4.4 The SCCs Functions for the Four Stages

By [Eq. 9, 11] and the four AES stages' functions [Eq. 1, 2, 3, 4], we have the SCC predictor functions as:

- AddRoundKey ($P_{det} \geq 1 - \frac{2}{2^8} = 99.2\%$):
$$\omega_{\text{AddRoundKey}} = (a_{i,j} \oplus k_{i,j})^3. \tag{13}$$
- SubBytes ($P_{det} \geq 1 - \frac{2}{2^8} = 99.2\%$):
$$\omega_{\text{SubByte}} = (M_{inv} \otimes a_{i,j} \oplus M_{aff})^3. \tag{14}$$
with $P_{det} \geq 1 - \frac{2}{2^8} = 99.2\%$.
- ShiftRows ($P_{det} \geq 1 - \frac{1}{2^8} = 99.6\%$), each row with two SCCs denoted by α, β:

$$\begin{aligned}
\omega_{\text{ShiftRows0-}\alpha} &= (a_{0,0} \otimes a_{0,1}), & \omega_{\text{ShiftRows0-}\beta} &= (a_{0,2} \otimes a_{0,3});\\
\omega_{\text{ShiftRows1-}\alpha} &= (a_{1,1} \otimes a_{1,2}), & \omega_{\text{ShiftRows1-}\beta} &= (a_{1,3} \otimes a_{1,0});\\
\omega_{\text{ShiftRows2-}\alpha} &= (a_{2,2} \otimes a_{2,3}), & \omega_{\text{ShiftRows2-}\beta} &= (a_{2,0} \otimes a_{2,1});\\
\omega_{\text{ShiftRows3-}\alpha} &= (a_{3,3} \otimes a_{3,0}), & \omega_{\text{ShiftRows3-}\beta} &= (a_{3,1} \otimes a_{3,2}).
\end{aligned} \tag{15}$$

- MixColumns ($P_{det} \geq 1 - \frac{1}{2^8} = 99.6\%$), each column with two SCCs denoted by α, β:

$$\begin{aligned}
\omega_{\text{MixColumns-}\alpha} =& (2a_{0,j} \oplus 3a_{1,j} \oplus a_{2,j} \oplus a_{3,j})\\
&\otimes (a_{0,j} \oplus 2a_{1,j} \oplus 3a_{2,j} \oplus a_{3,j});\\
\omega_{\text{MixColumns-}\beta} =& (a_{0,j} \oplus a_{1,j} \oplus 2a_{2,j} \oplus 3a_{3,j})\\
&\otimes (3a_{0,j} \oplus a_{1,j} \oplus a_{2,j} \oplus 2a_{3,j}).
\end{aligned} \tag{16}$$

The decoders are to verify [Eq. 13, 14, 15, 16] under the existence of errors. The error correction probability for lazy errors (lasts for at least 3 rounds) is 100%.

5 EVALUATION

We expanded and optimized the four predictor functions [Eq. 13, 14, 15, 16] over finite field $GF(2^8)$, as well as the decoder functions. Thus the overlay of $g(f())$ functions in the Robust predictors can be precomputed into a simpler function instead of applying $f()$ and $g()$ successively and separately. In our experimentation, we injected 4,019,798 errors of various complexities in the computation stages and measure the error detection rates. To test the lazy error correction capability, the errors are made to last for at least 3 rounds in a given stage, such that [Eq. 10 & 12] can be computed. We used the Xilinx Vertex 7 XC7VX330T FPGA board for our implementations and testing.

Table 1: Hardware and Timing Overhead

Stages	P_{det}	**Overhead** (C-AED)	**Overhead** (C-AED-AEC)
AddRoundKey	99.4%	56.3%	92.7%
SubBytes	99.3%	63.7%	101.3%
ShiftRows	99.6%	80.3%	144.0%
MixColumns	99.6%	77.9%	132.9%

[I] Hardware Overhead = $\frac{\text{Stage + Predictor + Decoder}}{\text{Stage}} - 1$.

