On the Algebraic Immunity - Resiliency trade-off, implications for Goldreich's Pseudorandom Generator

Aurélien Dupin[1], Pierrick Méaux[2], Mélissa Rossi[3]

[1] Thales SIX
aurelien.dupin@thalesgroup.fr
[2] University of Luxembourg, Luxembourg
pierrick.meaux@uclouvain.be
[3] ANSSI
melissa.rossi@ssi.gouv.fr

Abstract. Goldreich's pseudorandom generator is a well-known building block for many theoretical cryptographic constructions from multi-party computation to indistinguishability obfuscation. Its unique efficiency comes from the use of random local functions: each bit of the output is computed by applying some fixed public n-variable Boolean function f to a random public size-n tuple of distinct input bits. The characteristics that a Boolean function f must have to ensure pseudorandomness is a puzzling issue. It has been studied in several works and particularly by Applebaum and Lovett (STOC 2016) who showed that resiliency and algebraic immunity are key parameters in this purpose.
In this paper, we propose the first study on Boolean functions that reach together maximal algebraic immunity and high resiliency.
1) We assess the possible consequences of the asymptotic existence of such optimal functions. We show how they allow to build functions reaching all possible algebraic immunity-resiliency trade-offs (respecting the algebraic immunity and Siegenthaler bounds). We provide a new bound on the minimal number of variables n, and thus on the minimal locality, necessary to ensure a secure Goldreich's pseudorandom generator. Our results come with a granularity level depending on the strength of our assumptions, from none to the conjectured asymptotic existence of optimal functions.
2) We extensively analyze the possible existence and the properties of such optimal functions. Our results show two different trends. On the one hand, we were able to show some impossibility results concerning existing families of Boolean functions that are known to be optimal with respect to their algebraic immunity, starting by the promising XOR-MAJ functions. We show that they do not reach optimality and could be beaten by optimal functions if our conjecture is verified. On the other hand, we prove the existence of optimal functions in low number of variables by experimentally exhibiting some of them up to 12 variables. This directly provides better candidates for Goldreich's pseudorandom generator than the existing XOR-MAJ candidates for polynomial stretches from 2 to 6.

Keywords: Boolean functions, local PRG, algebraic immunity, resiliency.

1 Introduction

The core of our paper lies in the Boolean function domain but our results help providing new optimal instances for Goldreich's PseudoRandom Generator (PRG) in a provable way for low localities and in a conjectured way for the asymptotic version. Our results allow to reduce any algebraic immunity-resiliency trade-off arising in local pseudorandom generators to the existence of a particular family of Boolean functions. We suggest two reading paths depending if the reader is more interested in the implications on Goldreich's PRG, or on the Boolean function's side: on the possible trade-offs between algebraic immunity and resiliency of Boolean functions.

- For a reader interested in Goldreich's PRG, we suggest to follow most of the introduction. We provide here some background on local pseudorandom generators in Section 1.1. In Section 1.2, we introduce the algebraic immunity and resiliency criteria. In Section 1.3, we motivate the study of algebraic immunity/resiliency trade-offs from both random local functions and Boolean functions perspectives. Then, our contributions are summarized in Section 1.5. After the introduction, we advise the reader to focus on Section 3 then Section 5, and Section 4.1 if the reader is interested by XOR-MAJ functions.

– For a reader more interested in the trade-off algebraic immunity/resiliency from the Boolean function's perspective, we suggest to directly move to Section 1.4, and then Section 1.5 for our contributions. After the introduction, we advise the reader to look at Definition 14 and the conjectures in Section 3.3, and then to focus on Section 4, Section 5, and Appendix A.

1.1 Goldreich's pseudorandom generator

Local pseudorandom generators are an intriguing foundation stone of a variety of cryptographic constructions. This primitive allows to expand a short random string into a long pseudorandom string, such that each output bit only depends on a constant number n of input bits. As introduced by Goldreich in 2000 [Gol00], Goldreich's PRG has become the most known construction that achieves this goal. It consists in applying a simple n-local function f to random (public) size-n subsets of the bits of the input.

Before focusing on criteria on n-local functions for ensuring pseudorandomness, let us briefly introduce more formally the context. We first introduce the definition of a PRG to fix the notations. Throughout, for $n \in \mathbb{N}^*$ we denote $[n]$ the set $\{k \in \mathbb{N} \mid 1 \leq k \leq n\}$. We also denote $a \leftarrow_\$ S$ when a is taken uniformly at random from the set S.

Definition 1 (Pseudorandom Generator). *Let $t \in \mathbb{N}^*$ and let m be a polynomial in t. An $m(t)$-stretch pseudorandom generator is an efficient uniform deterministic algorithm* PRG *which, on input a seed $x \in \mathbb{F}_2^t$, outputs a string $y \in \mathbb{F}_2^{m(t)}$. It satisfies the following security notion: for any probabilistic polynomial-time adversary* Adv*:*

$$\left|\Pr[y \leftarrow_\$ \mathbb{F}_2^{m(t)} : \mathsf{Adv}(\mathsf{pp}, y) = 1] - \Pr[x \leftarrow_\$ \mathbb{F}_2^t, y \leftarrow \mathsf{PRG}(x) : \mathsf{Adv}(\mathsf{pp}, y) = 1]\right| \leq \mathsf{negl}.$$

Here negl *means negligible in the security parameters, and* pp *stands for the public parameters of the PRG. A pseudorandom generator* PRG *is n-*local *(for a constant n) if for any $t \in \mathbb{N}^*$, every output bit of* PRG_t *depends on at most n input bits.*

Definition 2 (Goldreich's Collection). *Let $n, t \in \mathbb{N}^*$ and $\mathsf{s} > 1$, called* stretch*, and let f be a Boolean function $f : \mathbb{F}_2^n \mapsto \mathbb{F}_2$. Setting $m := t^{\mathsf{s}}$, let $(\sigma^1, \ldots, \sigma^m)$ be a list of m sublists of $[t]$, such that each sublist is of small size, denoted n and called* locality*. The Goldreich's collection is defined as the following m-tuple.*

$$(f(x_{\sigma_1^1}, \ldots, x_{\sigma_n^1}), \ldots, f(x_{\sigma_1^m}, \ldots, x_{\sigma_n^m})).$$

For the readers who are familiar with Goldreich's collection, note that we omit the expander graph notions required on the subsets as they are not necessary for understanding the rest of the paper. In this work, we just retain that if the m subsets $(\sigma^1, \ldots, \sigma^m)$ of Definition 2 are chosen uniformly at random or under some formally defined expansion properties (we refer to [App13] for these properties), and if the Boolean function f validates several criterion (detailed later on in Section 1.2), one can assume that Goldreich's Collection is a PRG. Throughout this paper, we define by $\mathsf{GPRG}(f, \mathsf{s})$ and call Goldreich's PRG a Goldreich's collection with a fixed $(\sigma^1, \ldots, \sigma^m)$ enjoying such expanding properties.

In the past few years, there has been a renewed interest in the study of this local PRG and its generalizations [AY09; App12; OW14; Coo+14; App15; ABR16; AL16; LV17; Boy+17; Cou+18; Ana+19; Gay+20; Yan+22]. Intuitively, Goldreich PRG can be used to design cryptographic primitives that can be evaluated in constant time, using polynomially many cores. Later on, it was observed in several works that the existence of local PRGs had a number of non-trivial implications for several high-end cryptographic primitives. In a nutshell, the applications include the construction of secure computation with constant computational overhead [Ish+08], MPC-friendly primitives [Alb+15; Can+; Méa+16; Gra+16; Méa+19a], indistinguishability obfuscation [Ana+19; Jai+19; JLS19; Gay+20] and cryptographic capsules [Boy+17]. Furthermore, the existence of local PRGs with polynomial stretch

implies strong bounds on the average-case inapproximability of constraint satisfaction problems, such as Max3SAT [AIK08], and hardness-of-learning results [DV21].
[Removed details on the designs using Goldreich PRG]

1.2 Criteria ensuring pseudorandomness

The security of random local functions has been studied in several works [MST03; AHI05; AY09; ABR12; OW14; Coo+14; Cou+18; Yan+22], for a detailed and well-written overview we refer the reader to [App15]. Today, two classes of poly-time attacks are known to apply on Goldreich's PRG [AL16; AL18]: $\mathbb{F}_2$-linear tests and algebraic attacks. The principle of $\mathbb{F}_2$-linear tests consists in distinguishing the PRG output from a random string by exhibiting a biased $\mathbb{F}_2$-linear function of the output. Algebraic attacks against a function $g : \{0,1\}^t \to \{0,1\}^m$ start with an output y (presumably in the image of g) and use it to initialize a system of polynomial equations over the hidden input variables $x = (x_1, ..., x_t)$. The system is further manipulated and extended until a solution is found via polynomial techniques, or the existence of a solution is refuted. In the rest of the paper, we denote both these families of attacks as *linear algebraic attacks* and we refer to [AL16] for a detailed description.

In [AL16], Applebaum and Lovett show how two properties on the function f allow to study the security against these two classes: the *resiliency* and the *algebraic immunity*, also called rational degree.

Informal description of the criteria. An n-variable Boolean function f is called k-resilient if it has no nontrivial correlation with any linear combination of less than (or equal to) k of its inputs (formalized later in Definition 6). The term of resiliency has been introduced in [Cho+85], it is a standard cryptographic criterion of Boolean functions to measure the resistance to an attack due to Siegenthaler [Sie84] on stream ciphers from the combiner model, called correlation attack. For an n-variable Boolean function f we will denote by $\mathsf{res}(f)$ its resiliency order: the maximal value of $k < n$ such that f is uncorrelated with all the combinations of k of its inputs.

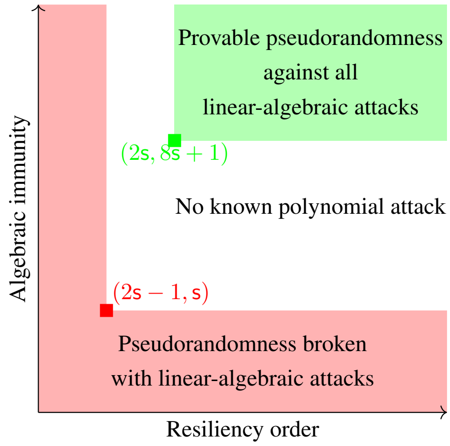
An n-variable Boolean function f has rational degree e if it is the smallest integer for which there exist degree e polynomials g and h, not both zero, such that $f \cdot g = h$ (see Definition 8 for a formal introduction). It has been used to study the security of candidate simple weak PRF constructions [Aka+14; Bon+18; Boy+20]. Under the name of *Algebraic Immunity* (AI), it is a standard cryptographic criterion of Boolean functions to measure the resistance of the so-called algebraic attack on stream ciphers [CM03]. A recent result [Che+20] shows that functions with high algebraic immunity allow to build secret sharing schemes. For an n-variable Boolean function f we will denote by $\mathsf{AI}(f)$ its algebraic immunity.

The results of [AL16, Theorems 1.1 and 1.4] give resistance properties for the class of linear-algebraic attacks, or for any poly time attacks under the assumption that local functions are too simple to "separate" these two notions. Throughout this paper, we will graphically represent the resiliency order and algebraic immunity as x-axis and y-axis in a graph[4]. Each integer point corresponds to a possible couple $(\mathsf{res}, \mathsf{AI})$ for a function.

Denoting the polynomial stretch as $\mathsf{s} \in \mathbb{R}$, $\mathsf{s} > 1$, that is $m = t^{\mathsf{s}}$, the authors of [AL16] point out that to resist the linear algebraic attacks, it is necessary to instantiate Goldreich's PRG with predicate f with $\mathsf{res}(f) > a(\mathsf{s})$ and $\mathsf{AI}(f) > b(\mathsf{s})$ where a and b are affine functions. We can summarize these results in the following theorem.

[4] we do not introduce the bit-fixing degree and focus on the AI for assessing linear and algebraic attacks. Indeed, the assumptions on the AI are capturing the assumptions on the bit-fixing degree (see [AL16, Section 1.2.2]). More precisely, for $r \in \mathbb{N}$ an algebraic immunity $\mathsf{AI}(f)$ implies r-bit fixing degree of at least $\mathsf{AI}(f) - r$ for any $r < \mathsf{AI}(f)$.

Theorem 1 (Predicate's Requirements from [AL16]).



Let f be an n-variable Boolean function, $\mathsf{s} \in \mathbb{R}^+$ be a stretch, and $\mathsf{GPRG}(f, \mathsf{s})$ be a Goldreich's PRG,

- *If $\mathsf{res}(f) < 2\mathsf{s} - 1$ or $\mathsf{AI}(f) \leq \mathsf{s}$*[a] *then $\mathsf{GPRG}(f, \mathsf{s})$ is* not *pseudorandom against linear-algebraic attacks. This can be represented as an "L" zone at the bottom left of the $(\mathsf{AI}, \mathsf{res})$ graph (in red).*
- *If $\mathsf{res}(f) \geq 2\mathsf{s}$ and $\mathsf{AI}(f) > 8\mathsf{s} + 1$, then $\mathsf{GPRG}(f, \mathsf{s})$ is pseudorandom against linear-algebraic attacks. This can be represented as a rectangle at the top right of the $(\mathsf{AI}, \mathsf{res})$ graph (in green).*
- *Otherwise, on the one hand, there is no provable result on the pseudorandomness but on the other hand there are no known polynomial attacks.*

[a] $\mathsf{AI}(f) < \mathsf{s}$ from [AL16] and the polynomial attack of [Cou+18] applies for $\mathsf{s} = \mathsf{AI}(f)$

Remark 1. The security requirement bounds of Theorem 1 could evolve with the state of the art. The implications of our conjectures on Goldreich pseudorandom generator (see Theorem 3 and Corollary 2 in Section 3 below) are using explicitly-defined affine functions for the bounds, notably $a(\mathsf{s}) = 2\mathsf{s}$ and $b(\mathsf{s}) = 8\mathsf{s} + 1$, but they can apply straightforwardly to any affine functions a and b.

1.3 Towards optimal functions according to these criteria

The locality n of a Goldreich PRG, $\mathsf{GPRG}(f, \mathsf{s})$, is the number of variables of the Boolean function f. Hence, the smaller the locality gets, the more efficient $\mathsf{GPRG}(f, \mathsf{s})$ becomes. In other words, determining the minimal locality that ensures pseudorandomness leads to upper-bounds on the number of pseudorandom bits that can be generated securely.

As an open question, Applebaum and Lovett ([AL16; AL18]) ask what is the minimal number of variables that allows either pseudorandomness against the known linear-algebraic attacks (*i.e.* existing functions f with $(\mathsf{res}(f), \mathsf{AI}(f))$ parameters outside of the red domain) or provable pseudorandom against linear-algebraic attacks (*i.e.* existing functions f with $(\mathsf{res}(f), \mathsf{AI}(f))$ parameters in the green domain). This question boils down to finding the minimal number of variables (that will be denoted $n_0(k, e)$) such that there exists a function with resiliency order k and algebraic immunity e. While this open question could not be solved tightly, Applebaum and Lovett give a first upper bound on this minimum, that we provide later in Lemma 1.

In addition to the possibility of providing security guarantees for Goldreich PRG, the problem of finding the minimal number of variables such that there exists function with resiliency order k and algebraic immunity e is also an interesting theoretical question. In the domain of Boolean functions used in cryptography, the resiliency and the algebraic immunity have not been studied together. The problem of minimal locality, or best trade-off between resiliency order and algebraic immunity corresponds to one of the open question highlighted by Carlet [Car21]: *"Determine, for any n, what is the best possible resiliency order of n-variable Boolean functions with optimal algebraic immunity".*
Indeed, over the years, the criterion of degree has been forsaken in favor of the algebraic immunity since having a Boolean function f of algebraic immunity e is equivalent to having a Boolean function g of degree e always canceling f or always canceling $f + 1$ ([CM03]). Then, the attacks based on the

degree of f, targeting the resolution of an algebraic system can be transposed to attacks targeting the resolution of an algebraic system of degree $\mathsf{AI}(f)$. The AI can be seen as a thinner algebraic property than the degree, and for all non-null function f $\mathsf{AI}(f) \leq \mathsf{deg}(f)$. Determining the best trade-off between resiliency order and algebraic immunity can be seen as an extension of the Siegenthaler bound which characterize the best trade-off resiliency-order/degree a Boolean function can have. This bound is known to be reached for all n.

Theorem 2 (Siegenthaler's Bound, [Sie84]).
Let $n \in \mathbb{N}^*$ and f be an n-variable Boolean function, then

$$\begin{cases} \mathsf{deg}(f) + \mathsf{res}(f) \leq n & \textit{if } \mathsf{deg}(f) = 1, \\ \mathsf{deg}(f) + \mathsf{res}(f) \leq n - 1 & \textit{if } \mathsf{deg}(f) \geq 2, \end{cases}$$

1.4 A short introduction independent from Goldreich's PRG

In this article we study the possible (or impossible) trade-offs between the algebraic immunity and the resiliency of a Boolean function. We investigate the theoretical limits of this trade-off, the position of known constructions relatively to it, and exhibit optimal functions in a small number of variables.

Both the algebraic immunity and the resiliency criteria were introduced in cryptography to analyze the security of stream ciphers. The resiliency is used to measure the resistance to the correlation attack of Siegenthaler on the combiner model [Sie84]. The term of resiliency itself has been introduced in [Cho+85], an n-variable Boolean function f is called k-resilient if it has no nontrivial correlation with any linear combination of less than (or equal to) k of its inputs. For an n-variable Boolean function f we will denote by $\mathsf{res}(f)$ its resiliency order: the maximal value of $k < n$ such that f is uncorrelated with all the combinations of k of its inputs. The algebraic immunity is used to measure the resistance to the algebraic attack of Courtois and Meier on the filtered linear feedback shift register model [CM03]. The term of algebraic immunity itself has been introduced in [Arm+06], an n-variable Boolean function f has algebraic immunity $e > 0$ if there exists a degree e function annihilating f (or its complementary $f+1$) and there is no function (not null) of lower degree having this property. For an n-variable Boolean function f we will denote by $\mathsf{AI}(f)$ its algebraic immunity.

Due to their relevance in the security of many symmetric ciphers, the resiliency and algebraic immunity criteria have been thoroughly studied in the past decades (*e.g.* [BGS94; Tar00; MPC04; Car+06; Car21]) . So far the two criteria have been studied independently, the motivation to investigate functions optimizing both is more recent. In the context of local pseudorandom generators Applebaum and Lovett ([AL16; AL18]) leave as an open problem to determine what is the minimal number of variables $n_0(k, e)$ for a Boolean function to reach a resiliency order of k and an algebraic immunity of e. They first give the upper bound of $k + 2e + 1$ on this minimum. In the area of Boolean functions used in cryptography this problem corresponds to one of the open question recently highlighted by Carlet [Car21]: *"Determine, for any n, what is the best possible resiliency order of n-variable Boolean functions with optimal algebraic immunity".*

The algebraic immunity of a function is optimal when it reaches $\lceil (n+1)/2 \rceil$ as shown in [CM03]. For the resiliency it's value is between -1 (the function is more correlated to one of the two constant functions than the other) and $n-1$, but a high resiliency is incompatible with a high degree as shown by Siegenthaler in 1984:

Theorem (Siegenthaler's Bound, [Sie84]). *Let $n \in \mathbb{N}^*$ and f be an n-variable Boolean function, then*

$$\begin{cases} \mathsf{deg}(f) + \mathsf{res}(f) \leq n & \textit{if } \mathsf{deg}(f) = 1, \\ \mathsf{deg}(f) + \mathsf{res}(f) \leq n - 1 & \textit{if } \mathsf{deg}(f) \geq 2, \end{cases}$$

Since the algebraic immunity of a Boolean function is always upper bounded by its degree ($f+1$ and f annihilate one another), the trade-off between algebraic immunity and resiliency cannot overcome

Siegenthaler's bound. Therefore, our study starts with the following bounds on $n_0(k, e)$:

$$k + e + 1 \leq n_0(k, e) \leq k + 2e + 1.$$

To study this minimum we will mostly focus on functions with optimal algebraic immunity and study how high can (or in most cases cannot) be their resiliency order.

1.5 Our contributions

Our work provides the first study of Applebaum and Lovett's open question. It is two-fold.

1. *Conjectures and implications.* In the first part of the study presented in Section 3, we introduce new conjectures on the existence of optimal functions and prove some implications. The high-level idea is to consider known non-optimal constructions in low localities and analyze how we can use them as building blocks for deriving more general constructions. We sketch our search procedure and introduce conjectures on the existence of optimal functions. Our main conjecture, Conjecture 1, assumes the following.

Main conjecture (informal): *It is possible for all n to construct a Boolean function that reaches together the highest algebraic immunity and Siegenthaler's bound.*

We first exhibit all the possible AI-resiliency trade-offs depending on the strength of our conjectures (Lemma 7). Next, we improve the minimal locality required for local PRGs of polynomial stretch s and open the door for more improvement with our conjectures (Corollary 2). Similarly to the results of [CM01] (who ruled out the existence of PRGs in NC^0_3 with stretch $m > 4n$) and [MST03] (who ruled out the existence of PRGs in NC^0_4 with stretch $m > 24n$), our new bounds contribute to ruling out the pseudorandomness of Goldreich's PRG for stretches s smaller than certain new bounds. On the other side, it opens the possibility of finding n-local PRG with stretch $\mathsf{s} \in \mathbb{N}$ for which no polynomial attacks are known in $\mathsf{NC}^0_{4\mathsf{s}}$ and even in $\mathsf{NC}^0_{3\mathsf{s}+1}$ assuming one of our conjectures (and proven for $\mathsf{s} \in [2, 6[$). Similar results are shown for the case where we look for provable pseudorandomness against polynomial attacks. As stressed in Remark 1, our results on the minimal locality (Theorem 3 and Corollary 2) are based on the explicitly-defined affine functions a and b from Theorem 1, they can be adapted to any arbitrary affine functions a' and b' (coming from future better attacks or tighter security reductions). The high-level reduction of the locality problem to Conjecture 1 is performed by exhibiting different constructions, showing that one function satisfying optimal AI and reaching Siegenthaler's bound implies the existence of functions satisfying any of the other trade-offs (respecting the maximal AI and Siegenthaler's bounds).

2. *Towards validating or invalidating our conjectures.* We realize the first study on functions with both optimal algebraic immunity and high resiliency, focusing on the one reaching Siegenthaler bound. Their existence for all n is our main conjecture, we extensively analyze this conjecture and provide theoretical and experimental arguments. Our results show two different trends. On the one hand, in the theoretical side, we demonstrate impossibility results for some known constructions. On the other hand, our experimental arguments allow to exhibit such optimal functions in low locality.

(a) In Section 4, we investigate known families of functions with optimal algebraic immunity to highlight a negative tendency. We review a large number of families provided by the literature in Boolean function theory and show that the resiliency of existing constructions is too low (no more than 0 or 1). Then we focus on two main families, and explain why AI-optimal constructions inside these families are not compatible with a high resiliency. In the first part of the section we review the possibility of constructing the desired optimal functions from XOR-MAJ functions. We prove that they do not reach optimality with respect to their resiliency, and they could be beaten by optimal functions if our conjecture is verified. Majority functions, or any functions in their affine equivalence class, are at most balanced, and consequently provide the lowest amount of resiliency a function with optimal algebraic immunity can provide. Thus, XOR-MAJ functions are asymptotically useless for our purpose and one needs to look in another direction for constructing optimal functions. Then, we focus on rotational symmetric functions. We prove that the resiliency of existing constructions from this family is too low for being candidates optimal functions, and that small modifications of these constructions are also suboptimal.

(b) In Section 5, we experimentally demonstrate the existence of optimal Boolean function in low locality. More precisely, we classify the Boolean functions depending on their algebraic immunity and resiliency up to locality 5 and 7 for the class of rotational symmetric functions, determining all the optimal functions in these sets. In addition, we construct optimal functions for small n up to $n = 12$ providing verifiable examples with truth tables. As expected from Section 4, the found optimal functions are not in the XOR-MAJ family. They directly lead to *better candidates for Goldreich's pseudorandom generator*, as stated in Proposition 4 for polynomial stretches $\mathsf{s} \in [2, 6[$. These results in small locality also provide confidence in the validity of our conjectures.

(c) Additionally, in Appendix A, we sketch a possible direction towards positive theoretical results. We study the properties and possible quantity of optimal functions, based on the properties of their Walsh spectrum. We take a step towards an asymptotic construction method by giving necessary and sufficient conditions to recursively build these functions. These results allow to narrow the conditions to prove or disprove our conjecture.

