A characterisation of S-box fitness landscapes in cryptography

Domagoj Jakobovic[1], Stjepan Picek[2], Marcella Scoczynski[3], Markus Wagner[4]

University of Zagreb, Croatia

TU Delft, The Netherlands

Federal University of Technology, Brazil

University of Adelaide, Australia

GECCO '19, Prague, Czech Republic, July 13, 2019

Outline

Introduction

- We rely on secure communication in everyday life
- Strong cryptographic properties are an absolute requirement of modern communication systems
- A common choice in secure communication: *block ciphers*
  - symmetric key cryptography
  - Substitution-Permutation Network (SPN) ciphers
  - use of *substitution boxes* (S-box) to induce nonlinearity
- An (n, m) S-box is a mapping from n to m Boolean variables
- Examples: 4×4 (PRESENT), 5×5 (Keccak), 8×8 (AES)

Motivation

Objectives

- Strong S-boxes are necessary in block ciphers to make the whole cipher strong

Motivation

Objectives

- Strong S-boxes are necessary in block ciphers to make the whole cipher strong
- We need efficient ways to generate S-boxes with good cryptographic properties

Motivation

Objectives

- Strong S-boxes are necessary in block ciphers to make the whole cipher strong
- We need efficient ways to generate S-boxes with good cryptographic properties
- Evolutionary algorithms? They do well, for smaller S-box sizes...

Motivation

Objectives

- Strong S-boxes are necessary in block ciphers to make the whole cipher strong
- We need efficient ways to generate S-boxes with good cryptographic properties
- Evolutionary algorithms? They do well, for smaller S-box sizes...
- Even if EAs work (or do not), we do not understand how difficult is this problem and how to solve it better

Motivation

Objectives

- Strong S-boxes are necessary in block ciphers to make the whole cipher strong
- We need efficient ways to generate S-boxes with good cryptographic properties
- Evolutionary algorithms? They do well, for smaller S-box sizes...
- Even if EAs work (or do not), we do not understand how difficult is this problem and how to solve it better
- We need to understand the fitness landscape to design better search methodologies

Substitution Boxes

- S-box is a vectorial Boolean function with n input variables and m output values
- In SPN type ciphers: we consider only *bijective* functions (each input vector corresponds to a unique output vector)
  - as a consequence: number of inputs is equal to the number of outputs ($n \times n$)

Substitution Boxes

- S-box is a vectorial Boolean function with n input variables and m output values
- In SPN type ciphers: we consider only *bijective* functions (each input vector corresponds to a unique output vector)
  - as a consequence: number of inputs is equal to the number of outputs ($n \times n$)
- A suitable representation of a *bijective* $n \times n$ S-box is the *permutation encoding* on $[0, 2^n - 1]$
  - permutation preserves the bijectivity property
- Resulting search space: $2^n!$ possible solutions

Cryptographic Properties of S-boxes

- To resist linear cyptanalysis, S-box needs to have a *high nonlinearity* (among other things)
- Nonlinearity N_F is evaluated using the Walsh-Hadamard transform and is bounded above by

$$N_F \leq 2^{n-1} - 2^{\frac{n-1}{2}}$$

Cryptographic Properties of S-boxes

- To resist linear cyptanalysis, S-box needs to have a *high nonlinearity* (among other things)
- Nonlinearity N_F is evaluated using the Walsh-Hadamard transform and is bounded above by

$$N_F \leq 2^{n-1} - 2^{\frac{n-1}{2}}$$

$n \times n$	3×3	4×4	5×5	6×6	7×7
Size	$8! \approx 2^{15}$	$16! \approx 2^{44}$	$32! \approx 2^{117}$	$64! \approx 2^{296}$	$128! \approx 2^{716}$
max N_F	2	4	12	24	56

Cryptographic Properties of S-boxes

- To resist linear cyptanalysis, S-box needs to have a *high nonlinearity* (among other things)
- Nonlinearity N_F is evaluated using the Walsh-Hadamard transform and is bounded above by

$$N_F \leq 2^{n-1} - 2^{\frac{n-1}{2}}$$

$n \times n$	3×3	4×4	5×5	6×6	7×7
Size	$8! \approx 2^{15}$	$16! \approx 2^{44}$	$32! \approx 2^{117}$	$64! \approx 2^{296}$	$128! \approx 2^{716}$
max N_F	2	4	12	24	56

- N_F only assumes even positive values! $(0, 2, 4 \ldots)$
  - Is there a way of obtaining any gradient information...?

