On the Cardinality of the Walsh Support of Boolean Functions (Extended Abstract)

Maxence Jauberty, Pierrick Méaux[0000−0001−5733−4341]

University of Luxembourg, Luxembourg
pierrick.meaux@uni.lu, maxence.jauberty@ext.uni.lu

1 Introduction

Functions from $\mathbb{F}_2^n$ to $\mathbb{F}_2$ are called Boolean functions and are central to cryptography, coding theory, and several branches of discrete mathematics. In this extended abstract , we focus on the Walsh transform of a Boolean function, where the Walsh transform of the Boolean function f at the point $a \in \mathbb{F}_2^n$ is defined as $W_f(a) := \sum_{x\in\mathbb{F}_2^n}(-1)^{f(x)\oplus a\cdot x}$ where $a \cdot x$ denotes the usual inner product in $\mathbb{F}_2^n$. More precisely, we focus on the support of the Walsh transform of a function f $\mathsf{Wsupp}_f := \{a \in \mathbb{F}_2^n \mid W_f(a) \neq 0\}$, and in particular the attainable cardinalities of that set. For an integer $n \geq 1$ we denote by $C_n \subset \mathbb{N}$ the set of cardinalities of the Walsh support of Boolean functions in n variables.

The Walsh transform is the principal analytic tool for evaluating cryptographic indicators of Boolean functions. Specifically, the nonlinearity of f is given by $2^{n-1} - \frac{1}{2}\max_{a\in\mathbb{F}_2^n}\left|W_f(a)\right|$, while the order of resilience equals the largest integer m for which $W_f(a) = 0$ whenever $1 \leq \mathsf{w_H}(a) \leq m$, where $\mathsf{w_H}$ denotes the Hamming weight. Beyond these global parameters, the geometry of the Walsh support itself has recently been exploited in the characterization of plateaued functions [7] and of spectra with only a few distinct values [8, 14].

The Walsh support encodes resilience properties and provides insight into whether affine-equivalent functions may exhibit improved resilience. A motivation to study this support arises from [5], which investigates the existence and significance of Boolean functions combining optimal algebraic immunity with high resilience. On the negative side, the structure of the Walsh support is used in [5] to rule out the existence of 1-resilient functions within the affine equivalence class of majority functions in an odd number of variables. On the positive side, a deeper understanding of the Walsh support may offer a foundation for constructing functions that simultaneously achieve optimal algebraic immunity and high resilience. These parameters are critical for instantiating Goldreich's PseudoRandom Generator [6] (PRG) within the class NC^0, as explored in *e.g.* [1,4,13,15]. The existence of a secure PRG in NC^0[1] has far-reaching implications in cryptology, including the construction of indistinguishability obfuscation [9].

Despite its importance, the structure of the Walsh support remains poorly understood; even the set of its possible cardinalities is not fully determined. To the best of our knowledge, the first systematic study was conducted by Pei and Qin [11], who showed that a Walsh support cannot have cardinality 2, 3, 5, 6, or 7, and fully characterized the cases of cardinalities 4 and 8. In 2004, Carlet and Mesnager [3] carried out a more in-depth investigation. They enumerated all possible Walsh supports for functions in five variables , and studied in particular those with support $\mathbb{F}_2^n \setminus \{0\}$. They proved that no such support arises for $n \leq 5$, but provided constructions for $n \geq 10$. More recently, Lou and Wang [10] resolved the remaining open cases for cardinality $2^n - 1$: they constructed examples for $n \in \{7, 8, 9\}$, and proved by exhaustive search that no such function exists for $n = 6$.

From [3], we deduce that $C_5 = \{1, 4, 8, 10, 13, 16, 18, 20, 21, 22, 23, 24, 25, 26, 28, 32\}$. Experimental evidence shows that certain elements of $[1, 2^5]$ which do not belong to C_5 appear in C_6 (*e.g.* $27, 29, 30, 31$

[1] Nick's class 0, NC^0 is the class of decision problems decidable by uniform Boolean circuits of constant depth and polynomial size where each gate has bounded fan-in$[a, b]$.

), while some elements of $[2^5+1, 2^6]$ are absent from C_6 (*e.g.* 63). These observations raise two main questions: (1) Are there always missing elements in the interval $[2^{n-1}+1, 2^n]$ for each n? (2) Which elements not in C_n eventually belong to some C_m with $m > n$?