2 Preliminaries

For readability, we use the notation $+$ instead of $\oplus$ to denote the addition in $\mathbb{F}_2$. For a vector $a \in \mathbb{F}_2^n$ we denote $\mathsf{w_H}(a)$ its Hamming weight: $\mathsf{w_H}(a) = |\{a_i \neq 0,\, i \in [n]\}|$. For $a \in \mathbb{F}_2^n$, $b \in \mathbb{F}_2^n$ we denote $\mathsf{d_H}(a, b) = \mathsf{w_H}(a + b)$ the Hamming distance between a and b. We denote $\mathsf{E}_{k,n}$ the set of elements $a \in \mathbb{F}_2^n$ such that $\mathsf{w_H}(a) = k$. We note that $|\mathsf{E}_{k,n}| = \binom{n}{k}$. For a vector $a \in \mathbb{F}_2^n$ we denote $\mathsf{supp}(a) = \{i \in [n],\, a_i = 1\}$ its support.

2.1 Boolean functions and cryptographic criteria

We introduce here some core notions of Boolean functions in cryptography, restricting our study to the following definition of Boolean function, more restrictive than a vectorial Boolean function. We extract from the literature all the tools for introducing two key parameters of Boolean functions: the *resiliency order* and *algebraic immunity*.

Definition 3 (Boolean Function). *A Boolean function f with n variables is a function from $\mathbb{F}_2^n$ to $\mathbb{F}_2$. The set of all Boolean functions in n variables will be denoted $\mathcal{B}_n$.*

Definition 4 (Equivalences Notions (adapted from [Car21], Definition 5)). *Two n-variable Boolean functions f and $a_0 + f \circ L$ where:*

$$L : (x_1, \ldots, x_n) \mapsto (x_1, \ldots, x_n) \times \mathbf{M} + (a_1, \ldots, a_n), \text{ are called:}$$

- *affine equivalent if $a_0 \in \mathbb{F}_2$, L is an affine automorphism of $\mathbb{F}_2^n$, $\mathbf{M}$ being an $n \times n$ nonsingular matrix over $\mathbb{F}_2$ and $(a_1, \ldots, a_n) \in \mathbb{F}_2^n$,*
- *linear equivalent if $a_0 = 0$, L is a linear automorphism of $\mathbb{F}_2^n$, $\mathbf{M}$ being an $n \times n$ nonsingular matrix over $\mathbb{F}_2$ and $(a_1, \ldots, a_n) = 0_n$,*
- *permutation equivalent if they are linear equivalent with $\mathbf{M}$ having exactly one 1 by row and by column.*

Definition 5 (Algebraic Normal Form (ANF)). *We call Algebraic Normal Form of a Boolean function f its n-variable polynomial representation over $\mathbb{F}_2$ (i.e. belonging to $\mathbb{F}_2[x_1, \ldots, x_n]/(x_1^2 + x_1, \ldots, x_n^2 + x_n)$):*

$$f(x_1, \ldots, x_n) = \sum_{I \subseteq [n]} a_I \left(\prod_{i \in I} x_i \right)$$

where $a_I \in \mathbb{F}_2$. The (algebraic) degree of f is:

$$\mathsf{deg}(f) := \begin{cases} \max_{I \subseteq [n]}\{|I| \mid a_I = 1\} \text{ if } f \text{ is not null} \\ 0 \text{ otherwise}. \end{cases}$$

Resiliency and Walsh transform

Definition 6 (Balancedness and Resiliency). *A Boolean function $f \in \mathcal{B}_n$ is said to be balanced if $|f^{-1}(0)| = |f^{-1}(1)| = 2^{n-1}$. The function f is called k-resilient if any of its restrictions obtained by fixing at most k of its coordinates is balanced. We denote by $\mathsf{res}(f)$ the maximum resiliency (also called resiliency order) of f and set $\mathsf{res}(f) = -1$ if f is unbalanced.*

We remark that the resiliency order is not an affine equivalent criteria, neither linear equivalent, but it is permutation equivalent.

Definition 7 (Walsh Transform and Walsh Support). *Let $f \in \mathcal{B}_n$ be a Boolean function, its Walsh transform W_f at $a \in \mathbb{F}_2^n$ is defined as:*

$$\mathsf{W}_f(a) := \sum_{x \in \mathbb{F}_2^n} (-1)^{f(x)+a\cdot x}.$$

The Walsh support is the set $\mathsf{Wsupp}_f := \{a \in \mathbb{F}_2^n \mid \mathsf{W}_f(a) \neq 0\}$.

We give useful properties on the Walsh transform:

Property 1 (Walsh Transform and Resiliency, *e.g.* [Car21]). *Let $f \in \mathcal{B}_n$, f is k-resilient if and only if $\mathsf{W}_f(a) = 0$ for all a of Hamming weight at most k. Additionally, f has resiliency order k if there exists an $a \in \mathsf{E}_{k+1,n}$ such that $\mathsf{W}_f(a) \neq 0$.*

Property 2 (Walsh support structure, *e.g.* [CM04] Section 3.1). *Let $f \in \mathcal{B}_n$, the Walsh support has the following properties:*

- *The Walsh support is globally affine invariant. Let $a_0 \in \mathbb{F}_2$ and L be an affine automorphism of $\mathbb{F}_2^n$ (Definition 4) then: $\mathsf{Wsupp}_{a_0+f\circ L} = \{L'(x) \mid x \in \mathsf{Wsupp}_f\}$, where L' is an affine automorphism of $\mathbb{F}_2^n$.*
- *The Walsh support of an affine function is a singleton.*
- *If f is the direct sum (the sum of functions acting on different variables) of g and h then: $\mathsf{Wsupp}_f = \mathsf{Wsupp}_g \times \mathsf{Wsupp}_h$, where $\times$ denotes the Cartesian product.*
- $|\mathsf{Wsupp}_f| \neq 2$.

Property 3 (Covering radius bound *e.g.* [Coh97] Corollary 8.1.4). *Let $\mathcal{C}$ be a length-n dimension-k binary linear code, its covering radius, the maximum distance between an element of $\mathbb{F}_2^n$ and $\mathcal{C}$, R is such that $R \leq n - k$.*

Algebraic Immunity

Definition 8 (Algebraic Immunity and Annihilators). *The algebraic immunity of a Boolean function $f \in \mathcal{B}_n$, denoted as $\mathsf{AI}(f)$, is defined as:*

$$\mathsf{AI}(f) := \min_{g \neq 0}\{\mathsf{deg}(g) \mid fg = 0 \text{ or } (f+1)g = 0\},$$

where $\mathsf{deg}(g)$ *is the algebraic degree of* g*. The function* g *is called an annihilator of* f *(or* $f+1$*). We additively use the notation* $\mathsf{AN}(f)$ *for the minimum algebraic degree of non null annihilator of* f*:*

$$\mathsf{AN}(f) := \min_{g \neq 0}\{\mathsf{deg}(g) \mid fg = 0\}.$$

We also use the notation $\mathcal{D}\mathsf{AN}(f)$ *for the dimension of the vector space made of the annihilators of* f *of degree* $\mathsf{AI}(f)$ *and the zero function. Note that, for every function* f *we have* $\mathcal{D}\mathsf{AN}(f) \leq \binom{n}{\mathsf{AI}(f)}$*.*

Note that this definition directly leads to the following properties:

Property 4 (Algebraic Immunity Properties, *e.g.* [Car21])**.** *Let* $f \in \mathcal{B}_n$*:*

- *The null and the all-one functions are the only functions such that* $\mathsf{AI}(f) = 0$*.*
- *All monomial (non constant) functions* f *are such that* $\mathsf{AI}(f) = 1$*.*
- *For all non constant* f*,* $\mathsf{AI}(f) \leq \mathsf{AN}(f) \leq \mathsf{deg}(f)$*.*
- *Let* $g \in \mathcal{B}_n$*,* $\mathsf{AI}(f) - \mathsf{deg}(g) \leq \mathsf{AI}(f+g) \leq \mathsf{AI}(f) + \mathsf{deg}(g)$*.*
- *If* f *and* f' *are affine equivalent then* $\mathsf{AI}(f) = \mathsf{AI}(f')$*.*
- $\mathsf{AI}(f) \leq \lfloor (n+1)/2 \rfloor$*. If the bound is reached, we say that* f *has an optimal AI.*
- *If* n *is odd and* $\mathsf{AI}(f) = (n+1)/2$ *(i.e. AI-optimal) then* f *is balanced.*

2.2 Special families and constructions of Boolean functions

In our research of ideal Boolean functions, we will consider several families and constructions of functions that verify specific properties. We present them in this section.

Majority and XOR functions

Definition 9 (Majority Function). *For any positive integer* n *we define the Boolean function* MAJ_n *as:*

$$\forall x = (x_1, \ldots, x_n) \in \mathbb{F}_2^n, \quad \mathsf{MAJ}_n(x) := \begin{cases} 0 & \text{if } \mathsf{w_H}(x) \leq \frac{n}{2}, \\ 1 & \text{otherwise.} \end{cases}$$

Property 5 (Properties of the Majority Functions, *e.g.* [CM19] Lemmas 5-6)**.** *Let* $t \in \mathbb{N}$ *and* $\varepsilon \in \{0,1\}$*, the majority* $\mathsf{MAJ}_{2t+\varepsilon}$ *function has the following cryptographic properties:*

- *Resiliency:* $\mathsf{res}(\mathsf{MAJ}_{2t+\varepsilon}) = \varepsilon - 1$*.*
- *Algebraic Immunity:* $\mathsf{AI}(\mathsf{MAJ}_{2t+\varepsilon}) = t + \varepsilon$*.*
- *Annihilators:* $\mathsf{AN}(\mathsf{MAJ}_{2t+\varepsilon}) = t + \varepsilon$*,* $\mathsf{AN}(1 + \mathsf{MAJ}_{2t+\varepsilon}) = t + 1$*.*

Property 6 (Majority Functions and Walsh spectrum, *e.g.* [DMS06] Lemma 4)**.** *Let* $t \in \mathbb{N}$*, the majority functions in* $2t+1$ *variables has the following properties:*

- $\mathsf{Wsupp}_{\mathsf{MAJ}_{2t+1}} = \{a \in \mathbb{F}_2^{2t+1} \,|\, \mathsf{w_H}(a) = 1 \mod 2\}$,
- *for all* $a \in \mathsf{E}_{1,2t+1}$*,* $\mathsf{W}_{\mathsf{MAJ}_{2t+1}}(a) = 2\binom{2t}{t}$*.*

Property 7 (Properties of XOR Functions)**.** *Let* $n \in \mathbb{N}^*$*, and* $k \in [n]$*, the* XOR_k *function* $\mathsf{XOR}_k(x) = \sum_{i \in [k]} x_i$ *has the following cryptographic properties:* $\mathsf{res}(\mathsf{XOR}_k) = k - 1$ *and* $\mathsf{AI}(\mathsf{XOR}_k) = 1$*.*

Secondary Constructions: Direct Sum and Siegenthaler's

Definition 10 (Direct Sum). *Let* $f \in \mathcal{B}_n$ *and* $g \in \mathcal{B}_m$*,* f *and* g *depending on distinct variables, the direct sum* h *of* f *and* g *is defined by:*

$$h(x,y) := f(x) + g(y), \qquad \text{where } x \in \mathbb{F}_2^n \text{ and } y \in \mathbb{F}_2^m.$$

Definition 11 **(XOR-MAJ Function).** *For any positive integers k and n we define the direct sum* $\mathsf{XOR}_k\mathsf{MAJ}_n$ *for all* $z = (x_1, \ldots, x_k, y_1, \ldots, y_n) \in \mathbb{F}_2^{k+n}$ *as:*

$$(\mathsf{XOR}_k\mathsf{MAJ}_n)(z) := x_1 + \cdots + x_k + \mathsf{MAJ}_n(y_1, \ldots, y_n) = \mathsf{XOR}_k(x) + \mathsf{MAJ}_n(y).$$

The Siegenthaler construction is a secondary construction which combines two n-variable functions to obtain an $(n+1)$-variable function:

Definition 12 **(Siegenthaler's Construction).** *Let $n \in \mathbb{N}$, $f, g \in \mathcal{B}_n$, we call Siegenthaler construction h from components f and g:*

$$h \in \mathcal{B}_{n+1}, \quad \forall x \in \mathbb{F}_2^n, \forall y \in \mathbb{F}_2,\ h(x, y) = (1 + y) \cdot f(x) + y \cdot g(x).$$

Note that any function of $\mathcal{B}_{n+1}$ can be built using this construction, and in a unique way when the variable playing the role of y is fixed. We recall some properties of this construction in Section A.1.

3 Conjectures on the existence of optimal functions and implications

In the following lemma, we give Applebaum and Lovett's upper bound on the minimal number of variables such that a function has algebraic immunity e and resiliency order k. Their results were obtained from the properties they proved on the XOR-MAJ functions [AL16; AL18].

Lemma 1 **(Locality Upper Bound of [AL16; AL18] modified).** *Let $e \geq 1$ and $k \geq -1$ be two integers. We denote by $n_0(k, e)$ the minimal number of variables n such that there exists an n-variable Boolean function f such that $\mathsf{AI}(f) = e$ and $\mathsf{res}(f) = k$. This value is upper bounded as follows.*

$$n_0(k, e) \leq k + 2e + 1.$$

A function reaching[5] *this bound is* $\mathsf{XOR}_{k+1}\mathsf{MAJ}_{2e}$.

In this section, we study the possibility of obtaining a tight bound by analyzing the existence of functions that reach maximal algebraic immunity and high resiliency. More precisely:

1. we improve and add granularity to Lemma 1 by introducing new conjectures (formulated in Theorem 3);
2. we show the impact of such new bound with the decrease of the locality required for local PRGs of polynomial stretch s (written in Corollary 2).

3.1 Definitions

Definition 13. *Let $n \geq 3$. We say that a res/AI pair (k, e) is "accessible with n variables" if there exists an n-variable function with resiliency order k and algebraic immunity e.*
We extend the definition for sets: a set S is accessible with n variables if every $(k, e) \in S$ is accessible with n variables.

[5] In [AL16], the bound $n_0 \leq k + 2e$ is claimed to be reached by $\mathsf{XOR}_k\mathsf{MAJ}_{2e}$ but this is actually not enough for proving such a bound since its resiliency order is $k - 1$ instead of k.

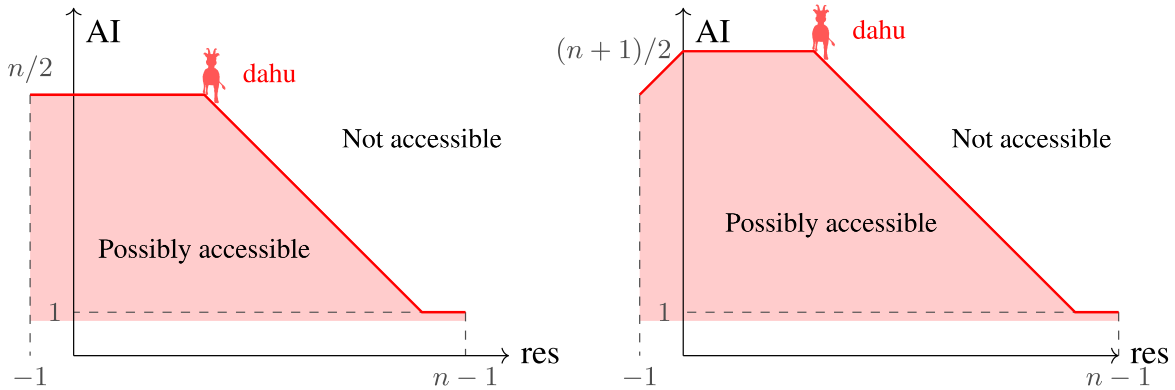
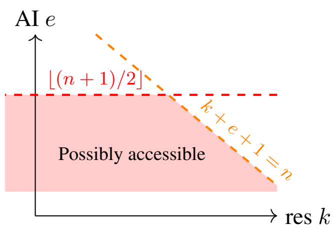


Fig. 1: Representation of the possibly accessible couple $(\mathsf{res}, \mathsf{AI})$ for a fixed **even** $n \in \mathbb{N}^*$ on the left and for a fixed **odd** $n \in \mathbb{N}^*$ on the right.

Lemma 2 (Locality Lower Bound).



Let $n \geq 3$, $e \geq 1$ and $k \geq -1$ be integers. For any function $f \in \mathcal{B}_n$ of degree at least 2 such that $\mathsf{AI}(f) = e$ and $\mathsf{res}(f) = k$ then

$$\begin{cases} k+e+1 \leq n & \textit{(Siegenthaler's bound),} \\ e \leq \lfloor (n+1)/2 \rfloor & \textit{(Optimal AI).} \end{cases}$$

Proof. From the third item of Property 4, $\mathsf{AI}(f) \leq \deg(f)$ (as $f+1$ is an annihilator of f of degree $\deg(f)$). Then, Theorem 2 allows us to conclude: $n \geq \mathsf{res}(f) + \deg(f) + 1 \geq k + e + 1$. Finally, the bound on the AI is provided by the sixth item of Property 4. □

The pairs (k, e) that stand above Lemma 2's bounds can never be parameters of an n-variable function. Indeed, all the points above either the Siegenthaler derived limit ($k + e + 1 \leq n$) or the optimal AI bound cannot be accessed by n-variable functions. However, below both limits, one cannot state with certainty that all the points are accessible by an n-variable function. We tackle this question in this paper using new conjectures. We will see that the zone at the top right, close to where the two bounds intersect, is the most difficult to obtain constructively and that a pair at the intersection would imply the existence of all possibly accessible pairs.
Unfortunately, the better suited candidates for local PRGs are the functions reaching the top-right border, with optimal or almost-optimal AI and high resiliency, exactly in the zone where the constructions are difficult. The intuition of these constraints was presented in Theorem 1 and it will be detailed in Corollary 3. Thus, it is important to understand the potential existence of functions with such properties.

To obtain a more complete bound, in Figure 1, we graphically add the extreme cases when $\mathsf{res}(f) = -1$ and[6] $\deg(f) = 1$ (which corresponds to the point $(\mathsf{res}(f), \mathsf{AI}(f)) = (n-1, 1)$). The colored domain will be formally defined in Definition 15. The cases of even and odd n should be treated separately because when n is odd, optimal algebraic immunity cannot be reached for unbalanced functions (see Property 4).

As it is not known if AI-optimal functions with highest resiliency (i.e. reaching the Siegenthaler derived bound) exist for any n, we name them like the mystical mountain creatures[7]: "dahus". Their

[6] When $\mathsf{AI} = 0$, $(\mathsf{res}, \mathsf{AI}) = (-1, 0)$ are accessed by the two constant functions, so we exclude it from the graphs as it is not relevant for the following study.
[7] https://en.wikipedia.org/wiki/Dahu

existence will be conjectured later on (Conjecture 1) and we will highlight the impact of such a result in Theorem 3 and Corollary 2. We formally introduce the definition of a dahu in Definition 14.

Definition 14 (Dahus). *Let $n \geq 3$, we denote Dahu_n the set of n-variable functions with optimal algebraic immunity reaching the locality lower bound:*

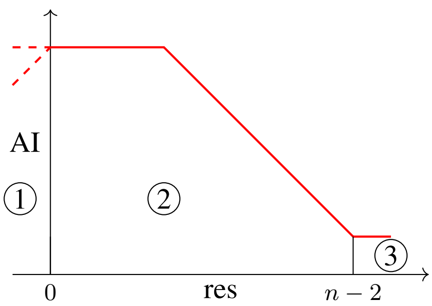
$$f \in \mathsf{Dahu}_n \Leftrightarrow \begin{cases} \mathsf{AI}(f) + \mathsf{res}(f) + 1 = n, \\ \mathsf{AI}(f) = \lfloor (n+1)/2 \rfloor. \end{cases}$$

The properties of dahus and $|\mathsf{Dahu}_n|$ are studied in Section A.2.

3.2 Technical lemmas

Let us first introduce technical definitions and lemmas before stating the implications in the next subsection in Lemma 7 and Corollary 2.

Definition 15. *Let $n \in \mathbb{N}, n \geq 3$. We define the set A_n as follows.*



For $t \in \mathbb{N}^*$ and $\varepsilon \in \{0, 1\}$,

$$\begin{aligned} A_{2t+\varepsilon} := \quad & \{(-1, e) \mid 0 < e \leq t\} && \text{①} \\ & \cup \{(k, e) \in [0, n-2] \times [1, t+\varepsilon] \mid k + e + 1 \leq n\} && \text{②} \\ & \cup \{(2t + \varepsilon - 1, 1)\}. && \text{③} \end{aligned}$$

Note that for all $n \geq 3$, $A_n \subsetneq A_{n+1}$.

Let us introduce a lemma naturally resulting from Definition 15.

Lemma 3. *Let $n \geq 3$. Assume that f is an n-variable function not constant, then*

1. *$(\mathsf{res}(f), \mathsf{AI}(f)) \in A_n$;*
2. *for any $n' \geq n$, there exists an n'-variable function with parameters $(\mathsf{res}(f), \mathsf{AI}(f))$.*

Proof. The first item is obtained from Lemma 2 for the functions with degree higher than 2 (②), and recalling that by definition $\mathsf{res} \geq -1$, and $\mathsf{AI} \geq 1$ for non constant functions (Property 4 item 1). We also remark that when n is odd, optimal algebraic immunity cannot be reached for unbalanced functions (see Property 4) (①). When the function have a degree one, Theorem 2 shows that the resilience cannot be larger than $n - 1$ (③).

For the second item, let us build $h(x_1, \ldots, x_n, x_{n+1}, \ldots, x_{n'}) = f(x_1, \ldots, x_n) + g(x_{n+1}, \ldots, x_{n'})$ where g is the null function. Using Property 4 (item 1), $\mathsf{AI}(g) = 0$, and since g is not balanced $\mathsf{res}(g) = -1$. Since h is the direct sum of f and g we apply Property 14: $\mathsf{res}(h) = \mathsf{res}(f)$ and $\mathsf{AI}(h) = \mathsf{AI}(f)$. □

Following Lemma 3, our interest is to prove that the fact that $(k, e) \in A_n$ implies the existence of a predicate with $(\mathsf{res}, \mathsf{AI}) = (k, e)$, which corresponds to a more constructive result. Such an equivalence would have an impact on the locality of Goldreich PRG constructions as detailed later in Section 3.3. We introduce two lemmas that provide existence implications between functions. That way, the accessibility issue can be reduced to the existence of one subfamily of functions with specific parameters. Both existence implications could be summarized on the res/AI graph as in Figure 2.

Fig. 2: Graphical representation of Lemma 4 and 5. The red (resp. blue) square represents the existence of a function for $n = 2t + 1$ (resp. $n = 2t + m$).

Lemma 4. *Let $n \in \mathbb{N}^*$, if $\exists f \in \mathcal{B}_n$ such that $\mathsf{AI}(f) = e$ and $\mathsf{res}(f) = k > 0$, then $\forall k' \in \mathbb{N}$ such that $0 \leq k' < k$, there exists a function f' such that $\mathsf{AI}(f') = e$ and $\mathsf{res}(f') = k'$.*

Proof. We show that for each k' there is a function linear equivalent to f fulfilling the requirements. The algebraic immunity is an affine invariant criteria (see Property 4, item 5), hence we focus on linear transformations that reduce the resiliency. First, we recall the link between the Walsh spectrum of two linear equivalent functions. Let L be a linear automorphism of $\mathbb{F}_2^n$, we define g as $g(x) = f((L^*)^{-1}(x))$ where L^* is the unique linear automorphism which verifies $\forall x, y \in \mathbb{F}_2^n, x \cdot L^*(y) = L(x) \cdot y$. Then, $\forall a \in \mathbb{F}_2^n$:

$$\begin{aligned}\mathsf{W}_g(a) &= \textstyle\sum_{x \in \mathbb{F}_2^n} (-1)^{f((L^*)^{-1}(x)) + a \cdot x} \\ &= \textstyle\sum_{L^*(x) \in \mathbb{F}_2^n} (-1)^{f(x) + a \cdot L^*(x)} \\ &= \textstyle\sum_{L^*(x) \in \mathbb{F}_2^n} (-1)^{f(x) + L(a) \cdot x} \\ &= \mathsf{W}_f(L(a)).\end{aligned}$$

In other words, the value of the Walsh transform of g at a is the one of f at $L(a)$.

