A High-Performance Fault Diagnosis Approach for the AES SubBytes Utilizing Mixed Bases

Mehran Mozaffari Kermani and Arash Reyhani-Masoleh

Presented by

Mehran Mozaffari Kermani

Department of Electrical and Computer Engineering

The University of Western Ontario

Outline

- Introduction
- The Advanced Encryption Standard
- Presented Fault Detection Scheme
- Complexity Analysis
- ASIC Implementations and Comparison
- Conclusions

Introduction

- The Advanced Encryption Standard (AES) is the current NIST standard used for secure communications

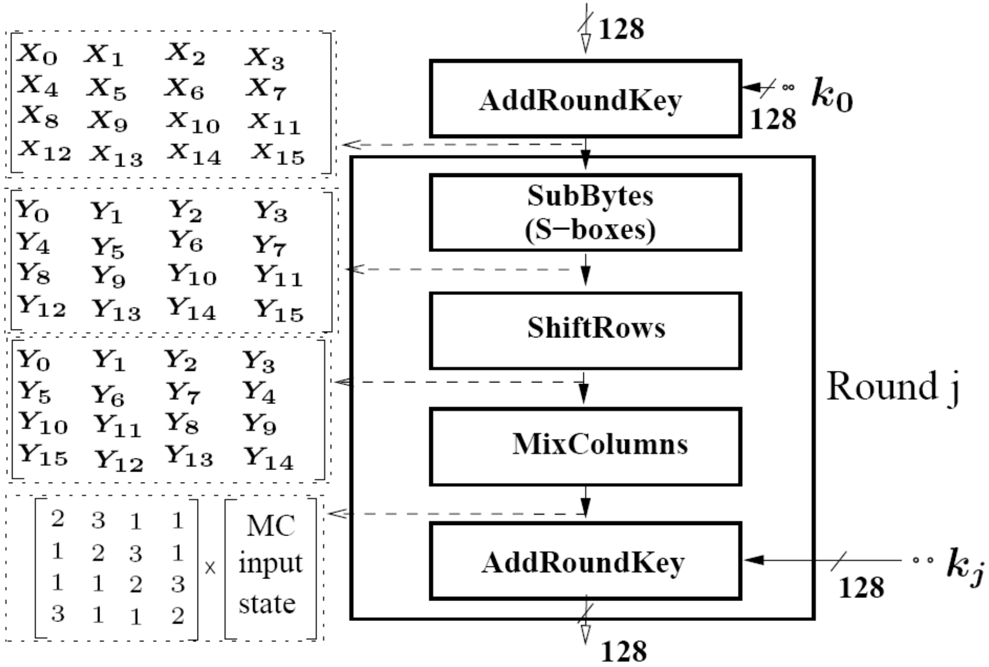
- Faults in the AES
  - Natural faults
  - Malicious faults injected by attackers

- Effective fault detection schemes
  - Acceptable error coverage
  - Low overhead in terms of area and delay

Advanced Encryption Standard (AES)

AES-128

-128-bit plaintext/key
-10 rounds
-4 transformations



$$\begin{bmatrix} X_0 & X_1 & X_2 & X_3 \\ X_4 & X_5 & X_6 & X_7 \\ X_8 & X_9 & X_{10} & X_{11} \\ X_{12} & X_{13} & X_{14} & X_{15} \end{bmatrix}$$

$$\begin{bmatrix} Y_0 & Y_1 & Y_2 & Y_3 \\ Y_4 & Y_5 & Y_6 & Y_7 \\ Y_8 & Y_9 & Y_{10} & Y_{11} \\ Y_{12} & Y_{13} & Y_{14} & Y_{15} \end{bmatrix}$$

$$\begin{bmatrix} Y_0 & Y_1 & Y_2 & Y_3 \\ Y_5 & Y_6 & Y_7 & Y_4 \\ Y_{10} & Y_{11} & Y_8 & Y_9 \\ Y_{15} & Y_{12} & Y_{13} & Y_{14} \end{bmatrix}$$

$$\begin{bmatrix} 2 & 3 & 1 & 1 \\ 1 & 2 & 3 & 1 \\ 1 & 1 & 2 & 3 \\ 3 & 1 & 1 & 2 \end{bmatrix} \times \begin{bmatrix} \text{MC input state} \end{bmatrix}$$

S-box

- The nonlinear and most complex transformation among those in the encryption of the AES is the S-boxes.