Fine-grained Nonlinearity

- S-box nonlinearity is calculated with regard to its *component functions*, of which there are 2^n
- Nonlinearity of an S-box is equal to the *smallest* nonlinearity of each of its component functions, e.g.

$$N_F(CF) = \{4, \mathbf{2}, 6, 4, \mathbf{2}, \mathbf{2}, 4, \dots\}$$

- Total nonlinearity equals 2 (the lowest value)

Fine-grained Nonlinearity

- S-box nonlinearity is calculated with regard to its *component functions*, of which there are 2^n
- Nonlinearity of an S-box is equal to the *smallest* nonlinearity of each of its component functions, e.g.

$$N_F(CF) = \{4, \mathbf{2}, 6, 4, \mathbf{2}, \mathbf{2}, 4, \dots\}$$

- Total nonlinearity equals 2 (the lowest value)
- Grade different S-boxes of the *same* nonlinearity on the basis of the *number of occurrences* of the lowest value (the smaller, the better)

Fitness Functions

- We define two fitness functions, both to maximize nonlinearity:
  - fitness 1: $NL = N_F$
  - fitness 2: $NL_f = N_F + \frac{1}{num\_occurrences}$
- *num_occurrences*: the number of smallest nonlinearity values in all component functions

$$\{4, \mathbf{2}, 6, 4, \mathbf{2}, \mathbf{2}, 4, \dots\} \implies NL = 2, NL_f = 2.333$$

$$\{4, \mathbf{2}, 6, 4, 4, 6, 4, \dots\} \implies NL = 2, NL_f = 3$$

- The above objective functions define two separate landscapes to analyze

Fitness Landscapes

Fitness Landscape

- Fitness landscape analysis: investigates the dynamics of search techniques using models representation;

Fitness Landscapes

Fitness Landscape

- Fitness landscape analysis: investigates the dynamics of search techniques using models representation;
- Fitness landscape: A graph G=(N,E) where nodes represent solutions, and edges represent the existence of a neighbourhood relation given a move operator:
  - Defining the neighbourhood matrix for N can be very expensive;
  - Hard to extract useful information about the search landscape from G.

Fitness Landscape Analysis

- Local Optima Network: A simplified landscape representation...
  - Nodes: Local optima / Basins of attraction;
  - Edges: Connections between the local optima;
  - Two basins of attraction are connected if at least one solution within a basin has a neighbour solution within the other basin, given a defined move operator.

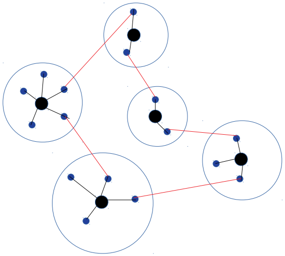


Figure: A LON example

Local Search

- To build a LON, we employ a greedy deterministic hill climber
- The algorithm relies on a given neighbourhood $\mathcal{N}(.)$

$s \leftarrow$ initial solution
while there is an improvement **do**
    $s^* = s$
    for each s^{**} in $\mathcal{N}(s)$ **do**
        if $F(s^{**}) > F(s^*)$ **then**
            $s^* \leftarrow s^{**}$
        end if
    end for
    $s = s^*$
end while

Neighbourhood Structure

- Individuals are permutation vectors of size 2^n
- We consider two neighbourhoods:
  - SWAP (toggle): exchange two elements in the permutation
  - INVERT: invert the order of elements between two points
- Neighbourhood size - the same for both operators:

$$\frac{2^n(2^n-1)}{2}$$

  - e.g. in case of 7×7 S-box, there are 8127 neighbours

LON Building

- The same local search is performed starting from a set of initial solutions (ideally, a whole search space)
- All the local optima and their basins of attraction (sets of solutions) are recorded
- The second phase: build connections between LO's basins of attraction
- If any solution from one basin is a neighbour to any solution in the second basin, a connection is formed
- Repeat for every pair of basins (local optima)

Experiments

S-box experiment variants

- S-box size (3×3 and larger);
- fitness function: NL or NL_f;
- neighbourhood type (swap, invert);
- number of samples (unique initial solutions).

