Multiplicative complexity in block cipher design and analysis

Pavol Zajac

Institute of Computer Science and Mathematics
Slovak University of Technology

pavol.zajac@stuba.sk

Fewer Multiplications in Cryptography — From Theory to Applications

Outline

P. Zajac, M. Jókay: **Multiplicative complexity of bijective 4×4 S-boxes.**
Cryptography and Communications 6 (3), 255–277, 2014.

Affine equivalence

Definition

Affine equivalence: $S_1 \sim S_2$

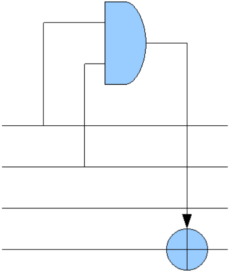
$$\forall x \in \mathbb{Z}_2^n, \exists A, B \in GL(2, n), c, d \in \mathbb{Z}_2^n : A \cdot S_1(B \cdot x \oplus c) \oplus d = S_2(x)$$

Theorem

Multiplicative complexity is invariant within the affine class of S-boxes.

- For $n = 4$, there are 302 affine equivalence classes.
- 11! normalized representatives (for fast computation):
  `0 1 2 * 4 * * * 8 * * * * * * *`

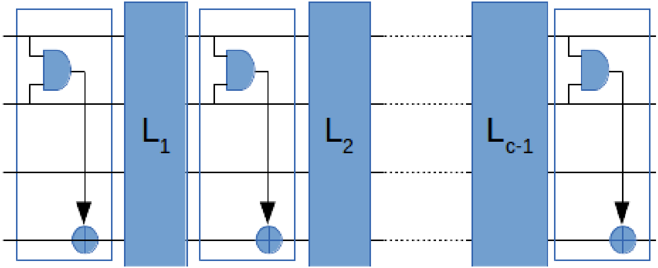
MC1: 1 class



Theorem

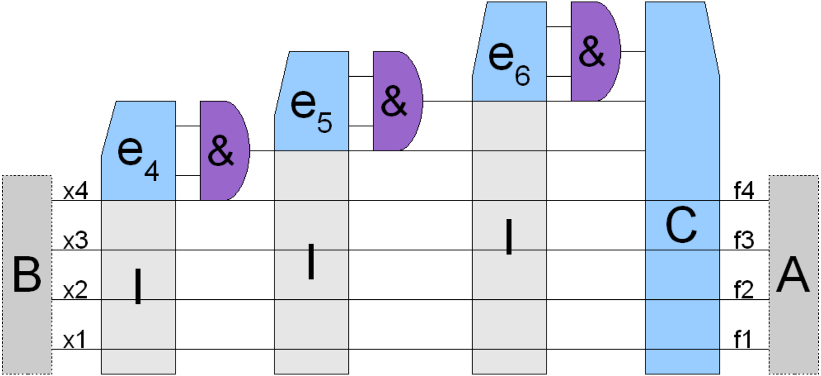
There is only one affine class of bijective S-boxes for any n.

Composition construction



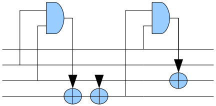
- $MC(S) \leq c$
- Only *even* permutations: replace initial part by swap ($MC = 2$) to generate odd permutations.
- With $c \leq 5$: all affine classes covered.

Expand and Compress under affine equivalence

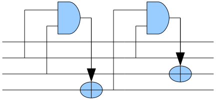


Complexity: 2^{44} S-boxes (not necessarily distinct) generated to identify all classes with $MC(S) \leq 4$ (optimised version)

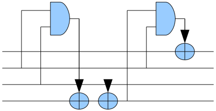
MC2: 3 MC1 decomposable + 2 non-decomposable classes



