Lightweight SCA Secure 4 × 4 S-Boxes from Cellular Automata Rules

Ashrujit Ghosal [1], **Rajat Sadhukhan** [1], Sikhar Patranabis [1], Nilanjan Datta [1], Stjepan Picek [2] and Debdeep Mukhopadhyay [1]

1. **Indian Institute of Technology, Kharagpur, India**
2. Delft University of Technology, The Netherlands

FSE, 2019 March 27, 2019

Overview

Introduction

Designing Light-weight Ciphers

Motivation

To provide solutions tailored for resource-constrained devices such as RFID tags, smart cards, sensor nodes.

Light-weight Metrics

- Cost: Area, Memory, Energy consumption.
- Performance: Throughput, Power consumption.

Side Channel Resilience

- SCA: Implementation vulnerability of cryptographic algorithms due to timing, power and EM attacks.
- NIST Light-weight competition requirement: "...the ability to provide it easily and at low cost is highly desired. Side channel resistance may be necessary in some applications."

Light-weight Side-Channel resistant Block Cipher Design

Designing Light-weight Linear Layer:

- Bit-permutation (e.g. PRESENT, GIFT)
- Shuffle-cells + Light-weight Mix-column operations (e.g. MIDORI)
- SCA countermeasures for linear layer is cheap.

Light-weight Side-Channel resistant Block Cipher Design

Designing Light-weight Linear Layer:

- Bit-permutation (e.g. PRESENT, GIFT)
- Shuffle-cells + Light-weight Mix-column operations (e.g. MIDORI)
- SCA countermeasures for linear layer is cheap.

Designing Light-weight S-Boxes:

- 4×4 S-Boxes with good cryptographic properties
- SCA countermeasures for S-Box is costly: requires dedicated Design

Light-weight Side-Channel resistant Block Cipher Design

Designing Light-weight Linear Layer:

- Bit-permutation (e.g. PRESENT, GIFT)
- Shuffle-cells + Light-weight Mix-column operations (e.g. MIDORI)
- SCA countermeasures for linear layer is cheap.

Designing Light-weight S-Boxes:

- 4×4 S-Boxes with good cryptographic properties
- SCA countermeasures for S-Box is costly: requires dedicated Design

Our Goal

Designing dedicated Light-weight 4×4 S-Boxes with Side channel resistance.

Our Contribution

Light-weight and SCA Resistant S-Box Design

- Novelty of using cellular automata (CA) rules to design class of optimal S-Boxes with inherently lightweight (focusing area only) implementations.
- Choice of the best (area and power efficient) class depending on the (cubic, quadratic, linear) terms of ANF.
- Our CA-based S-Boxes have 49.42% (35.36%) smaller area-footprint, consumes 52.3% (44.46%) lesser power as compared to the PRESENT (GIFT) S-Box.

Applications

Two design paradigms for combining the CA-based optimal S-Boxes with the linear layer to achieve SPN block ciphers with low-area and low-power TI circuits.

Background

Optimal 4×4 S-Boxes

- Non-linearity: $NL_F = 2^{n-1} - \frac{1}{2} \max_{a,\, v} |W_F(a, v)|$, where $W_F(a, v) = \sum_{x \in \mathbb{F}_2^n} (-1)^{v \cdot F(x) + a \cdot x}$ is the Walsh Hadamard transform of the function F.
- Delta Uniformity: $\delta_F = \max_{a,b} |\{x \in \mathbb{F}_2^n : F(x) \oplus F(x \oplus a) = b\}|$.

Optimal 4×4 S-Box

- Bijective,
- Non-linearity: 4,
- Differential-uniformity: 4.

Side Channel Countermeasures

Masking

- One of the most efficient and powerful approaches to thwart DPA
- Targets to break the correlation between the power traces and the intermediate values of the computations.
- Achieves security by randomizing the intermediate values using secret sharing and carrying out all the computations on the shared values.

