Optimal FPGA Implementations of a Very Low-Cost Countermeasure Based on Rotating S-Boxes Masking Countermeasure

Sylvain Guilley, **Shivam Bhasin**,
Ankit Khandelwal and Jean-Luc Danger

Institut TELECOM / TELECOM ParisTech,
46 rue Barrault, Paris, France.

Secure-IC S.A.S.,
80 avenue des Buttes de Coësmes, Rennes, France.

June 26, 2012

1. Introduction
   - Context
   - Motivations
2. RSM: Rotating Sboxes Masking
   - Rationale of the Countermeasure
   - Security Evaluation
3. Optimal Implementation on Modern FPGA
   - Solution 1
   - Solution 2
   - Solution 3
4. Conclusions and Perspectives

1 Introduction
- Context
- Motivations

2 RSM: Rotating Sboxes Masking
- Rationale of the Countermeasure
- Security Evaluation

3 Optimal Implementation on Modern FPGA
- Solution 1
- Solution 2
- Solution 3

4 Conclusions and Perspectives

Context

Side-Channel Attacks pose a serious threat to embedded cryptography.

Countermeasures

- Extrinsic:
  - Noise addition .. makes the attack difficult but not impossible.
  - Delay insertion needs traces synchronization before the attack.
- Intrinsic:
  - Hiding the power ..... require design skills [Danger et al. [DGBN09] ✖]
  - Masking the power ..... susceptible to HO-SCA [Prouff et al. [PRB09]✔]

Motivation behind this work

- $+$ Security ☺ $\Longrightarrow$ $+$ Area ☹
  $\Longrightarrow$ $-$ Speed ☹
  $\Longrightarrow$ $+$ Consumption ☹
- Trade-offs?
  - Maximal security within a given budget
  - Minimal spendings for a target security level (CC EALx?)
- The countermeasure presented here provides elevated security at reasonable cost.

1 Introduction
- Context
- Motivations

2 RSM: Rotating Sboxes Masking
- Rationale of the Countermeasure
- Security Evaluation

3 Optimal Implementation on Modern FPGA
- Solution 1
- Solution 2
- Solution 3

4 Conclusions and Perspectives

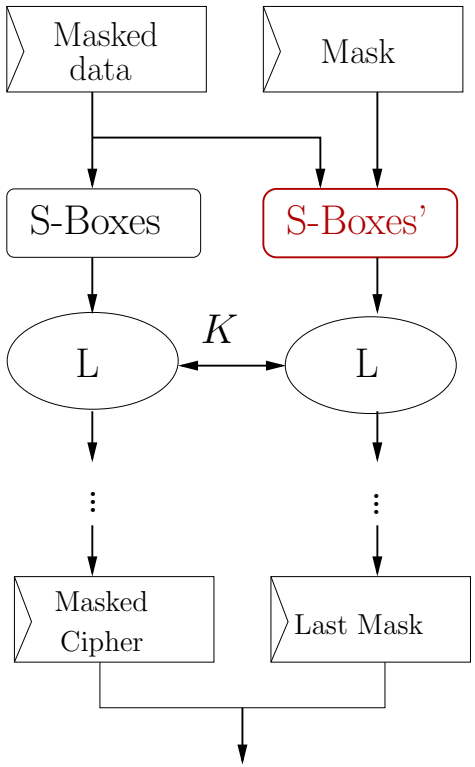
Masking: Principle

Basic Principle

- Make the average power consumption uncorrelated to data.
- $\Rightarrow$ Randomization of the sensitive data.

Rationale

- Requires a RNG.
- Two paths: masked sensitive data + mask updating.
- $\oplus$ Performances, low resource consumption for linear parts.
- $\ominus$ Area/performance of S-Boxes, vulnerability to VPA, HO-SCAs.