In this work, we show that for all $n \geq 7$, the set C_n can be completely characterized as:

$$C_n = [1, 2^n] \setminus \{2, 3, 5, 6, 7, 9, 11, 12, 14, 15, 17, 19\}.$$

Our approach begins with a characterization of the structure of the Walsh support s of cardinality less than 16. We then establish the impossibility of several small cardinalities through direct arguments. Finally, we provide constructions that allow us to prove, by induction, that all cardinalities greater than 19 are possible.

2 Preliminaries

A *Boolean function* f in n variables (an n-variable Boolean function) is a function from $\mathbb{F}_2^n$ to $\mathbb{F}_2$. The set of all Boolean functions in n variables is denoted by $\mathcal{B}_n$.

The *Walsh transform* of $f \in \mathcal{B}_n$ is the function $W_f : \mathbb{F}_2^n \to \mathbb{Z}$ defined by:

$$\forall a \in \mathbb{F}_2^n,\ W_f(a) := \sum_{x \in \mathbb{F}_2^n} (-1)^{f(x) \oplus a \cdot x}.$$

The Walsh support of f is the set $\mathsf{Wsupp}_f := \{a \in \mathbb{F}_2^n \mid W_f(a) \neq 0\}$, and the Walsh (absolute) spectrum is the multiset $\mathsf{AWspec}_f = \{w \times m(w) \mid \exists a \in \mathbb{F}_2^n,\ |W_f(a)| = w\}$ where $m(w) = |\{a \in \mathbb{F}_2^n \mid\ |W_f(a)| = w\}|$.

We will mainly focus on the cardinality of the Walsh support. Therefore, we also define the set $\mathcal{B}_{n,s}$ of n -variable Boolean functions having a Walsh support of cardinality s, i.e. $\mathcal{B}_{n,s} := \{f \in \mathcal{B}_n \mid \left|\mathsf{Wsupp}_f\right| = s\}$.

Two Boolean functions $f, g \in \mathcal{B}_n$ are said *extended affine equivalent* if there exist an automorphism $L : \mathbb{F}_2^n \to \mathbb{F}_2^n$, two vectors $a, b \in \mathbb{F}_2^n$ and $c \in \mathbb{F}_2$ such that $g(x) = f(a + L(x)) \oplus b \cdot x \oplus c$. Two extended affine equivalent Boolean functions f and g have the same structure of Walsh support (see [3]), that is, for any decomposition of the Walsh support of f as a disjoint union of affine spaces, the Walsh support of g also admits a decomposition into a disjoint union of the same number of affine spaces with the same respective dimensions.

In this work, we frequently use a secondary construction of Boolean functions, known both as *Siegenthaler's construction* [12] and as the concatenation construction . For any functions $f, g \in \mathcal{B}_n$, we define the Siegenthaler 's construction $h = \mathsf{Sieg}\,[f, g] \in \mathcal{B}_{n+1}$ of f and g as the function: $h(x, y) = (1 \oplus y)f(x) \oplus yg(x)$ for $(x, y) \in \mathbb{F}_2^n \times \mathbb{F}_2$. f and g are also called the sub-functions of h. One can deduce the expression of W_h using W_f and W_g using the following relation:

$$\forall (u, v) \in \mathbb{F}_2^n \times \mathbb{F}_2,\ W_h(u, v) = W_f(u) + (-1)^v W_g(u). \tag{1}$$

Since any function $h \in \mathcal{B}_n$ can be seen as a Siegenthaler's construction by identifying one variable (as $\mathsf{Sieg}\,[h(x, 0), h(x, 1)]$), Relation 1 can be used to study the Walsh spectrum of h using the Walsh support s of its subfunctions. In particular, we study for any functions $f, g \in \mathcal{B}_n$ the following sets:

$$K(f, g) := \mathsf{Wsupp}_f \cap \mathsf{Wsupp}_g \quad \text{and} \quad \Xi(f, g) := \{a \in K(f, g) \mid\ |W_f(a)| = |W_g(a)|\}.$$

We also denote by k and ξ the cardinalities of $K(f, g)$ and $\Xi(f, g)$, respectively, when there is no ambiguity about f or g. Based on these sets, we can study in more details the cardinality of the Walsh support obtained from Siegenthaler's construction:

Lemma 1. *Let $f \in \mathcal{B}_{n,s}$, $g \in \mathcal{B}_{n,t}$ and $h = \mathsf{Sieg}\,[f, g]$. Denote $k = |K(f, g)|$ and $\xi = |\Xi(f, g)|$, then:*

$$|\mathsf{Wsupp}_h| = 2(s + t) - 2k - \xi.$$

3 Structure of the Walsh Supports of Small Cardinality

In this section, we give results on the Walsh supports of small cardinalities . The few results already established show that for small cardinalities the number of possible structures is limited. The first example corresponds to the Walsh supports of cardinality 1, they are the singletons of $\mathbb{F}_2^n$, and correspond to the affine functions. In [11], it has been established that a Walsh support has cardinality 4 or 8 if and only if it is an affine subspace of $\mathbb{F}_2^n$, respectively of dimension 2 and 3.