Side Channel Countermeasures

Masking

- One of the most efficient and powerful approaches to thwart DPA
- Targets to break the correlation between the power traces and the intermediate values of the computations.
- Achieves security by randomizing the intermediate values using secret sharing and carrying out all the computations on the shared values.

Threshold Implementation (Nikova et al.)

Countermeasure against Differential Power Attacks (DPA).

Side Channel Countermeasure

Threshold Implementation (TI)

Boolean masking technique based on secret sharing and secure multi-party computation.

Side Channel Countermeasure

Threshold Implementation (TI)

Boolean masking technique based on secret sharing and secure multi-party computation.

Desired Properties

- Correctness.
- Non-Completeness.
- Uniformity.

Threshold Implementation: A Simple Example

TI of a two-bit multiplier circuit: $\mathbf{a} = \mathbf{xy}$

$$\mathbf{x} = (x_1 \oplus x_2 \oplus x_3 \oplus x_4)$$
$$\mathbf{y} = (y_1 \oplus y_2 \oplus y_3 \oplus y_4)$$
$$\mathbf{a} = (a_1 \oplus a_2 \oplus a_3 \oplus a_4)$$

where the output shares a_1, a_2, a_3, a_4 are computed as:

$$a_1 = (x_2 \oplus x_3 \oplus x_4)(y_2 \oplus y_3) \oplus y_3$$
$$a_2 = (x_1 \oplus x_3)(y_1 \oplus y_4) \oplus x_1 y_3 \oplus x_4$$
$$a_3 = (x_2 \oplus x_4)(y_1 \oplus y_4) \oplus x_4 \oplus y_4$$
$$a_4 = x_1 y_2 \oplus y_3$$

Cellular Automata and Vectorial Boolean Function

- Parallel computational models to simulate and analyze discrete complex systems
- Consists of a regular grid (lattice) of cells
- At every time step every cells update their states synchronously
- Vectorial Boolean function: every cell is in state 0 or 1 and the lattice is a linear array

Periodic Boundary CA (PBCA)

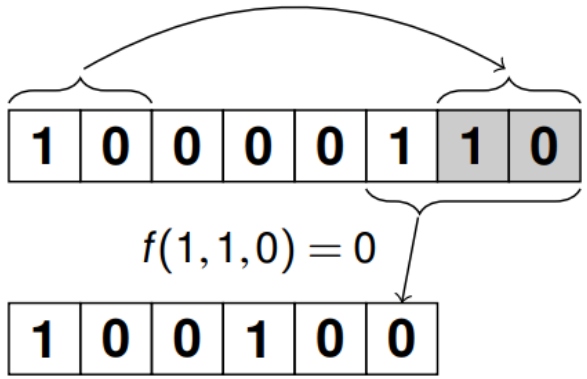
$$F(x_1, x_2, \cdots, x_n) = (f(x_1, \cdots, x_d), \cdots, f(x_n, \cdots, x_{d-1})),$$

where f is local rule.

CA as Vectorial Boolean Function

A Simple Example

- PBCA with $n = 6$
- $f(x_1, x_2, x_3) = x_1 \oplus x_2 \oplus x_3$



Periodic Boundary CA – PBCA

Design Optimal Light-weight 4×4 CA-based S-Boxes with TI

Motivation and Choice of CA based S-Boxes

Why CA-based S-Boxes?

- Choosing a local CA rule is essentially a 4×1 Boolean function.
- 4×4 S-Box mapping is obtained by applying the same CA rule to four different (cyclic) permutations of the input bits.
- Allows an iterative implementation in hardware:
  - CA rule implemented once in the data-path
  - control unit applying a cyclically shifted variant of the input bits in each clock cycle.
- Instead of a 4×4 function, we need the area of a 4×1 function.