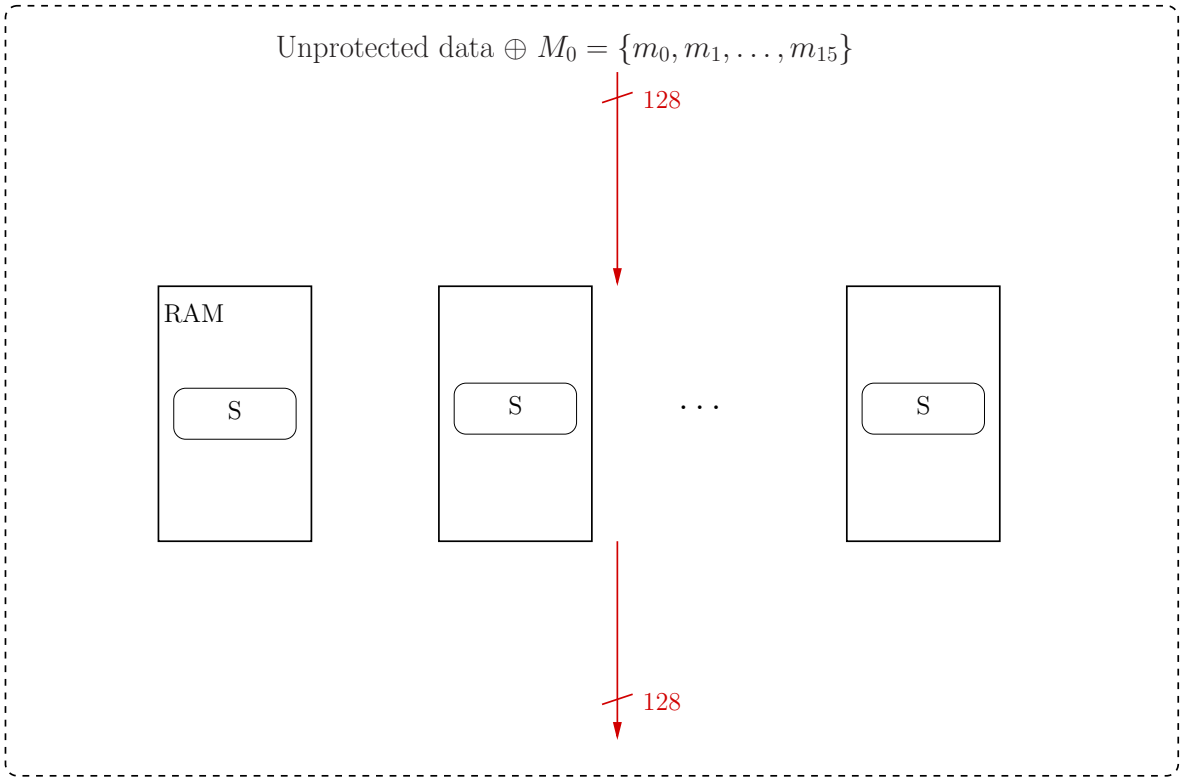
Rotating S-Box Masking (RSM)

RSM Principle

- Dedicated to SPN cipher (like AES).
- Goal:
  - Complexity and performances close to unprotected architecture
  - Secure against 1^{st} order CPA and VPA.
- Principle:
  - n chosen mask.
  - n Customized masked S-Boxes implemented in memory.
  - Rotation of S-boxes to change the mask.

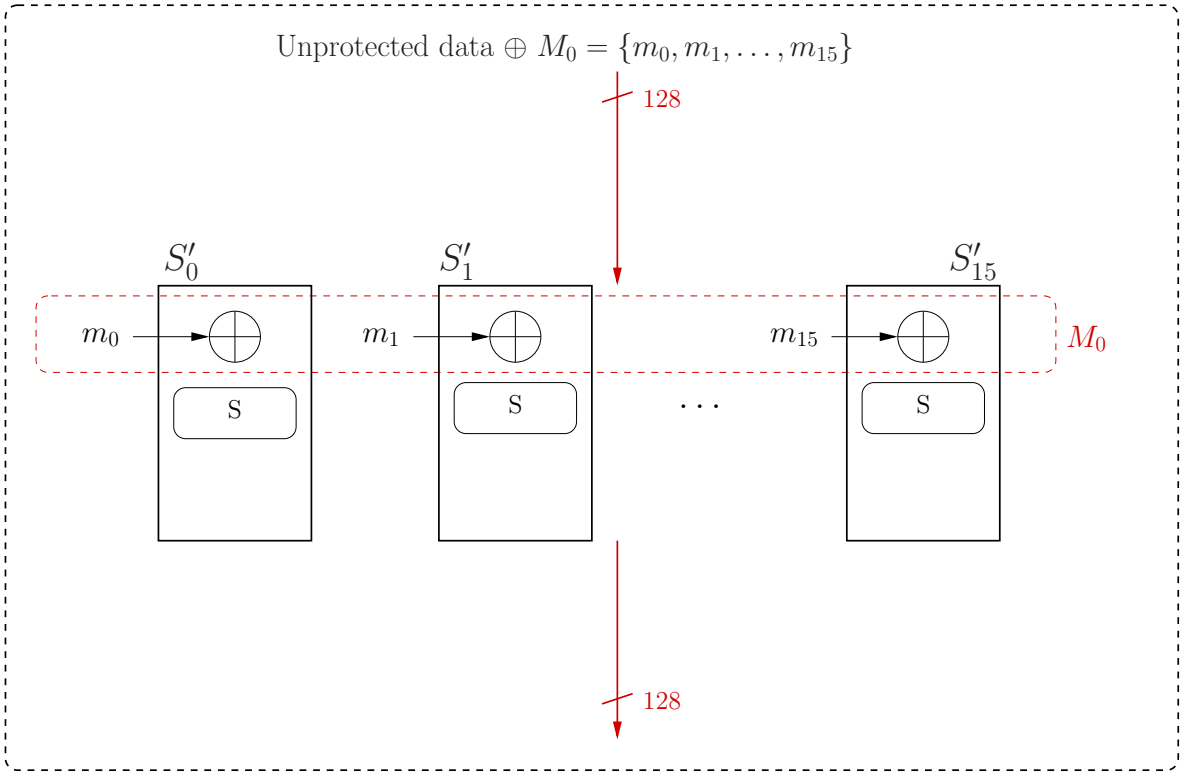
Computing S-Boxes

$\Rightarrow$ Unprotected S-Box.