Proposition 1 ([11]). *Let $f \in \mathcal{B}_{n,s}$, then we have:*

- *$s = 4$ if and only if Wsupp_f is an affine subspace of $\mathbb{F}_2^n$ of dimension 2.*
  Moreover, $\mathsf{AWspec}_f = \{2^{n-1} \times 4,\ 0 \times (2^n - 4)\}$,
- *$s = 8$ if and only if Wsupp_f is an affine subspace of $\mathbb{F}_2^n$ of dimension 3.*
  Moreover, $\mathsf{AWspec}_f = \{3 \cdot 2^{n-2} \times 1,\ 2^{n-2} \times 7,\ 0 \times (2^n - 8)\}$.

We derive properties on the cardinality of the Walsh support based on Siegenthaler's construction. It allows us to study the structure of Walsh support further by characterizing the Walsh supports of cardinalities 10 and 13, and derive properties on the Walsh supports of cardinality 16. Finally, it enables us to discard potential cardinalities lower than 20.

3.1 More from Siegenthaler's Construction

The following result bounds the cardinality of the Walsh support of a function obtained from Siegenthaler's construction:

Lemma 2. *Let $h \in \mathcal{B}_{n+1,r}$ such that $h = \mathsf{Sieg}\,[f, g]$ with $f \in \mathcal{B}_{n,s}$ and $g \in \mathcal{B}_{n,t}$. Then, $\max\{s, t\} \leq r \leq 2(s + t)$.*

Therefore, given s, t, one may observe, according to the properties of the Walsh supports of cardinalities s and t, that k and ξ are constrained. For example, if $s, t \leq 8$, then k must be 0 or a power of two since the Walsh supports are affine spaces.

There are simple examples for the two extremes of Lemma 2. Taking twice the function f, we have $f \in \mathcal{B}_{n,s}$, $g = f$ and $h \in \mathcal{B}_{n+1,s}$. Taking f and g such that $K(f, g) = \emptyset$ is an example of the other extreme case: $f \in \mathcal{B}_{n,s}, g \in \mathcal{B}_{n,t}$ and $h \in \mathcal{B}_{n+1,2s+2t}$.

Using that $\mathcal{B}_1 = \mathcal{B}_{1,1}$ and for $n \geq 2$ any function can be written as the result of Siegenthaler's construction, Lemma 2 allows us to derive the impossibility of some cardinalities :

Lemma 3. *Let $r \geq 2$, if for all $s \in [t, r - 1]$ there exists no $n \in \mathbb{N}$ such that a 4-tuple (s, t, k, ξ) with $r = 2(s + t - k) - \xi$ satisfies Lemma 1, then for all $n \in \mathbb{N}$, there exists no function $f \in \mathcal{B}_{n,r}$.*

3.2 The Walsh Support s of cardinalities 10, 13 and 16

The main method to characterize the structure of the Walsh supports of small cardinalities is to search for the 4-tuples (s, t, k, ξ) as in Lemma 1 such that $2(s + t) - 2k - \xi$ equals the desired cardinality and reason using Titsworth's relation (*e.g.* [2] Equation 2.51). We first give the characterization of the supports of cardinalities 10 and 13.

Theorem 1. *Let $f \in \mathcal{B}_{n,s}$, then we have:*

- *$s = 10$ if and only if $\mathsf{Wsupp}_f = V \cup D$ where V is an affine subspace of dimension 3 and D is an affine subspace of dimension 1 such that D is parallel to one edge of V. Moreover, for $u \in D$, $|W_f(u)| = 2^{n-1}$ and for $u \in V$, $|W_f(u)| = 2^{n-2}$.*

– $s = 13$ *if and only if* $\mathsf{Wsupp}_f = V_1 \cup V_2 \setminus \{b\}$ *where* V_1 *and* V_2 *are two affine subspaces of dimension* 3 *such that* $V_1 \cap V_2 = \{a, b\}$. *Moreover,* $|W_f(a)| = 2^{n-1}$ *and* $\forall u \in \left(\mathsf{Wsupp}_f \setminus \{a\}\right)$, $|W_f(u)| = 2^{n-2}$.