Then, we show that provided $\mathsf{res}(f) = k \geq 1$ there exists a linear automorphism such that $\mathsf{res}(g) = k - 1$. Using Property 1 on f we obtain that for all $w \in \mathbb{F}_2^n$ of Hamming weight at most k $\mathsf{W}_f(w) = 0$ and for at least one element b of Hamming weight $k+1$ $\mathsf{W}_f(b) \neq 0$. Since $\mathsf{w_H}(b) \geq 2$ there exist i and j such that $1 \leq i < j \leq n$ and $b_i = b_j = 1$. We define the linear automorphism $L_{i,j}$ as: $\forall a \in \mathbb{F}_2^n, L_{i,j}(a) = a'$ where $a'_i = a_i + a_j$ and $\forall \ell \in [n] \setminus i, a'_\ell = a_\ell$. $L_{i,j}$ fulfills the two following properties:

1. $\forall a \in \mathbb{F}_2^n$, $|\mathsf{w_H}(a) - \mathsf{w_H}(L_{i,j}(a))| \leq 1$.
2. $\exists c \in \mathsf{E}_{k,n} \,|\, L_{i,j}(c) = b$.

The first property enhances $\forall a \,|\, \mathsf{w_H}(a) \leq k-1, \ \mathsf{w_H}(L_{i,j}(a)) \leq k$, therefore $\mathsf{W}_g(a) = 0$, giving $\mathsf{res}(g) \geq k - 1$. The second property guarantees $\exists c \in \mathsf{E}_{k,n}$ such that $\mathsf{W}_g(c) = \mathsf{W}_f(b) \neq 0$, therefore $\mathsf{res}(g) < k$. It allows to conclude $\mathsf{res}(g) = k - 1 = \mathsf{res}(f) - 1$.

Finally, the existence of such automorphism being only conditioned by $\mathsf{res}(f) \geq 1$, the same reasoning can be applied on g, and recursively. It provides k functions linear equivalent to f each one with a different resiliency order between $k - 1$ and 0. $\square$

Lemma 5. *Let $t \in \mathbb{N}^*$. Let f be a Boolean function in $n = 2t + 1$ variables with optimal AI, then for any $m \in \mathbb{N}$ there exists a function g in $n + m$ variables such that:*

$$\mathsf{AI}(g) = \mathsf{AI}(f), \quad \textit{and } \mathsf{res}(g) = \mathsf{res}(f) + m.$$

The direct sum $g = \mathsf{XOR}_m + f$ is an example of such functions.

Proof. Proving that $g = \mathsf{XOR}_m + f$ satisfies the constraints proves the lemma. g has $n + m$ variables by construction, and using Property 14 we get that $\mathsf{res}(g) = m - 1 + \mathsf{res}(f) + 1 = m + \mathsf{res}(f)$. For the algebraic immunity, using the expression of g as a direct sum, we have $t + 1 \le \mathsf{AI}(g) \le t + 2$. We give another expression of g to show that $\mathsf{AI}(g) \le t + 1$. Since $\mathsf{AI}(f) = t + 1$, Property 4 indicates that $\deg(f) \ge t + 1$. Then Siegenthaler's bound (Theorem 2) gives $\mathsf{res}(f) \le t - 1$. It implies that there exist t variables of f, x_1 to x_t without loss of generality, such that $h = f + \sum_{i\in[t]} x_i$ is unbalanced. Since h is an unbalanced function in $2t + 1$ variables, $\mathsf{AI}(h) \le t$ (Property 4 item 7). Then applying the fourth item of Property 4, with h and the degree-1 function $\mathsf{XOR}_m + \sum_{i\in[t]} x_i$ gives $\mathsf{AI}(g) \le t + 1$, finishing the proof. □

We introduce a corollary on the existence of dahus.

Corollary 1. *Let $t \in \mathbb{N}^*$, $|\mathsf{Dahu}_{2t+2}| \ge |\mathsf{Dahu}_{2t+1}|$.*

Proof. Applying Lemma 5, one can deduce that for all $f \in \mathsf{Dahu}_{2t+1}$, the function $\mathsf{XOR}_1 + f$ belongs in Dahu_{2t+2}. Hence the following function is well-defined.

$$\begin{aligned} \Psi : \mathsf{Dahu}_{2t+1} &\to \mathsf{Dahu}_{2t+2} \\ f &\mapsto \mathsf{XOR}_1 + f \end{aligned}$$

The function Ψ is injective: Let $f \ne g$ be two dahus in Dahu_{2t+1}. The addition of XOR_1 with a new variable leads to $f + \mathsf{XOR}_1 \ne g + \mathsf{XOR}_1$. Thus, we can conclude that $|\mathsf{Dahu}_{2t+2}| \ge |\mathsf{Dahu}_{2t+1}|$. □

3.3 Conjectures and existence implications for local PRGs

We make the following conjectures on the existence of dahus. We start with the most natural conjecture.

Conjecture 1 (Dahus exist). $\forall n \ge 3$, $\mathsf{Dahu}_n \ne \emptyset$.

We introduce now another family of weaker conjectures denoted $\mathcal{C}_\ell$ for more granularity in our results. For this purpose we set

$$\ell \in \mathbb{N} \cup \{+\infty\}.$$

This $\mathcal{C}_\ell$ conjecture captures the existence of n-variable functions on vertical lines, *i.e.* for all $0 \le k \le \ell$, the set $\{(k, e) \,|\, 0 < e \le \min(\lfloor (n+1)/2 \rfloor, n - k - 1)\}$ can be accessed by n-variable functions. More formally, the conjecture is stated as follows.

Conjecture ($\mathcal{C}_\ell$). For all $0 \le k \le \ell$, for all $n > k + 1$, there exists an n-variable function f such that

$$\begin{cases} \mathsf{res}(f) = k, \\ \mathsf{AI}(f) = \min(\lfloor (n+1)/2 \rfloor, n - k - 1). \end{cases}$$

Property 8. *The introduced conjectures have the following properties*

1. *For all $\ell \ge 0$, Conjecture $\mathcal{C}_{\ell+1} \implies$ Conjecture $\mathcal{C}_\ell$.*
2. *For all $\ell \ge 0$, Conjecture $\mathcal{C}_\ell \implies \forall n$ such that $3 \le n \le 2\ell + 4$, $\mathsf{Dahu}_n \ne \emptyset$.*
3. *Conjecture $\mathcal{C}_\infty \iff$ Conjecture 1.*

Proof. 1. Let us assume that $\mathcal{C}_{\ell+1}$ is verified for an $\ell \ge 0$. Thus, for every $0 \le k \le \ell$, and $n > k+1$ the existence of an n-variable function f validating the equations of Conjecture $\mathcal{C}_\ell$ is provided by $\mathcal{C}_{\ell+1}$.

2. For $\ell \geq 0$, let us assume Conjecture $\mathcal{C}_\ell$. Let us fix

$$0 \leq (e-2) \leq \ell.$$

We apply $\mathcal{C}_\ell$ with $k = e-2$ and $n = 2e-1 > (e-2)+1$ (because $e > 0$). By definition, there exists a $(2e-1)$-variable function f such that $(\mathsf{res}(f), \mathsf{AI}(f)) = (e-2, e)$. Indeed,

$$\min(\lfloor((2e-1)+1)/2\rfloor, (2e-1)-(e-2)-1) = e.$$

Furthermore, since $\mathsf{res}(f) + \mathsf{AI}(f) + 1 = (e-2)+e+1 = (2e-1)$ and $\lfloor((2e-1)+1)/2\rfloor = e$, using Definition 14, $f \in \mathsf{Dahu}_{2e-1}$.
In addition, using Lemma 5 with $m = 1$ and $t = e-1$, $\mathsf{XOR}_1 + f \in \mathsf{Dahu}_{2e}$.
Finally, we have proved that $\mathsf{Dahu}_{2e-1} \neq \emptyset$ and $\mathsf{Dahu}_{2e} \neq \emptyset$ for all $2 \leq e \leq \ell+2$. Hence, $\forall n$ such that $3 \leq n \leq 2(\ell+2)$, $\mathsf{Dahu}_n \neq \emptyset$.
3. If Conjecture $\mathcal{C}_\infty$ is verified, an n-variable dahu can be accessed with the choice of $k = n-1-\lfloor(n+1)/2\rfloor$ (we note that $n > k+1$). Indeed, for any $n \geq 3$, $\mathcal{C}_\infty$ implies the existence of an n-variable function f such that

$$\begin{cases} \mathsf{res}(f) = n-1-\lfloor(n+1)/2\rfloor, \\ \mathsf{AI}(f) = \min(\lfloor(n+1)/2\rfloor, n-n+1+\lfloor(n+1)/2\rfloor-1) = \lfloor(n+1)/2\rfloor. \end{cases}$$

This function f validates Definition 14. Hence, Conjecture 1 is also verified.
Now, for the other way, assume that Conjecture 1 is verified. We fix $k \geq 0$ and $n > k+1$ and we build an n-variable function validating the two equations of Conjecture $\mathcal{C}_\ell$.

   - If
   $$k \leq n-1-\left\lfloor\frac{n+1}{2}\right\rfloor,$$
   by Conjecture 1, there exists an n-variable function $f \in \mathsf{Dahu}_n$ such that $\mathsf{res}(f) = n-1-\left\lfloor\frac{n+1}{2}\right\rfloor \geq k$ and $\mathsf{AI}(f) = \left\lfloor\frac{n+1}{2}\right\rfloor$. Hence, using Lemma 4, there exists an n-variable function f' such that $\mathsf{res}(f') = k$ and $\mathsf{AI}(f) = \left\lfloor\frac{n+1}{2}\right\rfloor$. The fact that $\min(\lfloor(n+1)/2\rfloor, n-1-k) = \left\lfloor\frac{n+1}{2}\right\rfloor$ allows to conclude that we have built a function f' that validates $\mathsf{res}(f') = k$ and $\mathsf{AI}(f') = \min(\lfloor(n+1)/2\rfloor, n-k-1)$.
   - Otherwise, assume now that
   $$n-1-\left\lfloor\frac{n+1}{2}\right\rfloor < k < n-1.$$
   By Conjecture 1, there exists a $(2n-3-2k)$-variable function $f \in \mathsf{Dahu}_{2n-3-2k}$. Note that
   $$\begin{aligned} 2n-3-2k &\leq 2n-3-2(n-1-\lfloor\tfrac{n+1}{2}\rfloor). \\ &\leq 2n-3-2n+2+n+1. \\ &\leq n. \end{aligned}$$
   The function f has algebraic immunity
   $$\left\lfloor\frac{(2n-3-2k)+1}{2}\right\rfloor = n-1-k = \min(\lfloor(n+1)/2\rfloor, n-1-k)$$
   and resiliency order $(2n-3-2k)-(n-1-k)-1 = n-k-3 \leq k$. Hence, using Lemma 5 with $m = 2k-n+3$, as $(2n-3-2k)+(2k-n+3) = n$, we can build an n-variable function f' that is such that $\mathsf{res}(f') = k$ and $\mathsf{AI}(f') = \min(\lfloor(n+1)/2\rfloor, n-k-1)$.

□

Lemma 6. *The Conjecture $\mathcal{C}_0$ is valid.*

Proof. Let $n > 1$. Since $\min(\lfloor (n+1)/2 \rfloor, n-1) = \lfloor (n+1)/2 \rfloor$, we aim at constructing a n-variable function that verifies $\mathsf{res}(f) = 0$ and $\mathsf{AI}(f) = \lfloor (n+1)/2 \rfloor$.

1. If $n = 2$, the function $f = \mathsf{XOR}_2 = x_1 + x_2$ verifies $\mathsf{res}(f) = 0$ and $\mathsf{AI}(f) = 1$ (see Property 7).
2. For any odd n, by Property 5, the n-variable function $f = \mathsf{MAJ}_n$ gives access to $\mathsf{res}(f) = 0$ and $\mathsf{AI}(f) = \lfloor (n+1)/2 \rfloor$. In addition, using Lemma 3, we can build an $(n+1)$-variable function g from f with the same parameters $\mathsf{res}(g) = 0$ and $\mathsf{AI}(g) = \lfloor (n+1)/2 \rfloor = \lfloor ((n+1)+1)/2 \rfloor$.

This proves the result for all $n \geq 2$. □

Remark 2. With Lemma 6, one can apply item 2 of Property 8 for $\ell = 0$ and show that $\mathsf{Dahu}_3 \neq \emptyset$ and $\mathsf{Dahu}_4 \neq \emptyset$. Note that in this work, we go further in Section 5 and prove with experiments that Dahu_5 up to Dahu_{12} are not empty.

Let us now introduce a Lemma exhibiting all the possible algebraic immunity/resiliency trade-offs depending on the strength of the conjectures.

Lemma 7 (Accessibility and conjectures).
As illustrated in Figure 3, the following accessibility results hold.

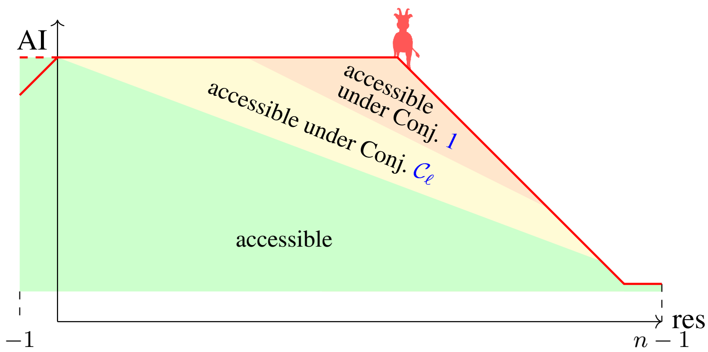


Fig. 3: Accessibility domains for an **odd** n (continuous red line), and for an **even** n (dashed line)

1. *Let $n \in \mathbb{N}$. We write $n = 2t + \varepsilon$ with $t \geq 1$ and $\varepsilon \in \{0, 1\}$. All the pairs in:* $\{(-1, e) \mid 0 < e \leq t\} \cup \{(k, 1) \mid 0 < k \leq n-1\}$ $\cup \{\{(k, e) \in [0, n-2] \times [2, t+\varepsilon] \mid k + 2e - 1 \leq n\}$ *are accessible.*
2. *For the same $n \in \mathbb{N}$ as in item 1 and $\ell \in \mathbb{N} \cup \{\infty\}$, we define* $B_{n,\ell} := \{(k, e) \in [0, n-2] \times [2, t+\varepsilon] \mid k + 2e - 1 - \min(\ell, e-2, k) \leq n\}$. *Then, Conjecture $\mathcal{C}_\ell \implies B_{n,\ell}$ is accessible.*
3. *Conjecture 1 $\iff \forall n \geq 3, A_n$ is accessible.*

Proof. Let us fix $n \in \mathbb{N}$ and write $n = 2t + \varepsilon$ with $t \geq 1$ and $\varepsilon \in \{0, 1\}$.
We prove the result by separating the zones and hypotheses.

– First we tackle the zone $\{(-1, e) \mid 0 < e \leq t\} \cup \{(k, 1) \mid 0 < k \leq n-1\}$, which is a part of the accessible zone (in green on the figure). On the one hand, for any $e \leq t$, by Property 5 the function MAJ_{2e} has $2e \leq n$ variables and gives access to resiliency order -1 and algebraic immunity e. Hence, by Lemma 3 item 2, any pair $(-1, e)$ with $e \leq t$ is accessible. On the other hand, for any $k \leq n$, by Property 7, XOR_k has $k \leq n$ variables and gives access to resiliency order $k-1$ and algebraic immunity 1. Hence, by Lemma 3 item 2, any pair $(k, 1)$ with $k \leq n-1$ is accessible.
– For a fixed $\ell \in \mathbb{N}$, let $(k, e) \in B_{n,\ell}$. We aim at proving that if $\mathcal{C}_\ell$ is valid there exists a function that gives access to parameters (k, e) with n variables.

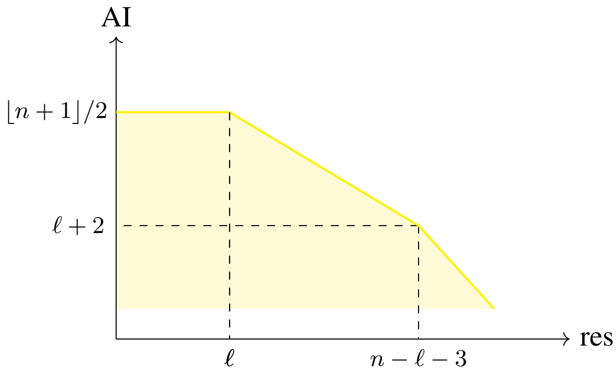


Fig. 4: Graphical representation of $B_{n,\ell}$ in the case where $\ell \leq n-\ell-3$.

By definition, $(k, e) \in B_{n,\ell}$ is equivalent to assume $(k, e) \in [0, n-2] \times [2, t+\varepsilon]$ and the three following equations:

$$\begin{aligned} 2e - 1 &\leq n, \\ k + 2e - 1 - \ell &\leq n, \\ k + e + 1 &\leq n. \end{aligned}$$

We separate the proof of existence into two cases.

- If $k \leq \ell$, in this case $\min(\ell, e-2, k) = \min(e-2, k)$. We define

$$n' := 2e + k - 1 - \min(e-2, k) = \begin{cases} e + k + 1 & \text{if } e \leq k+2 \\ 2e - 1 & \text{if } e > k+2 \end{cases}$$

  We note that $n' > k+1$. Using Conjecture $\mathcal{C}_\ell$, there exists a n'-variable function f with

$$\begin{cases} \mathsf{res}(f) = k, \\ \mathsf{AI}(f) = \min(\lfloor (n'+1)/2 \rfloor, n' - k - 1) = e. \end{cases}$$

  By hypothesis, we have $n' \leq n$. Using Lemma 3, we conclude that (k, e) is accessible with a n-variable function.
- If $k > \ell$, we apply Conjecture $\mathcal{C}_\ell$ with parameter $k' := \min(e-2, \ell)$ and $n' := 2e-1$ variables. We note that $n' > \min(e-2, \ell) + 1$. There exists a n'-variable function f such that

$$\begin{cases} \mathsf{res}(f) = \min(e-2, \ell), \\ \mathsf{AI}(f) \ = \min\left(\lfloor (n'+1)/2 \rfloor, n' - \min(e-2, \ell) - 1\right) = e. \end{cases}$$

  Hence, since f has optimal algebraic immunity, using Lemma 5 with $m = k - \min(e-2, \ell) > 0$, we can build a $(n'+m)$-variable function f' that is such that

$$\begin{cases} \mathsf{res}(f') = \mathsf{res}(f) + m = \min(e-2, \ell) + (k - \min(e-2, \ell)) = k \\ \mathsf{AI}(f') \ = \mathsf{AI}(f) = e. \end{cases}$$

Let us show that the number of variables of f' does not exceed n.

$$n' + m = (2e - 1) + (k - \min(e - 2, \ell))$$

By hypothesis, since $(k, e) \in B_{n,\ell}$, $n' + m \leq n$. Lemma 3 also allows to conclude that (k, e) is accessible with a n-variable function.

It proves the second item of the lemma(Conjecture $\mathcal{C}_\ell \implies B_{n,\ell}$ is accessible). Since $\mathcal{C}_0$ is valid (see Lemma 6) $B_{n,0}$ is accessible, which finishes to prove the first item of the lemma.

– We tackle the third item of the lemma. Using item 3 of Property 8, assuming Conjecture 1 is equivalent to assuming Conjecture $\mathcal{C}_\infty$. So, we focus instead on proving that

$$\text{Conjecture } \mathcal{C}_\infty \iff \forall n \geq 3, A_n \text{ is accessible with } n \text{ variables.}$$

If A_n is accessible for all $n \geq 3$, for any $k \geq 0$ and $n > k+1$, then the pair $(k, \min(\lfloor (n+1)/2 \rfloor, n - k - 1)) \in A_n$ is accessible by a function f and thus $\mathcal{C}_\infty$ is verified.

If Conjecture $\mathcal{C}_\infty$ is verified, we note that $A_n = B_{n,\infty} \cup \{(-1, e) \mid 0 < e \leq t\} \cup \{(k, 1) \mid 0 < k \leq n - 1\}$ and thus item 2 and 1 allow to conclude.

□

Now that the accessibility is related to the conjectures, we can introduce the theorem that was the goal of this section. We recall that in Lemma 1, issued from [AL16] results, Applebaum and Lovett state that the minimal n_0 such that there exists an n-variable Boolean function f such that $\mathsf{AI}(f) = e$ and $\mathsf{res}(f) = k$ is such that $n_0 \leq k + 2e + 1$. In the next theorem, we improve and introduce granularity in this result.

Theorem 3 (Minimal number of variables for existence). *Let k, e be integers such that $k \geq 0$ and $e \geq 2$, we denote $n_0(k, e)$ the minimal $n \in \mathbb{N}^*$ such that there exists an n-variable function f such that $\mathsf{AI}(f) = e$, and $\mathsf{res}(f) = k$. Let $\ell \in \mathbb{N} \cup \{\infty\}$. Table 1 gives bounds on the minimal $n_0(k, e)$ depending on the conjectures. Furthermore, in the particular case where $e = 1$, for any $k \geq 0$, the minimal number of variables is $n_0(k, 1) = k + 1$.*

Without conjecture	$n_0(k, e) \leq k + 2e - 1$
Under Conjecture $\mathcal{C}_\ell$	$n_0(k, e) \leq k + 2e - 1 - \min(\ell, e - 2, k)$
Under Conjecture 1	$n_0(k, e) = k + 2e - 1 - \min(e - 2, k)$

Table 1: Bounds on $n_0(k, e)$ depending on the conjectures.

Note that the equal sign in the last line of Table 1 shows that the bound is *tightly reached*: no function f with less than n_0 variables can provide $\mathsf{AI}(f) = e$ and $\mathsf{res}(f) = k$.

Proof. If $e = 1$ and $k \geq 0$, the $(k + 1)$-variable function $f = \mathsf{XOR}_{k+1}$ verifies $\mathsf{AI}(f) = e$, and $\mathsf{res}(f) = k$, thus $n_0(k, 1) \leq k+1$. In addition, using Theorem 2, f has a degree 1 thus $k+1 \leq n_0(k, 1)$. Finally, $n_0(k, 1) = k + 1$.

Now let $(k, e) \in [0, +\infty) \times [2, +\infty)$.

- We start by proving the second line of the table. We assume Conjecture $\mathcal{C}_\ell$ for $\ell \in \mathbb{N} \cup \{\infty\}$. Let $n' := k + 2e - 1 - \min(\ell, e-2, k)$, by definition $n' \geq k + e + 1$ hence $k \leq n' - 2$ and $n' \geq 2e - 1$ hence $e \leq \lfloor (n+1)/2 \rfloor$, then (k, e) belongs to $B_{n',\ell}$ and using Lemma 7 (k, e) is accessible with n' variables.

  Thus, the minimum number of variables necessary to ensure the existence of a function with resiliency order k and algebraic immunity e is thus such that

$$n_0(k, e) \leq k + 2e - 1 - \min(\ell, e-2, k),$$

  which allows to conclude.
- Then, the first line can be directly deduced by setting $\ell = 0$ in the second line and using Lemma 6, in this case $\min(\ell, e-2, k) = 0$ hence $n_0(e, k) \leq k + 2e - 1$.
- Finally, assuming Conjecture 1 is the same as assuming $\mathcal{C}_\infty$ (item 3 of Property 8), and setting $\ell = \infty$ in the second line provides $n_0(k, e) \leq k + 2e - 1 - \min(e-2, k)$. Using Lemma 2, we also have a lower bound:

$$n_0(k, e) \geq k + e + 1 \text{ and } n_0(k, e) \geq 2e - 1$$

  Thus, $n_0(k, e) \geq k + 2e - 1 - \min(e-2, k)$ which provides the equality.

□

We introduce two minimal numbersof variables, denoted n_1 and n_2, that are necessary for ensuring pseudorandomness of Goldreich's PRG.

