Linear and Differential Properties of S-boxes with Respect to Modular Addition

Matúš Jókay Peter Špaček Pavol Zajac[1]

Institute of Computer Science and Mathematics
Slovak University of Technology

pavol.zajac@stuba.sk

Central European Conference on Cryptology 2019

[1] Supported by grant VEGA 1/0159/17.

Outline

Introduction

Definitions
- D-spectrum
- L-spectrum

Modular affine equivalence (MAE)

Experimental results
- All MAE classes
- Optimal S-boxes

Summary

Introduction

S-boxes are typically studied in the context of Boolean functions:

- $S : \mathbb{F}_2^n \rightarrow \mathbb{F}_2^m$,
- Linear profile: $Pr(a^T \cdot x = b^T \cdot S(x))$.
- Differential profile: $Pr(S(x) \oplus S(x \oplus \delta_x) = \delta_y)$.
- Small S-boxes can be easily characterised using affine equivalence [2] (302 classes):

$$S_2(x) = \mathbf{A}_1 \cdot S_1(\mathbf{A}_2 \cdot x \oplus b_2) \oplus b_1$$

[2] Leander, G., Poschmann, A.: On the classification of 4 bit S-boxes. 2007

Modular S-box properties

Research question

What properties have small bijective S-boxes with respect to modular addition?

Research question refinement

Do the modular properties depend on the quality of S-box w.r.t. standard S-box criteria?

Motivation

- Alternative cipher designs:
  - Rotor machines: clocking can be expressed as $S(x + t)$, with $+$ over some $\mathbb{Z}_n$
  - GOST, Kalyna (and others): Key addition or linear layer with $+$ over some $\mathbb{Z}_{2^n}$
- Theoretical generalizations of non-linearity properties[3]
- Attacks based on alternative[4] operations[5]

---

[3] O Grošek, K Nemoga, L Satko: Generalized perfectly nonlinear functions.2000

[4] Calderini M., Sala M.: Elementary abelian regular subgroups as hidden sums for cryptographic trapdoors. 2017

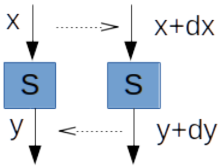
[5] Civino R, Blondeau C, Sala M. Differential attacks: using alternative operations. 2019

Notation

- We work in ring $\mathbb{Z}_{2^n} = (\mathbb{Z}/2^n\mathbb{Z})$
- Addition/subtraction: $+/-$
- Multiplication: ax
- Division: $x/a = a^{-1}x$, for a with $\gcd(a, 2) = 1$
- Affine permutations:

$$A(x) = ax + b, \text{ with } \gcd(a, 2) = 1$$

Differential properties

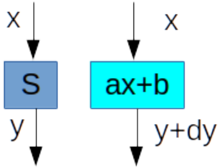


- Table of differences:

$$D_{(d_x,d_y)} = \left|\{x, S(x+d_x) - S(x) = d_y\}\right|$$

- D-spectrum: multiset $\{D_{(d_x,d_y)}\}$
- D-criterium: $D(S) = \max\{D_{(d_x,d_y)}\}$
- Affine function: $D(f) = 2^n$

Linear properties



- Linear approximation:

$$L_{(a,b)} = \left|\{x, S(x) = ax + b\}\right|$$

- L-spectrum: multiset $\{L_{(a,b)}\}$
- L-criterium: $L(S) = \max\{L_{(a,b)}\}$
- Affine function: $L(f) = 2^n$

Modular affine equivalence

To explore (modular) S-box properties, we can use (modular) affine equivalence (MAE):

$$S_1 \equiv S_2 \text{ iff } A_1 \circ S_1 = S_2 \circ A_2$$

Explicitly:

$$\forall x : S_2(x) = a_1 \cdot S_1(a_2 \cdot x + b_2) + b_1$$

S-box criteria $L(S)$ and $D(S)$ are invariant under MAE.