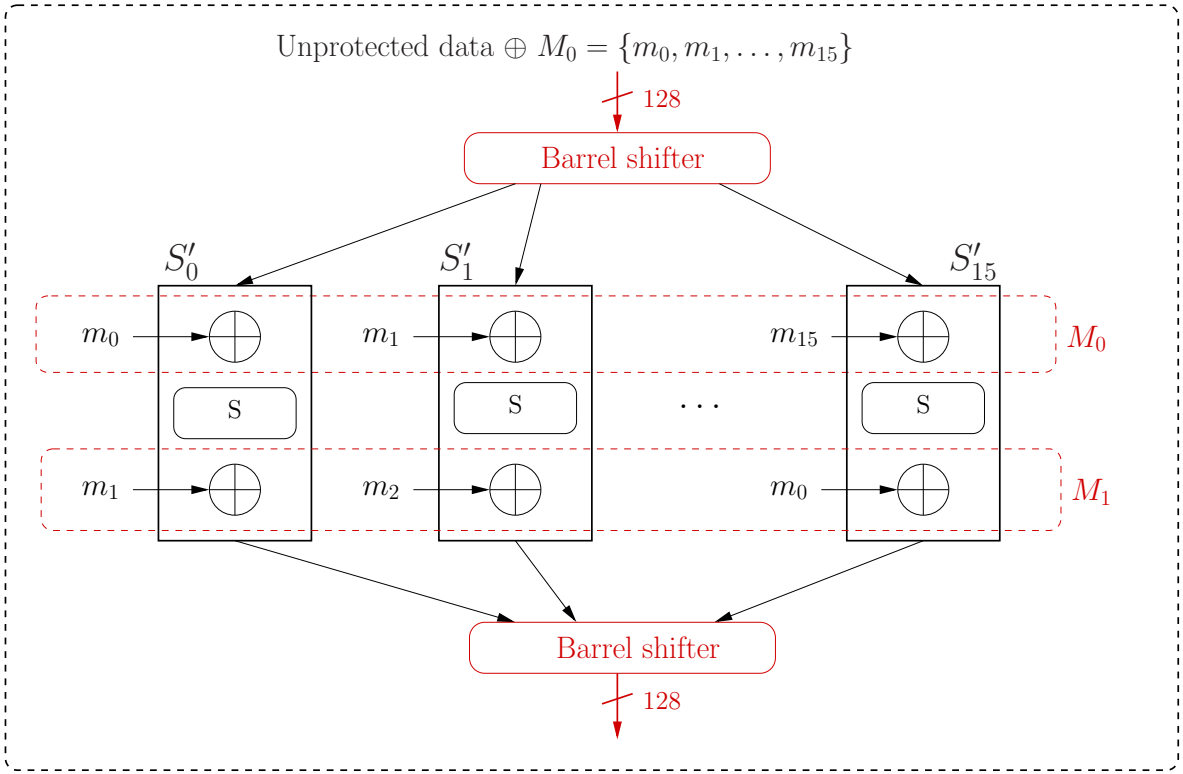
Computing S-Boxes

$\Rightarrow$ Unprotected S-Box + unmasking input.



