SAND2019-8176D

The Center for Cyber Defenders

Expanding computer security knowledge

Tailoring to a Fabric for Fit and Efficiency

Sew you want to design in fabric? One design may seam right but another may better suit.

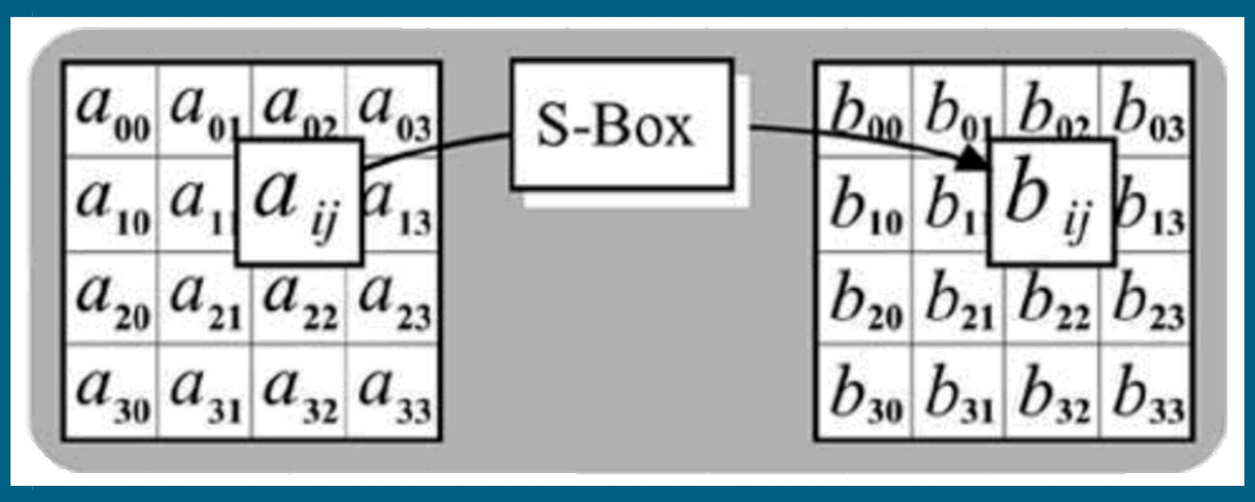
Ken Goss, University of Missouri
Mentor: Andrew N. Fisher, Org: 5846

Problem Statement:

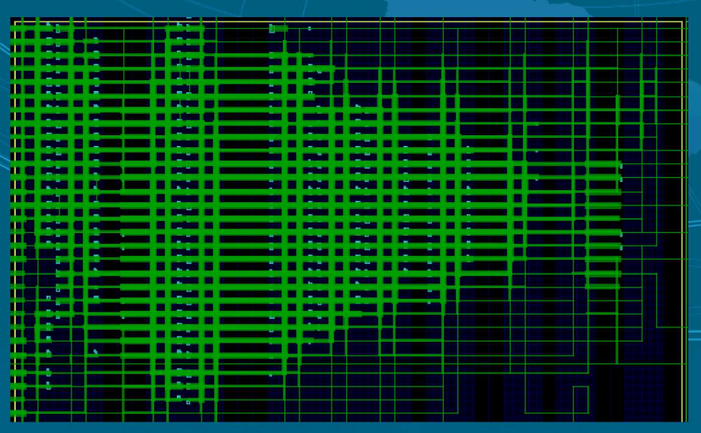
- AES is an important functionality implemented in fabric, & multiple means of implementation exist
- Analyze these various means of implementation for the S-box component of AES in particular and measure their resource use
- Propose situations in which the tradeoffs may each be beneficial for a target setting

Objectives and Approach:

- AES encryption and decryption are applications which are often implemented in a variety of hardware settings
- There is significant interest in optimizing the implementation of AES for a number of criteria such as area(hardware use) power, or throughput
- The S-Box step provides a wide array of implementation methods



- Look-up table (LUT)
- Direct calculation in GF(2^8)
- Calculation via the use of subfields
- Calculation via isomorphic groups and changing representation



Results:

- Benefits are highly dependent on resources available
- Block RAM presence is the key discriminator between the primary types (LUT vs EE)

Type	Gate Eq use
Naive	859978
LUT BRAM Conv	3220096
LUT	20096+5BRAM
Subfield	518000
Isomorph + Subfield opt.	192896

Impact and Benefits:

- Understanding the mathematical underpinning of algorithms allows for functionally equivalent, more efficient implementations
- Understanding the resource availability of a particular hardware architecture allows for the tailoring of optimizations for the resources available
- Understanding both allows for optimal performance to be achieved for the particular pairing of functionality and hardware

[1] D. Canright, "A very compact S-box for AES," in *International Workshop on Cryptographic Hardware and Embedded Systems*, 2005, pp. 441–455.

[2] A. Rudra, P. K. Dubey, C. S. Jutla, V. Kumar, J. R. Rao, and P. Rohatgi, "Efficient Rijndael encryption implementation with composite field arithmetic," in *International Workshop on Cryptographic Hardware and Embedded Systems*, 2001, pp. 171–184.

[3] T. Ichikawa, T. Kasuya, and M. Matsui, "Hardware Evaluation of the AES Finalists.," in *AES Candidate Conference*, 2000, pp. 279–285.

[4] B. Weeks, M. Bean, T. Rozylowicz, and C. Ficke, "Hardware Performance Simulations of Round 2 Advanced Encryption Standard Algorithms.," in *AES Candidate Conference*, 2000, pp. 286–304.

Sandia National Laboratories

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology and Engineering Solutions of Sandia, LLC., a wholly owned subsidiary of Honeywell International, Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525. SAND2017-XXXXC.

U.S. DEPARTMENT OF ENERGY | NNSA National Nuclear Security Administration