT ALGORITHM

- Test coverage
  - Extra ciphers are tested thanks to test procedure of original circuit

	Triple-DES	Pipelined AES 128	Pipelined AES 256	RSA 1024	LEON 3*
#SFF	8 808	7 873	12 736	16 459	107 518
#Patterns	77	246	357	2 393	107
Scan chain encryption Test Coverage	100%	100%	100%	100%	100%

*: for LEON3, number of patterns are evaluated to obtain a test coverage of 70% due to limits of ATPG tools TetraMAX (patterns memory allocation)

  - Maximum fault coverage achieved for all circuits

SUMMARY

1) Scan attacks presentation
2) Overview of Scan chain encryption
3) Experimentations on Scan chain encryption
4) **Conclusion**

Conclusion

- New countermeasure against scan attacks with a marginal cost on area and test time

- Optimization proposed to compensate extra test time

- Accepted for publication:
  - Mathieu Da Silva, Marie-Lise Flottes, Giorgio Di Natale, Bruno Rouzeyre, Marco Restifo, Paolo Prinetto. Scan Chain Encryption for the Test, Diagnosis and Debug of Secure Circuits. 22nd IEEE European Test Symposium (ETS'17)

Remarks / Questions

ACKNOWLEDGEMENTS

- FUI#20 TEEVA Project

- Partners

TRUSTONIC

LABORATOIRE
HUBERT CURIEN
UMR • CNRS • 5516 • SAINT-ETIENNE