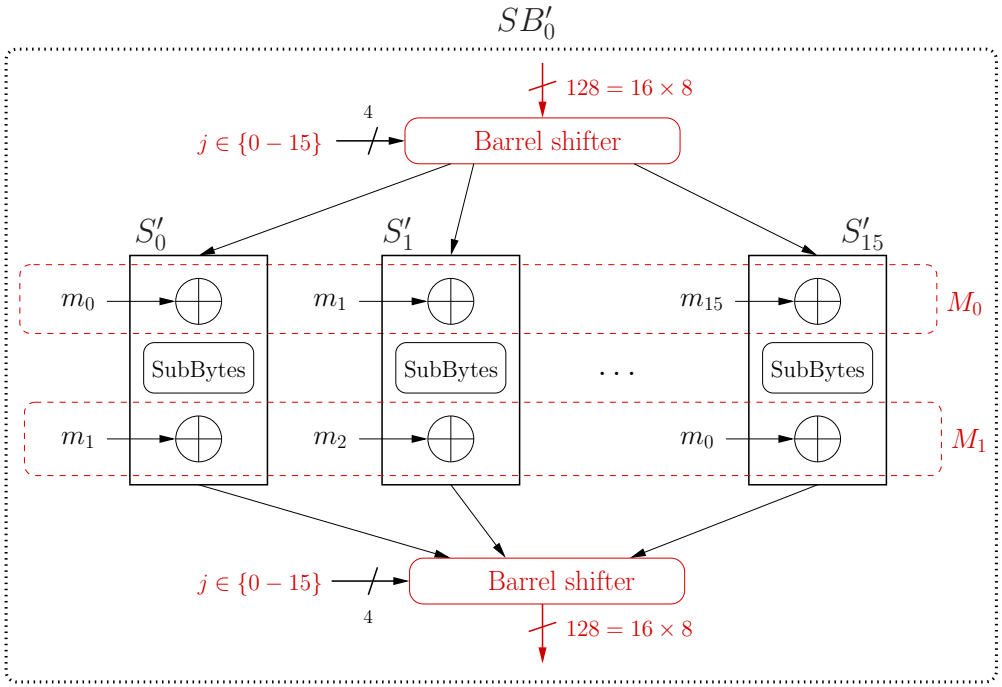
Computing S-Boxes

$\Rightarrow$ Unprotected S-Box + unmasking input + remasking output.

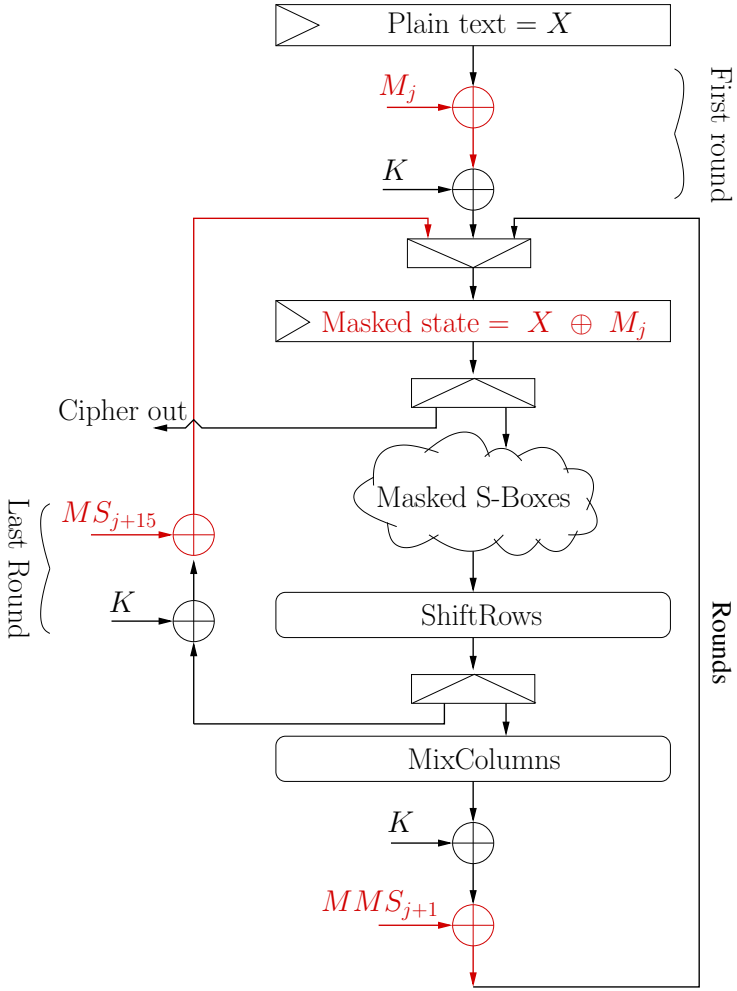


Rotating S-Boxes

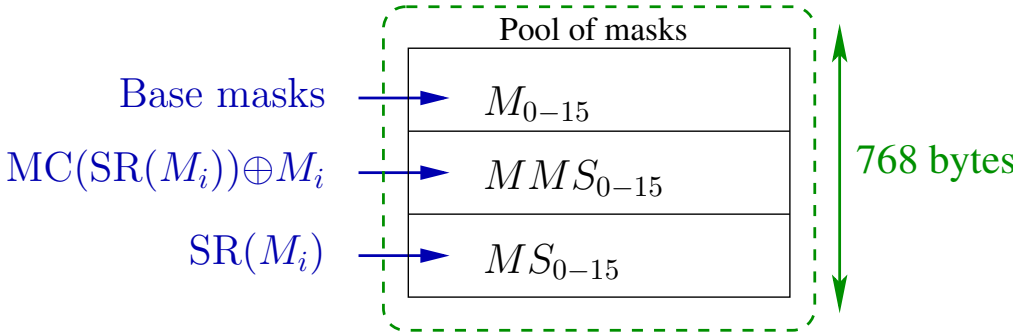
- Built-in masking $\Rightarrow$ precompute S-Boxes.
- Choose $\{m_0, m_1, \ldots, m_{15}\}$: $S'_{0-15}(x) = S(m_j \oplus x) \oplus m_{j+1}$.
- Rotation: output mask $\leftrightarrow$ next input mask.
- Random offset.