- The S-box consists of multiplicative inversion and affine transformation.

- Most commonly are implemented using look-up tables and composite fields in hardware.

S-box in Hardware

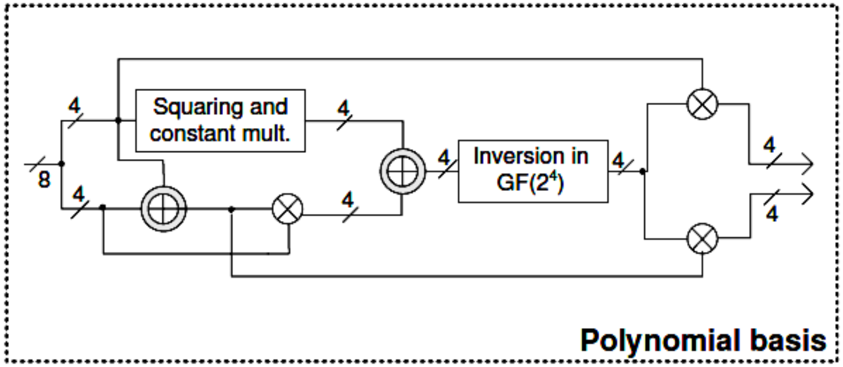
– Look-up Tables (LUTs)

- Not preferred for high performance applications
  - Because of high area and the fact that unbreakable delay of the LUTs cannot be pipelined

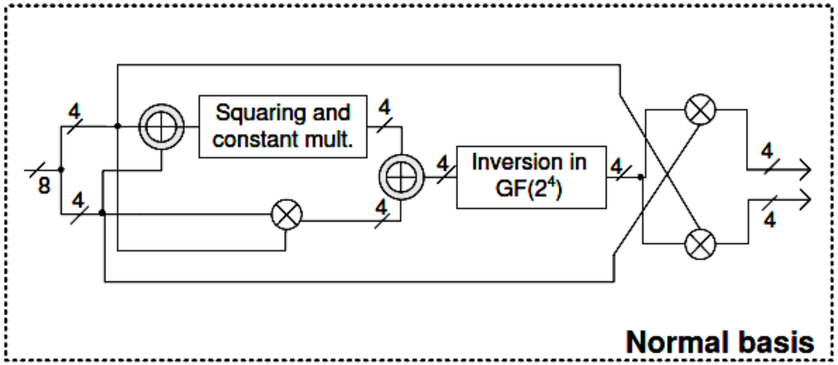
– Composite Fields

- Low area, can be sub-pipelined
- Most commonly are based on polynomial, normal, and mixed bases