Modular affine equivalence

- Class size: at most 2^{4n-2}
  - $n = 3$: 58 classes
  - $n = 4$: 1277100855 classes ($\approx 2^{30}$)
- Representatives:
  - can always normalize to $S(0) = 0$, $S(1) = 1$
  - representative is the first S-box in lex order

Modular S-box properties and affine equivalence

Research question reformulation

What is the statistical distribution of L- and D-criterium in MAE classes of small S-boxes?

All MAE classes

Statistics of class representatives based on exhaustive enumeration of 4-bit S-boxes:

All 1277099568 classes

D \ L	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
1																
2			0.00%	0.00%	0.00%											
3		0.00%	0.78%	5.04%	2.10%	0.20%	0.00%									
4		0.00%	4.84%	30.44%	15.09%	2.77%	0.22%	0.00%								
5		0.00%	2.82%	15.92%	7.94%	1.89%	0.36%	0.03%	0.00%							
6		0.00%	0.70%	3.78%	2.44%	0.83%	0.24%	0.05%	0.00%							
7		0.00%	0.12%	0.53%	0.28%	0.10%	0.04%	0.02%	0.00%	0.00%						
8		0.00%	0.02%	0.10%	0.13%	0.07%	0.03%	0.01%	0.00%	0.00%	0.00%					
9		0.00%	0.00%	0.01%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%				
10		0.00%	0.00%	0.00%	0.01%	0.01%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%				
11		0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%			
12		0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%			
13						0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%		
14		0.00%														
15																
16				0.00%		0.00%		0.00%		0.00%		0.00%		0.00%		0.00%

All MAE classes

Modular S-box criteria in numbers:

- 30% of S-boxes: $D = 4, L = 4$
- 95% of S-boxes: $D, L \in \{4, 5\}$
- 0.5% of S-boxes: $D \geq 8$ or $L \geq 8$
- $L = 2, D = 3$: 170 classes
- $L = 3, D = 2$: 411 classes

Selected S-boxes

Selected 4-bit S-boxes from (Saarinen, 2011)[6]:

- $D, L \in \{3, 4, 5, 6, 7\}$, most of them: $L = 4, D = 4$
- DES S5-1: $D = 7$, $L = 4$ (0.53%):

$$Pr(S(x+3) - S(x) = 8) = 7/16$$

- GOST K8: $D = 5$, $L = 7$ (0.36%):

$$Pr(S(x) = 5x + 1) = 7/16$$

- HAMSI, Serpent S2 (G1): $D = 7$, $L = 3$ (0.12%)

[6] Saarinen MJ. Cryptographic analysis of all 4×4-bit S-boxes. SAC 2011.

Modular S-box properties and optimal S-box classes

Research question reformulation

What is the statistical distribution of L- and D-criterium in MAE classes of small S-boxes?

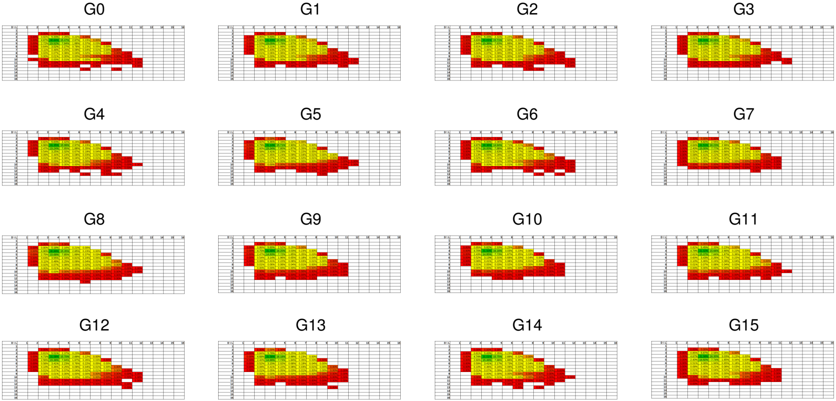
Additional question

What is the statistical distribution of L- and D-criterium in case of optimal S-boxes (in 16 optimal LA classes)?

