Secured Embedded Architecture Laboratory (SEAL)

Parsimonious Design Strategy for Linear Layers with High Diffusion in Block Ciphers

Sikhar Patranabis, Debapriya Basu Roy, Yash Shrivastava, Debdeep Mukhopadhyay, and Santosh Ghosh

Department of Computer Science and Engineering, IIT Kharagpur
Intel Labs, Oregon

http://cse.iitkgp.ac.in/resgrp/seal/

INTRODUCTION

Linear Layers in Block Ciphers

Necessary Building Blocks

- Linear layers are crucial building blocks in the design of block ciphers

Security and Efficiency

- Provide the much needed diffusion
- Ensure low implementation costs

Systematic Design Techniques

- Limited work on generic construction techniques
- Need to combine both efficiency and security requirements

Objectives

A New Design Technique

- A hierarchical design technique for lightweight linear layers
- Technique applies to SPN block ciphers such as AES, PRESENT and PRIDE

Practical Demonstration of Proposed Technique

- Case Study on PRIDE
- Alternative linear layer designed using our new technique

Notion of Lightweightness

- Standard metric for testing lightweightness of any design is the ***area footprint on chip***
  - In ASIC based implementations, the aim is to reduce the Gate Equivalent of the design
  - On FPGA, the number of LUTs (look up tables) is minimized
- Ensure that the design functions at low frequency (usually around 100KHz) with less energy consumption
- Ensure optimal area-throughput product of the design

A POSSIBLE DESIGN TECHNIQUE

MDS Matrices for Linear Layers

- MDS matrices are suitable for linear layers due to their good diffusion properties.
- Must have a minimum number of ones in each row and each column to achieve desirable diffusion
- However, MDS matrices are not inherently lightweight by construction

Combining Lightweightness with MDS Properties

- Choose MDS matrices with lightweight roots that have less hardware requirements
- Implement these lightweight roots in hardware
- Iterate them to obtain the necessary diffusion properties
- Example : PHOTON linear layer

Challenges: Not Too Generic!!!

- The space for MDS matrices is too large
- For 32x32 binary MDS matrices with adequate diffusion levels, the space is almost as large as 2^{896}!!
  - Too large to search for MDS matrices with lightweight roots

OUR PROPOSED DESIGN TECHNIQUE

An Alternative Approach

- Start from lightweight matrices *A* of the form

$$A = \begin{pmatrix} 0 & 1 & 0 & 0 & \cdots & 0 \\ 0 & 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & \cdots & 1 \\ Z_1 & Z_2 & Z_3 & Z_4 & \cdots & Z_m \end{pmatrix}$$

or

$$A = \begin{pmatrix} Z_1 & Z_2 & Z_3 & Z_4 & \cdots & Z_m \\ 1 & 0 & 0 & 0 & \cdots & 0 \\ 0 & 1 & 0 & 0 & \cdots & 0 \\ 0 & 0 & 1 & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 1 & 0 \end{pmatrix}$$

An Alternative Approach (contd.)

- Iterate the underlying as many times as required to arrive at desired MDS matrix
- Search space for optimal choice much smaller : **reduced to the last row only**
- Can still be large for large dimension matrices

Divide and Conquer : Block Interleaving

- Construct the larger linear layer L from smaller linear layers $L_1, L_2,\ldots.L_k$

$$L = \begin{pmatrix} L_1 & \varnothing & \varnothing & \varnothing & \cdots & \varnothing \\ \varnothing & L_2 & \varnothing & \varnothing & \cdots & \varnothing \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ \varnothing & \varnothing & \varnothing & \varnothing & \cdots & L_k \end{pmatrix}$$

- Ensure the smaller layers are optimally constructed from underlying lightweight matrices
- The diffusion of the smaller layers *guarantees diffusion for the larger linear layer* L

Secured Embedded Architecture Laboratory (SEAL)

