Summary of some cryptographic criteria of functions in 8 variables

Agnese Gini, Pierrick Méaux

September 8, 2023

Abstract

The purpose of this document is to collect the state of the art about criteria of WPB functions in 8 variables.

Disclaimer: This document may be outdated, incomplete, containing mistakes. Please check the original references and contact us if you believe there is something that should be added/corrected.

1 Summary tables

We summarise notions about *degree* Table 1, *algebraic immunity* Table 4, *weightwise nonlinearity* Table 3, *nonlinearity* Table 2 of WPB functions in 8 variables.

Construction	Algebraic degree
Minimum	4
Maximum	7
[GM23b]	$[4, 7]$

Table 1: Degree 8-variable WPB constructions.

Construction	Nonlinearity
Minimum	8
[GM23a] seeded with ℓ_4	8
[TL19]	$[66, 82]$
[CMR17] f_8	88
[GM22b] $g_{6,8}$	96
Average*	103.49
Mode*	104
[MKCL22]	$[110, 112]$
[GM23a]seeded with $\sigma_{2,8} + \ell_4$	$[112, \mathbf{116}]$
Upper Bound	118

Table 2: Nonlinearity 8-variable WPB constructions. [GM23c]

Construction	NL_2	NL_3	NL_4
Minimum	1	0	0
f_m [MS21]	2	0	3
f_m [MSL21]	2	8	8
[GM22a]	2	10	14
[CMR17, Su21]	2	12	19
[LS20]	2	12	19
g_m [MS21]	2	14	19
g_m [MSL21]	6	8	26
[LM19]	$\{6, \mathbf{9}\}$	$\{0, 8, 14, 16, 18, 20, 21, \mathbf{22}\}$	$\{19, [22, 27]\}$
[GM22a] (sampled)	$[1, \mathbf{9}]$	$[8, 21]$	$[8, 27]$
[ZJZQ23]	6	17	23
[YCL+23]	**9**	21	**28**
Average* [GM22a]	6.61	17.36	23.09
Mode* [GM22a]	7	18	24
Upper Bound	11	24	30

Table 3: Weightwise nonlinearities of 8-variable WPB constructions. Update of table [GM22a].

Construction	Algebraic immunity
Minimum [GM23c]	2
Maximum	4
[TL19]	4
[CMR17]	4
[GM22b]	3
[MKCL22]	4
[GM23a, GM23c]	2
[ZJZQ23]	4

Table 4: Algebraic immunity 8-variable WPB constructions.

2 Criteria of explicitly functions

	deg	AI	NL	NL_2	NL_3	NL_4	NL_5	NL_6	Reference	Verified
f_8	4	4	88	2	12	19	12	6	[CMR17]	✓
l	7	4	108	6	21	27	**22**	**9**	[LM19]	✓
l'	7	4	96	**9**	8	19	20	6	[LM19]	✓
l''	7	4	104	**9**	16	19	16	6	[LM19]	✓
a_1	7	4	88	8	8	22	8	7	[TL19]	✓
a_2	7	4	88	6	8	22	8	6	[TL19]	✓
a_3	7	4	88	6	8	20	8	7	[TL19]	✓
a_4	7	4	90	6	8	24	8	7	[TL19]	✓
s_{112}	7	2	112	2	0	3	0	2	[GM23a]	✓
s_{114}	7	2	114	2	0	3	0	2	[GM23a]	✓
s_{116}	7	2	**116**	2	0	3	0	2	[GM23a]	✓
p_1	7	2	64	6	19	21	11	3	[GM23c]	✓
p_2	7	2	76	6	14	20	11	6	[GM23c]	✓
p_3	7	2	82	7	15	18	14	6	[GM23c]	✓
$g_{2,8}$	4	3	88	5	10	16	12	5	[GM22b]	✓
$g_{4,8}$	4	3	88	3	7	15	11	3	[GM22b]	✓
$g_{6,8}$	4	3	96	2	12	18	12	2	[GM22b]	✓
g_1	7	4	106	7	17	21	18	7	SUR	✓
g_2	7	4	104	7	15	19	19	7	SUR	✓
g_3	7	4	104	5	18	23	17	6	SUR	✓
	6	4	112	6	19	23	18	8	[MKCL22]	✓
	7	4	112	6	18	25	17	6	[MKCL22]	✓
h_3	7	4		6	17	23	17	6	[ZJZQ23]	
F_8	7	4		4	16	20	16	4	[DM]	

Table 5: Criteria of some 8-variable WPB functions from known constructions, referred in the last column. SUR corresponds to functions sampled uniformly at random. ✓ indicates that we were able to recompute this values.

3 Selection of $\mathcal{S}_0$-classes

We report the $\mathcal{S}_0$-classes [GM23b, Definition 15] of some known constructions in 8 variables from Table 5 from [GM23b, Section 6].

NL	84	88	92	96	100	104
#	8	68	16	20	4	12

deg	4	5	6	7
#	16	16	32	64

AI	3	4
#	36	92

Table 6: Distribution of nonlinearities, degree and algebraic immunity in $\mathcal{S}_0(f_8)$.