AES Architecture protected with RSM



Masking with one path: $Z \rightarrow Z \oplus M$ (ex. AES)



3 sets of 16 128-bit masks are precomputed

1. Base masks: $M_0 = \{m_0, m_1, \ldots, m_{15}\}$ + its 15 rotations by 1 byte $M_{1-15} \Rightarrow$ AES first round.
2. $MMS_j = MC \circ SR(M_j) \oplus M_j, \quad \forall j \in \{1-15\} \Rightarrow$ rounds.
3. $MS_j = SR(M_j), \quad \forall j \in \{1-15\} \Rightarrow$ last round.

Implementation on StratixII : 16 different masks

	Unprotected	RSM	Overhead
Number of ALUTs	1451	2049	48%
Number of M4K ROM Blocs	20	28	40%
Frequency (MHz)	133.8	88.5	34%

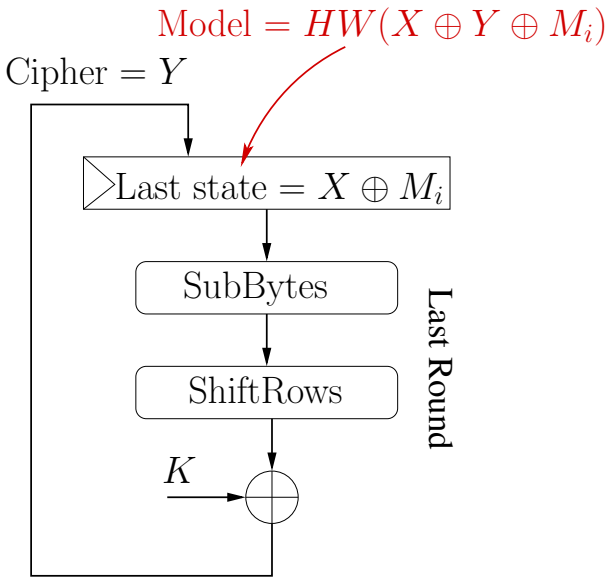
Additional cost wrt. unprotected AES

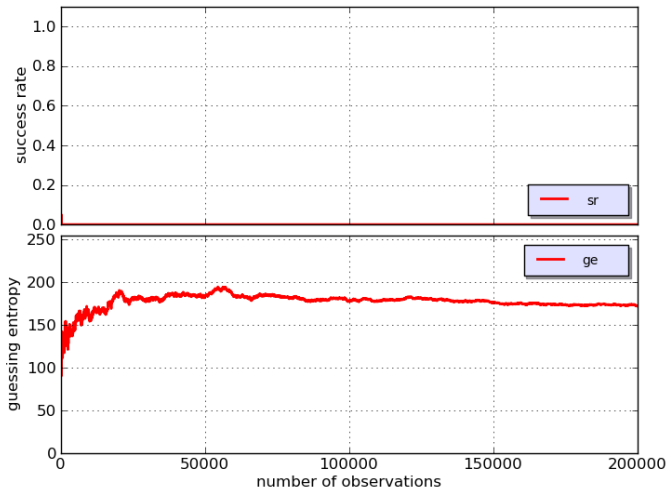
- Barrel shifters (critical path).
- Xor (critical path).
- Few logic elements.
- 48 128-bit masks (ROM).
- 4-bit RNG.

Experimental Security Evaluation

CPA and VPA on RSM

- Model = HD of the state register.
- CPA and VPA unsuccessful on 200000 observations without noise.





- CPA and VPA unsuccessful on 150000 real measurements where as reference AES breaks in $\sim$ 12000 traces with CPA.
- Detailed evaluation can be found in [Guilley et al. [NGD11, NSGD12]]