Topological properties of local optima networks

Function	**Operator**	n_v	n_e	z	C_r	C	l	π	S
NL	*swap*	10,752	169,344	31.5000	0.0029	0.0748	3.6373	1.00	1.00
	invert	10,752	593,376	110.375	0.0103	0.0947	2.5466	1.00	1.00
NL_f	*swap*	10,752	203,616	37.8750	0.0035	0.1044	3.5359	1.00	1.00
	invert	10,752	657,888	122.375	0.0114	0.1006	2.4918	1.00	1.00

Table: General LON and basins' statistics for S-box size 3×3.

Graph metrics:

- n_v - number of vertices (nodes, local optima)
- n_e - number of edges;
- z - average degree;
- C - average clustering coefficient (C_r of corresponding random graphs);
- l - average shortest path length between any two local optima;
- π - connectivity, S - number of non-connected components

Topological properties of 3×3 S-boxes

Function	Operator	n_v	n_e	z	C_r	C	l	π	S
NL	*swap*	10,752	169,344	31.5000	0.0029	0.0748	3.6373	1.00	1.00
	invert	10,752	593,376	110.375	0.0103	0.0947	2.5466	1.00	1.00
NL_f	*swap*	10,752	203,616	37.8750	0.0035	0.1044	3.5359	1.00	1.00
	invert	10,752	657,888	122.375	0.0114	0.1006	2.4918	1.00	1.00

Table: General LON and basins' statistics for S-box size 3×3.

- The results cover the whole search space ($8! = 40,320$ solutions)
- The entire LON is a single graph (for both neighbourhoods)
- High number of local optima, high degree, small minimum distances
- A method like Tabu search should be able to explore the whole network

For larger sizes, we retain the NL_f fitness only.

Topological properties for larger sizes, NL_f

Size	Operator	Samples	n_v	n_e	z	C_r	C	l	π	S
4x4	*swap*	100,000	74,641	908,454	24.3420	0.0003	0.0026	5.3995	1.00	1.00
	swap	500,000	351,313	4,943,785	28.1446	0.0001	0.0035	5.8146	1.00	1.00
	invert	100,000	81,388	7,135,032	175.334	0.0022	0.3530	2.9936	1.00	1.00
5x5	*swap*	10,000	7,370	65,383	17.7430	0.0023	0.0108	4.4546	1.00	1.00
	swap	100,000	85,087	1,376,947	32.3656	0.0004	0.0262	4.1791	1.00	1.00
	invert	10,000	9,112	2,181,838	478.893	0.0526	0.6978	1.9653	1.00	1.00
6x6	*swap*	10,000	9,676	97,447	20.1420	0.0021	0.0088	5.5936	1.00	1.00
	swap	100,000	99,583	1,420,307	28.5251	0.0003	0.0010	5.6097	1.00	1.00
	invert	10,000	9,695	1,821,963	375.856	0.0388	0.8029	1.9693	1.00	1.00
7x7	*swap*	10,000	9,998	103,048	20.6137	0.0020	0.0001	5.0521	1.00	1.00
	invert	10,000	9,653	673,460	139.534	0.0145	0.6575	1.9901	1.00	1.00

- Almost linear increase of LO with samples: a large number of LO
- Higher degree of clustering than random graphs: LO are connected in dense local clusters with sparse interconnections
- Many plateaus: difficult to exploit

Degree Distributions

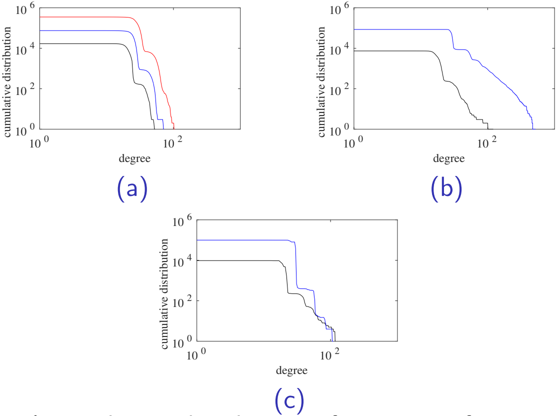
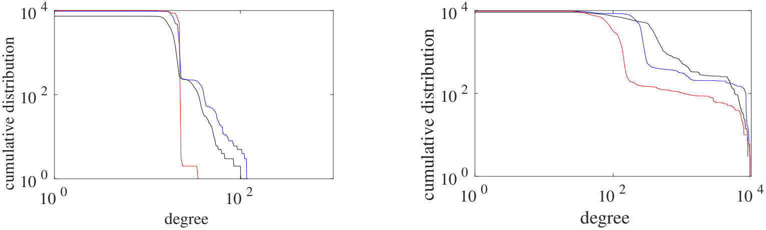