AN ILLUSTRATION OF THE PROPOSED TECHNIQUE

- **Aim** : Construct 4 x 4 MDS matrix L over $GF(2^8)$ with target differential and linear branch number 5

- **Step-1** : Choose the underlying smaller lightweight matrices optimally via exhaustive search

$$A_{1,2^8} = \begin{pmatrix} 0 & 1 \\ 1 & 3 \end{pmatrix} \quad A_{2,2^8} = \begin{pmatrix} 3 & 1 \\ 1 & 0 \end{pmatrix}$$

- **Step-2** : Iterate 4 times to arrive at the desired smaller MDS matrices

$$L_{1,2^8} = \begin{pmatrix} 4 & 15 \\ 15 & 21 \end{pmatrix} \quad L_{2,2^8} = \begin{pmatrix} 21 & 15 \\ 15 & 4 \end{pmatrix}$$

- Combine to form the final linear layer

$$L_{2^8} = \begin{pmatrix} 4 & 15 & 0 & 0 \\ 15 & 21 & 0 & 0 \\ 0 & 0 & 21 & 15 \\ 0 & 0 & 15 & 4 \end{pmatrix}$$

- Comparison with PRIDE matrix : our matrix has 20% better diffusion properties with only 10% increase in area overhead

Comparison With Other Approaches

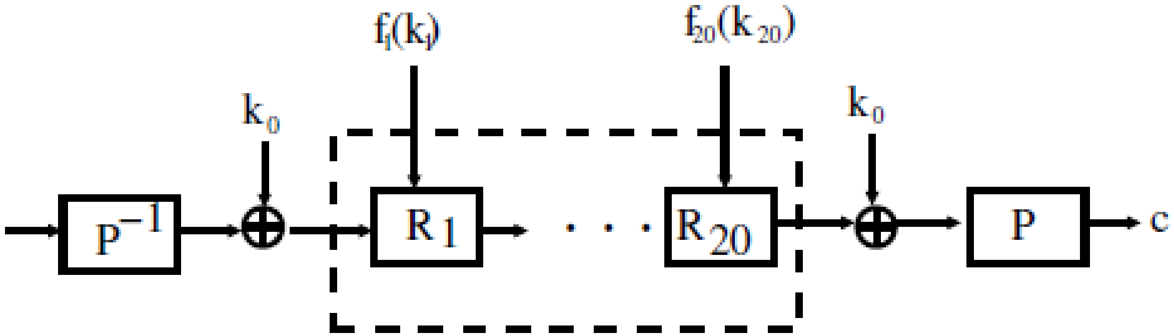
- For PRIDE like linear layer constructions, block interleaving is not used and search space for underlying matrices is 2^{16} times larger than in our construction

- Thus our proposed methodology yields cipher linear layers with similar area footprint, and good diffusion properties, while also reducing the computational complexity of the construction process.