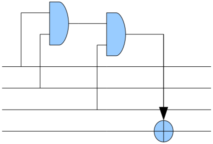
MC2 – 11



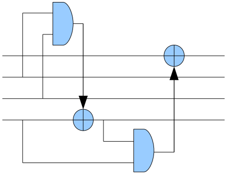
MC2 – 15



MC2 – 232



MC2 – 2



MC2 – 5

Statistics of MC classes

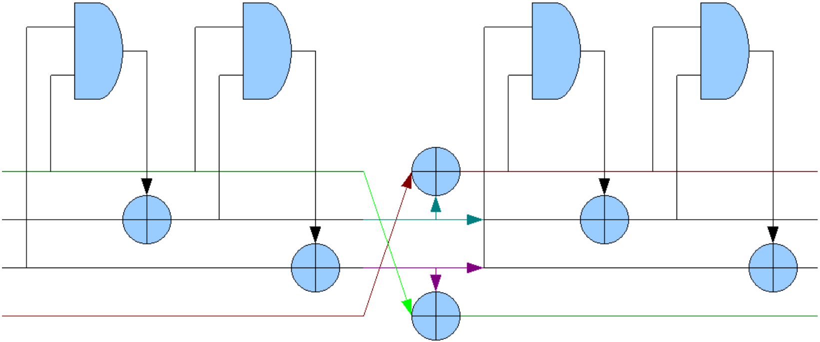
MC	Classes	*Comp. Classes*	Classes[%]	NormRep[%]
0	1	*1*	0.33	0.00
1	1	*1*	0.33	0.00
2	5	*3*	1.66	0.01
3	25	*22*	8.28	1.18
4	140	*120*	46.36	46.38
5	130	*155*	43.05	52.42

- Comp.classes: as identified just by composition construction.
- Norm.rep: fraction of normalized representatives.

A note on Optimal S-boxes

- Notation: Leander & Poschmann, 2007
- Best linear and differential characteristics: 16 classes
- MC4: 6 classes
  - 4 classes, MC1-decomposable: $G_0 \sim_{CCZ} G_1 \sim_{CCZ} G_2 \sim_{CCZ} G_8$
  - 2 classes, non-MC1-decomposable: $G_{14} \sim_{CCZ} G_{15}$
- MC5: 10 classes (including $GF(2^4)$ inverse)
  - 4 MC1-decomposable, no CCZ equivalence between them

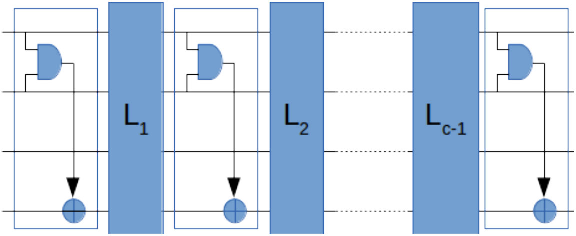
PRESENT-class S-box decomposition (G_1)

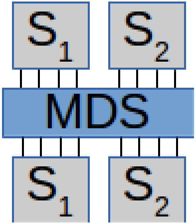


P. Zajac: **Constructing S-boxes with low multiplicative complexity.**
Studia Scientiarum Mathematicarum Hungarica 52 (2), 135–153, 2015.

Composition construction of S-boxes

Let $S = S_k \circ \cdots \circ S_2 \circ S_1$, then $MC(S) \leq \sum MC(S_i)$.





- random composition
- greedy composition

- structured approach

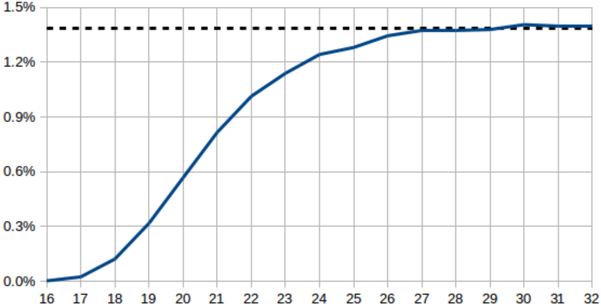
S-box quality criteria

- Multiplicative complexity bound:
  $MC(F)$
- Algebraic degree (vectorial):
  $DD(F) = \min\{\deg(\mathbf{a} \cdot F); \mathbf{a} \neq 0\}$
- Linear weight:
  $w_L(F) = -\log_2 \max_{\mathbf{a}\neq 0, \mathbf{b}\neq 0}\{|2Prob(\mathbf{a} \cdot X = \mathbf{b} \cdot F(X)) - 1|\}$
- Differential weight:
  $w_D(F) = -\log_2 \max_{\mathbf{a}\neq 0, \mathbf{b}\neq 0}\{Prob\,(F(X) \oplus F(X + \mathbf{a}) = \mathbf{b})\}$