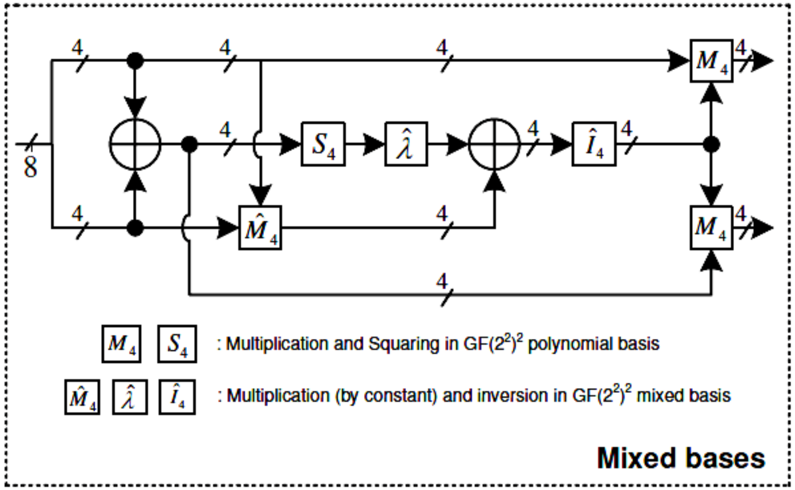
S-box Using Composite Fields



(a)



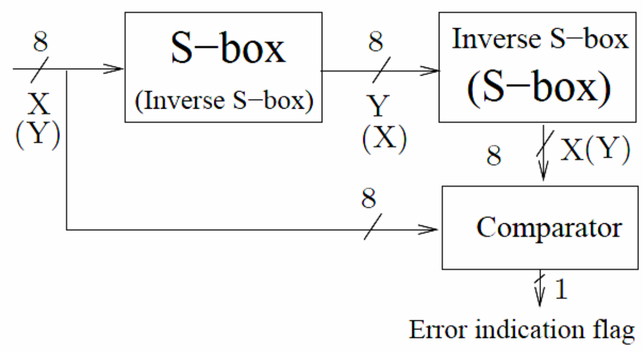
(b)


8
4
4
4
4
4
4
4
4
4
4
M_4
S_4
$\hat{\lambda}$
$\hat{I}_4$
$\hat{M}_4$
M_4
M_4 S_4 : Multiplication and Squaring in GF($(2^2)^2$) polynomial basis
$\hat{M}_4$ $\hat{\lambda}$ $\hat{I}_4$: Multiplication (by constant) and inversion in GF($(2^2)^2$) mixed basis
Mixed bases

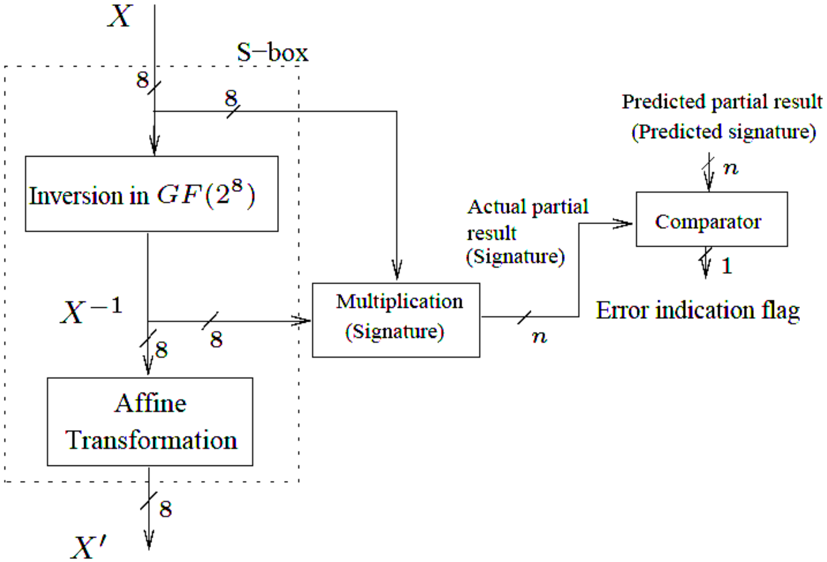
(c)

[28] Y. Nogami, K. Nekado, T. Toyota, N. Hongo, and Y. Morikawa, "Mixed Bases for Efficient Inversion in $F_{((2^2)^2)^2}$ and Conversion Matrices of SubBytes of AES," *In Proc. of CHES '10*, pp. 234-247, Aug. 2010.