Corollary 2 (Minimal number of variables for a secure local PRG). *Let $\mathsf{s} \in \mathbb{R}$ be such that $\mathsf{s} \geq 1$. We denote by $n_1(\mathsf{s})$ (resp. $n_2(\mathsf{s})$), the minimal number of variables for a $\mathsf{PRG}_{n,\mathsf{s}}$ secure (as defined in Definition 2) against known linear-algebraic attacks (resp. provably secure against linear-algebraic attacks). Table 2 provides the values of $n_1(\mathsf{s})$ and $n_2(\mathsf{s})$ depending on the conjectures. Note that for all cases, the upper bound provides a positive result, for example, without conjecture there exists a local PRG secure against known linear-algebraic attacks in $\lceil 2\mathsf{s} \rceil + 2\lfloor \mathsf{s}+1 \rfloor$ variables.*

Hypothesis	Secure against known linear-algebraic attacks	Provably secure against linear-algebraic attacks
Without conjecture	$n_1(\mathsf{s}) \leq \lceil 2\mathsf{s} \rceil + 2\lfloor \mathsf{s} \rfloor$	$n_2(\mathsf{s}) \leq \lceil 2\mathsf{s} \rceil + 2\lfloor 8\mathsf{s} \rfloor + 3$
Under Conjecture $\mathcal{C}_\ell$	$n_1(\mathsf{s}) \leq \lceil 2\mathsf{s} \rceil + 2\lfloor \mathsf{s} \rfloor - \min(\ell, \lfloor \mathsf{s} \rfloor - 1)$	$n_2(\mathsf{s}) \leq \lceil 2\mathsf{s} \rceil + 2\lfloor 8\mathsf{s} \rfloor + 3 - \min(\ell, \lceil 2\mathsf{s} \rceil)$
Under Conjecture 1	$n_1(\mathsf{s}) = \lceil 2\mathsf{s} \rceil + \lfloor \mathsf{s} \rfloor + 1$	$n_2(\mathsf{s}) = 2\lfloor 8\mathsf{s} \rfloor + 3$

Table 2: Bounds on $n_1(\mathsf{s})$ and $n_2(\mathsf{s})$ depending on the conjectures.

Proof. Let $\mathsf{s} \geq 1$. Using Theorem 1, $n_1(\mathsf{s})$ and $n_2(\mathsf{s})$ are defined such that

$$n_1(\mathsf{s}) = \min_{\substack{k \geq 2\mathsf{s}-1 \\ e > \mathsf{s}}} n_0(k, e) \text{ and } n_2(\mathsf{s}) = \min_{\substack{k \geq 2\mathsf{s} \\ e > 8\mathsf{s}+1}} n_0(k, e).$$

Hence, the table is obtained from Theorem 3 with

$$n_1(\mathsf{s}) \leq n_0(\lceil 2\mathsf{s} - 1 \rceil, \lfloor \mathsf{s} + 1 \rfloor) \text{ and } n_2(\mathsf{s}) \leq n_0(\lceil 2\mathsf{s} \rceil, \lfloor 8\mathsf{s} + 2 \rfloor).$$

For proving the equality in the last line, we show that assuming Conjecture 1 the two upper bounds in the previous equation become equalities (and the final result is given by the formula of n_0 in Theorem 1). Indeed, let us assume that for all pair of integers $k \geq -1$ and $e \geq 2$,

$$n_0(k,e) \leq n_0(k,e+1) \text{ and } n_0(k,e) \leq n_0(k+1,e), \tag{1}$$

then

$$\min_{\substack{k \geq 2\mathsf{s}-1 \\ e > \mathsf{s}}} n_0(k,e) = n_0(\lceil 2\mathsf{s}-1 \rceil, \lfloor \mathsf{s}+1 \rfloor) \text{ and } \min_{\substack{k \geq 2\mathsf{s} \\ e > 8\mathsf{s}+1}} n_0(k,e) = n_0(\lceil 2\mathsf{s} \rceil, \lfloor 8\mathsf{s}+2 \rfloor).$$

Let us now prove Equation 1. We use that by construction the set A_n (see Definition 15) contains the element (k,e) for $k \geq -1$ and $e \geq 2$ if it contains $(k+1,e)$ or $(k,e+1)$.

Assuming Conjecture 1 all the sets A_n are accessible (Lemma 7 item 3), then by definition $n_0(k,e+1)$ is the minimal n such that $(k,e+1) \in A_n$. Since $k \geq -1$ and $e+1 \geq 3$ then (k,e) also belongs to A_n and since for all $n \geq 4$ $A_n \supsetneq A_{n-1}$ it gives $n_0(k,e) \leq n_0(k,e+1)$. Similarly, $n_0(k+1,e)$ is the minimal n such that $(k+1,e) \in A_n$, since $k+1 \geq 0$ and $e \geq 2$ then $(k,e) \in A_n$ and we can conclude $n_0(k,e) \leq n_0(k+1,e)$, finishing the proof.

□

Particular case of Corollary 2 Let $\mathsf{s} \in \mathbb{N}^*$ be an integer. The table of Corollary 2 can be simplified as shown in Table 3.

Hypothesis	Secure against known linear-algebraic attacks	Provably secure against linear-algebraic attacks
Without conjecture	$n_1(\mathsf{s}) \leq 4\mathsf{s}$	$n_2(\mathsf{s}) \leq 18\mathsf{s}+3$
Under Conjecture $\mathcal{C}_\ell$	$n_1(\mathsf{s}) \leq 4\mathsf{s} - \min(\ell, \mathsf{s}-1)$	$n_2(\mathsf{s}) \leq 18\mathsf{s}+3-\min(\ell, 2\mathsf{s})$
Under Conjecture 1	$n_1(\mathsf{s}) = 3\mathsf{s}+1$	$n_2(\mathsf{s}) = 16\mathsf{s}+3$

Table 3: Particular case of Table 2 when s is an integer.

For example, for $\mathsf{s} = 3$, one can hope to obtain a function secure against known linear-algebraic attacks (resp. provably secure function against linear-algebraic attacks) if $n \geq 12$ (resp. if $n \geq 57$). If Conjecture 1 is valid, the number of variables for a secure function against known linear-algebraic attacks (resp. provably secure function against linear-algebraic attacks) is $n = 10$ (resp. $n = 51$).

4 Known families and negative results

Since the introduction of algebraic attacks on stream ciphers [CM03] and the formal definition of algebraic immunity [Arm+06], finding Boolean functions with optimal AI (resisting to these attacks) has been the focus of many works. In this section we consider known constructions with high algebraic immunity and study them relatively to the existence of dahus, or the validity of our conjectures. More precisely we begin with a brief survey on the different known constructions with optimal algebraic immunity, and explain their relations with our conjectures. Then, the main part of this section is devoted to two families, XOR-MAJ (Definition 11) and Rotation Symmetric Functions (RSF).

First, different works with an experiment component found sporadic cases of functions with optimal algebraic immunity such as [DGM04; CG05; MC13] for small values of n. The first constructions giving functions with optimal AI for infinitely many n were majorities or similar functions [BP05; DMS06], and iterative constructions [DGM05; Car+06], and later [Pas09; Son+10; PFZ11]. Then, new families were obtained by the construction by flats [Car07; Car+09], and by swapping chosen elements of the truth table of the majority function [LQ06; Li+08; LKK13]. Later, various constructions using the univariate representation [CF08; Riz10; Zen+11; Li+14] (as functions from $\mathbb{F}_{2^n}$ to $\mathbb{F}_2$), or performing swaps on such functions [LKK13; LK18], gave families with optimal algebraic immunity and other good cryptographic properties such as high algebraic degree and better nonlinearity (a common criteria on Boolean functions used in stream ciphers to avoid attacks using good linear approximations). Similarly, the bi-variate representation enabled to exhibit more AI-optimal constructions [TD11; TCT13; TCT14; Tan+17; JLW11; LL14; LL17; Jin+11; WZL15; Tan+10; TD12; Zhe+14; WLL13] with other good cryptographic criteria. Finally, many known functions with optimal algebraic immunity are rotation symmetric functions, the AI of which is proven by considering swaps on the majority functions [SM07] or the construction by flats [Car+09]. AI-optimal functions from this family are also given in [Fu+09; ZS19; ST14; Che+19; CGR19; Zha+12; CZT14; Fu+11; MSZ21].

The sporadic cases give a few examples of dahus. In [DGM04] the authors found 7-variable RSF with resiliency order 2 and algebraic immunity 4, they found 24 such dahus (experiment 1). Moreover, in the same article, the Example 1 from a construction of resilient function of Tarannikov [Tar00], H_1, is an 8-variable function with $\mathsf{res} = 3$, and $\mathsf{AI} = 4$, hence another example of dahu. We did not find other sporadic examples in the literature (either they are not dahus, or only one of the two parameters is given and the second one is not deducible). For $n = 3$, any AI-optimal function is a dahu since such function is balanced (see Property 4 Item 7), hence all known families from the works cited above give a dahu when they are defined for $n = 3$. Nevertheless, these constructions do not allow to find dahus for n greater than 4: for all the optimal-AI constructions we could find, when the resiliency order is given or derivable from the paper's result, either the resiliency order is 0 for odd n, or no more than 1 for even n. We summarize these results in Table 4.

Relatively to the conjectures introduced in Section 3, it means that the exhibited families allow to verify at most $\mathcal{C}_0$. It also implies that all constructions giving AI-optimal balanced functions for odd n ([BP05; CF08; CGR19]) allow to get local functions with the same properties as the XOR-MAJ functions using Lemma 5. Note that, finding an AI-optimal family with prescribed resiliency ℓ for all n big enough would be the main requirement to prove $\mathcal{C}_\ell$ and would be sufficient to prove an asymptotic version of Theorem 3 line 2. The current situation seems paradoxical: examples of dahus have been found for values of n up to 8 whereas known AI-optimal families have a resiliency order stuck at 0 (or 1 for even n).[8] To illustrate this paradox, we study in more details two families of functions, explain the sporadic cases where they give dahus, and why these constructions do not allow to overcome $\mathcal{C}_\infty$.

First, we focus on XOR-MAJ functions since the majority functions were one of the first examples of AI-optimal functions, and they are the main candidate to instantiate Goldreich's PRG. In Section 4.1 we give the parameters of XOR-MAJ functions, and show that no function of this family nor affine equivalent can verify more than $\mathcal{C}_\prime$. Then, we focus on the family of rotation symmetric functions. In Subsection 4.2 we define this family and give the necessary notations we use in the algorithms experimentally determining dahus for n up to 11 (the experimental results are given in Section 5). In Subsection 4.3 we show that various AI-optimal RSF families do not contain dahus (for $n \geq 5$) based on the knowledge of their Walsh transform, and in Subsection 4.3 we show a more general result preventing some AI-optimal functions to be dahus and we apply it to two known AI-optimal RSF families showing that such functions are at most balanced.

[8] Despite the resiliency order is a major criterion, some of these constructions were also designed to target a high algebraic degree which forces a low resiliency order (see Theorem 2).

Reference	n	res()	type	resiliency limitation
[BP05], classes $1, 2, 3$	even	-1	symmetric	unbalanced
[BP05], class 1	odd	0	majority	$\mathsf{W}_f(\mathsf{E}_{1,n}) \neq \mathbf{0}$
[DGM05], Construction 1 $f_0 = x_1$	even	0	iterative	$\mathsf{res}(f_0)$
[DGM05], Construction 1 $f_0 = x_1 + x_2$	even	1	iterative	$\mathsf{res}(f_0)$
[CF08]	$n \geq 2$	0	univariate	$\mathsf{deg} = n - 1$
[Car+09], f, f_0, f_1, f_2	even	≤ 0	flats	$\mathsf{W}_f(\mathsf{E}_{1,n}) \neq \mathbf{0}$
[Fu+09], Construction 2	even	-1	RSF	$\mathsf{W}_f(\mathbf{0}) \neq 0$
[Pas09], Theorem 3	even	≤ 0	iterative	$\mathsf{deg} \geq n - 1$
[Pas09], Theorem 4	even	≤ 1	iterative	$\mathsf{deg} \geq n - 2$
[Tan+10] Construction 1	even	0	bi-variate	$\mathsf{deg} = n - 1$
[Tan+10] Construction 2	even	1	bi-variate	$\mathsf{deg} = n - 2$
[Jin+11] Construction 4.1	even	-1	bi-variate	bent
[Jin+11] Construction 5.1	even	0	bi-variate	$\mathsf{deg} = n - 1$
[JLW11]	even	1	bi-variate	$\mathsf{deg} = n - 2$
[TD11] Construction 1	even	-1	bi-variate	bent
[TD11] Construction 2	even	0	bi-variate	$\mathsf{deg} = n - 1$
[TD12]	even	1	bi-variate	$\mathsf{deg} = n - 2$
[TCT13] Construction 1	even	1	bi-variate	$\mathsf{deg} = n - 2$
[TCT13] Construction 2	even	0	bi-variate	$\mathsf{deg} = n - 1$
[WLL13]	even	1	bi-variate	$\mathsf{deg} = n - 2$
[LL14]	even	0	bi-variate	$\mathsf{deg} = n - 1$
[TCT14] Construction 2	even	1	bi-variate	$\mathsf{deg} = n - 2$
[Zhe+14] Construction 4.1	even	-1	bi-variate	unbalanced
[Zhe+14] Construction 5.1	even	0	bi-variate	$\mathsf{deg} = n - 1$
[WZL15] Constructions $1, 3$	even	1	bi-variate	$\mathsf{deg} = n - 2$
[WZL15] Constructions $2, 4$	even	0	bi-variate	$\mathsf{deg} = n - 1$
[Tan+17]	even	1	bi-variate	$\mathsf{deg} = n - 2$
[CGR19], f	odd	0	RSF	$\mathsf{W}_f(\mathsf{E}_{1,n}) \neq \mathbf{0}$
[CGR19], f'	odd $\neq 2^m+1$	0	RSF	$\mathsf{deg} = n - 1$
[MSZ21]	even	0	RSF	$\mathsf{W}_f(\mathsf{E}_{1,n}) \neq \mathbf{0}$

Table 4: Constructions with optimal algebraic immunity and their resiliency order res(). "Type" denotes the method of construction, and "resiliency limitation" the criterion in the paper allowing to state the resiliency order. In the last column, $\mathsf{W}_f(\mathsf{E}_{1,n}) \neq \mathbf{0}$ means that the Walsh spectrum is not null on all elements of $\mathsf{E}_{1,n}$, allowing to conclude using Property 1, the degrees allow to conclude using Theorem 2, and bent functions are unbalanced.

4.1 XOR-MAJ functions, dahus and limitations

The family of XOR-MAJ functions has been presented in [AL16] as a good candidate in the context of local PRG. In this section, we study further the parameters of XOR-MAJ functions and their properties.

We show that, on small localities certain instances of XOR-MAJ can be dahus. However, it turned out to be a dead end: asymptotically we end up in a negative result arguing that XOR-MAJ may not be the best candidates for constructing dahus or optimal functions. More precisely, we prove that no function linear equivalent to XOR-MAJ functions can improve the minimal locality bound of Theorem 3.

Parameters of XOR-MAJ

Determining the resiliency order of XOR-MAJ functions (Definition 11) can be done combining the results of direct sum constructions and the resiliency of majority function. Finding the exact AI is more complex, it can be achieved using the partitioned algebraic normal form coefficients as in [Méa+19b; CM20; CM22].

Lemma 8 **(Algebraic Immunity Increase, [Méa+19b] Lemma 16).** *Let f be the direct sum of two Boolean functions g and h in respectively n and m variables such that $\mathsf{AI}(g) \geq \mathsf{AI}(h)$. If $\deg(h) > 0$, and $\mathsf{AN}(g) \neq \mathsf{AN}(g+1)$ then $\mathsf{AI}(f) > \mathsf{AI}(g)$.*

In the following lemma, we give the algebraic immunity and resiliency order of XOR-MAJ functions. This result is not entirely novel, in certain cases the parameters are obtained using Lemma 8 (they are a sub-family of "XOR-threshold" functions which parameters are determined in [CM22]). But, the last part of the proof ($\mathsf{AI}(\mathsf{XOR}_k\mathsf{MAJ}_{2t+1})$) is new.

Lemma 9 **(Parameters of XOR-MAJ functions).** *Let $k, t \in \mathbb{N}^*$, let $\varepsilon \in \{0,1\}$,*

$$\mathsf{AI}(\mathsf{XOR}_k\mathsf{MAJ}_{2t+\varepsilon}) = t+1, \ \mathsf{res}(\mathsf{XOR}_k\mathsf{MAJ}_{2t+\varepsilon}) = k-1+\varepsilon.$$

Proof. Let $k, t \in \mathbb{N}^*$, let $\varepsilon \in \{0,1\}$. We first address the resiliency. Property 14 gives $\mathsf{res}(\mathsf{XOR}_k\mathsf{MAJ}_{2t+\varepsilon}) = k-1+\mathsf{res}(\mathsf{MAJ}_{2t+\varepsilon})+1$. The first item of Property 5 allows us to conclude.
Let us consider now the algebraic immunity.

1. Assume that the majority is taken on an even number of variables (*i.e.* $\varepsilon = 0$). We use Lemma 8 with

$$g = \mathsf{MAJ}_{2t} \text{ and } h = \mathsf{XOR}_k.$$

The lemma's requirements are satisfied because
(a) $\mathsf{AI}(\mathsf{MAJ}_{2t}) = t \geq 1 = \mathsf{AI}(\mathsf{XOR}_k)$ given by Properties 5 and 7,
(b) $\mathsf{AN}(\mathsf{MAJ}_{2t}) \neq \mathsf{AN}(1+\mathsf{MAJ}_{2t})$ given by Property 5.
Thus, we obtain $\mathsf{AI}(\mathsf{XOR}_k\mathsf{MAJ}_{2t}) > \mathsf{AI}(\mathsf{MAJ}_{2t}) = t$.
Furthermore, $\mathsf{AI}(\mathsf{XOR}_k\mathsf{MAJ}_{2t}) \leq t+1$ by Property 14. Finally, $\mathsf{AI}(\mathsf{XOR}_k\mathsf{MAJ}_{2t}) = t+1$.

2. Assume now that the majority is taken on an odd number of variables (*i.e.* $\varepsilon = 1$), combining Property 5 with Property 14,

$$t+1 \leq \mathsf{AI}(\mathsf{XOR}_k\mathsf{MAJ}_{2t+1}) \leq t+2.$$

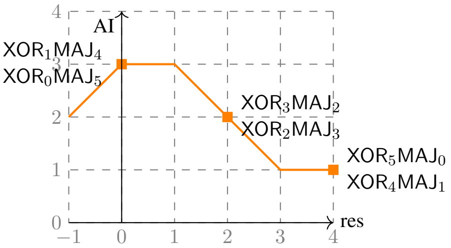
We show that the lower bound is reached, by expressing $\mathsf{XOR}_k\mathsf{MAJ}_{2t+1}$ differently. According to Definition 6, there exists a variable, denoted x_1, such that $\mathsf{MAJ}_{2t+1} + x_1$ is unbalanced. Therefore, $\mathsf{AI}(\mathsf{MAJ}_{2t+1}+x_1) \leq t$; since a function in an odd number of variables reaching the optimal algebraic immunity cannot be unbalanced (see item 3 of Property 4).
Using Properties 14 and 4, the direct sum of this function with the null function in k variables results in a function f (in $k+2t+1$ variables) of algebraic immunity of at most $t+0=t$. Finally, adding the degree 1 function $x_1 + \mathsf{XOR}_k$ to f gives the function $\mathsf{XOR}_k\mathsf{MAJ}_{2t+1}$ with algebraic immunity

$$\mathsf{AI}(\mathsf{XOR}_k\mathsf{MAJ}_{2t+1}) \leq t + \deg(x_1 + \mathsf{XOR}_k) = t+1,$$

applying the fourth item of Property 4. This inequality concludes the proof.

$\square$

Remark 3. This result is another way to prove the part without conjecture of Theorem 3. Indeed, for k, e such that $k \geq 0$ and $e \geq 2$, the functions $\mathsf{XOR}_k\mathsf{MAJ}_{2e-1}$ and $\mathsf{XOR}_{k+1}\mathsf{MAJ}_{2e-2}$ verify $\mathsf{AI}(f) = e$, and $\mathsf{res}(f) = k$. And, their number of variables is $k + 2e - 1$. Thus, $n_0(k, e) \leq k + 2e - 1$.



Example 1. For a locality $n = 5$, we present all the possible XOR-MAJ functions on the left hand. Lemma 9 give the parameters when the majority part is over at least 2 variables, and since $\mathsf{MAJ}_1 = \mathsf{XOR}_1$ Property 7 gives the two remaining cases.

Remark 4. In Example 1 we notice XOR-MAJ functions have the same parameters two by two. In the next lemma we show that in the general case there are two XOR-MAJ functions in the same affine equivalence class. Moreover, these affine equivalent functions are the one having the same parameters in Lemma 9.

Lemma 10 (Affine equivalent XOR-MAJ functions). *Let $r \in \mathbb{N}$ and $t \in \mathbb{N}^*$, $\mathsf{XOR}_r\mathsf{MAJ}_{2t+1}$ and $\mathsf{XOR}_{r+1}\mathsf{MAJ}_{2t}$ are affine equivalent.*

Proof. We show that these 2 functions are affine equivalent since MAJ_{2t+1} and $\mathsf{XOR}_1\mathsf{MAJ}_{2t}$ are affine equivalent for all $t \in \mathbb{N}^*$. Let consider the linear transformation φ over $\mathbb{F}_2^{2t+1}$ defined as $(x_1, y_1, \cdots, y_{2t}) \mapsto (x_1, y_1 + x_1, \cdots, y_{2t} + x_1)$, and denote y the vector composed by the y_i. We study the expression of $\mathsf{MAJ}_{2t+1}(\varphi(x))$ depending on the value of x_1:

-When $x_1 = 0$, $\mathsf{MAJ}_{2t+1}(\varphi(x)) = \mathsf{MAJ}_{2t+1}(0, y) = \mathsf{MAJ}_{2t}(y)$.

-When $x_1 = 1$, $\mathsf{MAJ}_{2t+1}(\varphi(x)) = \mathsf{MAJ}_{2t+1}(1, \bar{y})$, where $\bar{y}$ denotes the complementary vector of y. The majority gives 1 if and only if $\mathsf{w_H}(\bar{y}) \in [t, 2t]$, which corresponds to $0 \leq \mathsf{w_H}(y) \leq t$ and then: $\mathsf{MAJ}_{2t+1}(\varphi(x)) = 1 + \mathsf{MAJ}_{2t}(y)$ in this case.

Combining the two cases, $\forall x \in \mathbb{F}_2^{2t+1}$:

$$\mathsf{MAJ}_{2t+1}(\varphi(x)) = (1 + x_1)\mathsf{MAJ}_{2t}(y) + x_1(1 + \mathsf{MAJ}_{2t}(y)) = x_1 + \mathsf{MAJ}_{2t}(y).$$

Since φ is linear, MAJ_{2t+1} and $\mathsf{XOR}_1\mathsf{MAJ}_{2t}$ are affine equivalent. Combining φ with the identity function on $\mathbb{F}_2^r$ (with $r \in \mathbb{N}^*$) guarantees the affine equivalence of $\mathsf{XOR}_r\mathsf{MAJ}_{2t+1}$ and $\mathsf{XOR}_{r+1}\mathsf{MAJ}_{2t}$. $\square$

Limitations of XOR-MAJ functions for local PRGs

In the following we address the limitations of XOR-MAJ relatively to local PRGs. More precisely we prove that they are sufficient to prove $\mathcal{C}_{\prime}$, but not to go beyond. We show in Theorem 4 that the structure (a vector space of high dimension) of the Walsh co-support of the majority function prevent these families (and any affine equivalent ones) to contain dahus.

Let us start with a positive result for a small locality. Combining Property 5, Lemma 9 and Definition 14, one can verify that

$$\{\mathsf{MAJ}_3, \mathsf{XOR}_1\mathsf{MAJ}_2\} \in \mathsf{Dahu}_3.$$

However, for higher localities, we will show that XOR-MAJ functions offer limited perspectives for constructing dahus or optimal functions.

For the MAJ functions, their degree equals to $2^{\lceil \log((n+1)/2) \rceil}$ for n odd (*e.g.* [DMS06]), already restricts the possibilities: the degree and the algebraic immunity can be equal only if $n+1$ is a power of two. As an illustration, in the following lemma we show that for any odd $n \geq 5$ no function affine equivalent to MAJ_n is a dahu.

Lemma 11 (Majority Functions and dahus). *Let n be an odd integer strictly greater than 3, $\mathsf{MAJ}_n \notin \mathsf{Dahu}_n$ and none of the functions affine equivalent to MAJ_n is a dahu.*

Proof. Let $k, t \in \mathbb{N}^*$, let $\varepsilon \in \{0, 1\}$. We first address the resiliency. Property 14 gives $\mathsf{res}(\mathsf{XOR}_k\mathsf{MAJ}_{2t+\varepsilon}) = k - 1 + \mathsf{res}(\mathsf{MAJ}_{2t+\varepsilon}) + 1$. The first item of Property 5 allows us to conclude.
Let us consider now the algebraic immunity.