Note that the description of the Walsh support for $s = 13$ is not given as a disjoint union of affine spaces in order to preserve the geometric intuition; however, it can still be described as a disjoint union of affine spaces of dimensions 0, 1 and 2.

We also give some properties on the Walsh supports of cardinality 16, they are essential to derive the results for the impossible cardinalities stated in the next part.

Proposition 2. *Let* $f \in \mathcal{B}_{n,16}$, *then we have:*

– AWspec_f *equals*
$\{7 \cdot 2^{n-3} \times 1,\ 2^{n-3} \times 15,\ 0 \times (2^n - 16)\}$ *or* $\{5 \cdot 2^{n-3} \times 1,\ 3 \cdot 2^{n-3} \times 3,\ 2^{n-3} \times 12,\ 0 \times (2^n - 16)\}$ *or* $\{2^{n-2} \times 16,\ 0 \times (2^n - 16)\}$,
– $\bigoplus_{u \in \mathsf{Wsupp}_f} u = 0$.

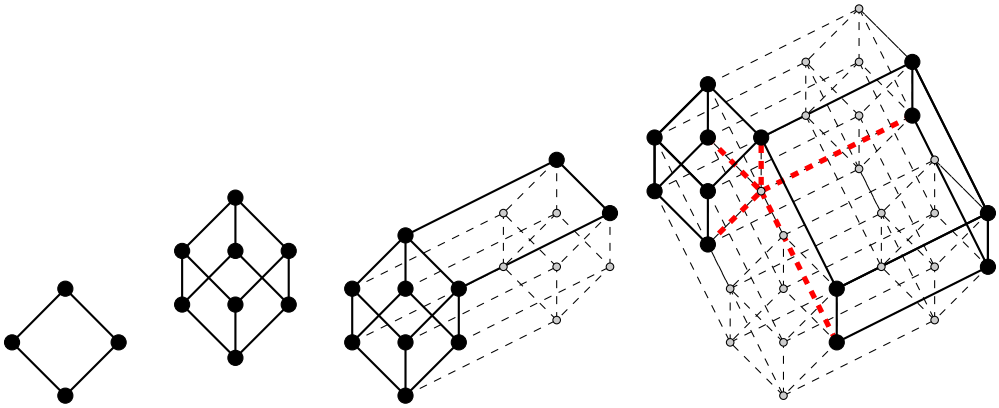

Fig. 1: Representation of each structure with cardinality $s \in \{4, 8, 10, 13\}$ from left to right. The black nodes are the points of the Walsh support belonging respectively to $\mathbb{F}_2^2, \mathbb{F}_2^3, \mathbb{F}_2^4, \mathbb{F}_2^5$.

3.3 Impossible Cardinalities for Walsh Supports

In Figure 2, we give the possible 4- tuples leading to a cardinality between 9 and 20. The results are obtained by combining the different lemmas, theorems and propositions from the previous parts. They result in the following theorem:

Theorem 2. *Let* $n \in \mathbb{N}$, *if* $r \in \{9, 11, 12, 14, 15, 17, 19\}$ *then* $\mathcal{B}_{n,r} = \emptyset$.

4 Constructing the Walsh Supports of Large Cardinalities

4.1 Constructions to Reach Larger Supports

In this part, we present generic constructions such that given a function f having a Walsh support of cardinality s, we obtain a function having a Walsh support of cardinality $m \cdot s + l$. We introduce constructions using the Walsh support s of cardinality 1.

Construction 1 ($s \to 2s$)**.** *Let* $f \in \mathcal{B}_{n,s}$ *such that* $s > 1$. *Consider* $a \in \mathsf{Wsupp}_f$ *and let* $g : x \mapsto a \cdot x$. *Define* $h = \mathsf{Sieg}\,[f, g]$. *We have then* $|\mathsf{Wsupp}_h| = 2s$.

r	(s_1,t_1,k_1,ξ_1)	(s_2,t_2,k_2,ξ_2)	(s_3,t_3,k_3,ξ_3)	r	(s_1,t_1,k_1,ξ_1)	(s_2,t_2,k_2,ξ_2)	(s_3,t_3,k_3,ξ_3)	(s_4,t_4,k_4,ξ_4)
9				15				
10	$(1,4,0,0)$	$(4,4,2,2)$	$(8,8,8,6)$	16	$(1,8,1,0)$	$(4,4,0,0)$	$(10,10,8,8)$	$(13,13,12,12)$
11				17				
12				18	$(1,8,0,0)$	$(4,10,4,2)$	...	...
13	$(4,4,1,1)$	$(8,10,8,7)$	$(10,10,9,9)$	19				
14				20	$(1,10,1,0)$	...	...	...