1 Introduction
- Context
- Motivations

2 RSM: Rotating Sboxes Masking
- Rationale of the Countermeasure
- Security Evaluation

3 Optimal Implementation on Modern FPGA
- Solution 1
- Solution 2
- Solution 3

4 Conclusions and Perspectives

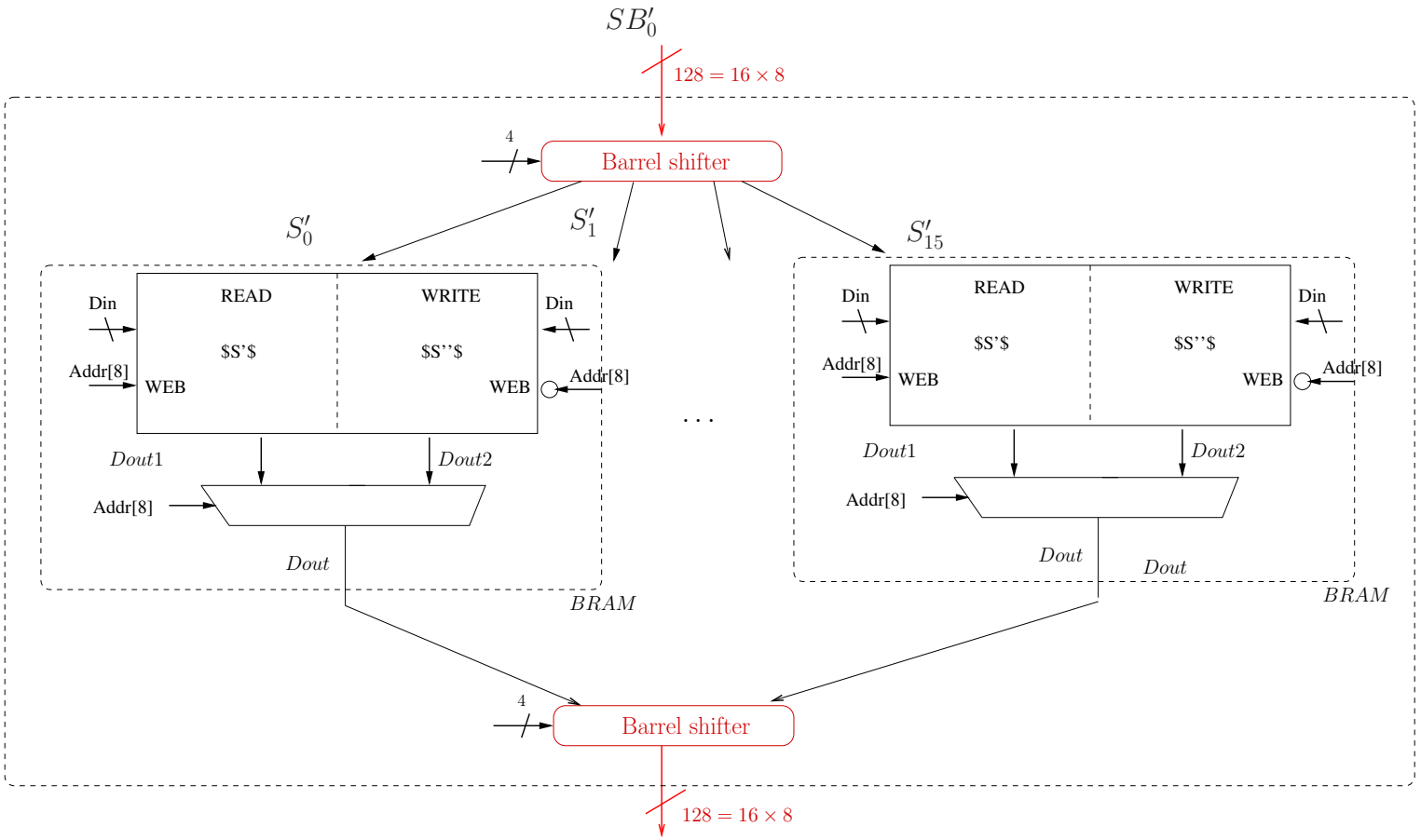
Possible Optimizations

- **Robustness:** Regularly compute new sets of masks: $\searrow$ information leakage.
  - Double datapath: AES + mask recomputation in parallel (Area$\nearrow$).
  - Pause the cryptographic operations and update mask (Throughput$\searrow$).
- **Complexity:** Better performance/ Lesser area with 16 masks.
  - Mask update without time penality.
  - Removal of barrel shift registers.
  - Overuse of FPGA BRAMs.

(Robustness) Solution 1:Refreshing the Mask

- Modern FPGA like Virtex 5 contain 36Kb of dual-port RAM.
- Each AES Sbox is 2Kb.
- Implement a 4Kb Sbox.
- **Solution:** One-half of ROM for encryption; Other half is refreshed from the dual-port.
- **Overhead:** Routing one extra address bit.