Optimal 4×4 S-Boxes using CA Rules

- Total CA based 4×4 S-Boxes: $2^{2^4} = 65536$
- Optimal 4×4 CA-based S-Boxes: 512

Classification of Optimal 4×4 S-Boxes

- Area and Power: Relation with the ANF representation of the S-Boxes.
- All S-Boxes under consideration has optimal algebraic degree 3.

Observations

- Boolean functions with the same # (cubic, quadratic, linear) terms in their ANF form have similar area footprint and expected power consumption in hardware.
- CA-based S-Boxes with the same # (cubic, quadratic, linear) terms in their ANF form have nearly identical TI circuits owing to their nearly identical algebraic structure.

Classification of Good CA-based S-Boxes

Table: Grouping S-Boxes into classes by ANF properties

Class	**Representative CA Rule** $f(X, Y, Z, W)$
(1,2,2)	$XZW \oplus XY \oplus YW \oplus Y \oplus Z$
(1,3,1)	$YZW \oplus XZ \oplus YZ \oplus YW \oplus X$
(1,3,3)	$YZW \oplus XY \oplus XZ \oplus YW \oplus Y \oplus Z \oplus W$
(1,4,2)	$YZW \oplus XY \oplus XZ \oplus XW \oplus ZW \oplus X \oplus W$
(1,5,1)	$XYW \oplus XY \oplus XZ \oplus XW \oplus YW \oplus ZW \oplus Z$
(1,5,3)	$XYW \oplus XY \oplus XZ \oplus XW \oplus YZ \oplus YW \oplus Y \oplus Z \oplus W$
(3,2,2)	$XYZ \oplus XZW \oplus YZW \oplus XZ \oplus YZ \oplus X \oplus Y$
(3,3,1)	$XYZ \oplus XZW \oplus YZW \oplus XZ \oplus XW \oplus YW \oplus Z$
(3,3,3)	$XYW \oplus XZW \oplus YZW \oplus XY \oplus XZ \oplus YW \oplus X \oplus Z \oplus W$
(3,4,2)	$XYZ \oplus XYW \oplus XZW \oplus XY \oplus XZ \oplus XW \oplus YZ \oplus Z \oplus W$
(3,5,1)	$XYZ \oplus XYW \oplus YZW \oplus XZ \oplus XW \oplus YZ \oplus YW \oplus ZW \oplus Y$
(3,5,3)	$XYZ \oplus XYW \oplus XZW \oplus XY \oplus XZ \oplus YZ \oplus YW \oplus ZW \oplus X \oplus Y \oplus W$