1. Assume that the majority is taken on an even number of variables (*i.e.* $\varepsilon = 0$). We use Lemma 8 with

$$g = \mathsf{MAJ}_{2t} \text{ and } h = \mathsf{XOR}_k.$$

   The lemma's requirements are satisfied because
   (a) $\mathsf{AI}(\mathsf{MAJ}_{2t}) = t \geq 1 = \mathsf{AI}(\mathsf{XOR}_k)$ given by Properties 5 and 7,
   (b) $\mathsf{AN}(\mathsf{MAJ}_{2t}) \neq \mathsf{AN}(1 + \mathsf{MAJ}_{2t})$ given by Property 5.
   Thus, we obtain $\mathsf{AI}(\mathsf{XOR}_k\mathsf{MAJ}_{2t}) > \mathsf{AI}(\mathsf{MAJ}_{2t}) = t$.
   Furthermore, $\mathsf{AI}(\mathsf{XOR}_k\mathsf{MAJ}_{2t}) \leq t + 1$ by Property 14. Finally, $\mathsf{AI}(\mathsf{XOR}_k\mathsf{MAJ}_{2t}) = t + 1$.

2. Assume now that the majority is taken on an odd number of variables (*i.e.* $\varepsilon = 1$), combining Property 5 with Property 14,

$$t + 1 \leq \mathsf{AI}(\mathsf{XOR}_k\mathsf{MAJ}_{2t+1}) \leq t + 2.$$

   We show that the lower bound is reached, by expressing $\mathsf{XOR}_k\mathsf{MAJ}_{2t+1}$ differently. According to Definition 6, there exists a variable, denoted x_1, such that $\mathsf{MAJ}_{2t+1} + x_1$ is unbalanced. Therefore, $\mathsf{AI}(\mathsf{MAJ}_{2t+1} + x_1) \leq t$; since a function in an odd number of variables reaching the optimal algebraic immunity cannot be unbalanced (see item 3 of Property 4).
   Using Properties 14 and 4, the direct sum of this function with the null function in k variables results in a function f (in $k + 2t + 1$ variables) of algebraic immunity of at most $t + 0 = t$. Finally, adding the degree 1 function $x_1 + \mathsf{XOR}_k$ to f gives the function $\mathsf{XOR}_k\mathsf{MAJ}_{2t+1}$ with algebraic immunity

$$\mathsf{AI}(\mathsf{XOR}_k\mathsf{MAJ}_{2t+1}) \leq t + \mathsf{deg}(x_1 + \mathsf{XOR}_k) = t + 1,$$

   applying the fourth item of Property 4. This inequality concludes the proof.

□

Generalizing the approach of Lemma 11, we show that no function affine equivalent to a XOR-MAJ function can optimize both the algebraic immunity and the resiliency order. It proves that no function of this class can improve on the bound of Theorem 3.

Theorem 4 (XOR-MAJ limitations). *Let $f \in \mathcal{B}_n$ be affine equivalent to a XOR-MAJ function ($\mathsf{XOR}_r\mathsf{MAJ}_m$ where $r, m \in \mathbb{N}^*$, $r + m = n$) such that $\mathsf{AI}(f) = e \geq 2$ and $\mathsf{res}(f) = k \geq 0$, then $n \geq k + 2e - 1$. In particular, if $n > 4$ then $f \notin \mathsf{Dahu}_n$.*

Proof. Let $f \in \mathcal{B}_n$ be affine equivalent to a XOR-MAJ function such that $\mathsf{AI}(f) = e \geq 2$ and $\mathsf{res}(f) = k \geq 0$. Since the algebraic immunity is affine invariant (Property 4), $\mathsf{AI}(f) = e \geq 2$ implies that f is affine equivalent to $\mathsf{XOR}_r\mathsf{MAJ}_{2e-1}$ or to $\mathsf{XOR}_{r+1}\mathsf{MAJ}_{2e-2}$, where $r = n - 2e + 1 \in \mathbb{N}$ (see Lemma 9). From Lemma 10, we know that $\mathsf{XOR}_r\mathsf{MAJ}_{2e-1}$ and $\mathsf{XOR}_{r+1}\mathsf{MAJ}_{2e-2}$ are affine equivalent, hence f is affine equivalent to $\mathsf{XOR}_r\mathsf{MAJ}_{2e-1}$ and we will study the structure of the Walsh support of $\mathsf{XOR}_r\mathsf{MAJ}_{2e-1}$ to deduce an upper bound on the resiliency order of f.

The function $\mathsf{XOR}_r\mathsf{MAJ}_{2e-1}$ is the direct sum of XOR_r and MAJ_{2e-1}, then, by Property 2 its Walsh support is the Cartesian product: $\mathsf{Wsupp}_{\mathsf{XOR}_r} \times \mathsf{Wsupp}_{\mathsf{MAJ}_{2e-1}}$.

$$\mathsf{Wsupp}_{\mathsf{XOR}_r} \times \mathsf{Wsupp}_{\mathsf{MAJ}_{2e-1}}.$$

The function XOR_r is affine therefore its Walsh support is a singleton (Property 2), and by Property 6 the Walsh support of MAJ_{2e-1} is the set of odd weight vectors of $\mathbb{F}_2^{2e-1}$. Thereafter, $\mathsf{Wsupp}_{\mathsf{XOR}_r\mathsf{MAJ}_{2e-1}}$ is an affine sub-space which can be written as $a + V$, where $a \in \mathbb{F}_2^{r+2e-1}$ and V is a vector space of dimension $2e - 2$. Using Property 2, since f is affine equivalent to $\mathsf{XOR}_r\mathsf{MAJ}_{2e-1}$:

$$\mathsf{Wsupp}_f = L(\mathsf{Wsupp}_{\mathsf{XOR}_r\mathsf{MAJ}_{2e-1}}) = L(a + V) = b + W,$$

where L is an affine automorphism of $\mathbb{F}_2^n$, $b \in \mathbb{F}_2^n$ and W is a vector space of dimension $2e - 2$.

Then, we show that Wsupp_f has at least one element of Hamming weight at most $n - 2e + 2$. We identify the vector space of $\mathbb{F}_2^n$ W as a linear code over $\mathbb{F}_2^n$, which gives a binary code of length n and dimension $2e - 2$. The covering radius of a code, the maximum distance between an element of the space and the code, is always upper bounded by its length minus its dimension (Property 3), hence:

$$\max_{u \in \mathbb{F}_2^n}(\mathsf{d_H}(u, v) \mid v \in W) \leq n - 2e + 2.$$

Thereafter, any affine subspace $u+W$ contains a least one element of Hamming weight at most $n-2e+2$, hence:

$$\min_{v \in \mathsf{Wsupp}_f} \mathsf{w_H}(v) = \min_{v \in u+W} \mathsf{w_H}(v) \leq n - 2e + 2.$$

Property 1 allows to conclude $\mathsf{res}(f) \leq n - 2e + 1 = r$, and from Lemma 9 $\mathsf{res}(\mathsf{XOR}_r\mathsf{MAJ}_{2e-1}) = r$. Therefore, XOR-MAJ functions have the best resiliency order in its affine equivalence class, and for any functions f affine equivalent to a n-variable XOR-MAJ, $\mathsf{AI}(f) = e \geq 2$ and $\mathsf{res}(f) = k \geq 0$ implies $n \geq k + 2e - 1$.

Finally we show that in particular if $n > 4$ then $f \notin \mathsf{Dahu}_n$. From Definition 14, $g \in \mathsf{Dahu}_n$ implies $\mathsf{AI}(g) + \mathsf{res}(g) + 1 = n$, and $n > 4$ implies $\mathsf{AI}(g) > 2$. On the other side, $\mathsf{AI}(f) + \mathsf{res}(f) + 1 = k + e + 1$ and we proved $n \geq k + 2e - 1 = k + e + 1 + (e - 2)$. Then, for $n > 4$, $\mathsf{AI}(f) + \mathsf{res}(f) + 1 > n$ or $\mathsf{AI}(f) \leq 2$ hence $f \notin \mathsf{Dahu}_n$.

□

4.2 Rotation Symmetric Functions

Rotation symmetric Boolean functions have been introduced in [PQ98], and then studied for their cryptographic properties in different works *e.g.* [CS00; SMC04; DM05; Kav+06; SM07; Fu+09]. This class of function is known to have elements with good cryptographic properties, and it allows easier exhaustive search than with all Boolean Functions. Indeed, there are around $\left(2^{2^n}/n\right)$ RSF with n variables (compared to 2^{2^n} Boolean functions), and compact representations allow more efficient algorithms to determine their properties.

Definition 16 (Rotation Symmetric Function (adapted from [Car21] Definition 59)). *Let $n \in \mathbb{N}$, a Boolean function over $\mathbb{F}_2^n$ is called rotation symmetric function (RSF) if it is invariant under any cyclic shift of input coordinates, i.e. it is invariant under a primitive cyclic shift, for instance: $(x_1, \cdots, x_n) \to (x_n, x_1, \cdots, x_{n-1})$. We denote RSF_n the set of Boolean rotation symmetric functions in n variables.*

We add some notations and vocabulary as in [SM07]. For $x \in \mathbb{F}_2^n$ we call orbit of x, denoted O_x the set of elements obtained by cyclic shifts (or rotations) of x. The number of different orbits is denoted g_n, and the number of orbits with elements of Hamming weight w is denoted $g_{n,w}$. Since an RSF takes the same value on inputs from the same rotation orbit, having the value for one element of each orbit is sufficient to characterize an RSF. We therefore consider only one representative element by orbit, the first one in lexicographic order, we denote these representatives Λ_1 to Λ_{g_n}.

For n odd, we order the representative in the following way, up to the weight $(n-1)/2$ first by Hamming weight and then following the lexicographic order. The second part contains the complements of the first part, we order them in the reverse order: a representative and its complement have indexes i and $g_n + 1 - i$.

Example 2. $n = 5$, $g_n = 8$, the list of representatives is:

$$[(0,0,0,0,0),(1,0,0,0,0),(1,1,0,0,0),(1,0,1,0,0),$$
$$(1,1,0,1,0),(1,1,1,0,0),(1,1,1,1,0),(1,1,1,1,1)].$$

We define the simplified truth table, ANF, Walsh spectrum of the RSF family, and two matrices as in [SMC04].

Definition 17 (Simplified Truth Table, ANF and Walsh Spectrum of RSF). *Let $f \in \mathsf{RSF}_n$, we define:*

- *the simplified truth table:* $\mathsf{STT}(f) = [f(\Lambda_1), \cdots, f(\Lambda_{g_n})]$,
- *the simplified algebraic normal form :* $\mathsf{SANF}(f) = [a_{\mathsf{supp}(\Lambda_1)}, \cdots, a_{\mathsf{supp}(\Lambda_{g_n})}]$,
- *the simplified Walsh spectrum:* $\mathsf{SWS}(f) = [\mathsf{W}_f(\Lambda_1), \cdots, \mathsf{W}_f(\Lambda_{g_n})]$.

Any of the three representations characterizes f.

Proposition 1. *Let $n \in \mathbb{N}^*$, $\mathbf{A} \in \mathbb{Z}^{g_n \times g_n}$ and $\mathbf{B} \in \mathbb{F}_2^{g_n \times g_n}$ such that:*

$$\forall i, j \in [g_n],\ \mathbf{A}_{i,j} = \sum_{x \in O_{\Lambda_i}} (-1)^{x \cdot \Lambda_j} \text{ and } \mathbf{B}_{i,j} = \bigoplus_{x \in O_{\Lambda_i}} x \preceq \Lambda_j.$$

Then, $\mathsf{SWS}(f) = (1_{g_n} - 2\mathsf{STT}(f))\mathbf{A}$, *and* $\mathsf{STT}(f) = \mathsf{SANF}(f)\mathbf{B}$.

Proof. We begin with the Walsh spectrum. Since $f(x) \in \mathbb{F}_2$ embedding it in $\mathbb{Z}$ we get $1 - 2f(x) = (-1)^{f(x)}$. Then, the j-th element of $\mathsf{SWS}(f)$ can be written as:

$$\sum_{i=1}^{g_n} (-1)^{f(\Lambda_i)} \mathbf{A}_{i,j} = \sum_{i=1}^{g_n} (-1)^{f(\Lambda_i)} \sum_{x \in O_{\Lambda_i}} (-1)^{x \cdot \Lambda_j} = \sum_{i=1}^{g_n} \sum_{x \in O_{\Lambda_i}} (-1)^{x \cdot \Lambda_j + f(x)},$$
$$= \sum_{x \in \mathbb{F}_2^n} (-1)^{x \cdot \Lambda_j + f(x)} = \mathsf{W}_f(\Lambda_j).$$

For the conversion between $\mathsf{STT}(f)$ and $\mathsf{SANF}(f)$, note that by definition $\mathbf{B}_{i,j}$ gives the value $g(\Lambda_j)$ where g is the elementary RSF: $g(x) = \bigoplus_{y \in O_{\Lambda_i}} \prod_{k \in \mathsf{supp}\{y\}} x_k$. Thereafter, each column of $\mathbf{B}$ gives the STT of an elementary RSF, by definition f is the sum of the elementary RSF appearing in its SANF, and therefore $\mathsf{STT}(f)$ is the sum of the corresponding STT.

□

Based on Proposition 1 we can easily go from one representation of an RSF to another, using $\mathbf{A}$, $\mathbf{B}$ and their inverses. We use these representations to efficiently find dahus in the RSF class. Different strategies can be implemented to find dahus in the RSF class, exhausting the potential candidates based on the restrictions applying on one representation. The results of our computational search on RSF are given in Section 5.3.

4.3 Negative results on existing RSF constructions

RSF constructions with Walsh spectrum partially known

Various families of RSF with optimal algebraic immunity have been provided over the last two decades. Since the nonlinearity of these constructions has been studied, the value of the Walsh spectrum in 0 and in elements of Hamming weight 1 is often provided.

In these cases, we show that these functions cannot be dahus (or even overcome $\mathcal{C}_1$) since this Walsh spectrum value is not 0 for the chosen parameters, giving the maximum resiliency order of functions obtained from these constructions. We list such constructions in Table 5 and summarize their resiliency order in Proposition 2.

Reference	n	res()	Walsh transform
[Fu+11], Construction 1	$2t = 2^m \geq 16$	0	$\mathsf{W}_f(1)' = 2\binom{2t-1}{t} - 6$
[Fu+11], Construction 2	$2t = 2^m \geq 16$	0	$\mathsf{W}_f(1)' = 2\binom{2t-1}{t} - t^2 + 5t - 12$
[Zha+12], Construction 2	$2t > 14$	-1	$\mathsf{W}_f(0)' = \binom{2t}{t} - 4t(\lfloor t/2 \rfloor - 1)$
[CZT14]	$2t$	-1	$\mathsf{W}_f(0)' = -\left[\binom{2t}{t} - (2t)2^{t-2}\right]$
[ST14], Construction 4.1	$2t+1 \geq 11$	0	$\mathsf{W}_f(1)' = 2\left[\binom{2t}{t} - 2^t + 2\right]$
[ST14], Construction 5.1	$2t \geq 10$	-1	$\mathsf{W}_f(0)' = -\left[\binom{2t}{t} - (2t)2^{t-2}\right]$
[Che+19], Construction 1	$2t+1$	0	$\mathsf{W}_f(1)' = 2\binom{2t}{t} - 2^{t-3}(t-3)(t-2)$
[ZS19], Construction 3.1	$2t+1$	0	$\mathsf{W}_f(1)' = 2\left[\binom{2t}{t} - (t-5)2^{t-1} - 2t - 2\right]$
[ZS19], Construction 4.1	$2t$	-1	$\mathsf{W}_f(0)' = \left[\binom{2t}{t}/2 - (t-1)2^{t-3} + 4t - 10\right]$

Table 5: RSF Constructions with optimal algebraic immunity, with Walsh transform partially studied. $\mathsf{W}_f(\varepsilon)'$ denotes the Walsh transform in any element of Hamming weight $\varepsilon \in \{0, 1\}$.

Proposition 2. *The RSF constructions with optimal AI listed in Table 5 have resiliency order -1 or 0. Thus, they cannot provide dahus in more than 4 variables.*

Proof. We show that the Walsh transforms of Table 5 are all different from zero, which is sufficient to conclude on their resiliency order using Property 1. We start with the case of [ZS19] (Construction 3.1) which is representative of many others. We use a central binomial coefficient identity $\binom{2t}{t} \geq \frac{4^t}{2\sqrt{t}}$, which we simplify as $\binom{2t}{t} \geq \frac{4^t}{2t}$.

$$\mathsf{W}_f(1)' = g(t) = 2\left[\binom{2t}{t} - (t-5)2^{t-1} - 2t - 2\right] \geq 2\left[\frac{4^t}{2t} - (t-5)2^{t-1} - 2t - 2\right],$$
$$\geq 2^t \underbrace{\left(\frac{2^t}{t} - t + 5\right)}_{g_1(t)} - 4t - 4.$$

We analyze in particular $g_1(t) = \frac{2^t}{t} - t + 5$ part and compute its derivative function:

$$g_1'(t) = \frac{2^t(t\ln 2 - 1)}{t^2} - 1\ .$$

Since this derivative is positive for $t \geq 4$ and since $g_1(4) = 5$, the following implication can be established:

$$t \geq 4 \implies g_1(t) > 1 \implies g(t) > \underbrace{\left(2^t - 4t - 4\right)}_{g_2(t)}.$$

We now study $g_2(t)$, its derivative and second derivative functions:

$g_2''(t) = 2^t(\ln 2)^2$	$g_2'(t) = 2^t \ln 2 - 4$	$g_2(t) = 2^t - 4t - 4$
> 0	$g_2'(3) > 1.54$	$g_2(5) = 8$

Then, for any $t \geq 5$, $\mathsf{W}_f(1)'$ is non null (and is in particular positive). It remains to compute $\mathsf{W}_f(1)'$ for $t < 5$, which ends the proof for Construction 3.1 of [ZS19].

t	1	2	3	4
$g(t)$	4	12	40	136

The Walsh transform of [ZS19] (Construction 4.1) and [ST14] (Construction 4.1) are of the same type as [ZS19] (Construction 3.1):

$$a_0\left[\binom{2t}{t} + (a_1 t - a_2)2^{t-a_3} + a_5 t + a_6\right]$$

where $a_0 > 0$. Only the coefficients a_0 to a_6 differs between them. Then, following the same steps, we can prove that $\mathsf{W}_f(0)' > 0$ (respectively $\mathsf{W}_f(1)' > 0$) in all those constructions. Similarly, this proof can be adapted to show that $\mathsf{W}_f(0)' < 0$ in [ST14] (Construction 5.1) and [CZT14], with $a_0 < 0$.

In the construction of [Che+19] (Construction 1), a term $a_7 t^2$ must be added to the previous form, but it does not change the proof's strategy since the value of the Walsh transform is still dominated by the binomial term.

We now analyze the case of [Zha+12] (Construction 2), using another binomial coefficient identity: $\binom{n}{k} \geq \frac{n^k}{k^k}$ (indeed, $\binom{n}{k}$ can be seen as a product of k terms greater than or equal to $\frac{n}{k}$).

$$\mathsf{W}_f(0)' = h(t) = \binom{2t}{t} - 4t(\lfloor t/2 \rfloor - 1) \geq \frac{2^t t^t}{t^t} - 4t(t/2 - 1),$$
$$\geq \underbrace{2^t - 2t^2 + 4t}_{h_1(t)}.$$

The derivatives of $h_1(t)$ can be studied:

$$h_1''(t) = 2^t(\ln 2)^2 - 4 \qquad h_1'(t) = 2^t \ln 2 - 4t + 4$$
$$h_1''(4) > 3.68 \qquad h_1'(5) > 6.18$$

The second derivative of this function is positive for all $t > 4$ and the derivative function therefore increases and is positive for $t > 5$. We have $\mathsf{W}_f(0)' = 232$ for $t = 5$ and is increasing for greater values of t. Since the construction from [Zha+12] only considers the case $t > 7$, it ends the proof for this construction.

The same steps allow to prove that $\mathsf{W}_f(1)' \neq 0$ for Constructions 1 and 2 of [Fu+11]. □

More general results for arbitrary Walsh transforms

We recall two constructions of RSF with optimal AI in an odd number of variables. Then, using their Hamming distance to the majority function, we show that these functions belong to a larger family of AI-optimal functions with resiliency order 0. The key element (as used in Lemma 12) used here to show that a known construction has a low resiliency is its proximity (in Hamming distance) to functions with high absolute value of the Walsh transform in the coefficients of low Hamming weight. The same strategy can be applied to non RSF functions, and relatively to other functions than the majority functions.

Definition 18 (Construction 1 [SM07]). *Let $n \geq 5$ odd, take Λ_p such that $\mathsf{w_H}(\Lambda_q) = (n-1)/2$ and Λ_q such that $\mathsf{w_H}(\Lambda_p) = (n+1)/2$ such that $|O(\Lambda_q)| = |O(\Lambda_p)| = n$ and or each $x \in O_{\Lambda_p}$ there is a unique $y \in O_{\Lambda_q}$ such that $x \preceq y$. Construct:*

$$R_n(x) = \begin{cases} \mathsf{MAJ}_n(x) & \text{if } x \in O_{\Lambda_p} \cup O_{\Lambda_q}, \\ \mathsf{MAJ}_n(x) + 1 & \text{otherwise.} \end{cases}$$

Definition 19 (Construction 1 [Fu+09]). *Let $n \geq 5$ odd, take Λ_p such that $\mathsf{w_H}(\Lambda_p) = (n-1)/2$ and Λ_q such that $|O_{\Lambda_q}| = |O_{\Lambda_p}| = n$ and for all $a \in \mathbb{F}_2^n \setminus \{0\}$ the equation $\sum_{i=1}^n a_i \sum_{y \in O_{\Lambda_q}} \prod_{j=1}^n (x_j)^{y_j} = 1$ has at least one solution in O_{Λ_q}. Construct:*

$$T_n(x) = \begin{cases} \mathsf{MAJ}_n(x) + 1 & \text{if } x \in O_{\Lambda_p} \cup O_{\Lambda_q}, \\ \mathsf{MAJ}_n(x) & \text{otherwise.} \end{cases}$$

The following lemma shows that functions with high resiliency order cannot be too close (in Hamming distance of their truth tables) to functions with high absolute value in their Walsh spectrum.

Lemma 12 (Distance to Resilient Functions). *Let $f, g \in \mathcal{B}_n$ and $t \in \mathbb{N}$ such that $t < n$. If $\mathsf{res}(f) \geq t$ then:*

$$\mathsf{d_H}(f,g) \geq \max_{a \in \mathbb{F}_2^n, \mathsf{w_H}(a) \leq t} \frac{|\mathsf{W}_g(a)|}{2}, \quad \text{and } \mathsf{d_H}(f, g+1) \max_{a \in \mathbb{F}_2^n, \mathsf{w_H}(a) \leq t} \geq \frac{|\mathsf{W}_g(a)|}{2}.$$

Proof. First, we denote:

$$m = \min_{\substack{a \in \mathbb{F}_2^n \\ \mathsf{w_H}(a) \leq t}} \frac{\mathsf{W}_g(a)}{2}, \quad \text{and } M = \max_{\substack{a \in \mathbb{F}_2^n \\ \mathsf{w_H}(a) \leq t}} \frac{\mathsf{W}_g(a)}{2},$$

and we show that $\mathsf{res}(f) \geq t$ implies $\mathsf{d_H}(f,g) \geq M$ and $\mathsf{d_H}(f, g+1) \geq -m$.

Using Property 10 the Walsh transform in a is related to the distance with the linear function $l_a = \sum_{i \in \mathsf{supp}(a)} x_i$ in the following way:

$$\mathsf{d_H}(g, l_a) = \mathsf{w_H}(g + l_a) = 2^{n-1} - \frac{\mathsf{W}_g(a)}{2}.$$

We use the triangle inequality of the Hamming distance with f, g and l_a:

$$\mathsf{d_H}(f,g) + \mathsf{d_H}(g,l_a) \geq \mathsf{d_H}(f,l_a) \tag{2}$$

Using Property 1, if $\mathsf{res}(f) \geq \mathsf{w_H}(a)$ then $\mathsf{d_H}(f,l_a) = 2^{n-1}$, therefore the Equation 2 can be rewritten as $\mathsf{d_H}(f,g) \geq 2^{n-1} - \mathsf{d_H}(g,l_a)$. Using the expression of $\mathsf{d_H}(g,l_a)$ in term of Walsh transform it gives $\mathsf{d_H}(f,g) \geq \mathsf{W}_g(a)/2$. Since $\mathsf{W}_{h+1} = -\mathsf{W}_h$ for all function h, we get $\mathsf{d_H}(f,g+1) \geq -\mathsf{W}_g(a)/2$. Taking the minimum and maximum over all functions l_a such that $0 \leq \mathsf{w_H}(a) \leq t$ we get $\mathsf{d_H}(f,g) \geq M$ and $\mathsf{d_H}(f,g+1) \geq -m$.