	NL	96	100	104	106	108	110	112
$\mathcal{S}_0(l)$	#	0	0	4	16	24	48	36
$\mathcal{S}_0(l')$	#	16	0	48	12	40	8	4
$\mathcal{S}_0(l'')$	#	16	4	80	8	0	20	0

deg	7
#	128
#	128
#	128

AI	3	4
#	0	128
#	0	128
#	14	114

Table 7: Distribution of nonlinearities, degree and algebraic immunity in $\mathcal{S}_0(l)$, $\mathcal{S}_0(l')$ and $\mathcal{S}_0(l'')$.

	AI	2	3	4
$\mathcal{S}(s_{112})$	#	24	96	8
$\mathcal{S}(s_{114})$	#	32	88	8
$\mathcal{S}(s_{116})$	#	32	88	8

deg	7
#	128
#	128
#	128

	NL	8	16	24	32	40	48	56	64	72	88	90	92	94	96	104	110	112	114	116
$\mathcal{S}_0(s_{112})$	#	4	8	4	8	16	8	4	16	12	16	2	2	2	10	4	8	4	0	0
$\mathcal{S}_0(s_{114})$	#	4	8	4	8	16	8	4	16	12	16	2	4	2	8	4	8	2	2	0
$\mathcal{S}_0(s_{116})$	#	4	8	4	8	16	8	4	16	12	16	4	4	0	8	4	8	0	0	4

Table 9: Distribution of nonlinearities, degree and algebraic immunity in $\mathcal{S}_0(s_{112})$, $\mathcal{S}_0(s_{114})$ and $\mathcal{S}_0(s_{116})$.

	AI	2	3	4
$\mathcal{S}_0(p_1)$	#	4	56	68
$\mathcal{S}_0(p_2)$	#	4	56	68
$\mathcal{S}_0(p_3)$	#	4	58	66

deg	7
#	128
#	128
#	128

	NL	64	66	70	72	74	76	78	80	82	84	86	88	90	92	94	96	98	100	102	104	106	108	110
$\mathcal{S}_0(p_1)$	#	2	2	4	4	0	2	4	2	2	6	6	6	16	14	20	6	12	0	8	0	8	2	2
$\mathcal{S}_0(p_2)$	#	0	0	0	2	6	6	4	6	6	2	6	6	14	4	16	8	6	20	6	10	0	0	0
$\mathcal{S}_0(p_3)$	#	0	0	2	4	2	4	8	4	2	6	6	2	6	14	10	12	10	6	8	16	6	0	0

Table 10: Distribution of nonlinearities, degree and algebraic immunity and in $\mathcal{S}_0(p_1)$, $\mathcal{S}_0(p_2)$ and $\mathcal{S}_0(p_3)$.

	AI	3	4
$\mathcal{S}_0(a_1)$	#	64	64
$\mathcal{S}_0(a_2)$	#	64	64
$\mathcal{S}_0(a_3)$	#	64	64
$\mathcal{S}_0(a_4)$	#	64	64

deg	7
#	128
#	128
#	128
#	128

NL	80	88	90	92	94	96	98	100	102
#	16	36	8	6	16	22	14	8	2
#	16	36	10	10	12	32	12	0	0
#	16	36	10	10	18	36	2	0	0
#	16	34	6	8	14	34	4	6	6

Table 8: Distribution of nonlinearities, degree and algebraic immunity in $\mathcal{S}_0(a_1)$, $\mathcal{S}_0(a_2)$, $\mathcal{S}_0(a_3)$ and $\mathcal{S}_0(a_4)$.

	NL	94	96	98	100	102	104	106	108	110
$\mathcal{S}_0(g_1)$	#	2	6	14	4	24	34	30	14	0
$\mathcal{S}_0(g_2)$	#	0	2	14	8	52	24	26	2	0
$\mathcal{S}_0(g_3)$	#	0	0	8	8	24	48	34	4	2

Table 11: Distribution of nonlinearities in $\mathcal{S}_0(g_1)$, $\mathcal{S}_0(g_2)$ and $\mathcal{S}_0(g_3)$.