Figure: Cumulative degree distribution of NL_f swap for 10 000 samples (black), 100 000 samples (blue) and 500 000 samples (red, when available) for a) 4x4, b) 5x5 and c) 6x6.

Degree Distributions



(a) (b)

Figure: Cumulative degree distribution of NL_f for 5x5 (black), 6x6 (blue) and 7x7 (red) S-boxes with 10 000 samples for a) *swap* and b) *invert*.

Degree Distribution Model

- Can these degree distributions be represented with a model?
- Degree distributions are tested with Kolmogorov-Smirnov test for adequacy of power-law model and exponential model
- Motivation: a power-law graph can be searched more rapidly (the edges preferentially lead to high degree nodes)

Degree Distributions

Kolmogorov-Smirnov test

Size	Function	Operator	Samples	Power-Law	Exponential
4x4	NI_f	*swap*	100, 000	0.0954	0.1547
	NI_f	*swap*	500, 000	0.0460	0.3215
	NI_f	*invert*	100, 000	0.0654	0.1234
5x5	NIf	*swap*	10, 000	0.0321	0.1325
	NI_f	*swap*	100, 000	0.0647	0.1795
	NI_f	*invert*	10, 000	0.0325	0.2154
6x6	NL_f	*swap*	10, 000	0.0990	0.2178
	NI_f	*swap*	100, 000	0.0217	0.3154
	NI_f	*invert*	10, 000	0.0645	0.3165
7x7	NL_f	*swap*	10, 000	0.0548	0.2981
	NI_f	*invert*	10, 000	0.0487	0.3152

Table: The p-values for the Kolmogorov-Smirnov hypothesis test with a significance level of 0.1. If $p - value > 0.1$, the test fails to reject power-law and exponential as plausible distribution models.

Basin of Attraction Sizes

- Exponential degree distributions do not provide a good interpretation of local search behaviour as the power law –> consider the size of the basins of attraction
- Explore correlation between node degrees and the basin sizes

Basin of Attraction Sizes

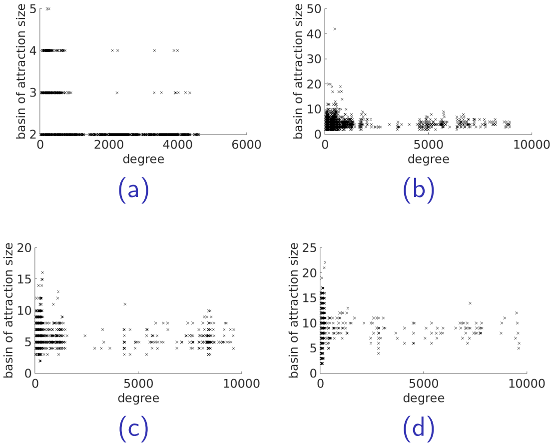


Figure: Correlation between the degree of local optima and their corresponding basin sizes for a) 4x4, b) 5x5, c) 6x6 and d) 7x7

Basin of Attraction Sizes

- Nodes with high degree and small basin size –> large plateaus with many small basins
- Many small basins of comparable fitness –> hard to navigate the landscape (little information for the search heuristic)

Conclusions

Summary

- First fitness-landscape analysis of S-boxes for cryptographic;
- Almost every single initial solution finds a *different* local optimum! –> many small basins of attraction;
- Future experiments can combine Tabu lists or niching approaches with restarts –> control the perturbation magnitude from the previous starting point

Acknowledgements

Australian Research Council project DE160100850.
COST (European Cooperation in Science and Technology).

FUNDAÇÃO ARAUCÁRIA
Apoio ao Desenvolvimento Científico e Tecnológico do Paraná

PARANÁ
GOVERNO DO ESTADO