Then, since $\mathsf{res}(f+1) = \mathsf{res}(f)$, $\mathsf{res}(f+1) \geq t$ implies $\mathsf{d_H}(f+1,g) \geq M$ which means $\mathsf{d_H}(f,g+1) \geq M$ and $\mathsf{d_H}(f+1,g+1) \geq -m$ which means $\mathsf{d_H}(f,g) \geq -m$. The four equations allow to conclude $\mathsf{d_H}(f,g) \geq \max(M,-m) = \max_{\substack{a\in\mathbb{F}_2^n \\ \mathsf{w_H}(a)\leq t}} |\mathsf{W}_g(a)|/2$ and $\mathsf{d_H}(f,g+1) \geq \max_{\substack{a\in\mathbb{F}_2^n \\ \mathsf{w_H}(a)\leq t}} |\mathsf{W}_g(a)|/2$

□

Proposition 3. *Let $t \in \mathbb{N}^*$, $\varepsilon \in \{0,1\}$, $W \subset \mathbb{F}_2^{2t+1}$ such that $|W| < \binom{2t}{t}$, and $f \in \mathcal{B}_{2t+1}$ defined as:*

$$f(x) = \begin{cases} \mathsf{MAJ}_{2t+1}(x) + \varepsilon + 1 & \text{if } x \in W, \\ \mathsf{MAJ}_{2t+1}(x) + \varepsilon & \text{otherwise.} \end{cases}$$

If $|W \cap \bigcup_{k=0}^{t} \mathsf{E}_{k,2t+1}| \neq |W|/2$ then $\mathsf{res}(f) = -1$, otherwise $\mathsf{res}(f) = 0$.

Proof. We denote $W \cap \bigcup_{k=0}^{t} \mathsf{E}_{k,2t+1}$ as $W_{\leq}$. First, if $|W_{\leq}| \neq |W|/2$ it implies that f is unbalanced, we show it by studying the size of the support of $f+\varepsilon$:

$$|\mathsf{supp}_{f+\varepsilon}| = |W_{\leq}| + 2^{2t} - |W \setminus W_{\leq}| = 2^{2t} - |W| + 2|W_{\leq}| \neq 2^{2t},$$

hence $|\mathsf{supp}_f \neq 2^{2t}|$. In this case f is unbalanced therefore $\mathsf{res}(f) = -1$, and in the other case (*i.e.* $|W_{\leq}| = |W|/2$) f is balanced hence $\mathsf{res}(f) \geq 0$.

Then, we show that f is too close to the majority function or its complement to be 1-resilient, using Lemma 12. We determine the value of the Walsh transform of the majority function for elements of Hamming weight 0 and 1: from Property 6, $\mathsf{W}_{\mathsf{MAJ}_{2t+1}}(0) = 0$ and for all $a \in \mathsf{E}_{1,2t+1}$ we have $\mathsf{W}_{\mathsf{MAJ}_{2t+1}}(a) = 2\binom{2t}{t}$, therefore:

$$\max_{\substack{a\in\mathbb{F}_2^n \\ \mathsf{w_H}(a)\leq 1}} \frac{|\mathsf{W}_{\mathsf{MAJ}_{2t+1}+\varepsilon}(a)|}{2} = \binom{2t}{t}.$$

Since $\mathsf{d_H}(f, \mathsf{MAJ}_{2t+1} + \varepsilon) = |W| < \binom{2t}{t}$ the contrapositive of Lemma 12 (with $g = \mathsf{MAJ}_{2t+1} + \varepsilon$ and $t = 1$) gives $\mathsf{res}(f) < 1$, hence $\mathsf{res}(f) = 0$, concluding the proof.

□

Corollary 3. *All functions from the constructions of Definitions 18 and 19 have resiliency order 0.*

Proof. The two constructions can been written as f in Proposition 3, where $W = \Delta_p \cup \Delta_q$. In both cases $|W \cap \bigcup_{k=0}^{t} \mathsf{E}_{k,2t+1}| = |O_{\Lambda_p}| = n = |W|/2$ and $|W| = 2(2t+1)$. Since for $t \geq 3$ we have $2(2t+1) < \binom{2t}{t}$ Proposition 3 directly proves the result for all $n \geq 7$.

For $n = 5$ a more precise result is needed. First, we write the Walsh transform of f (as R_n or T_n) in terms of the Walsh transform of $\mathsf{MAJ}_n + \varepsilon$, for $a \in \mathbb{F}_2^n$:

$$\begin{aligned}\mathsf{W}_f(a) &= \sum_{x \in \mathbb{F}_2^n} (-1)^{f(x)+a\cdot x}, \\ &= \sum_{x \in \mathbb{F}_2^n \setminus \{O_{\Lambda_p} \cup O_{\Lambda_q}\}} (-1)^{\mathsf{MAJ}_n(x)+\varepsilon+a\cdot x} + \sum_{x \in \{O_{\Lambda_p} \cup O_{\Lambda_q}\}} (-1)^{\mathsf{MAJ}_n+\varepsilon+a\cdot x+1}, \\ &= \mathsf{W}_{\mathsf{MAJ}_n+\varepsilon}(a) - 2 \sum_{x \in \{O_{\Lambda_p} \cup O_{\Lambda_q}\}} (-1)^{\mathsf{MAJ}_n(x)+\varepsilon+a\cdot x}.\end{aligned}$$

Then, we focus on the contribution of an orbit to the Walsh transform when $\mathsf{w_H}(a) = 1$:

$$\begin{aligned}\sum_{x \in O_{\Lambda_i}} (-1)^{\mathsf{MAJ}_n(x)+\varepsilon+a\cdot x} &= \sum_{\substack{x \in O_{\Lambda_i} \\ a\cdot x = 0}} (-1)^{\mathsf{MAJ}_n(x)+\varepsilon} - \sum_{\substack{x \in O_{\Lambda_i} \\ a\cdot x = 1}} (-1)^{\mathsf{MAJ}_n(x)+\varepsilon}, \\ &= (n - 2\mathsf{w_H}(\Lambda_i))(-1)^{\mathsf{MAJ}_n(\Lambda_i)+\varepsilon}.\end{aligned}$$

When $n = 5$ for a of Hamming weight 1 from Property 6 we get $\mathsf{W}_{\mathsf{MAJ}_5+\varepsilon}(a) = \pm 2\binom{4}{2} = \pm 12$. The contribution from the orbit given by Λ_p is ± 1 and the one from Λ_q has absolute value upper bounded by 3 (since $\mathsf{w_H}(\Lambda_q) \in [4]$). Hence, all potential cases lead to $\mathsf{W}_f(a) \neq 0$ for all $a \in \mathsf{E}_{1,5}$.

$\square$

In this part we showed that various families of RSF with proven optimal AI (a prerequisite to contain dahus) do not contain dahus for $n \geq 5$, and cannot be used to validate $\mathcal{C}_1$. Nevertheless, the RSF family may not be eliminated from the search of dahus right away, for example we exhibit dahus in small localities which are RSF in Section 5, hence new constructions may lead to dahus.

5 Classification of functions for small values of n and dahus up to $n = 11$

In this section, we aim at classifying all functions of locality up to 5 and RSF up to 7 according to their resiliency order and algebraic immunity. We also use Proposition 5 to find functions of Dahu_7 and Proposition 1 of Section 4.2 in order to build RSF in Dahu_9 and Dahu_{11}. Dahus of odd locality are mainly considered since Corollary 1 allows to build even-variable dahus from them.

All algorithms of this section were implemented in Python and are available at

`https://github.com/88abaa99/DahuHunting`.

5.1 Classification of functions for $n \leq 5$

Algorithm 1 allows to count and build all functions that verifies a given number of variables, resiliency order and algebraic immunity. The progressive verification of the resiliency is made using a naive counter approach for all $\binom{n}{k}$ subsets of variables. While it is generally rather impractical, it appears to be very efficient in our recursive algorithm. The algebraic immunity is verified in a Reed-Muller manner, as in [Did07] (Chapter 10), which also benefits from our recursive approach to become very efficient.

Tables 6, 7 and 8 give the exhaustive numbers of functions with respective locality 3, 4 and 5 that strictly match a given resiliency order and AI. The two constant functions are omitted.

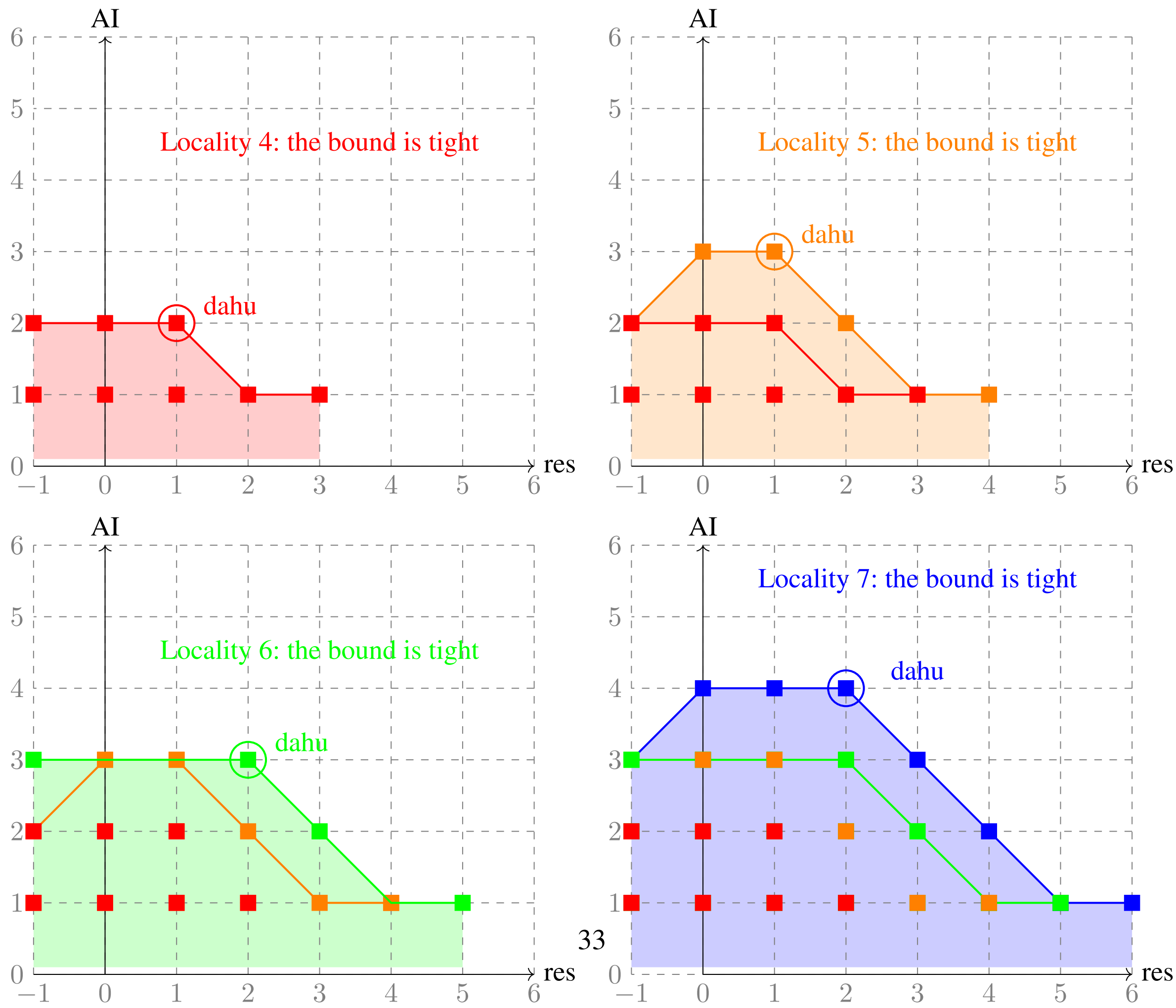
Our algorithm also allowed to exhaust 14923776 Boolean functions with locality 6, algebraic immunity 3 and resiliency order 2 (*i.e.* all functions of Dahu_6).

Input : Number of variables n, resiliency k and algebraic immunity e.
Output: List S of all functions for the specified locality, resiliency and AI.
Procedure `initialization`
  initialize the list of results $S \leftarrow \emptyset$.
  initialize an empty truth table $TT = \emptyset$.

Procedure `build(`TT`)`
  if `check(`TT`)` is false **then return**;
  if TT is 2^n-long **then**
    $S \leftarrow S \cup \{TT\}$;
    return;
  end
  `build(`$TT||0$`);`
  `build(`$TT||1$`);`

Procedure `check(`TT`)`
  if the partial truth table TT does not violate a resiliency k **then**
    if the partial truth table TT does not violate an AI e **then**
      return true;
    end
  end
  return false;
`initialization;`
`build(`TT`);`

Algorithm 1: Enumeration of all functions of a given number of variables, resiliency and algebraic immunity



AI / res	1	2
-1	184	0
0	6	56
1	6	0
2	2	0

Table 6: Functions with locality 3.

AI / res	1	2
-1	10552	42112
0	8	12640
1	12	200
2	8	0
3	2	0

Table 7: Functions with locality 4.

AI / res	1	2	3
-1	7666488	3686220416	0
0	10	402604048	197668352
1	20	710640	96768
2	20	520	0
3	10	0	0
4	2	0	0

Table 8: Functions with locality 5 separated by resiliency order and algebraic immunity.

As already observed, there exist 56 functions in Dahu_3. As shown in Table 9, they can be partitioned in 7 types regrouping the functions permutation invariant up to the addition of the constant 1.

There exists an affine transformation between the representative of any two of these types. Indeed, the representative of B can be obtained by turning x_1 into x_1+1 in the representative of A. Similarly, turning x_1 into x_+x_2 transforms B into C. The transformation $x_2 \to x_2+1$ allows to build the representative of D from the one of C. E is obtained from D by applying $x_2 \to x_2+x_3+1$. Applying $x_3 \to x_2+x_3$ turns E into F. Finally, applying $x_3 \to x_1+x_3$ to F allows to build G. Then all 56 functions of Dahu_3 are affine equivalent.

Type	ANF	Walsh transform	Number
A	$x_1x_2+x_1x_3+x_2x_3$	$[0,-4,-4,0,-4,0,0,4]$	2
B	$x_1x_2+x_1x_3+x_2x_3+x_1+x_2$	$[0,4,-4,0,-4,0,0,-4]$	6
C	$x_1x_2+x_1x_3+x_3$	$[0,0,-4,4,-4,-4,0,0]$	12
D	$x_1x_2+x_1x_3+x_1+x_3$	$[0,0,4,-4,-4,-4,0,0]$	12
E	$x_1x_2+x_3$	$[0,0,0,0,-4,-4,-4,4]$	6
F	$x_1x_2+x_2+x_3$	$[0,0,0,0,-4,4,-4,-4]$	12
G	$x_1x_2+x_1+x_2+x_3$	$[0,0,0,0,4,-4,-4,-4]$	6

Table 9: Functions of Dahu_3. "ANF" and "Walsh transform" are the algebraic normal form and the Walsh transform of one of the representative of this type, "number" represents the number of elements of Dahu_3 of this type.

5.2 Application of Proposition 5 for $n=7$

In this section, we look for functions satisfying the sufficient conditions of Proposition 5 and use the proposition to build dahus in more variables.

Algorithm 2 shows a probabilistic approach to implement the construction of Proposition 5. Taking a subset of Dahu_{2t+1} as input, it outputs hopefully some elements of Dahu_{2t+3}. It iteratively creates a new pair of dahus of Dahu_{2t+1} and checks whether it can be combined with an old pair such that it satisfies the conditions of Proposition 5, and stops when all combinations have been exhausted or, more likely, when it runs out of memory.

The annihilator basis is computed using Algorithm 2 of Didier et al. [DT06]. Alternatively, Proposition 4 of Armknecht et al. [Arm+06] for computing the basis have better asymptotic complexity

Procedure `initialization`

- Initialize the list of $(2t+1)$-variable dahus D_{2t+1} and pre-compute their ANF (of degree $t+1$), Walsh spectrum (of weight t), a basis of their annihilators (only the degree $t+1$ and t part, with a fixed degree $t+1$ part).
- Initialize a list of pairs of dahus $C \leftarrow \emptyset$.
- Initialize the list of results $D_{2t+3} \leftarrow \emptyset$.

Procedure `find_4_dahus`(d_1, d_2)

- Search all d_3, d_4 in C such that $(d_1 + d_2)$ and $(d_3 + d_4)$ share the same ANF of degree $t+1$ (condition 1 of Proposition 5).
- Keep only those verifying $(\mathsf{W}_{d_1}(a) + \mathsf{W}_{d_2}(a)) = (\mathsf{W}_{d_3}(a) + \mathsf{W}_{d_4}(a))$ for all a of Hamming weight t (condition 2 of Proposition 5).
- Keep only those, such that the sum of the annihilator basis is full rank (condition 3 of Proposition 5).
- Add the remaining results (d_1, d_2, d_3, d_4) to D_{2t+3}.

`initialization`
do
  Pick up randomly d_1 and d_2 in D_{2t+1}.
  Pre-compute the ANF of $(d_1 + d_2)$ (only the degree $t+1$ part).
  Pre-compute $(\mathsf{W}_{d_1}(a) + \mathsf{W}_{d_2}(a)) = (\mathsf{W}_{d_3}(a) + \mathsf{W}_{d_4}(a))$ for all a of weight t.
  `find_4_dahus`(d_1, d_2)
  Add (d_1, d_2) to C and store the pre-computed ANF and Walsh Spectrum.
until you run out of memory;

Algorithm 2: Combining four $(2t+1)$-variable dahus into a $(2t+3)$-variable dahu.

but is trickier to implement. For the considered parameters, it does not appear to be a bottleneck in practice. Note that, in order to speed up the computation, the list C of pairs of dahus is indexed by the sum of their $(t+1)$-degree monomials, and also indexed by the sum of their Walsh spectrum (only the weight t part).

Using the full set Dahu_5, this technique allowed us to find more than 900000 dahus of Dahu_7. However, so far it did not give any result for higher locality: our 64GB RAM is saturated before a positive result is found, although we tried billions of combinations. It seems that the proportion of dahus in RSF_9 (that can be built from Proposition 5) is too low to be exploited with our probabilistic algorithm.

The following hexadecimal represents the truth table of one of them[9], where the leftmost bit is mapped to $f(0, \cdots, 0)$, the second leftmost bit is mapped to $f(0, \cdots, 0, 1)$ and so on.

`0x0776b6c87c4a8973c5a97287a3789c1d`

5.3 Classification of Rotation Symmetric Functions

In our experimental results, to find all RSF in n variables with a resiliency order k and an algebraic immunity of e, we run the following procedure:

1. we exhaust over all the simplified ANF as defined in Definition 17;
2. combining Property 1 and Proposition 1, we can compute the simplified Walsh Spectrum of an RSF and check whether it is k-resilient;
3. if so, we can verify its algebraic immunity. In our experiments, this last part is done using the Algorithm 2 of Didier et al. [DT06].

[9] One can verify the resiliency order and algebraic immunity with the SageMath and the BooleanFunction package (https://doc.sagemath.org/html/en/reference/cryptography/sage/crypto/boolean_function.html).

res \ AI	1	2
-1	10	0
0	0	2
2	2	0

Table 10: RSF with locality 3.

res \ AI	1	2	3
-1	58	156	0
0	0	8	22
1	0	0	8
4	2	0	0

Table 11: RSF with locality 5.

res \ AI	1	2	3	4
-1	4122	86488	860724	0
0	0	300	66242	17304
1	0	116	9600	3396
2	0	8	140	132
6	2	0	0	0

Table 12: RSF with locality 7 separated by resiliency order and algebraic immunity.

Alternatively, the algebraic immunity can be computed efficiently using Algorithm 1 of Armknecht et al. [Arm+06]. Instead, we reuse the code of Section 5.2 and check that Algorithm 2 of Didier et al.[DT06] gives an empty basis of degree-$(e-1)$ annihilators. It was not a limiting factor in practice.

Tables 10, 11 and 12 give the number of RSF with locality 3, 5 and 7 that strictly match a given resiliency order and algebraic immunity. The constant functions are omitted. For the particular case of RSF in Dahu_{2t+1} (up to $t = 3$), we can speed up the exhaustive search by considering only simplified ANF having $a_{\mathsf{supp}(\Lambda)} = 0$ for all representatives Λ of Hamming weight greater than $t+1$ (since their degree is $t+1$ by Lemma 13 item 1). In [DGM04] the authors realize experiments on some RSF in 7, 8 and 9 variables to determine their algebraic immunity. Since their experiments are on RSF with a fixed resiliency, degree and nonlinearity, the overlap with our experiment is only for $n = 7$, over the 36 RSF they study, 12 have $\mathsf{AI} = 3$ and the 24 others are the dahus mentioned in the sporadic cases of Section **??**.

5.4 Higher-locality dahus in Rotation Symmetric Functions

The complexity of the algorithm described in Section 5.3 becomes prohibitive when it comes to locality above 7 and we are no longer able to classify all RSF. However, for the very particular case of dahus, considering the speed-up over the simplified ANF exhaustive search, we can find a few RSF in Dahu_9 and Dahu_{11}.

Using intensive computation and a hint of luck we managed to produce 1104 distinct RSF in Dahu_9. The following hexadecimal represents the full truth table of one of them.

```
69c3e14be916349ef8c3163c1e25c3e9aa95a55a167c4fb007b85d66e15eb883
99999666c9666399073c6eb434fa9e41556a9a9536a66c69f84762a9cb81915f
```

This dahu, like all others we found, has two representatives of Hamming weight 5 (the maximal degree for a dahu of locality 9) set in its simplified ANF. Surprisingly, our computations have shown that no RSF with a single representative of weight 5 is in Dahu_9. This observation is no longer true for locality 11. In order to find RSF in Dahu_{11}, we have to restrict the exhaustive search over the simplified ANF by:

- picking a single representative Λ_{max} of maximal Hamming weight (*i.e.* 6) and setting $a_{\mathsf{supp}(\Lambda_{max})} = 1$,
- setting $a_{\mathsf{supp}(\Lambda)} = 0$ for all $\Lambda \npreceq \Lambda_{max}$ (*i.e.* Λ_{max} does not cover Λ),
- make an exhaustive search over the remaining representatives.

Our first guess of Λ_{max} allowed us to produce four RSF in Dahu_{11}. The following hexadecimal represents the truth table of one of them. Using Lemma 5, it can be extended to an element of Dahu_{12}.

```
6da3985e92d467a9925ca7616d2b9896925c67a19d2b68566da3589e92d49769
965863a5692f9c5296a75c9a69d0636d69a79c5a66d093ad9658a365962f6c92
c33c36c13c4bc93669965cab96e1635c96699c6b66e1939c6996a354691e6ca3
3cc3c93ec3b436c96969a354961e9ca396696394991e6c6396695cab69e1935c
b14e4eb14e39b1464eb1718eb1c64e796c93936c63e49c9b936cac536c1b63a4
9669699696e1699e6969a956961e96a169969669991e6661699656a969e1995e
5aa5a55aa5d25aada55a9a655a2da59269966996991e6661966956a996e1995e
c33c3cc33c4bc334969656a969e1695e9669699666e1999e6996a956961e66a1
```

In this section, we have exhibited n-variables dahus verifying Conjecture 1 up to $n = 12$. Despite the low number of dahus in $\mathcal{B}_n$ (to compare with 2^{2^n}), we found some for all values of n reachable by computation, even in the restricted family of RSF. This is evidence in favor of Conjecture 1.

5.5 Optimal functions for small stretches

The dahus exhibited for n up to 12 allow to decrease the locality for small stretches, without any conjecture. It settles the case for the locality of functions secure against known linear-algebraic attacks for a stretch up to 6, giving better results than XOR-MAJ functions since $\mathsf{s} \geq 2$. We state it in the following proposition, and illustrate it in Figure 5.