8×8 S-boxes from random composition

$MC(S)$	deg(S)			w_L(S)				w_D(S)		
	< 6	6	7	≤ 1.25	1.83	1.91	≥ 2.00	≤ 4.19	4.42	≥ 4.68
≤ 12	94.4%	5.6%	0.0%	100.0%	0.0%	0.0%	0.0%	100.0%	0.0%	0.0%
≤ 13	76.7%	23.3%	0.0%	99.8%	0.6%	0.0%	0.0%	99.9%	0.1%	0.0%
≤ 14	52.6%	47.4%	0.0%	98.3%	3.2%	0.1%	0.0%	96.8%	3.2%	0.0%
≤ 15	31.6%	68.0%	0.5%	92.6%	8.5%	1.1%	0.1%	82.4%	17.2%	0.4%
≤ 16	17.4%	80.0%	2.6%	81.1%	14.1%	4.4%	0.4%	58.1%	38.7%	3.2%
≤ 17	9.1%	83.6%	7.2%	66.5%	17.3%	10.4%	1.3%	36.0%	54.3%	9.7%
≤ 18	4.7%	82.0%	13.3%	52.2%	18.0%	17.6%	2.8%	21.7%	60.2%	18.1%
≤ 19	2.3%	78.8%	18.9%	40.8%	17.4%	24.3%	4.7%	14.0%	60.5%	25.5%
≤ 20	1.2%	75.8%	23.0%	32.6%	16.3%	29.3%	6.5%	10.2%	58.8%	31.0%
≤ 21	0.6%	73.9%	25.5%	27.3%	15.4%	32.8%	8.0%	8.4%	57.3%	34.3%
≤ 22	0.3%	72.6%	27.1%	23.9%	14.6%	35.1%	9.1%	7.5%	56.2%	36.3%
≤ 23	0.1%	71.9%	27.9%	21.9%	14.1%	36.5%	9.8%	7.0%	55.3%	37.6%
≤ 24	0.1%	71.5%	28.4%	20.6%	13.8%	37.3%	10.3%	6.8%	54.7%	38.5%
≤ 25	0.0%	71.3%	28.7%	19.9%	13.5%	37.8%	10.6%	6.6%	54.5%	38.9%
≤ 26	0.0%	71.2%	28.8%	19.5%	13.4%	38.1%	10.9%	6.6%	54.3%	39.2%
≤ 27	0.0%	71.0%	29.0%	19.2%	13.3%	38.3%	10.9%	6.6%	54.0%	39.4%
≤ 28	0.0%	71.0%	29.0%	19.1%	13.4%	38.3%	11.0%	6.5%	54.0%	39.5%
≤ 29	0.0%	71.1%	28.9%	18.9%	13.2%	38.5%	11.1%	6.5%	54.0%	39.5%
RND	0.0%	71.0%	29.0%	18.8%	13.2%	38.5%	11.2%	6.4%	54.0%	39.6%

"Good" 8×8 S-boxes from random composition



Fraction of S-boxes:

$MC(S) \leq x$, $deg = 7$, $w_L \geq 2.0$, and $w_D \geq 4.68$.

Dotted line: random S-boxes (unknown MC)

"Good" 8×8 S-boxes

	Random	Greedy	MDS	AES
Samples	2^{20}	2^{19}	2^{30}	1
$MC(S) \leq$	16	16	16	32
$DD(S)$	7	7	6	5
$w_L(S)$	2.00	2.09	2.14	3.00
$w_D(S)$	4.68	5.00	4.68	6.00

AES with best $MC \leq 16$ S-box:

- Minimum correlation weight in 4 rounds: 52.25
- Minimum differential weight in 4 rounds: 125
- Saves 320 AND gates in each round

Note on LowMC

- $MC(S) = 3$ — affine equivalent to 3 T-gates and rotations.
- Experimentally: random linear layer composition seems too ”wasteful”.
- What is the multiplicative complexity of the whole cipher?
- *Extreme depth design: Use 1 T-gate per round, and linear transforms that ensure most AND-heavy output is used in next round.*

P. Zajac: **Upper bounds on the complexity of algebraic cryptanalysis of ciphers with a low multiplicative complexity.**
Designs, Codes and Cryptography 82 (1-2), 43–56, 2017.

Algebraic cryptanalysis

Denote (unknown) state bits by v, plaintext,ciphertext by x, y.