Direct Share Architecture

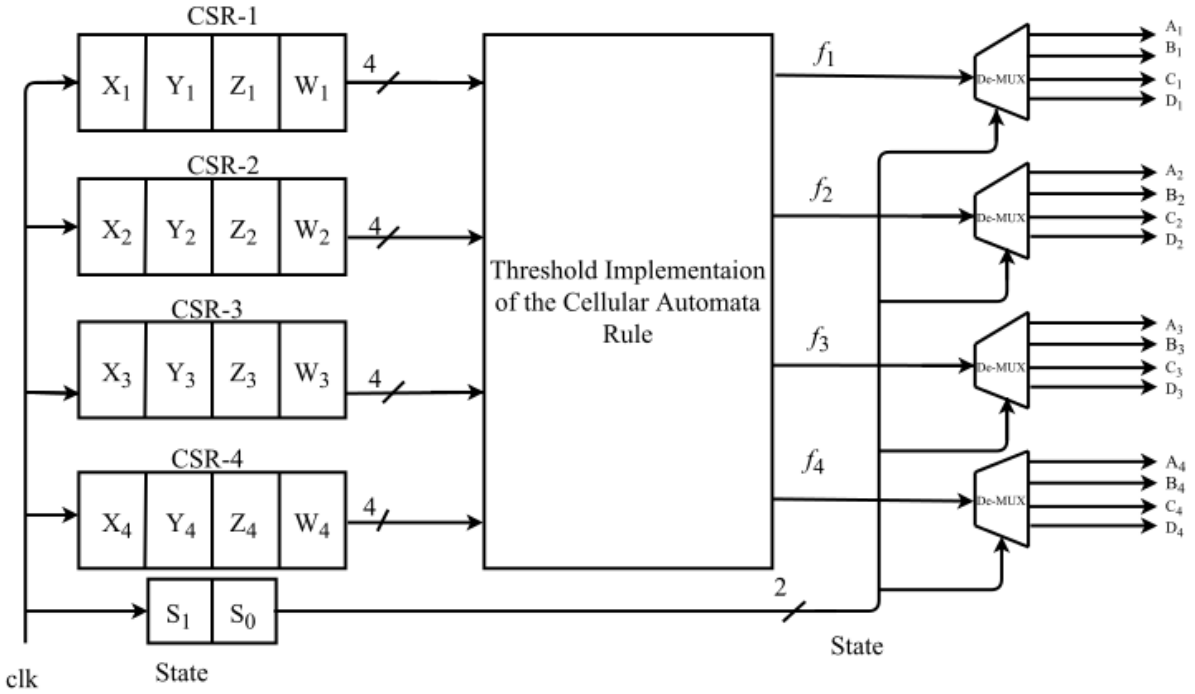


Figure: Basic Direct Share TI Architecture

TI of CA-based S-Boxes: Area and Power Consumption

S-Box Class	Area (GE)	Dyn. Power (μW)
(1,2,2)	265.03	232.51
(1,3,1)	259.23	222.36
(1,3,3)	276.06	247.78
(1,4,2)	288.35	254.89
(1,5,1)	276.55	244.97
(1,5,3)	298.7	284.19
(3,2,2)	378.98	349.76
(3,3,1)	393.83	357.6
(3,3,3)	415.21	398.51
(3,4,2)	405.57	381.00
(3,5,1)	397.10	381.46
(3,5,3)	418.16	413.14

TI of CA-based S-Boxes: Area and Power Consumption

Observation on CA-based S-Boxes

An S-Box of class (a_1, b_1, c_1) is area and power efficient than an S-Box of class (a_2, b_2, c_2) iff

- $a_1 < a_2$ or
- $(a_1 = a_2)$ and $(b_1 + c_1) < (b_2 + c_2)$.

Composite TI: Optimizing TI for Low Area and Power

Generic technique for highly optimized TI designs of CA rules:

- Express each 4×1 CA rule of algebraic degree 3 as a composition of Boolean sub-functions of degree 2.