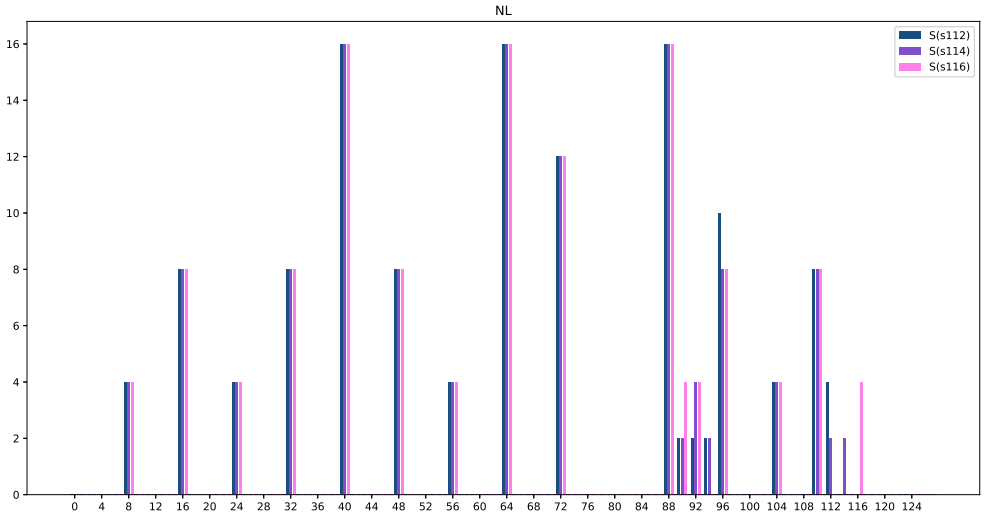

Figure 1: Display of nonlinearity's distribution in Table 9

References

[CMR17] Claude Carlet, Pierrick Méaux, and Yann Rotella. Boolean functions with restricted input and their robustness; application to the FLIP cipher. *IACR Trans. Symmetric Cryptol.*, 2017(3), 2017.

[DM] Deepak Kumar Dalai and Krishna Mallick. A class of weightwise almost perfectly balanced boolean functions with high weightwise nonlinearity (extended abstract). BFA2023.

[GM22a] Agnese Gini and Pierrick Méaux. On the weightwise nonlinearity of weightwise perfectly balanced functions. *Discret. Appl. Math.*, 322:320–341, 2022.

[GM22b] Agnese Gini and Pierrick Méaux. Weightwise almost perfectly balanced functions: Secondary constructions for all n and better weightwise nonlinearities. In Takanori Isobe and Santanu Sarkar, editors, *Progress in Cryptology - INDOCRYPT*, volume 13774 of *Lecture Notes in Computer Science*, pages 492–514. Springer, 2022.

[GM23a] Agnese Gini and Pierrick Méaux. Weightwise perfectly balanced functions and nonlinearity. In Said El Hajji, Sihem Mesnager, and El Mamoun Souidi, editors, *Codes, Cryptology and Information Security*, pages 338–359, Cham, 2023. Springer Nature Switzerland.

[GM23b] Agnese Gini and Pierrick Méaux. $\mathcal{S}_0$-equivalent classes, a new direction to find better weightwise perfectly balanced functions, and more. Cryptology ePrint Archive, Paper 2023/1101, 2023. `https://eprint.iacr.org/2023/1101`.

[GM23c] Agnese Gini and Pierrick Méaux. On the algebraic immunity of weightwise perfectly balanced functions. Cryptology ePrint Archive, Paper 2023/495, 2023. `https://eprint.iacr.org/2023/495`.

[LM19] Jian Liu and Sihem Mesnager. Weightwise perfectly balanced functions with high weightwise nonlinearity profile. *Des. Codes Cryptogr.*, 87(8):1797–1813, 2019.

[LS20] Jingjing Li and Sihong Su. Construction of weightwise perfectly balanced boolean functions with high weightwise nonlinearity. *Discret. Appl. Math.*, 279:218–227, 2020.

[MKCL22] Sara Mandujano, Juan Carlos Ku Cauich, and Adriana Lara. Studying special operators for the application of evolutionary algorithms in the seek of optimal boolean functions for cryptography. In Obdulia Pichardo Lagunas, Juan Martínez-Miranda, and Bella Martínez Seis, editors, *Advances in Computational Intelligence*, pages 383–396, Cham, 2022. Springer Nature Switzerland.

[MS21] Sihem Mesnager and Sihong Su. On constructions of weightwise perfectly balanced boolean functions. *Cryptography and Communications*, 2021.

[MSL21] Sihem Mesnager, Sihong Su, and Jingjing Li. On concrete constructions of weightwise perfectly balanced functions with optimal algebraic immunity and high weightwise nonlinearity. *Boolean Functions and Applications*, 2021.

[Su21] Sihong Su. The lower bound of the weightwise nonlinearity profile of a class of weightwise perfectly balanced functions. *Discret. Appl. Math.*, 297:60–70, 2021.

[TL19] Deng Tang and Jian Liu. A family of weightwise (almost) perfectly balanced boolean functions with optimal algebraic immunity. *Cryptogr. Commun.*, 11(6):1185–1197, 2019.

[YCL+23] Lili Yan, Jingyi Cui, Jian Liu, Guangquan Xu, Lidong Han, Alireza Jolfaei, and Xi Zheng. Iga: An improved genetic algorithm to construct weightwise (almost) perfectly balanced boolean functions with high weightwise nonlinearity. ASIA CCS '23, page 638–648, New York, NY, USA, 2023. Association for Computing Machinery.

[ZJZQ23] Qinglan Zhao, Yu Jia, Dong Zheng, and Baodong Qin. A new construction of weightwise perfectly balanced functions with high weightwise nonlinearity. *Mathematics*, 11(5), 2023.