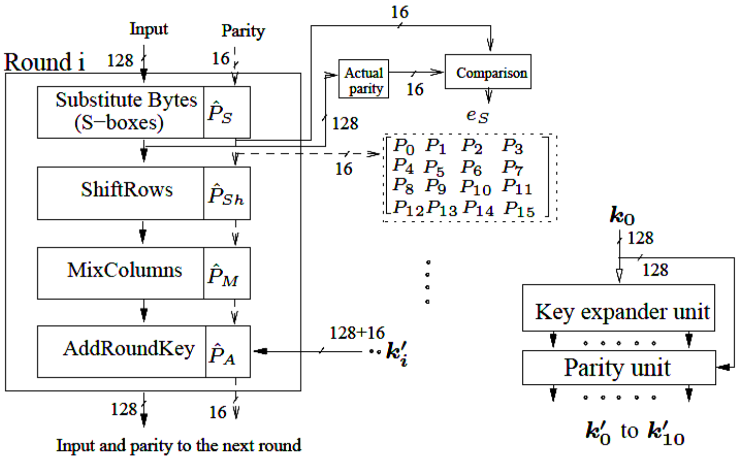
Previous Works



Redundancy-based

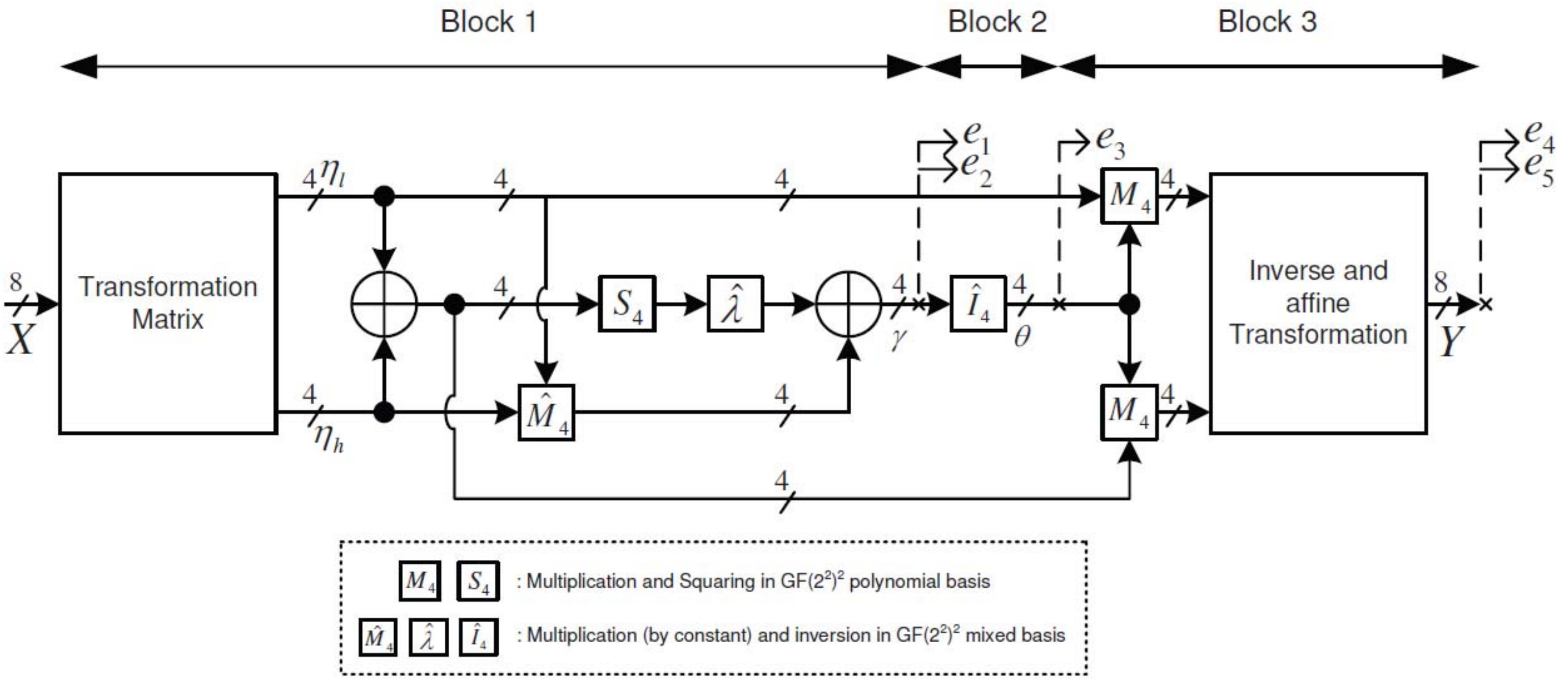


Multiplication-based



Parity-based

Proposed Fault Detection Scheme

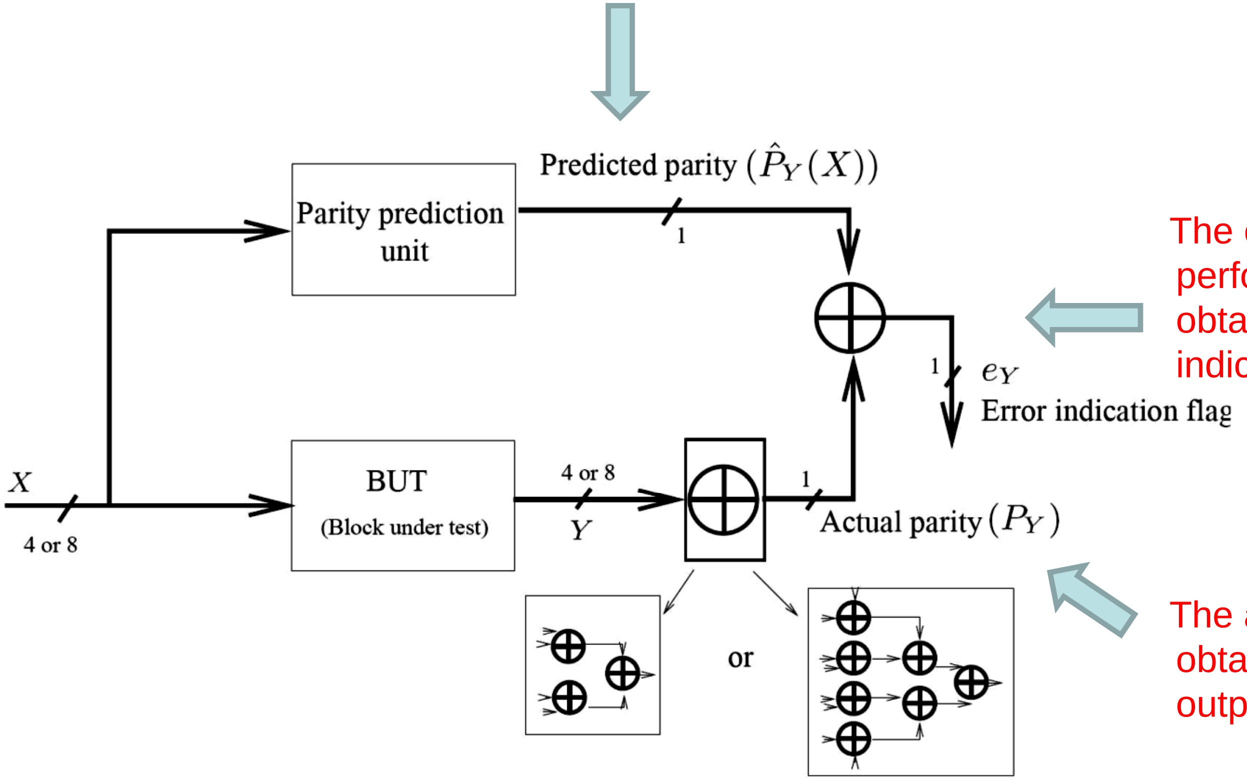

Block 1
Block 2
Block 3
8
X
Transformation Matrix
4 η_l
4
4
e_1
e_2
e_3
M_4
4
S_4
$\hat{\lambda}$
4
γ
$\hat{I}_4$
4
θ
4
η_h
$\hat{M}_4$
4
M_4
4
4
Inverse and affine Transformation
8
Y
e_4
e_5
M_4 S_4 : Multiplication and Squaring in GF(2^2)^2 polynomial basis
$\hat{M}_4$ $\hat{\lambda}$ $\hat{I}_4$: Multiplication (by constant) and inversion in GF(2^2)^2 mixed basis

S-box in mixed basis structure

-The operations are divided into 3 blocks.
-5 predicted parities (error flags) are obtained for the entire operations.

Fault Detection Scheme (cont.)

The predicted parity is obtained as the function of the inputs



The comparison is performed to obtain the error indication flag

The actual parity is obtained from the outputs of BUT