Proposition 4. *Let* $\mathsf{s} \in]1, 6[$ *and* $n = \lceil 2\mathsf{s} \rceil + \lfloor \mathsf{s} \rfloor + 1$*, there exists* $f \in \mathcal{B}_n$ *secure against known linear-algebraic attacks, and for* $\mathsf{s} \geq 2$ f *cannot be a XOR-MAJ.*

Proof. By Theorem 1 a function f is secure against known linear-algebraic attacks for a polynomial stretch s if $\mathsf{AI}(f) > \mathsf{s}$ and $\mathsf{res}(f) \geq 2\mathsf{s} - 1$. Hence for i an integer, a stretch $\mathsf{s} \in [i, i+1[$ requires an AI of $i + 1$ and a resiliency order of $2i - 1$ for $\mathsf{s} = i$, $2i$ for $\mathsf{s} \in]i, i + 0.5]$ and $2i + 1$ for $\mathsf{s} \in]i + 0.5, i + 1[$. For an integer stretch $\mathsf{s} = i$ we consider the direct sum g of $f \in \mathsf{Dahu}_{2i+1}$ and XOR_i, by definition 14 and Lemma 5 it gives $\mathsf{AI}(g) = i + 1$ and $\mathsf{res}(g) = 2i - 1$, hence g satisfied the required properties. Similarly, for a stretch in $]i, i + 0.5]$ (respectively $]i + 0.5, i + 1[$) the direct sum of $f \in \mathsf{Dahu}_{2i+1}$ and XOR_{i+1} (respectively XOR_{i+2}) satisfies the required properties. Since $\mathsf{Dahu}_{2i+1} \neq \emptyset$ for $i \in [1, 5]$ it provides secure against known linear-algebraic attacks for $\mathsf{s} \in]1, 6[$

From Lemma 9 an AI of $i + 1$ requires the majority to be on $2i + \varepsilon$ variables (for $\varepsilon \in \{0, 1\}$) and a XOR part on $2i - \varepsilon$ to provide a resiliency of $2i - 1$. It gives $4i$ variables (respectively $4i + 1$ for $\mathsf{s} \in]i, i + 0.5]$ and $4i + 2$ for $\mathsf{s} \in]i + 0.5, i + 1[$), and for $\mathsf{s} \geq 2$ we get $4i > 3i + 1$ (respectively $4i + 1 > 3i + 2$ and $4i + 2 > 3i + 3$) then the XOR-MAJ functions secure against known linear-algebraic attacks for a stretch $\mathsf{s} \geq 2$ have more than $\lceil 2\mathsf{s} \rceil + \lfloor \mathsf{s} \rfloor + 1$ variables.

$\square$

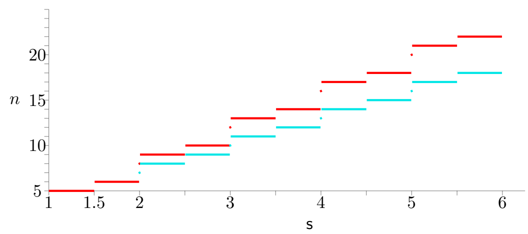


Fig. 5: Smallest locality of secure functions against known linear-algebraic attacks for small stretches. In red the limit from XOR-MAJ functions, in blue the limit reached by the dahus found in this section.

Open Questions

As a first study of Boolean functions reaching an optimal, namely the trade-off between algebraic immunity and resiliency order, this work raises many open questions on different difficulty levels.

Existence of dahus. The main open question is the validation or invalidation of Conjecture 1. One possible idea could be to estimate $|\mathsf{Dahu}_n|$ in order to apply Proposition 5 or Corollary 4. Such an estimation could also partially answer other open questions stated in [Car21] such as improving the bounds on the number of AI-optimal functions and on $(n-1-\lfloor (n+1)/2 \rfloor)$- resilient functions.

Another possible track for looking for dahus could be their study relatively to extra criteria like the nonlinearity and the fast algebraic immunity, which have been extensively studied in the past two decades. We do not see any natural way of combining them. First, an optimal fast algebraic immunity implies a high degree which is contradictory with a high resiliency. Then for the nonlinearity, the optimal ones, known as bent functions, are unbalanced.

Affine-equivalent resiliency. Furthermore, one can also focus on validating conjecture $\mathcal{C}_\ell$ in a constructive way for a particular ℓ starting by $\ell = 1$. A new criterion may be the following. Let us call the "extended resiliency order" of a function f, as the highest resiliency order for all the affine-equivalent functions to f. Showing that there exists an AI-optimal odd-variable function with extended resiliency order 1 would be enough to prove $\mathcal{C}_1$.

Building AI-optimal ℓ-resilient families. Hence, we may advice to study the possible construction of functions from another perspective. Proposition 3 shows that functions close to the majority function cannot have high resiliency. The same idea can be extended to other functions with known Walsh spectrum, for example a larger class of symmetric functions. Thus, combining the properties of the swaps on the support maintaining the optimal algebraic immunity (*e.g.* [LQ06]) and the minimum distance allowing high resiliency, could be used to reduce the search space and iteratively build new functions with the desired parameters.

An n without dahus. On another level, an interesting different research path could be to analyze the consequences of the existence of an integer $n \geq 13$ such that $|\mathsf{Dahu}_n| = \emptyset$. Does it provide a tight bound in the line one of Theorem 3? Proving the implication return of item 2 of Property 8 could maybe help invalidating Conjecture $\mathcal{C}_\ell$ for a certain $\ell > 0$ and thus obtaining a tight bound in the line two of Theorem 3.

References

[ABR12] Benny Applebaum, Andrej Bogdanov, and Alon Rosen. "A Dichotomy for Local Small-Bias Generators". In: *Theory of Cryptography*. Ed. by Ronald Cramer. Berlin, Heidelberg: Springer Berlin Heidelberg, 2012, pp. 600–617.

[ABR16] Benny Applebaum, Andrej Bogdanov, and Alon Rosen. "A Dichotomy for Local Small-Bias Generators". In: *J. Cryptol.* 29.3 (2016), 577–596. ISSN: 0933-2790.

[AHI05] Michael Alekhnovich, Edward A Hirsch, and Dmitry Itsykson. "Exponential lower bounds for the running time of DPLL algorithms on satisfiable formulas". In: *Journal of Automated Reasoning* 35.1-3 (2005), pp. 51–72.

[AIK08] Benny Applebaum, Yuval Ishai, and Eyal Kushilevitz. "On pseudorandom generators with linear stretch in NC 0". In: *Computational Complexity* 17.1 (2008), pp. 38–69.

[Aka+14] Adi Akavia, Andrej Bogdanov, Siyao Guo, Akshay Kamath, and Alon Rosen. "Candidate Weak Pseudorandom Functions in AC0 MOD2". In: *ITCS*. ITCS '14. 2014.

[AL16] Benny Applebaum and Shachar Lovett. “Algebraic attacks against random local functions and their countermeasures”. In: *48th ACM STOC*. Ed. by Daniel Wichs and Yishay Mansour. ACM Press, June 2016.

[AL18] Benny Applebaum and Shachar Lovett. “Algebraic Attacks against Random Local Functions and Their Countermeasures”. In: *SIAM J. Comput.* (2018), pp. 52–79.

[Alb+15] Martin R. Albrecht, Christian Rechberger, Thomas Schneider, Tyge Tiessen, and Michael Zohner. “Ciphers for MPC and FHE”. In: *EUROCRYPT 2015, Part I*. LNCS. 2015, pp. 430–454.

[Ana+19] Prabhanjan Ananth, Aayush Jain, Huijia Lin, Christian Matt, and Amit Sahai. “Indistinguishability Obfuscation Without Multilinear Maps: New Paradigms via Low Degree Weak Pseudorandomness and Security Amplification”. In: *CRYPTO*. 2019, pp. 284–332.

[App12] Benny Applebaum. “Pseudorandom generators with long stretch and low locality from random local one-way functions”. In: *44th ACM STOC*. Ed. by Howard J. Karloff and Toniann Pitassi. ACM Press, May 2012, pp. 805–816.

[App13] Benny Applebaum. “Cryptographic Hardness of Random Local Functions-Survey”. In: *TCC 2013*. Ed. by Amit Sahai. Vol. 7785. LNCS. Springer, Heidelberg, Mar. 2013, p. 599.

[App15] Benny Applebaum. “The Cryptographic Hardness of Random Local Functions - Survey”. In: *IACR Cryptology ePrint Archive* 2015 (2015), p. 165.

[Arm+06] Frederik Armknecht, Claude Carlet, Philippe Gaborit, Simon Künzli, Willi Meier, and Olivier Ruatta. “Efficient Computation of Algebraic Immunity for Algebraic and Fast Algebraic Attacks”. In: *EUROCRYPT 2006*. Ed. by Serge Vaudenay. Vol. 4004. LNCS. Springer, Heidelberg, 2006.

[AY09] Bogdanov Andrej and Qiao Youming. “On the security of Goldreich’s one-way function”. In: *RANDOM*. 2009, pp. 392–405.

[BGS94] Jürgen Bierbrauer, K. Gopalakrishnan, and Douglas R. Stinson. “Bounds for Resilient Functions and Orthogonal Arrays”. In: *CRYPTO’94*. Ed. by Yvo Desmedt. LNCS. Springer, Heidelberg, Aug. 1994, pp. 247–256.

[Bon+18] D. Boneh, Y. Ishai, A. Passelègue, A. Sahai, and D. J. Wu. “Exploring Crypto Dark Matter: - New Simple PRF Candidates and Their Applications”. In: *TCC*. 2018, pp. 699–729.

[Boy+17] Elette Boyle, Geoffroy Couteau, Niv Gilboa, Yuval Ishai, and Michele Orrù. “Homomorphic Secret Sharing: Optimizations and Applications”. In: *ACM SIGSAC*. New York, NY, USA, 2017, 2105–2122.

[Boy+20] Elette Boyle, Geoffroy Couteau, Niv Gilboa, Yuval Ishai, Lisa Kohl, and Peter Scholl. “Correlated Pseudorandom Functions from Variable-Density LPN”. In: *FOCS*. 2020, pp. 1069–1080.

[BP05] An Braeken and Bart Preneel. “On the Algebraic Immunity of Symmetric Boolean Functions”. In: *INDOCRYPT*. 2005, pp. 35–48.

[Can+] Anne Canteaut, Sergiu Carpov, Caroline Fontaine, Tancrède Lepoint, María Naya-Plasencia, Pascal Paillier, and Renaud Sirdey. “Stream Ciphers: A Practical Solution for Efficient Homomorphic-Ciphertext Compression”. In: *FSE 2016*. Ed. by Thomas Peyrin. Vol. 9783. LNCS.

[Car+06] C. Carlet, D. K. Dalai, K. C. Gupta, and S. Maitra. “Algebraic Immunity for Cryptographically Significant Boolean Functions: Analysis and Construction”. In: *IEEE* 52.7 (2006), 3105–3121.

[Car07] C. Carlet. “A method of construction of balanced functions with optimum algebraic immunity”. In: *International Workshop on Coding and Cryptography* (2007).

[Car+09] Claude Carlet, Xiangyong Zeng, Chunlei Li, and Lei Hu. “Further properties of several classes of Boolean functions with optimum algebraic immunity”. In: *DCC* 52 (Sept. 2009), pp. 303–338.

[Car21] Claude Carlet. *Boolean Functions for Cryptography and Coding Theory*. Cambridge University Press, 2021.

[CF08] Claude Carlet and Keqin Feng. “An Infinite Class of Balanced Functions with Optimal Algebraic Immunity, Good Immunity to Fast Algebraic Attacks and Good Nonlinearity”. In: *ASIACRYPT 2008*. Ed. by Josef Pieprzyk. Vol. 5350. LNCS. Springer, Heidelberg, Dec. 2008, pp. 425–440.

[CG05] Claude Carlet and Philippe Gaborit. “On the construction of Boolean functions with a good algebraic immunity”. In: *Boolean Functions: Cryptography and Applications*. Oct. 2005, pp. 1101 –1105.

[CGR19] Yindong Chen, Fei Guo, and Jie Ruan. “Constructing odd-variable RSBFs with optimal algebraic immunity, good nonlinearity and good behavior against fast algebraic attacks”. In: *Discrete Applied Mathematics* 262 (Mar. 2019).

[Che+19] Y. Chen, L. Lin, L. Liao, J. Ruan, F. Guo, and W. Cai. “Constructing Higher Nonlinear Odd-Variable RSBFs With Optimal AI and Almost Optimal FAI”. In: *IEEE Access* 7 (2019), pp. 133335–133341.

[Che+20] H. Chen, C. Ding, S. Mesnager, and C. Tang. “A Novel Application of Boolean Functions with High Algebraic Immunity in Minimal Codes”. In: *CoRR* abs/2004.04932 (2020).

[Cho+85] B. Chor, O. Goldreich, J. Hasted, J. Freidmann, S. Rudich, and R. Smolensky. “The bit extraction problem or t-resilient functions”. In: *FOCS*. 1985, pp. 396–407.

[CM01] Mary Cryan and Peter Bro Miltersen. “On pseudorandom generators in NC 0”. In: *International Symposium on Mathematical Foundations of Computer Science*. 2001.

[CM03] Nicolas Courtois and Willi Meier. “Algebraic Attacks on Stream Ciphers with Linear Feedback”. In: *EUROCRYPT 2003*. Ed. by Eli Biham. Vol. 2656. LNCS. Springer, Heidelberg, May 2003.

[CM04] Claude Carlet and Sihem Mesnager. *On the supports of the Walsh transforms of Boolean functions*. Cryptology ePrint Archive, Report 2004/256. 2004.

[CM19] Claude Carlet and Pierrick Méaux. “Boolean Functions for Homomorphic-Friendly Stream Ciphers”. In: *Algebra, Codes and Cryptology*. Ed. by Cheikh Thiecoumba Gueye, Edoardo Persichetti, Pierre-Louis Cayrel, and Johannes Buchmann. Cham: Springer, 2019, pp. 166–182.

[CM20] Claude Carlet and Pierrick Méaux. “A complete study of two classes of Boolean functions for homomorphic-friendly stream ciphers”. In: *IACR Cryptol. ePrint Arch.* 2020 (2020), p. 1562.

[CM22] Claude Carlet and Pierrick Méaux. “A Complete Study of Two Classes of Boolean Functions: Direct Sums of Monomials and Threshold Functions”. In: *IEEE Trans. Inf. Theory* 68.5 (2022), pp. 3404–3425. DOI: 10.1109/TIT.2021.3139804. URL: https://doi.org/10.1109/TIT.2021.3139804.

[Coh97] G. Cohen. *Covering Codes*. International Congress Series. Elsevier, 1997.

[Coo+14] James Cook, Omid Etesami, Rachel Miller, and Luca Trevisan. “On the one-way function candidate proposed by Goldreich”. In: *ACM Transactions on Computation Theory* 6.3 (2014), p. 14.

[Cou+18] Geoffroy Couteau, Aurélien Dupin, Pierrick Méaux, Mélissa Rossi, and Yann Rotella. “On the Concrete Security of Goldreich’s Pseudorandom Generator”. In: *ASIACRYPT*. 2018.

[CS00] Thomas Cusick and Pante Stănică. “Fast Evaluation, Weights and Nonlinearity of Rotation-Symmetric Functions”. In: *Discrete Mathematics* 258 (Sept. 2000).

[CS02] Claude Carlet and Palash Sarkar. “Spectral Domain Analysis of Correlation Immune and Resilient Boolean Functions”. In: *Finite Fields and Their Applications* 8.1 (2002), pp. 120 –130.

[CZT14] Y. D. Chen, Y. N. Zhang, and W. Tian. “Construction of Even-variable Rotation Symmetric Boolean Functions with Optimal Algebraic Immunity”. In: *Journal of Cryptologic Research* 1.5 (2014), p. 437.

[DGM04] Deepak Kumar Dalai, Kishan Chand Gupta, and Subhamoy Maitra. “Results on Algebraic Immunity for Cryptographically Significant Boolean Functions”. In: *INDOCRYPT*. LNCS. 2004, pp. 92–106.

[DGM05] D. Dalai, K. Gupta, and S. Maitra. “Cryptographically Significant Boolean Functions: Construction and Analysis in Terms of Algebraic Immunity”. In: *FSE 2005*. LNCS. 2005, pp. 98–111.

[Did07] Frédéric Didier. “Codes de Reed-Muller et cryptanalyse du registre filtré”. PhD thesis. École Polytechnique, Palaiseau, France, 2007.

[DM05] Deepak Kumar Dalai and Subhamoy Maitra. *Results on Rotation Symmetric Bent Functions*. Cryptology ePrint Archive, Report 2005/118. 2005.

[DMS06] D. K. Dalai, S. Maitra, and S. Sarkar. “Basic Theory in Construction of Boolean Functions with Maximum Possible Annihilator Immunity”. In: *DCC* (2006).

[DT06] Frédéric Didier and Jean-Pierre Tillich. “Computing the Algebraic Immunity Efficiently”. In: *FSE 2006*. Ed. by Matthew J. B. Robshaw. Vol. 4047. LNCS. Springer, Heidelberg, Mar. 2006, pp. 359–374.

[DV21] Amit Daniely and Gal Vardi. “From Local Pseudorandom Generators to Hardness of Learning”. In: *CoRR* abs/2101.08303 (2021).

[Fu+09] S. Fu, C. Li, K. Matsuura, and L. Qu. “Construction of Rotation Symmetric Boolean Functions with Maximum Algebraic Immunity”. In: *CANS 09*. Ed. by Juan A. Garay, Atsuko Miyaji, and Akira Otsuka. Vol. 5888. LNCS. Springer, Heidelberg, Dec. 2009, pp. 402–412.

[Fu+11] S. Fu, Longjiang Qu, C. Li, and Bing Sun. “Balanced rotation symmetric boolean functions with maximum algebraic immunity”. In: *Information Security, IET* 5 (July 2011), pp. 93 –99.

[Gay+20] Romain Gay, Aayush Jain, Huijia Lin, and Amit Sahai. “Indistinguishability Obfuscation from Simple-to-State Hard Problems: New Assumptions, New Techniques, and Simplification”. In: *IACR Cryptol. ePrint Arch.* 2020 (2020).

[Gol00] Oded Goldreich. “Candidate One-Way Functions Based on Expander Graphs”. In: *Electronic Colloquium on Computational Complexity (ECCC)* 7.90 (2000).

[Gra+16] Lorenzo Grassi, Christian Rechberger, Dragos Rotaru, Peter Scholl, and Nigel P. Smart. “MPC-Friendly Symmetric Key Primitives”. In: *ACM SIGSAC CCS*. Ed. by Edgar R. Weippl, Stefan Katzenbeisser, Christopher Kruegel, Andrew C. Myers, and Shai Halevi. 2016.

[Hou03] Xiang-dong Hou. “Group Actions on Binary Resilient Functions”. In: *Appl. Algebra Eng. Commun. Comput.* 14 (Aug. 2003), pp. 97–115.

[Ish+08] Yuval Ishai, Eyal Kushilevitz, Rafail Ostrovsky, and Amit Sahai. “Cryptography with constant computational overhead”. In: *40th ACM STOC*. ACM Press, May 2008, pp. 433–442.

[Jai+19] Aayush Jain, Huijia Lin, Christian Matt, and Amit Sahai. “How to Leverage Hardness of Constant-Degree Expanding Polynomials over R to build iO”. In: *EUROCRYPT*. Ed. by Yuval Ishai and Vincent Rijmen. Vol. 11476. Lecture Notes in Computer Science. 2019, pp. 251–281.

[JLS19] Aayush Jain, Huijia Lin, and Amit Sahai. “Simplifying Constructions and Assumptions for iO”. In: *IACR Cryptol. ePrint Arch.* 2019 (2019), p. 1252.

[Li+08] N. Li, L. Qu, W. Qi, G. Feng, C. Li, and D. Xie. “On the Construction of Boolean Functions With Optimal Algebraic Immunity”. In: *IEEE Transactions on Information Theory* 54.3 (2008), pp. 1330–1334.

[LK18] K. Limniotis and N. Kolokotronis. "Boolean functions with maximum algebraic immunity: further extensions of the Carlet–Feng construction". In: *DCC* 86 (2018), 1685–1706.

[LKK13] K. Limniotis, N. Kolokotronis, and N. Kalouptsidis. "Secondary constructions of Boolean functions with maximum algebraic immunity". In: *Cryptography and Communications* 5 (Sept. 2013).

[LQ06] Na Li and Wen-Feng Qi. "Construction and Analysis of Boolean Functions of 2t+1 Variables with Maximum Algebraic Immunity". In: *ASIACRYPT 2006*. Ed. by Xuejia Lai and Kefei Chen. Vol. 4284. LNCS. 2006, pp. 84–98.

[LV17] Alex Lombardi and Vinod Vaikuntanathan. "Limits on the Locality of Pseudorandom Generators and Applications to Indistinguishability Obfuscation". In: *TCC*. 2017, pp. 119–137.

[MC13] James McLaughlin and John A. Clark. *Evolving balanced Boolean functions with optimal resistance to algebraic and fast algebraic attacks, maximal algebraic degree, and very high nonlinearity.* Cryptology ePrint Archive, Report 2013/011. 2013.

[Méa+16] P. Méaux, A. Journault, F., and C. Carlet. "Towards Stream Ciphers for Efficient FHE with Low-Noise Ciphertexts". In: *EUROCRYPT*. 2016, pp. 311–343.

[Méa+19a] P. Méaux, C. Carlet, A. Journault, and F. Standaert. "Improved Filter Permutators for Efficient FHE: Better Instances and Implementations". In: *INDOCRYPT*. Ed. by Feng Hao, Sushmita Ruj, and Sourav Sen Gupta. Vol. 11898. LNCS. 2019, pp. 68–91.

[Méa+19b] Pierrick Méaux, Claude Carlet, Anthony Journault, and François-Xavier Standaert. *Improved Filter Permutators: Combining Symmetric Encryption Design, Boolean Functions, Low Complexity Cryptography, and Homomorphic Encryption, for Private Delegation of Computations*. Cryptology ePrint Archive, Report 2019/483. 2019.

[MST03] Elchanan Mossel, Amir Shpilka, and Luca Trevisan. "On e-Biased Generators in NC0". In: *44th FOCS*. IEEE Computer Society Press, Oct. 2003, pp. 136–145.

[O'D14] Ryan O'Donnell. *Analysis of Boolean Functions*. Cambridge University Press, 2014.

[OW14] Ryan ODonnell and David Witmer. "Goldreich's PRG: evidence for near-optimal polynomial stretch". In: *Conference on Computational Complexity (CCC)*. IEEE. 2014, pp. 1–12.

[Pas09] Enes Pasalic. "Almost Fully Optimized Infinite Classes of Boolean Functions Resistant to (Fast) Algebraic Cryptanalysis". In: *ICISC 08*. Ed. by Pil Joong Lee and Jung Hee Cheon. Vol. 5461. LNCS. Springer, Heidelberg, Dec. 2009, pp. 399–414.

[PFZ11] Sen-Shan Pan, Xiao-Tong Fu, and Wei-Guo Zhang. "Construction of 1Resilient Boolean Functions with Optimal Algebraic Immunity and Good Nonlinearity". In: *JCST* 26 (Mar. 2011), pp. 269–275.

[PQ98] Josef Pieprzyk and Cheng Xin Qu. "Rotation-symmetric functions and fast hashing". In: *Information Security and Privacy*. Ed. by Colin Boyd and Ed Dawson. Springer Berlin Heidelberg, 1998, pp. 169–180.

[Riz10] P. Rizomiliotis. "On the Resistance of Boolean Functions Against Algebraic Attacks Using Univariate Polynomial Representation". In: *IEEE Trans. on Inf. Theory* 56.8 (2010), pp. 4014–4024.

[Sie84] Thomas Siegenthaler. "Correlation-immunity of nonlinear combining functions for cryptographic applications". In: *IEEE* IT-30.5 (1984), pp. 776–780.

[SM07] Sumanta Sarkar and Subhamoy Maitra. *Construction of Rotation Symmetric Boolean Functions with Maximum Algebraic Immunity on Odd Number of Variables*. Cryptology ePrint Archive, Report 2007/290. 2007.

[SMC04] Pantelimon Stanica, Subhamoy Maitra, and John A. Clark. "Results on Rotation Symmetric Bent and Correlation Immune Boolean Functions". In: *FSE 2004*. Ed. by Bimal K. Roy and Willi Meier. Vol. 3017. LNCS. Feb. 2004, pp. 161–177.

[Son+10] Shouchao Song, Jie Zhang, Jiao Du, and Qiaoyuan Wen. "On the construction of Boolean functions with optimal algebraic immunity and good other properties by concatenation".

In: *2010 IEEE International Conference on Progress in Informatics and Computing*. Vol. 1. 2010, pp. 417–422.

[ST14] S. Su and X. Tang. "Construction of rotation symmetric Boolean functions with optimal algebraic immunity and high nonlinearity". In: *Designs, Codes and Cryptography* 71 (May 2014).

[Tar00] Yuriy Tarannikov. "On Resilient Boolean Functions with Maximal Possible Nonlinearity". In: *INDOCRYPT 2000*. Ed. by Bimal K. Roy and Eiji Okamoto. Vol. 1977. LNCS. Springer, Heidelberg, Dec. 2000, pp. 19–30.