Technical note

- To explore all S-boxes in 16 optimal classes would take $1303\times$ more time than to explore all class representatives.
- Our computation:
  - Let $Aff = \{\mathcal{A}; \mathcal{A}(x) = \mathbf{A} \cdot x \oplus c\}$,
  - Aff_L contains reps. of $a\mathcal{A}(x) + b$ — 20160 permutations
  - Aff_R contains reps. of $\mathcal{A}(ax + b)$ — 20160 permutations
  - compute $Aff_L \circ S \circ Aff_R$

All optimal classes



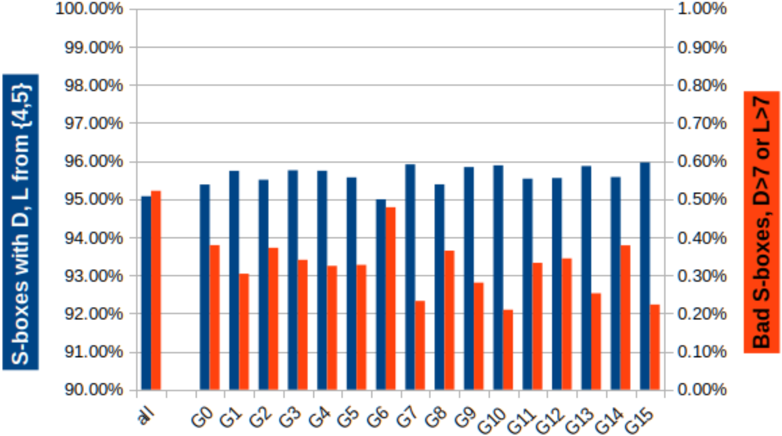
- Best S-boxes have always $(D, L) = (2, 3)$, or $(D, L) = (3, 2)$
- Maximum L is 11 (G7, G9, G10, G13), or 12
- Maximum D is 12 (G1, G3, G7, G9, G10, G11, G15), or 13

Class G3 (finite field inverse)

D \ L	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
1																
2			0.00%	0.00%	0.00%											
3		0.00%	0.83%	5.64%	2.46%	0.24%	0.00%									
4		0.00%	4.69%	31.31%	16.08%	2.96%	0.23%	0.00%								
5		0.00%	2.50%	15.19%	7.85%	1.86%	0.35%	0.03%	0.00%							
6		0.00%	0.55%	3.22%	1.99%	0.65%	0.19%	0.04%	0.00%							
7		0.00%	0.09%	0.44%	0.23%	0.08%	0.03%	0.01%	0.00%	0.00%						
8		0.00%	0.01%	0.07%	0.08%	0.05%	0.02%	0.01%	0.00%	0.00%	0.00%					
9			0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%					
10			0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%				
11			0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%		0.00%				
12			0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%							
13																
14																
15																
16																

- D and L in range 2 to 12
- 95.75% of S-boxes with $D, L \in \{4, 5\}$
- 0.34% of S-boxes with $D \geq 8$ or $L \geq 8$

S-box distribution within classes



Summary

Experimental results summary:

1. Optimal S-boxes w.r.t. standard linear and differential cryptanalysis have similar properties w.r.t. modular addition (with all classes and between them).
2. A small fraction of S-boxes optimal w.r.t. standard linear and differential cryptanalysis have very bad properties w.r.t. modular addition.

Open questions

- General theoretical analysis and good algebraic constructions?
- What about other operations, are there S-boxes good against every approximation?
- Can we break standard SL designs with bad modular S-boxes?
- Can weak modular S-boxes be used to backdoor[7] cipher designs?

[7] A Biryukov, L Perrin, A Udovenko: Reverse-Engineering the S-Box of Streebog, Kuznyechik and STRIBOBr1, 2016