CASE STUDY: PRIDE REVISITED

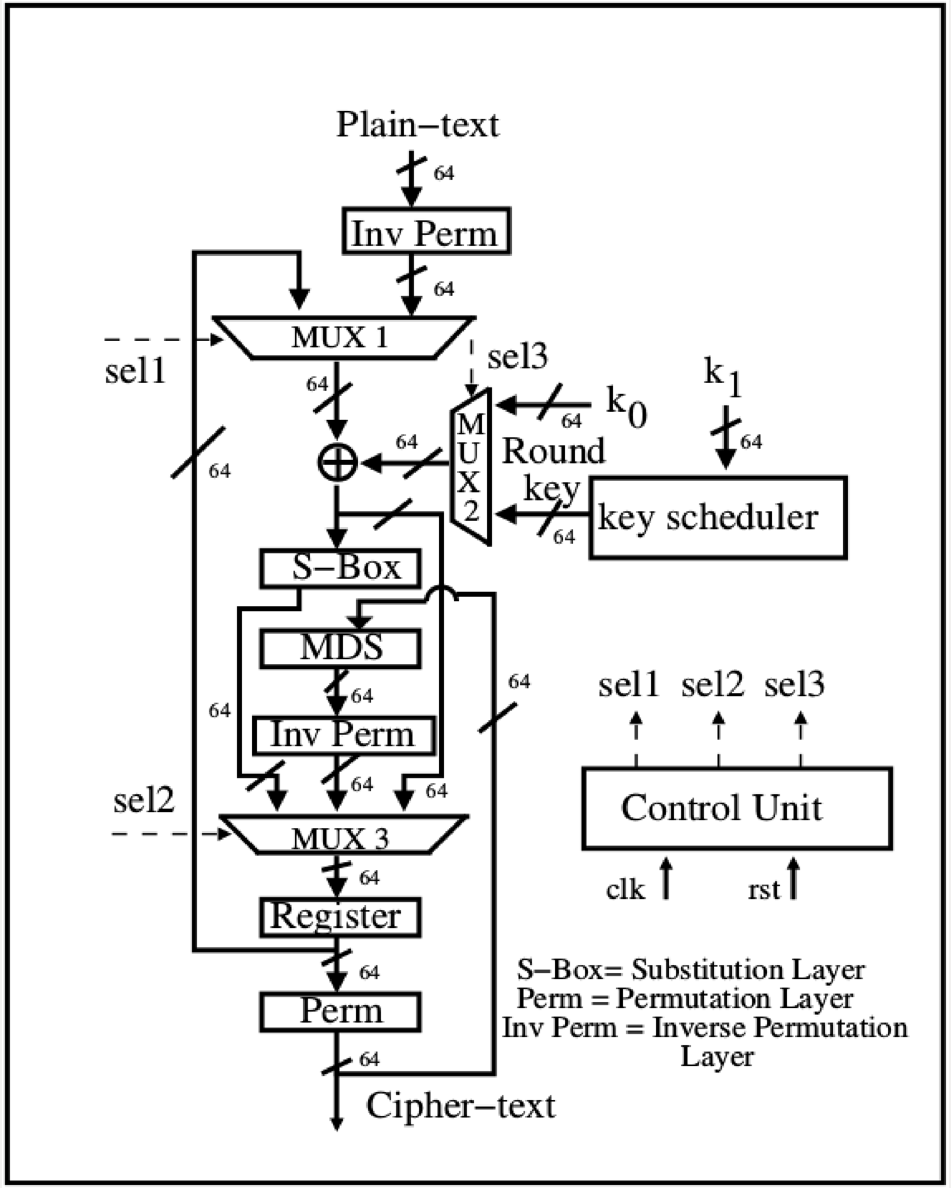
Case Study : PRIDE Revisited

We substitute the original linear layer of PRIDE with a linear layer constructed using our proposed technique. The interleaving construction is used, with each sub-matrix populated using $GF(2^8)$ elements that are chosen according to our proposed strategy



The Structure for PRIDE

PRIDE Redesigned : Lightweight Linear Layer



Results : PRIDE Redesigned

Strong Diffusion Layer

- 20% more diffusion than original
- Comparable security against linear and differential cryptanalysis

Lightweight PRIDE Construction

- 60% CMOS Gate Savings
- 50% LUT savings on FPGA
- Ideal for hardware oriented applications

Area Savings on Hardware – ASIC and FPGA results

Design Platform	Original PRIDE	Modified PRIDE	Percent Savings
ASIC	128 2-input XORs	50 2-input XORs	60
FPGA (expected)	64 LUTs	28 LUTs	56
FPGA (actual)	64 LUTs	32 LUTs	50

Conclusions

- We have proposed a generic construction strategy for linear layers in block ciphers which, to the best of our knowledge, is not yet very well studied in literature
- The focus is on minimizing the area footprint of block ciphers in the context of lightweight cryptography
- Our hierarchical construction provides a simple yet elegant technique of guaranteeing good diffusion properties while ensuring low hardware costs
- The technique has been validated via applications to the recently proposed block cipher PRIDE


THANK YOU
ANY QUESTIONS