Fig. 2: Table r is the cardinality constructed using Siegenthaler 's construction . Each possible (s,t,k,ξ) such that $s \leq t$ and $s,t \neq r$ are represented for each r. Dots in the array state that there are other 4- tuples but we do not have an exhaustive list.

Construction 2 ($s \to 2s+2$)**.** *Let $f \in \mathcal{B}_{n,s}$ such that $s < 2^n$. Consider $a \notin \mathsf{Wsupp}_f$ and let $g : x \mapsto a \cdot x$. Define $h = \mathsf{Sieg}[f,g]$. We have then $|\mathsf{Wsupp}_h| = 2s+2$ and $2^n \in \mathsf{AWspec}_h$.*

These constructions are of the form $\mathsf{Sieg}[f,g]$ with g being an affine function. We can use the structure of the Walsh support s of cardinality 4 to consider constructions of the form $\mathsf{Sieg}[f,g]$ with g having a Walsh support of cardinality 4. According to Lemma 1, if $\xi = 1$ we can construct Walsh support s of odd cardinalities .

Construction 3. *Let $f \in \mathcal{B}_{n,s}$ with $8 < s < 2^{n-1}$ and $2^{n-1} \in \mathsf{AWspec}_f$. Consider a function $g \in \mathcal{B}_{n,4}$ such that $|K(f,g)| = 2$ and $|\Xi(f,g)| = 1$. Define $h = \mathsf{Sieg}[f,g]$. Then we have $|\mathsf{Wsupp}_h| = 2s+3$.*

Construction 4. *Let $f \in \mathcal{B}_{n,s}$ with $8 < s < 2^{n-1}$ and $2^{n-1} \in \mathsf{AWspec}_f$. Consider a function $g \in \mathcal{B}_{n,4}$ such that $|K(f,g)| = |\Xi(f,g)| = 1$. Define $h = \mathsf{Sieg}[f,g]$. Then we have $|\mathsf{Wsupp}_h| = 2s+5$.*

The constraint $s < 2^{n-1}$ although not ideal ensures that both Constructions 3 and 4 always work. We develop the idea to use the Walsh support of cardinality 4 to construct odd cardinalities but we apply it on a function obtain through a $2s+2$ construction Construction 2 . Therefore, we can choose wisely the points of value 2^{n-1} that we are going to intersect with the support of cardinality 4 such that $k = 3$ or $k = 4$. We obtain the following proposition:

Proposition 3. *Let $f \in \mathcal{B}_{n,s}$ such that $2^{n-1} \leq s < 2^n$. Then,*

- *Then there exists $g_1 \in \mathcal{B}_{n+2}$ such that $2^{n+1} \in \mathsf{AWspec}_{g_1}$ and $\left|\mathsf{Wsupp}_{g_1}\right| = 4s+3$,*
- *If $s \neq 2^n - 1$, then there exists $g_2 \in \mathcal{B}_{n+2}$ such that $2^{n+1} \in \mathsf{AWspec}_{g_2}$ and $\left|\mathsf{Wsupp}_{g_2}\right| = 4s+5$.*

4.2 Construction of All Possible Cardinalities Over 19

To show the existence of a Walsh support of any cardinality greater than 19 we use the following lemma:

Lemma 4. *For $n \geq 6$, we denote by P_n the following properties:*

- $[2^n, 2^{n+1}] \subset C_{n+1}$,
- $\exists f \in \mathcal{B}_{n+2,2^{n+1}-1}$ *such that* $2^{n+1} \in \mathsf{AWspec}_f$.

Then, if P_n is verified then P_{n+2} is also verified.