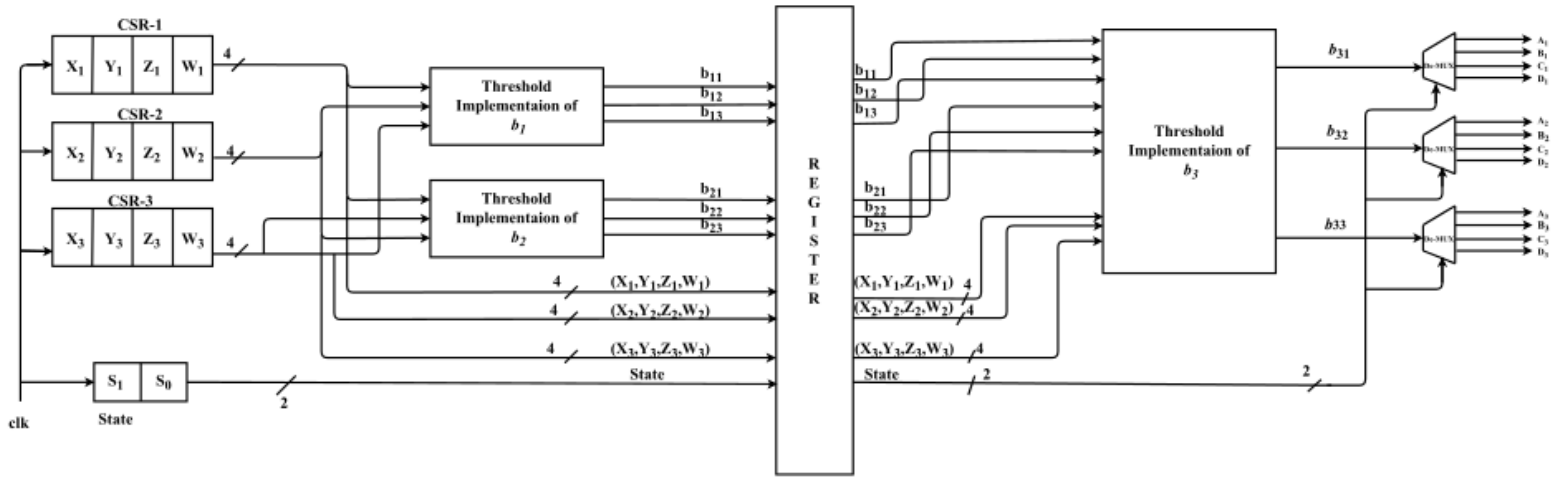


Figure: Composite TI Architecture

Table: Hardware overhead of highly optimized composite TI of CA-Based S-Boxes and Comparison with popular S-Boxes

S-Box		**Area (GE)**	**Dynamic Power (μW)**
CA-Based	**Class**		
	(1,2,2)	212.61	170.2
	(1,3,1)	140.62	113.3
GIFT		217.57	207.75
PRESENT		278.00	237.4
Skinny		321.24	282.3
Piccolo		324.75	281.1
Midori		367.29	331.5
Prince		475.55	411.8

Test Vector Leakage Assessment (TVLA)

Experimental Set-up

- Evaluation performed on a Virtex-5 FPGA on a SASEBO-GII board.
- Programming file generated using Xilinx ISE 14.7 with the Keep Hierarchy on.
- Total 10 00 000 power trace samples were collected.
- Fixed-vs-random statistical test performed on these collected traces.
- The fixed class for the test was chosen as the all-zero input in all our evaluations.

TVLA Result

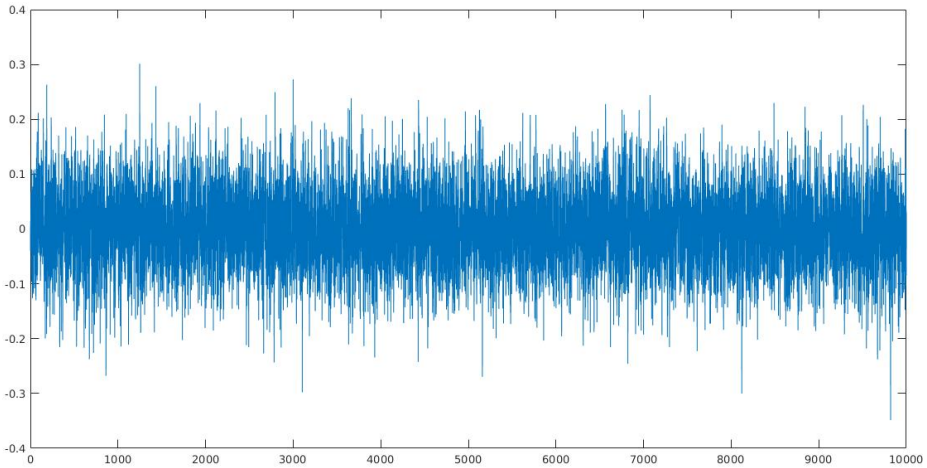


Figure: TVLA of Composite-TI circuit for CA-Based S-Box class $(1, 3, 1)$

- Range of the outcome values: $(-0.4, 0.3)$.
- Permissible range: $(-4.5.4.5)$.