Error indication for each block used in the fault detection scheme.

Parity Predictions

Theorem: *The parity predictions for the 3 blocks of the S-box using mixed basis in the presented fault detection scheme are as follows:*

$$\hat{P}_1 = x_6(x_7 + x_5 + x_0) + x_5 Z_3 + x_4(Z_7 + Z_1 + x_2) + x_2(\overline{x_5 + x_3}) + x_1 Z_1 + (x_7 \vee x_4) + (x_5 \vee x_1),$$

$$\hat{P}_2 = x_6(Z_4 + x_1 + x_0) + x_4\overline{Z_6} + x_3 x_7 + x_0 Z_2 + (x_7 \vee x_5) + (x_2 \vee x_1),$$

$$\hat{P}_3 = (\gamma_3\gamma_1 \vee \gamma_2) + \gamma_3\gamma_2\gamma_0,$$

$$\hat{P}_4 = \theta_3(Z_4 + Z_3 + x_6) + \theta_2(Z_8 + x_4) + \theta_1(Z_6 + x_6) + \theta_0(Z_5 + Z_2 + x_2),$$

$$\hat{P}_5 = \theta_3(Z_8 + Z_4) + \theta_2(Z_7 + x_7) + \theta_1(Z_9 + Z_5) + \theta_0(Z_5 + x_7 + x_1),$$

where $Z_1 = x_3 + x_0$, $Z_2 = x_5 + x_1$, $Z_3 = Z_2 + Z_1$, $Z_4 = x_7 + x_2$, $Z_5 = x_6 + x_3$, $Z_6 = Z_1 + x_5$, $Z_7 = x_6 + x_1$, $Z_8 = Z_7 + x_0$, *and* $Z_9 = Z_5 + Z_2$.

Parity Predictions (Other Variants)

Based on the reliability requirements and available resources, one may use different number of predicted parities, e.g., merging the ones for the first and last blocks:

$$\hat{P}_{1+2} = \eta_7(\eta_3 + \eta_1) + \eta_6(\eta_2 + \eta_0) + \eta_5\eta_3 + \eta_4\eta_2 + \eta_7 + \eta_4 + \eta_3 + \eta_0,$$

$$\hat{P}_{4+5} = \theta_3(\eta_6 + \eta_5 + \eta_3 + \eta_2 + \eta_1) + \theta_2(\eta_7 + \eta_6 + \eta_4 + \eta_3 + \eta_0) + \theta_1(\eta_7 + \eta_5 + \eta_3 + \eta_1 + \eta_0) + \theta_0(\eta_6 + \eta_4 + \eta_2 + \eta_1).$$

Error Simulations

Error Model:

- In this paper, we use stuck-at error model. The objective in using this model is to cover the malicious and natural errors caused by bit flips.
- In fault attacks, single error injection is the ideal case for gaining the maximum information. Nevertheless, due to technological constraints, a more realistic error model is to inject multiple errors.