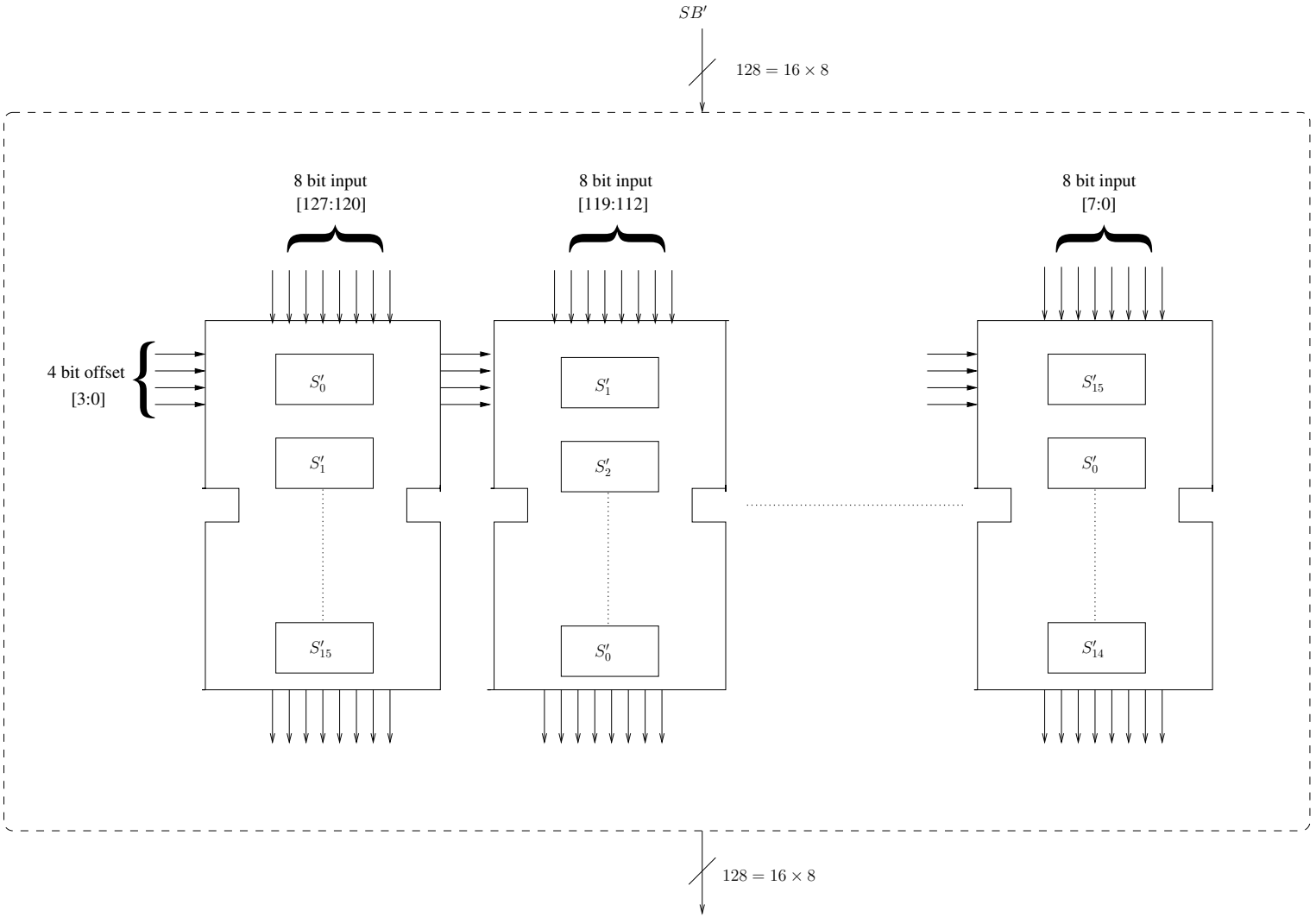
(Robustness) Solution 1:Refreshing the Mask



(Complexity) Solution 2: Removal of Barrel Shifters

- Barrel shifters consume a lot of logic.
- Implement all 16 masked Sboxes in one BRAM (often underused) to remove shifters.
- Offset can be implemented while writing the BRAM.