Applications

Application: Designing SPN Block Ciphers Focusing on Area Only

Use SPN based on Bit-Permutation

- Very Low Hardware Footprint.
- Less Diffusion $\Rightarrow$ More Rounds $\Rightarrow$ Lower Throughput.

Examples

- PRESENT: Optimal S-Box with branch number 3, 31 rounds.
- GIFT: Non-Optimal S-Box, branch number 2, Possess BOGI (Bad Output must go to Good Input) property, 28 rounds.

Application: Designing SPN Block Ciphers Focusing on Area Only

Using CA-Based S-Boxes with Bit-Permutation

- Optimal S-Box, branch number 2.
- Doesn't provide BOGI property.
- Number of rounds $\approx$ 40 (64-bit block ciphers).

Application: Design Paradigm II Focusing on Area and Throughput

Use SPN based on Bit-Permutation + Almost-MDS Mix Column

$$\text{Almost\_MDS\_MixColumns} : \begin{bmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{bmatrix}$$

- Better Diffusion $\Rightarrow$ Less Rounds $\Rightarrow$ Higher Throughput.
- Slightly Higher Hardware Footprint.

An Example: Midori-64

- Optimal S-Box, branch number 2, doesn't possess BOGI property.
- Number of rounds: 16.

Application: Design Paradigm II Focusing on Area and Throughput

Using CA-Based S-Boxes with Bit-Permutation + Almost-MDS Mix Column

- Optimal S-Box, branch number 2.
- Doesn't provide BOGI property.
- Number of rounds $\approx$ 16 (64 bit block ciphers).

Table: Area and Power Comparison for TI of SPN block cipher across different choices of S-Boxes and design paradigms (ASIC Technology: 180nm)

S-Box		Diffusion Layer	Area (GE)			Power (mW)
	Class		16 S-Boxes	Diffusion Layer	Total	
CA-Based	$(1, 2, 2)$	Bit permutation	3 401.76	3.15	3 404.91	2.72
		Almost-MDS		216.62	3 618.38	4.19
	$(1, 3, 1)$	Bit permutation	2 249.92	3.15	2 253.07	1.81
		Almost-MDS		216.62	2 466.54	3.28
PRESENT		Bit permutation	4 448.00	3.15	4 451.15	3.79
GIFT		Bit permutation	3 481.12	3.15	3 484.27	3.32
SKINNY		Almost-MDS	5 139.84	216.62	5 356.46	5.99
MIDORI		Almost-MDS	5 876.64	216.62	6 093.26	7.35

Table: Area, Power and Throughput Comparison for TI of SPN block cipher across different choices of S-Boxes and design paradigms (ASIC Technology: 180nm)

S-Box	Diffusion	Rounds	Area (GE)	Power (mW)	Throughput (MBps)
CA-Based $(1, 3, 1)$	Bit Permutation	40	2 253.07	1.81	17.54
CA-Based $(1, 3, 1)$	Almost-MDS	16	2 466.54	3.28	43.85
PRESENT	Bit Permutation	31	4 448.00	3.79	61.41
GIFT	Bit Permutation	28	3 484.27	2.72	71.42
SKINNY	Almost-MDS	32	5 356.46	5.99	62.5
MIDORI	Almost-MDS	16	6 093.26	7.35	125

Exploration of Non-optimal CA-Based S-Boxes

- Each of these S-Boxes have non-linearity 0 or 2 or linear and differential characteristics greater than or equals to $2^{-1.414}$.
- None of these 1024 non-optimal CA-based S-Boxes exhibit the BOGI property of the GIFT S-Box.

Conclusion

Side Channel Resistance Light-weight Primitive Design

- CA based Approach: Design Optimal 4×4 light-weight TI S-Box.
- Build Light-weight Block-ciphers of different Paradigm.

Extension to 8×8 CA-based S-Boxes

- Possible Choices 2^{256}, can not use brute force search.
- Can we combine 4×4 S-Boxes?

Thank You...