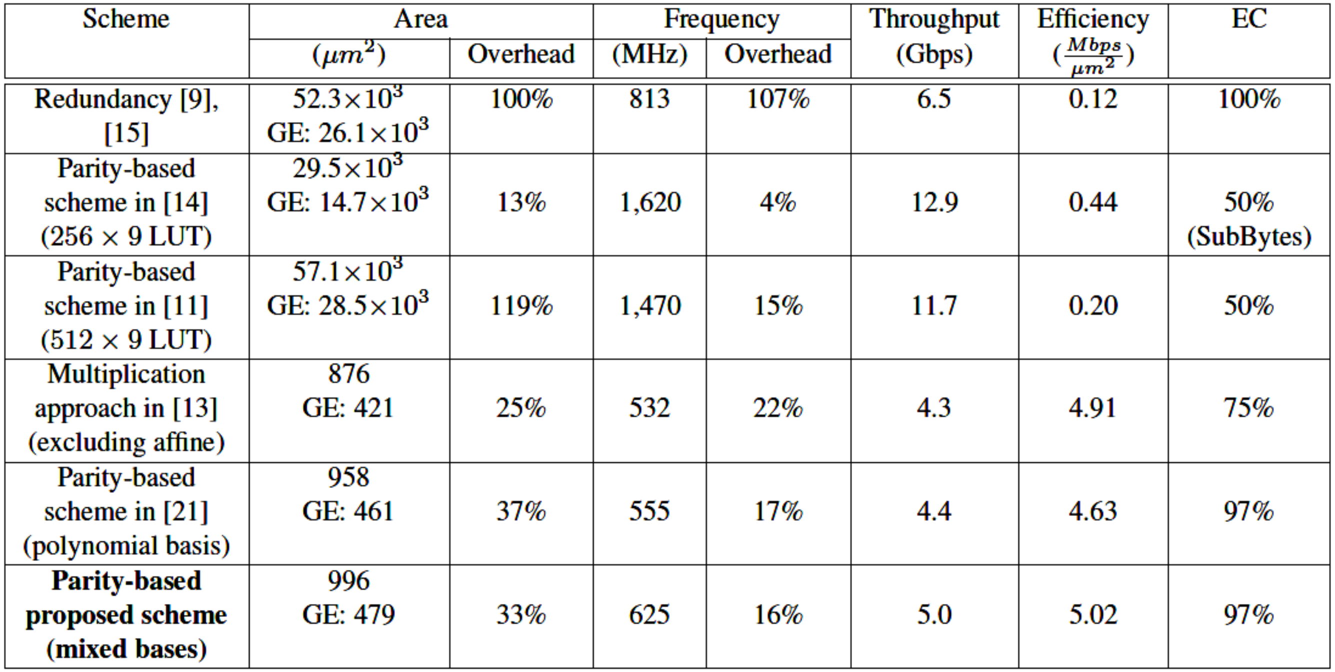
Our Scheme:

- Single stuck-at errors happening at the output of each S-box block are covered 100% in the proposed scheme.
- We have used LSFRs for multiple random error injections.
- After injecting 200,000 multiple errors, the error coverage of close to 100% is obtained.

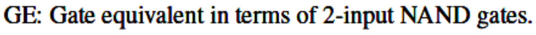
Performance Comparison on ASIC

- We have used the STM 65-nm CMOS standard technology.
- VHDL has been used as the design entry for different fault diagnosis approaches.
- The Synopsys Design Compiler has been utilized for specifying the constraints and performing the synthesis.

