Invariance-based CED architecture

- An AES Encryption Round can be represented as:
\[ A(K)(M(S(B(X)))) \]
- Invariance holds true for one AES round:
\[ A(K)(M(S(B(X)))) = P^{-1}(A(P(K))(M(S(B(P(X)))))) \]

FPGA Implementation

- Implement both AES encryption and decryption on Xilinx Virtex-4 and Virtex-5 FPGA families.
- Invariance-based CED achieves the highest fault coverage rate compared to previously proposed techniques.
- Invariance-based CED achieves lowest hardware overhead in AES encryption and has only 0.5% overhead in decryption and the most compact technique [5]
- Invariance-based CED has a slight delay overhead compared to the original AES implementation.

Fault Simulation

- 100% fault coverage for single-bit and single-byte stuck-at fault
- 99.99999997% fault coverage for multiple burst faults
- 10\(^{3}\) fault miss rate reduction compared to the state-of-the-art parity-based CED scheme [5]
- Near 100% fault coverage for multiple random faults

References


Acknowledgements

This work was supported by National Science Foundation, Cyber Trust Program

Invariance

- Invariance-based concurrent error detection scheme (CED) achieves 100% coverage for single-bit and single-byte fault.
- The scheme also provides 99.99999997% fault coverage rate with minimum hardware and performance overhead.
- The scheme is S-box implementation independent.
- The scheme applies to both AES encryption and decryption.