(Complexity) Solution 2: Removal of Barrel Shifters



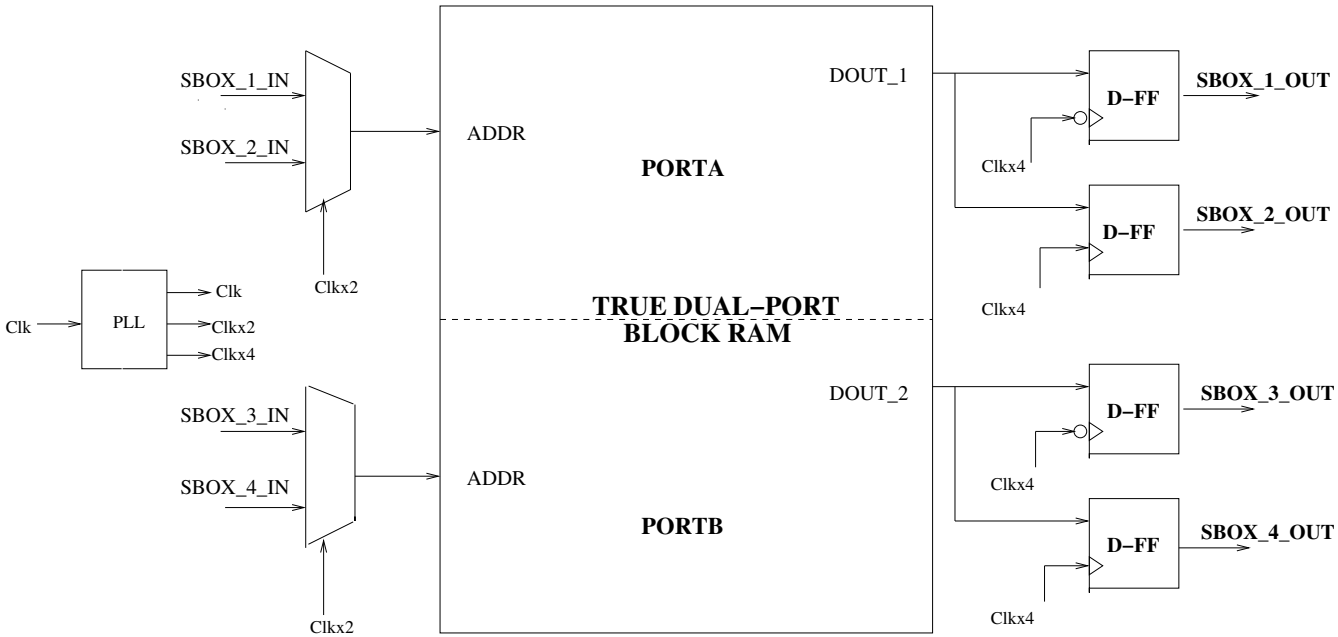
Cost Comparison on Virtex 5

	Unprotected	**RSM**	**Solution 2**
Number of LUT	1160	1957(68%)	1439(24%)
Number of 256X8 ROM	20	20	4
Number of 4096X8 ROM	0	0	16
Number of 16X128 ROM	0	3	3
Total Number of 36Kb BRAM	20	23(15%)	23(15%)
Frequency (MHz)	116.47	74.64(36%)	115.07(.01%)

Thus, >15X security at 1.24X and 1.15X overhead in logic and memory respectively.

(Complexity) Solution 3: Overclocking BRAM

A single BRAM can be overclocked to implement 2-4 sboxes.



1 Introduction
- Context
- Motivations

2 RSM: Rotating Sboxes Masking
- Rationale of the Countermeasure
- Security Evaluation

3 Optimal Implementation on Modern FPGA
- Solution 1
- Solution 2
- Solution 3

4 Conclusions and Perspectives

Conclusions and Perspectives

Conclusions

- RSM provides high-order security even with depleted entropy.
- Resist CPA and VPA, with 16 masks.
- Modern FPGAs allow to implement this countermeasures at a reasonable cost.
- Mask can be easily refreshed without time penality at reseaonable cost.

Perspectives

- Extension of presented solution to ASIC.
- Optimizing implementation of tweakable ciphers using Solution 2 & 3.

References

[DGBN09] Jean-Luc Danger, Sylvain Guilley, Shivam Bhasin, and Maxime Nassar.
Overview of Dual Rail with Precharge Logic Styles to Thwart Implementation-Level Attacks on Hardware Cryptoprocessors, — *New Attacks and Improved Counter-Measures* —.
In *SCS*, IEEE, pages 1–8, November 6–8 2009.
Jerba, Tunisia. DOI: 10.1109/ICSCS.2009.5412599.

[NGD11] Maxime Nassar, Sylvain Guilley, and Jean-Luc Danger.
Formal Analysis of the Entropy / Security Trade-off in First-Order Masking Countermeasures against Side-Channel Attacks.
In *INDOCRYPT*, volume 7107 of *LNCS*, pages 22–39. Springer, December 11-14 2011.
Chennai, India. DOI: 10.1007/978-3-642-25578-6_4.

[NSGD12] Maxime Nassar, Youssef Souissi, Sylvain Guilley, and Jean-Luc Danger.
RSM: a Small and Fast Countermeasure for AES, Secure against First- and Second-order Zero-Offset SCAs.
In *DATE*, pages 1173–1178, March 12-16 2012.
Dresden, Germany. (TRACK A: "Application Design", TOPIC A5: "Secure Systems"). On-line version: http://hal.archives-ouvertes.fr/hal-00666337/en.

[PRB09] Emmanuel Prouff, Matthieu Rivain, and Régis Bevan.
Statistical Analysis of Second Order Differential Power Analysis.
IEEE Trans. Computers, 58(6):799–811, 2009.

Optimal FPGA Implementations of a Very Low-Cost Countermeasure Based on Rotating S-Boxes Masking Countermeasure

Sylvain Guilley, **Shivam Bhasin**,
Ankit Khandelwal and Jean-Luc Danger

Institut TELECOM / TELECOM ParisTech,
46 rue Barrault, Paris, France.

Secure-IC S.A.S.,
80 avenue des Buttes de Coësmes, Rennes, France.

June 26, 2012