Solve a system of non-linear Boolean equations (on AND gates)

$$v_i = (\mathbf{v} \cdot \mathbf{a}_i^T \oplus c_i) \otimes (\mathbf{v} \cdot \mathbf{b}_i^T \oplus d_i),$$

along with linear input and output equations

$$\mathbf{v} = \mathbf{x} \cdot \mathbf{M}_{in} \qquad \mathbf{y} = \mathbf{v} \cdot \mathbf{M}_{out}.$$

Using MRHS representation

Transform each equation to MRHS form:

$$v_4 = (v \cdot (11000)^T \oplus 1) \otimes (v \cdot (01100)^T \oplus 0)$$

$$(v_1, v_2, v_3, v_4, v_5) \cdot \begin{pmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix} \in \left\{ \begin{matrix} 0 & 0 & 0, \\ 0 & 1 & 1, \\ 1 & 0 & 0, \\ 1 & 1 & 0, \end{matrix} \right\}$$

MRHS system

We get one MRHS equation for each AND gate:

$$v \cdot M_i \in S_i$$

MRHS equation system:

$$v \cdot (M_1 | M_2 | \cdots | M_k) \in S_1 \times S_2 \times \cdots \times S_k$$

Definition (of MRHS system solution)

Vector v is a solution of MRHS system, if for each i: $v \cdot M_i \in S_i$

Solving MRHS systems

- Agreeing and Gluing
  H. Raddum, I. Semaev. "Solving multiple right hand sides linear equations." Designs, Codes and Cryptography 49.1-3 (2008): 147-160.
- Global Gluing
  Zajac, Pavol. "A new method to solve MRHS equation systems and its connection to group factorization." Journal of Mathematical Cryptology 7.4 (2013): 367-381.

Solving MRHS systems via decoding

1. Reformulate MRHS system as intersection of two $GF(2)^{3k}$ subspaces:

$$v \cdot (M_1|M_2|\cdots|M_k) \in S_1 \times S_2 \times \cdots \times S_k$$

   - $v \cdot (M_1|M_2|\cdots|M_k)$ — linear code $\mathcal{C}$ with gen. matrix M
   - $S = S_1 \times S_2 \times \cdots \times S_k$ — explicit subspace of $GF(2)^{3k}$

2. Solution v is an information word for a codeword from S.
3. Apply parity check matrix for $\mathcal{C}$ to space S piece-wise:

$$(s_{1,i_1} \in S_1, s_{2,i_2} \in S_2, \ldots, s_{k,i_k} \in S_k) \cdot H^T = 0$$

Solving MRHS systems via decoding

- After linear algebra, we get a 1-regular decoding problem.
- Can be transformed to a smaller classical decoding problem.
- Complexity depends on the size of codewords:
  - $n = 3\mu$, where μ is the number of AND gates in the circuit.
  - **Multiplicative complexity** is directly related to a *minimum size of the decoding instance*.

Decoding attack on circuit with low MC

Let $F : GF(2)^\nu \to GF(2)^\kappa$ be implemented with μ AND-gates.

- MRHS system with μ MRHS equations, $\nu + \mu - \kappa$ unknowns, four 3-bit solutions each,
- Decoding problem: $(3\mu, \mu + \nu - \kappa, t)$-code, need to decode at most μ errors
- Code rate:

$$R = 1/3 + \frac{\nu - \kappa}{3\mu}$$

- Worst-case decoding complexity for $\nu = \kappa$:

$$O(2^{c \cdot n}) = O(2^{3c \cdot \mu})$$

- Brute-force $O(2^\nu)$: for $c = 0.1019$, we need $\mu > 3.27\nu$

Note on post-quantum crypto

- Standard solution for symmetric crypto and Grover's algorithm: *increase key size*.
- BUT: Quantum Information Set Decoding Algorithms (Kachigar and Tillich, 2017)
  - improved decoding algorithms on quantum computers, $c = 0.05869$
  - we also need more AND gates per bit to compensate:

$$\mu > 5.68\nu$$

Summary

- Multiplicative complexity of 4-bit S-boxes can be found by computer search. What about mathematical proofs, generalisations?
- Random composition of small-MC S-boxes requires a longer chain than greedy composition to achieve better cryptographic properties (degree, non-linearity, differential uniformity). More structure in linear layers gives better cipher designs?
- Multiplicative complexity is directly related to complexity of algebraic cryptanalysis and decoding problem. Can we get more precise classical and *quantum* bounds on required ANDs per encrypted bit?