DAC Young Fellows

DESIGN AUTOMATION CONFERENCE 60
FROM CHIPS TO SYSTEMS — LEARN TODAY, CREATE TOMORROW

S-box designs for an open-source AES ASIC

Phaedra Curlin, Calvin Chan, Tamara Lehman – University of Colorado Boulder

Motivation

- Cryptographic ASICs becoming increasingly popular
- Not many open-source designs (HDL/taped out)

Advanced Encryption Standard (AES)

- Symmetric block cipher
  - 128-bit block state
  - 128/192/256-bit keys
  - 10/12/14 rounds
- **`SubBytes`** → S-box
  - Non-linear
  - 256-byte substitution table
  - Computed using matrix transform + polynomial division
  - *How to compute S-box values in hardware?*

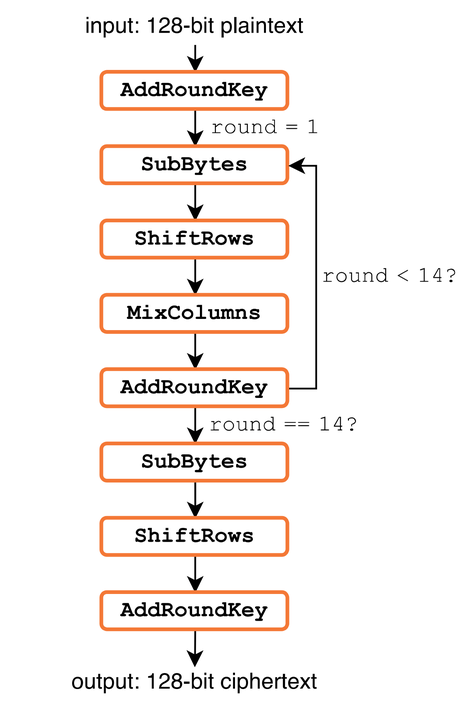

Figure 1: Cipher for 256-bit key encryption

S-box Design Optimizations

- **Area**: reduce footprint/cost
- **Power**: select gates minimize power
- **Throughput**: reduce critical path delay/registers used
- **Security**: masking/hiding schemes to prevent leakage
- **Randomness**: limit the dependence on an RNG

S-box Implementations

Look-Up Table (LUT)

- Pre-computed 256 bytes in a read-only memory/HDL case statements

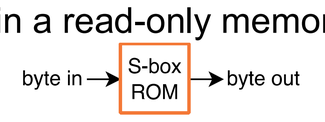

Figure 2: Example LUT-based S-box

Permutation Function

- Decode-Permute-Encode structure, one-hot representation

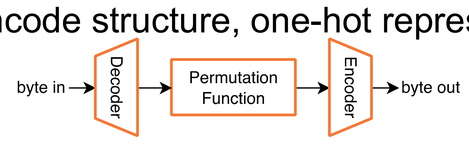

Figure 3: Permutation S-box

Binary Decision Diagram (BDD)

- BDD representation of S-box using MUXes

Positive-Polarity Reed Muller (PPRM)

- AND-XOR representation of S-box values

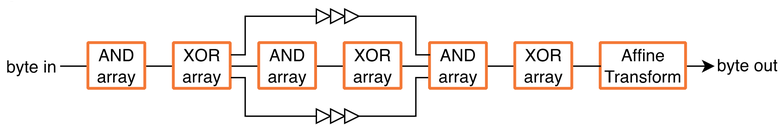

Figure 5: PPRM S-box

Composite Field

- Uses finite field properties to compute values

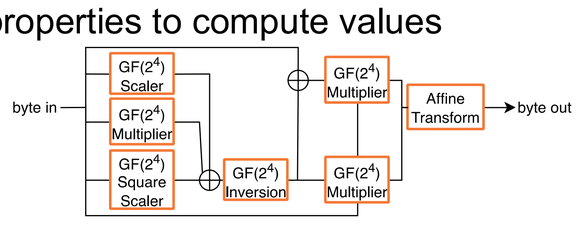

Figure 6: Example composite field S-box

Logically Optimized

- Optimize composite field design using heuristic algorithms

S-box Defenses

Provably Secure Masking

- Black-box, static model security

Threshold Implementations (TI)

- Divides secret variables of S-box into shares

Domain-Oriented Masking

- Divides secret variables into domains

Wave Dynamic Dual-rail Pre-charge Logic (WDDL)

- Hide power consumption using a propagation wave

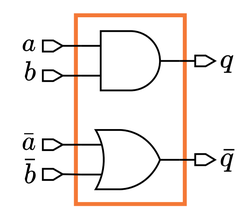

Figure 7: WDDL 2-input AND gate

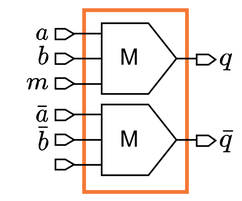

Figure 8: MDPL 2-input AND gate with mask bit.