We verified P_6 and P_7 with computer search, therefore we can prove by induction that for any $n \geq 6$ P_n is verified. In particular, for any $n \geq 7$ it implies that $[2^{n-1}+1, 2^n] \subset C_n$, which is sufficient to prove the following theorem:

Theorem 3. *Let $n \geq 7$, then we have:*

$$C_n = [1, 2^n] \setminus \{2, 3, 5, 6, 7, 9, 11, 12, 14, 15, 17, 19\}$$

Additionally we have the following for smaller values of n:

- $C_1 = \{1\}$, $C_2 = \{1, 4\}$, $C_3 = \{1, 4, 8\}$ and $C_4 = \{1, 4, 8, 10, 16\}$,
- $C_5 = [1, 2^5] \setminus \{2, 3, 5, 6, 7, 9, 11, 12, 14, 15, 17, 19, 27, 29, 30, 31\}$,
- $C_6 = [1, 2^6] \setminus \{2, 3, 5, 6, 7, 9, 11, 12, 14, 15, 17, 19, 63\}$.

References

1. Applebaum, B., Lovett, S.: Algebraic attacks against random local functions and their countermeasures. In: STOC. pp. 1087–1100. ACM (2016). https://doi.org/10.1145/2897518.2897554
2. Carlet, C.: Boolean Functions for Cryptography and Coding Theory. Cambridge University Press (2021). https://doi.org/10.1017/9781108606806
3. Carlet, C., Mesnager, S.: On the supports of the walsh transforms of boolean functions. IACR Cryptol. ePrint Arch. p. 256 (2004), `http://eprint.iacr.org/2004/256`
4. Couteau, G., Dupin, A., Méaux, P., Rossi, M., Rotella, Y.: On the concrete security of goldreich's pseudorandom generator. In: ASIACRYPT 2018. vol. 11273, pp. 96–124. Springer (2018). https://doi.org/10.1007/978-3-030-03329-3_4
5. Dupin, A., Méaux, P., Rossi, M.: On the algebraic immunity - resiliency trade-off, implications for goldreich's pseudorandom generator. Des. Codes Cryptogr. **91**(9), 3035–3079 (2023). https://doi.org/10.1007/S10623-023-01220-W
6. Goldreich, O.: Candidate one-way functions based on expander graphs. Electronic Colloquium on Computational Complexity (ECCC) **7**(90) (2000)
7. Hodzic, S., Pasalic, E., Wei, Y., Zhang, F.: Designing plateaued boolean functions in spectral domain and their classification. IEEE Trans. Inf. Theory **65**(9), 5865–5879 (2019). https://doi.org/10.1109/TIT.2019.2909910
8. Hodžić, S., Horak, P., Pasalic, E.: Characterization of basic 5-value spectrum functions through walsh-hadamard transform. IEEE Transactions on Information Theory **67**(2), 1038–1053 (2021). https://doi.org/10.1109/TIT.2020.3044059
9. Jain, A., Lin, H., Sahai, A.: Indistinguishability obfuscation from well-founded assumptions. In: Khuller, S., Williams, V.V. (eds.) STOC. pp. 60–73. ACM (2021). https://doi.org/10.1145/3406325.3451093
10. Lou, Y., Wang, Q.: An answer to an open problem on balanced boolean functions with the maximum possible walsh supports. In: ISIT. pp. 1608–1612 (2024). https://doi.org/10.1109/ISIT57864.2024.10619662
11. Pei, D., Qin, W.: The correlation of a boolean function with its variables. In: Roy, B.K., Okamoto, E. (eds.) INDOCRYPT. Lecture Notes in Computer Science, vol. 1977, pp. 1–8. Springer (2000). https://doi.org/10.1007/3-540-44495-5_1
12. Siegenthaler, T.: Correlation-immunity of nonlinear combining functions for cryptographic applications. IEEE **IT-30**(5), 776–780 (1984)
13. Ünal, A.: Worst-case subexponential attacks on prgs of constant degree or constant locality. In: EUROCRYPT 2023. vol. 14004, pp. 25–54. Springer (2023). https://doi.org/10.1007/978-3-031-30545-0_2
14. Wang, J., Fu, F.W.: Three new constructions of 5-valued spectrum functions with totally disjoint spectra duals. In: ISIT. pp. 1743–1748 (2022). https://doi.org/10.1109/ISIT50566.2022.9834570
15. Yang, J., Guo, Q., Johansson, T., Lentmaier, M.: Revisiting the concrete security of goldreich's pseudorandom generator. IEEE Trans. Inf. Theory **68**(2), 1329–1354 (2022). https://doi.org/10.1109/TIT.2021.3128315