The P_{det} for the AddRoundKey and SubBytes stages is below $(1 - \overline{P_{mask}} = 99.6\%)$, because there exists no error satisfying their EMEs in cubic forms. In contrast, there is always a solution satisfying the EMEs equations for the ShiftRows and MixColumns stages. The implementation overhead associated with the error detection plus the error correction (C-AED-AEC) is larger than that of the error detection alone (C-AED). This increase is due to the fact that questions [Eq. 10 & 12] are more complex when compared to the error detection decoders. Altogether, the additional cost is justified since the implementation supports a stronger error tolerance capability.

6 CONCLUSION

In this paper, we have proposed a new technique to harden the reliability and security of AES hardware implementations using a non-linear code self-checking checkers. The proposed method shows key advantages over conventional linear approaches. Unlike the linear ECC approaches, the non-linear technique can (a) detect any injected error with a high probability and (b) guarantee the correction of all lazy errors, which commonly appear in high speed AES hardware implementations. In addition, since the new scheme is built upon error control codes, its performance and capability can be analyzed and estimated using mathematical models. The strong theoretical modeling foundation makes it possible for designers to evaluate and determine the cost/performance trade-off with high accuracy.

7 ACKNOWLEDGMENTS

This research is partially supported by the NSF grant (No. CNS-1745808).

REFERENCES

[1] Luca Breveglieri, Israel Koren, and Paolo Maistri. 2005. Incorporating error detection and online reconfiguration into a regular architecture for the advanced encryption standard. *Defect and Fault Tolerance in VLSI Systems, 2005. DFT 2005. 20th IEEE International Symposium on. IEEE* (2005).

[2] Joan Daemen and Vincent Rijmen. 2013. The design of Rijndael: AES-the advanced encryption standard. *Springer Science and Business Media* (2013).

[3] G. Gaubatz, B. Sunar, and M. G. Karpovsky. 2006. Non-linear residue codes for robust public-key arithme. *Fault Diagnosis and Tolerance in Cryptography* (2006).

[4] Marc Joye and Amir Moradi. 2015. Smart Card Research and Advanced Applications. *Springer International Publishing* (2015).

[5] Ramesh Karri, Kaijie Wu, Piyush Mishra, and Yongkook Kim. 2001. Fault-Based Side-Channel Cryptanalysis Tolerant Rijndael Symmetric Block Cipher Architecture. *Defect and Fault Tolerance in VLSI Systems, 2001. Proceedings. 2001 IEEE International Symposium on. IEEE* (2001).

[6] Konrad Kulikowski, Mark Karpovsky, and Alexander Taubin. 2005. Robust codes for fault attack resistant cryptographic hardware. *Fault Diagnosis and Tolerance in Cryptography, 2nd International Workshop* (2005).

[7] K. Kulikowski, Z. Wang, and M. G. Karpovsky. 2008. Comparative analysis of robust fault attack resistant architectures for public and private cryptosystems. *IEEE 5th Workshop on Fault Diagnosis and Tolerance in Cryptography* (2008).

[8] Nachiketh R. Potlapally, Srivaths Ravi, Anand Raghunathan, and Niraj K. Jha. 2003. Analyzing the energy consumption of security protocols. *Proceedings of the 2003 international symposium on Low power electronics and design. ACM* (2003).

[9] Emmanuel Prouff. 2005. DPA attacks and S-boxes. *nternational Workshop on Fast Software Encryption* (2005).

[10] Cyril Roscian, Jean-Max Dutertre, and Assia Tria. 2013. Frontside laser fault injection on cryptosystems-Application to the AES last round. *Hardware-Oriented Security and Trust (HOST), 2013 IEEE International Symposium on. IEEE* (2013).

[11] Chih-Hsu Yen and Bing-Fei Wu. 2006. Simple error detection methods for hardware implementation of advanced encryption standard. *IEEE transactions on computers* (2006).

[12] W. Zhen, M. Karpovsky, and K. J. Kulikowski. 2009. Replacing linear hamming codes by robust nonlinear codes results in a reliability improvement of memories. *IEEE/IFIP International Conference on Dependable Systems and Networks* (2009).