Masked Dual-rail Pre-charge Logic (MDPL)

- Gate-level masking

Adiabatic Circuit

- Uses power clock, reversible logic

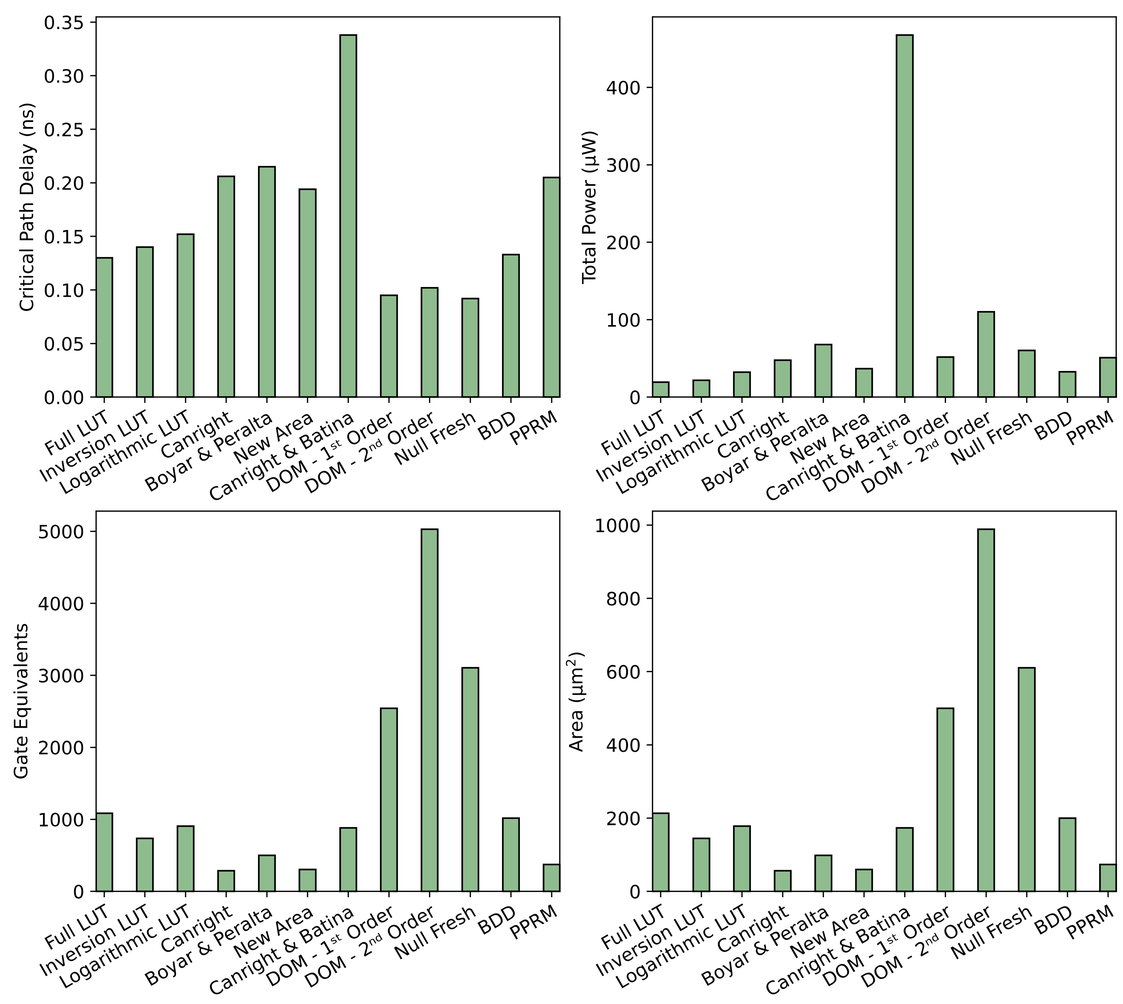

Figure 9: Evaluated AES S-boxes from the literature [1-7] using Silvaco's Open-Cell 15nm library [8].

Conclusion & Future Work

- Many AES S-box implementations suited for different needs
- Implement state-of-the-art S-box designs for each optimization into AES and tape out design

References

1. D. Canright, "A Very Compact S-Box for AES," in *Cryptographic Hardware and Embedded Systems – CHES 2005*, J. R. Rao and B. Sunar, Eds., Berlin, Heidelberg: Springer Berlin Heidelberg, 2005, pp. 441–455.
2. J. Boyar and R. Peralta, "A Small Depth-16 Circuit for the AES S-Box," in *Information Security and Privacy Research*, D. Gritzalis, S. Furnell, and M. Theoharidou, Eds., Berlin, Heidelberg: Springer Berlin Heidelberg, 2012, pp. 287–298.
3. A. Reyhani-Masoleh, M. Taha and D. Ashmawy, "New Area Record for the AES Combined S-Box/Inverse S-Box," 2018 *IEEE 25th Symposium on Computer Arithmetic (ARITH)*, Amherst, MA, USA, 2018, pp. 145-152, doi: 10.1109/ARITH.2018.8464780.
4. D. Canright and L. Batina, "A Very Compact 'Perfectly Masked' S-Box for AES," in *Applied Cryptography and Network Security*, S. M. Bellovin, R. Gennaro, A. Keromytis, and M. Yung, Eds., Berlin, Heidelberg: Springer Berlin Heidelberg, 2008, pp. 446–459.
5. H. Gross, S. Mangard, and T. Korak, "Domain-Oriented Masking: Compact Masked Hardware Implementations with Arbitrary Protection Order," in *Proceedings of the 2016 ACM Workshop on Theory of Implementation Security*, in TIS '16. New York, NY, USA: Association for Computing Machinery, 2016, p. 3.
6. A. Rezaei Shahmirzadi and A. Moradi, "Re-Consolidating First-Order Masking Schemes: Nullifying Fresh Randomness," *IACR Transactions on Cryptographic Hardware and Embedded Systems*, vol. 2021, no. 1, pp. 305–342, Dec. 2020,
7. S. Morioka and A. Satoh, "An Optimized S-Box Circuit Architecture for Low Power AES Design," in *Cryptographic Hardware and Embedded Systems - CHES 2002*, B. S. Kaliski, çetin K. Koç, and C. Paar, Eds., Berlin, Heidelberg: Springer Berlin Heidelberg, 2003, pp. 172–186.
8. Silvaco, Inc. "15nm Open-Cell Library and 45nm FreePDK". 2022. https://si2.org/open-cell-library/

University of Colorado **Boulder**

Sandia National Laboratories