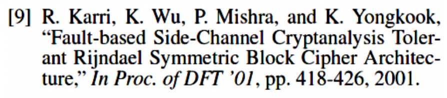
Performance Comparison on ASIC



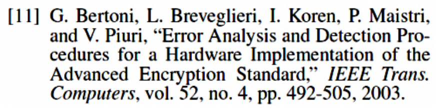
Scheme	Area		Frequency		Throughput	Efficiency	EC
	(μm^2)	Overhead	(MHz)	Overhead	(Gbps)	($\frac{Mbps}{\mu m^2}$)	
Redundancy [9], [15]	52.3×10^3 GE: 26.1×10^3	100%	813	107%	6.5	0.12	100%
Parity-based scheme in [14] (256×9 LUT)	29.5×10^3 GE: 14.7×10^3	13%	1,620	4%	12.9	0.44	50% (SubBytes)
Parity-based scheme in [11] (512×9 LUT)	57.1×10^3 GE: 28.5×10^3	119%	1,470	15%	11.7	0.20	50%
Multiplication approach in [13] (excluding affine)	876 GE: 421	25%	532	22%	4.3	4.91	75%
Parity-based scheme in [21] (polynomial basis)	958 GE: 461	37%	555	17%	4.4	4.63	97%
Parity-based proposed scheme (mixed bases)	996 GE: 479	33%	625	16%	5.0	5.02	97%



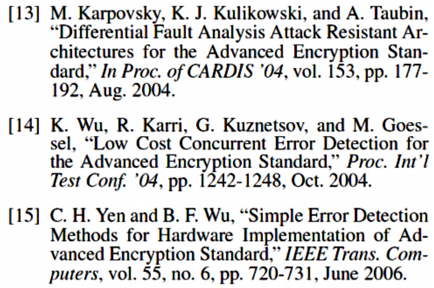
GE: Gate equivalent in terms of 2-input NAND gates.



[9] R. Karri, K. Wu, P. Mishra, and K. Yongkook, "Fault-based Side-Channel Cryptanalysis Tolerant Rijndael Symmetric Block Cipher Architecture," *In Proc. of DFT '01*, pp. 418-426, 2001.



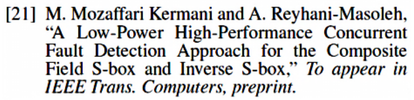
[11] G. Bertoni, L. Breveglieri, I. Koren, P. Maistri, and V. Piuri, "Error Analysis and Detection Procedures for a Hardware Implementation of the Advanced Encryption Standard," *IEEE Trans. Computers*, vol. 52, no. 4, pp. 492-505, 2003.



[13] M. Karpovsky, K. J. Kulikowski, and A. Taubin, "Differential Fault Analysis Attack Resistant Architectures for the Advanced Encryption Standard," *In Proc. of CARDIS '04*, vol. 153, pp. 177-192, Aug. 2004.

[14] K. Wu, R. Karri, G. Kuznetsov, and M. Goessel, "Low Cost Concurrent Error Detection for the Advanced Encryption Standard," *Proc. Int'l Test Conf. '04*, pp. 1242-1248, Oct. 2004.

[15] C. H. Yen and B. F. Wu, "Simple Error Detection Methods for Hardware Implementation of Advanced Encryption Standard," *IEEE Trans. Computers*, vol. 55, no. 6, pp. 720-731, June 2006.



[21] M. Mozaffari Kermani and A. Reyhani-Masoleh, "A Low-Power High-Performance Concurrent Fault Detection Approach for the Composite Field S-box and Inverse S-box," *To appear in IEEE Trans. Computers, preprint.*

Conclusions

- We have presented a lightweight concurrent fault detection scheme for the composite field realization of SubBytes using mixed basis.

- The presented fault detection scheme has low area cost and negligible degradation in the frequency (reaching the efficiency of 5020 Gbps/mm^2 while maintaining the throughput of 5 Gbps).

- The presented scheme has the error coverage of close to 100% for the entire SubBytes, suitable for secure environments.

- The presented scheme is also applicable for the inverse S-box and the merged structures.

Thank you!