[TCT13] D. Tang, C. Carlet, and X. Tang. "Highly Nonlinear Boolean Functions With Optimal Algebraic Immunity and Good Behavior Against Fast Algebraic Attacks". In: *IEEE Transactions on Information Theory* 59.1 (2013), pp. 653–664.

[TD11] Ziran Tu and Yingpu Deng. "A conjecture about binary strings and its applications on constructing Boolean functions with optimal algebraic immunity". In: *DCC* 60 (2011), pp. 1–14.

[Yan+22] Jing Yang, Qian Guo, Thomas Johansson, and Michael Lentmaier. "Revisiting the Concrete Security of Goldreich's Pseudorandom Generator". In: *IEEE Trans. Inf. Theory* 68.2 (2022), pp. 1329–1354. DOI: 10.1109/TIT.2021.3128315. URL: https://doi.org/10.1109/TIT.2021.3128315.

[Zha+12] Peng Zhang, Deshuai Dong, Shaojing Fu, and Chao Li. "New constructions of even-variable rotation symmetric Boolean functions with maximum algebraic immunity". In: *Mathematical and Computer Modelling* 55.3 (2012), pp. 828 –836.

[ZS19] H. Zhang and S. Su. "A new construction of rotation symmetric Boolean functions with optimal algebraic immunity and higher nonlinearity". In: *Discrete Applied Mathematics* 262 (2019), pp. 13 –28.

Supplementary material

A Towards constructing dahus: properties, necessary or sufficient conditions

A.1 Additional Preliminaries

We give additional preliminaries that will be used in the proofs.

Properties of cryptographic criteria on Boolean functions

Property 9 ($\mathcal{D}$AN Properties, *e.g.* [Car+06] Theorem 3)**.** *Let f be an n-variable Boolean function with optimal algebraic immunity. If n is odd then $\mathcal{D}\mathsf{AN}(f) = \binom{n}{(n+1)/2}$. If n is even and f is balanced then $\mathcal{D}\mathsf{AN}(f) > \binom{n}{n/2}$.*

Property 10 (Walsh Transform and Weight of f, *e.g.* [Car21])**.** *Let $f \in \mathcal{B}_n$, $a \in \mathbb{F}_2^n$, denote l_a the linear function $l_a(x) = \sum_{i \in \mathsf{supp}(a)} x_i$, the following relation holds:*

$$\mathsf{d_H}(f, l_a) := \mathsf{w_H}(f + l_a) = 2^{n-1} - \frac{\mathsf{W}_f(a)}{2},$$

where $\mathsf{d_H}$ is defined as the Hamming distance between f and l_a, the number of elements of $\mathbb{F}_2^n$ where f and l_a differ.

Property 11 ([CS02] Theorem 4.1)**.** *Let f be a non-constant n-variable Boolean function, then $\forall a \in \mathbb{F}_2^n$, $2^{\mathsf{res}(f)+2+\lfloor (n-\mathsf{res}(f)-2)/\mathsf{deg}(f) \rfloor}$ divides $\mathsf{W}_f(a)$.*

Transformations keeping the resiliency order

We remark that the resiliency order is not an affine equivalent criteria, neither linear equivalent, but it is permutation equivalent. In the following we give more details on the operations not decreasing the resiliency. In [Hou03], Hou studies the automorphism group of Boolean k-resilient functions (the group of automorphisms of $\mathbb{F}_2^n$ permuting the set of k-resilient functions):

Property 12 (Group acting on t-resilient functions,[Hou03])**.** *Let $n \in \mathbb{N}^*$ and $k \in [n-2]$, if k is odd the group action $\mathbb{Z}_2^n \rtimes < S_n >$ acts on $\mathcal{R}_{n,k}$, otherwise the group action $\mathbb{Z}_2^n \rtimes < S_n, \Delta >$ acts on $\mathcal{R}_{n,k}$, where:*

- *$\mathcal{R}_{n,k}$ denotes the sets of k-resilient n-variable Boolean functions modulo the constant functions.*
- *S_n denotes the group of permutation matrices, Δ denotes an involution which matrix M_Δ corresponds to the identity matrix I_n where the first row is replaced by the all-1 vector.*
- *$< \cdot >$ denotes the group obtained by composition, and $\rtimes$ the semi-direct product.*

This result can be rewritten in term of equivalent notion:

Definition 20 **(R_k-equivalence and R_k-equivalent set).** *Let $n \in \mathbb{N}^*$ and $k \in [n-2]$, we say two n-variable Boolean functions f and $a_0 + f \circ L$ where: $L : (x_1, \dots, x_n) \mapsto (x_1, \dots, x_n) \times \mathbf{M} + (a_1, \dots, a_n)$ are R_k-equivalent if $a_0 \in \mathbb{F}_2$, L is an affine automorphism of $\mathbb{F}_2^n$, where $(a_1, \dots, a_n) \in \mathbb{F}_2^n$, and $\mathbf{M}$ is a permutation matrix (exactly one 1 in each row and column) if $k \equiv 1 \mod 2$, and $\mathbf{M}$ is a either permutation matrix or the product of a permutation matrix by M_Δ otherwise.*

We denote $R_k(f)$ the set $\{g \in \mathcal{B}_n$ such that g is R_k-equivalent to $f\}$.

Note that the R_k-equivalence concept is based on Property 12, it guarantees that for f a k-resilient function all functions in $R_k(f)$ are also k-resilient. In term of resiliency order, it means than for all $g \in R_k(f)$ $\mathsf{res}(g) \geq \mathsf{res}(f)$.

Remark 5. We give details about the difference between the results of Property 12 and the automorphism group of the k-resilient functions.

In [Hou03] the largest sub-group of $GL(n, \mathbb{Z}_2)$, the general linear group over $\mathbb{Z}_2$, acting on the k-resilient function is determined, we denote it G. It corresponds to the linear transformations keeping the k-resiliency, and its action on a function f remains in its linear-equivalent class.

Since all the translations (addition of $a \in \mathbb{Z}_2^n$) do not modify the resiliency, $\mathbb{Z}_2^n \rtimes G$ acts on the k-resilient functions. It corresponds to affine transformations keeping the k-resiliency, and its action on a function f remains in its affine-equivalent class. It is the largest sub-group of $AGL(n, \mathbb{Z}_2)$, the affine general linear group over $\mathbb{Z}_2$, which keeps any k-resilient function f in its affine-equivalence class. It is the group introduced in Property 12 since we focus on affine-equivalent functions.

The sub-group of $AGL(n, \mathbb{Z}_2)$ acting on k-resilient functions considered in [Hou03] is larger than $\mathbb{Z}_2^n \rtimes G$ but it considers an indirect action, which can map functions out of there affine-equivalent class. Instead, the indirect action is compatible to the notion of extended-affine-equivalence of Boolean functions, where two functions are extended-affine-equivalent if they are affine equivalent up to the addition of a linear function (*i.e.* $f' = a_0 + \sum_{i=1}^{n} a_i x_i + f \circ L$). Hence, this group or a larger one (it is not proven than no other indirect actions are possible) is the largest sub-group of $AGL(n, \mathbb{Z}_2)$ acting on k-resilient functions, which corresponds to the denomination of automorphism group of k-resilient functions rather than the group described in Property 12.

Cryptographic properties of secondary constructions

We recall some of Siegenthaler's construction properties relatively to its algebraic immunity, resiliency and degree. We focus on the properties of h given by the properties of f and g.

Property 13 (Siegenthaler's Construction Properties (*e.g.* [Car21])**.** *Let $n \in \mathbb{N}$, $f, g \in \mathcal{B}_n$, h obtained through the Siegenthaler's construction with components f and g has the following properties:*

1. *Walsh transform:* $\forall a \in \mathbb{F}_2^n, \quad \mathsf{W}_h(a, 0) = \mathsf{W}_f(a) + \mathsf{W}_g(a),$ *and* $\mathsf{W}_h(a, 1) = \mathsf{W}_f(a) - \mathsf{W}_g(a)$.
2. *Resiliency: If* $\mathsf{res}(f) = \mathsf{res}(g) = k$ *and* $\forall a \in \mathsf{E}_{k+1,n}, \ \mathsf{W}_f(a) = -\mathsf{W}_g(a)$ *then* $\mathsf{res}(h) = \mathsf{res}(f) + 1$, *otherwise* $\mathsf{res}(h) = \min\{\mathsf{res}(f), \mathsf{res}(g)\}$.
3. *Degree: If* $\mathsf{deg}(f) = \mathsf{deg}(g) = d$ *and* $\mathsf{deg}(f + g) < d$ *then* $\mathsf{deg}(h) = \mathsf{deg}(f)$, *otherwise* $\mathsf{deg}(h) = 1 + \max\{\mathsf{deg}(f), \mathsf{deg}(g)\}$.
4. *Algebraic immunity: If* $\mathsf{AI}(f) = \mathsf{AI}(g) = e$ *and* $\exists f', g'$ *of degree* e, $\varepsilon \in \mathbb{F}_2$ *such that* $f'(f + \varepsilon) = 0 = g'(g + \varepsilon)$ *and* $\mathsf{deg}(f' + g') < e$ *then* $\mathsf{AI}(h) = \mathsf{AI}(f)$, *otherwise* $\mathsf{AI}(h) = 1 + \min\{\mathsf{AI}(f), \mathsf{AI}(g)\}$.

Property 14 (Direct Sum Properties, *e.g.* [Méa+16] Lemma 3)**.** *Let h be the direct sum of f and g with n and m variables respectively. Then h has the following properties:*

- *Resiliency:* $\mathsf{res}(h) = \mathsf{res}(f) + \mathsf{res}(g) + 1$.
- *Algebraic Immunity:* $\max(\mathsf{AI}(f), \mathsf{AI}(g)) \leq \mathsf{AI}(h) \leq \mathsf{AI}(f) + \mathsf{AI}(g)$.

From Corollary 1, we know that the existence of a $(2t + 1)$-variable dahu implies the existence of a $(2t + 2)$-variable dahu, therefore we focus on necessary and sufficient conditions implying the existence of a dahu in an odd number of variables. Since $\mathsf{Dahu}_3 \neq \emptyset$ as proved in Section 4.1, this would suffice to prove Conjecture 1 by recursively building dahus for all n. The different results narrowing the sufficient and necessary conditions to build odd-variable dahus are further steps towards proving (or disproving) Conjecture 1, and consequently the bounds of Theorem 3.

In Subsection A.2 we investigate the properties of dahus and the cardinal of Dahu_n. Then we focus on sufficient constructions to build dahus in an higher number of variables in Subsection A.3, and finally we determine necessary conditions in Subsection A.4

A.2 Dahus' properties

Lemma 13 (Dahu's properties). *Let $t \in \mathbb{N}$, $t \geq 2$, $\varepsilon \in \{0,1\}$, $n = 2t+\varepsilon$, if $f \in \mathsf{Dahu}_n$ then the following holds:*

1. $\mathsf{AI}(f) = t+\varepsilon$, *and* $\mathsf{res}(f) = t-1$,
2. $\mathsf{deg}(f) = \mathsf{AN}(f) = \mathsf{AN}(f+1) = t+\varepsilon$,
3. *when* $\varepsilon = 1$*:* $\mathcal{D}\mathsf{AN}(f) = \binom{2t+1}{t+1}$, *when* $\varepsilon = 0$*:* $\mathcal{D}\mathsf{AN}(f) \geq \binom{2t}{t}/2$,
4. $4 \leq |\mathsf{Wsupp}_f| \leq 2^{2(t+\varepsilon-1)}$, $\forall a \in \mathsf{Wsupp}_f : \; 2^{t+1} \leq |\mathsf{W}_f(a)| \leq 2^{2t+\varepsilon} - 2^{t+1}$,
5. $f+1 \in \mathsf{Dahu}_{2t+\varepsilon}$, *and more generally* $R_{t-1}(f) \subset \mathsf{Dahu}_{2t+1}$,
6. $|\mathsf{Dahu}_{2t+\varepsilon}| \geq 8$.

Proof. 1. The values of the algebraic immunity and resiliency order are equivalent to the definition of dahu (Definition 14).

2. From the precedent item $\mathsf{AI}(f) > 2$ hence f is not a constant function (Property 4 item 1) hence $\mathsf{AI}(f) \leq \mathsf{deg}(f)$ (Property 4 item 3). Using Siegenthaler's relation (see Theorem 2), we get $\mathsf{deg}(f) \leq n - \mathsf{res}(f) - 1$, The bounds collapse, giving $\mathsf{deg}(f) = t+\varepsilon$, therefore both f and $f+1$ have annihilators of degree $t+\varepsilon = \mathsf{AI}(f)$ explaining the relation on AN.
3. Since f has optimal AI and is balanced Property 9 gives this property on the $\mathcal{D}\mathsf{AN}$.
4. First we recall some results about the Walsh transform and support. For n-variable functions of degree d and resiliency order k such that $1 \leq k \leq n-2$, $\mathsf{W}_f(a)$ is a multiple of $2^{k+2+\lfloor (n-k-2)/d \rfloor}$ (Property 11). From the value of the resiliency order and degree of dahus, the Walsh transform values are multiple of 2^{t+1} (which gives the lower bound on $|\mathsf{W}_f(a)|$), hence for $f \in \mathsf{Dahu}_{2t+\varepsilon}$ we write $\mathsf{W}_f(a) = 2^{t+1}\mathsf{w}_f(a)$, where $\mathsf{w}_f(a) \in \mathbb{Z}$. For any n-variable Boolean function, the Walsh transform satisfies Perseval's relation: $\sum_{a \in \mathbb{F}_2^n} (\mathsf{W}_f(a))^2 = 2^{2n}$, and the inverse formula relation: $\sum_{a \in \mathbb{F}_2^n} \mathsf{W}_f(a)(-1)^{ax} = 2^n(-1)^{f(x)}$.
   Then, Perseval's relation and the inverse formula applied on $0 \in \mathbb{F}_2^n$ gives the following for $f \in \mathsf{Dahu}_{2t+\varepsilon}$:
   $$\sum_{a \in \mathsf{Wsupp}_f} (\mathsf{w}_f(a))^2 = 2^{2(t+\varepsilon-1)}, \text{ and } \sum_{a \in \mathsf{Wsupp}_f} \mathsf{w}_f(a) = \pm 2^{t+\varepsilon-1}.$$
   Since $\mathsf{w}_f(a)$ is not null if and only if $a \in \mathsf{Wsupp}_f$, the first sum gives the upper bound on the cardinal of the Walsh support.
   For the lower bound, we focus on the structure of the Walsh support. A cardinal of 1 corresponds to an affine function (which is impossible here since $\mathsf{AI}(f) \geq 2$), and a cardinal of 2 does not correspond to a Boolean function (Property 2). $|\mathsf{Wsupp}_f| = 3$ is also impossible, we show it by contradiction. Let us denote a, b and c the elements in the support, and α, β, γ the values of the Walsh transform. Since a, b and c are different there exist $x' \in \mathbb{F}_2^n \setminus \{0\}$ such that $a \cdot x' = b \cdot x'$ and $a \cdot x' \neq c \cdot x'$. Therefore the inverse formula applied on x' leads to $|\alpha + \beta - \gamma| = 2^n$ and the formula applied in 0 leads to $|\alpha + \beta + \gamma| = 2^n$. It gives two possibilities, either $\gamma = 0$ which is impossible since $c \in \mathsf{Wsupp}_f$, or $\alpha = -\beta$ and $|\gamma| = 2^n$, which contradicts Perseval's relation.
   Finally, considering a support of at least 2 elements, $\max(\mathsf{w}_f) < 2^{t+\varepsilon-1}$, giving the upper bound on $|\mathsf{W}_f(a)|$.
5. The complementary of f is also a dahu since it has the same algebraic immunity and resiliency. More generally, for all $g \in R_{t-1}(f)$ (Definition 20) we have $\mathsf{res}(g) \geq \mathsf{res}(f)$. Since g is affine equivalent to f, $\mathsf{deg}(g) = \mathsf{deg}(f) = t+\varepsilon$ and therefore $\mathsf{res}(g) \leq t-1$ using Siegenthaler's bound, which allows to conclude $\mathsf{res}(g) = \mathsf{res}(f) = t-1$. Using property 4 item 5 $\mathsf{AI}(g) = \mathsf{AI}(f) = t+\varepsilon$ and therefore, $g \in \mathsf{Dahu}_{2t+\varepsilon}$.
6. We show that $|R_{t-1}(f)| \geq 2|\mathsf{Wsupp}_f|$ which is sufficient since $|\mathsf{Dahu}_{2t+\varepsilon}| \geq |R_{t-1}(f)|$ by item 5 and $|\mathsf{Wsupp}_f| \geq 4$ by item 4. To do so, we prove that at least $2|\mathsf{Wsupp}_f|$ functions of $R_{t-1}(f)$ are different, by showing that at least $2|\mathsf{Wsupp}_f|$ different Walsh spectrum can be obtained. $R_{t-1}(f)$

contains the functions obtained by translation from f: $f_b(x) = f(x+b)$ which is defined for all $b \in \mathbb{F}_2^n$. We focus on the relation between the Walsh transform of f and f_b:

$$\begin{aligned}\forall a \in \mathbb{F}_2^n,\ \mathsf{W}_{f_b}(a) &= \textstyle\sum_{x\in\mathbb{F}_2^n}(-1)^{f_b(x)+a\cdot x}\\ &= \textstyle\sum_{x\in\mathbb{F}_2^n}(-1)^{f(x+b)+a\cdot x}\\ &= \textstyle\sum_{x'\in\mathbb{F}_2^n}(-1)^{f(x')+a\cdot x'+a\cdot b}\\ &= (-1)^{a\cdot b}\mathsf{W}_f(a).\end{aligned}$$

Hence, the 2^n translations of f have the same Walsh support, and the sign in a differs from the one of $\mathsf{W}_f(a)$ if and only if $a \cdot b = 1$. The family of 2^n functions indexed by b from $\mathbb{F}_2^n$ to $\{-1,1\}$ defined as $\chi_b(x) = (-1)^{b\cdot x}$ corresponds to the characters of $\mathbb{F}_2^n$ (more precisely the multiplicative characters of the Abelian group $(\mathbb{Z}_2,+)^n$), and therefore this family forms a basis of the functions from $\mathbb{F}_2^n$ to $\mathbb{C}$ (*e.g.* [O'D14] Proposition 8.55). Therefore, the matrix $\mathbf{W}$ with 2^n rows indexed by $b \in \mathbb{F}_2^n$ and $|\mathsf{Wsupp}_f|$ columns indexed by $a \in \mathsf{Wsupp}_f$ and entries in $\{-1,1\} \subset \mathbb{C}$ defined as $\mathbf{W}_{b,a} = (-1)^{b\cdot a}$ has rank $|\mathsf{Wsupp}_f|$ over $\mathbb{C}$. Then, there exists $|\mathsf{Wsupp}_f|$ rows such that the corresponding sub-matrix of size $|\mathsf{Wsupp}_f| \times |\mathsf{Wsupp}_f|$ is full rank, and multiplying all the elements of each column indexed by a by $\mathsf{W}_a(f)$ does not alter this property (since it is non-null). Therefore, taking $b_1,\dots,b_{|\mathsf{Wsupp}_f|}$, $|\mathsf{Wsupp}_f|$ rows satisfying this property, the Walsh spectrum of the functions f_{b_i} for i in $[|\mathsf{Wsupp}_f|]$ are all different. These vectors are also not opposed: there exists no pair (i,j) such that for all x $\mathsf{W}_{f_{b_i}}(x) = -\mathsf{W}_{f_{b_i}}(x)$, otherwise the sub-matrix would not have rank $|\mathsf{Wsupp}_f|$ in $\mathbb{C}$. The functions f_{b_i} for i in $[|\mathsf{Wsupp}_f|]$ give $|R_{t-1}(f)| \geq |\mathsf{Wsupp}_f|$, and using the relation between the Walsh transform between a Boolean function g and its complementary: $\forall a \in \mathbb{F}_2^n$, $\mathsf{W}_{g+1}(a) = -\mathsf{W}_g(a)$, the functions $f_{b_i}+1$ give $|\mathsf{Wsupp}_f|$ other Walsh spectra (with the same Walsh support), allowing to conclude $|R_{t-1}(f)| \geq 2|\mathsf{Wsupp}_f|$.

□

Remark 6. Note that the lower bound given by Item 6 is in fact a lower bound of $|R_{t-1}(f)|$. The number of affine transformations keeping the resiliency cannot be used directly to determine $|R_{t-1}(f)|$ since various of those transformations are mapping f to f. For example, for $t \in \mathbb{N}^*$ the majority function MAJ_{2t+1} is a fixed point for the $2(2t+1)!$ affine transformations $f \mapsto a_0 + f(\mathbf{M}x + (a_1,\dots,a_{2t+1}))$ where $\mathbf{M}$ is a permutation matrix and $a_i = \varepsilon$ for all $i \in [0, 2t+1]$, $\varepsilon \in \{0,1\}$. In the proof, we use the cardinal of the Walsh support of f to derive the lower bound on $|R_{t-1}(f)|$ but other approaches are possible, such as pursuing the work of [Hou03] by determining the minimal length of the orbits given by the group acting on $(t-1)$-resilient functions.

Note also that the lower bound on $|\mathsf{Dahu}_n|$ could be improved by enhancing the lower bound on $|\mathsf{Wsupp}_f|$, or showing that more than one affine equivalence class belongs to Dahu_n. For the particular case of $n = 3$ we will see in Section 5.2 that Dahu_3 consists in a unique class and $|\mathsf{Wsupp}_f| = 4$.

A.3 Sufficient conditions

In the following, we exhibit sufficient conditions for the existence of a $(2t+3)$-variable dahu, based on the existence of four $(2t+1)$-variable dahus having related properties. The interest of this secondary construction is twofold. First, it allows to experimentally find dahus by checking the sufficient conditions. It will be performed later in Section 5.2. Secondly, proving that these conditions hold on Dahu_n for all odd $n \geq 3$ would be enough to prove Conjecture 1.

Proposition 5. *Let $t \in \mathbb{N}^*$, y, z two Boolean variables and $d_1, d_2, d_3, d_4 \in \mathsf{Dahu}_{2t+1}$. Let $\mathcal{H}_{d,n}$ denote the set of degree-d n-variable homogeneous functions and for $\psi \in \mathcal{H}_{d,n}$ let $\mathsf{an}_f(\psi)$ denote the degree-d annihilator of f with degree-d part being ψ if it exists. If the following constraints are satisfied:*

- *degree:* $\deg(d_1+d_2) = t+1$, $\deg(\sum_{i=1}^4 d_i) < t+1$,

– *Walsh transform:* $\forall a \in \mathsf{E}_{t,2t+1}$, $\sum_{i=1}^{4} \mathsf{W}_{d_i}(a) = 0$,
– *annihilators:* $\forall \psi \in \mathcal{H}_{t+1,2t+1}$, $\deg(\sum_{i=1}^{4} \mathsf{an}_{d_i}(\psi)) = \deg(\sum_{i=1}^{4} \mathsf{an}_{d_i+1}(\psi)) = t$,

then $h = (1+z)((1+y)d_1 + yd_2) + z((1+y)d_3 + yd_4)$ *belongs to* Dahu_{2t+3}.

Proof. First, we denote $f = (1+y)d_1 + yd_2$ and $g = (1+y)d_3 + yd_4$, therefore h is a Siegenthaler construction (see Definition 12) from components f and g. Both of these functions are also obtained with the same construction with components d_1, d_2 and d_3, d_4 respectively. Hence, we study the resiliency order and algebraic immunity of h based on Property 13.

We begin with the resiliency order. First, we show that $\mathsf{res}(h) \leq t$ based on the degree of h. Indeed, the function h can be rewritten as $yz(d_1+d_2+d_3+d_4) + y(d_1+d_2) + z(d_1+d_3) + d_1$, and since $\deg(d_1+d_2+d_3+d_4) < t+1$, $\deg(d_1+d_2) = t+1$ and $\deg(d_1) = \deg(d_3) = t+1$ it gives $\deg(h) = t+2$. Hence, Theorem 2 provides $\mathsf{res}(h) \leq t$. Since the d_i are $(2t+1)$-variable dahus their resiliency order is $t-1$, and therefore the second item of Property 13 gives $\mathsf{res}(h) \geq t-1$, which is equivalent to $\forall a \in \mathbb{F}_2^{2t+3} \,|\, \mathsf{w_H}(a) \leq t-1, \mathsf{W}_h(a) = 0$ (Property 1). Hence, it remains to determine the value of the Walsh transform on $\mathsf{E}_{t,2t+3}$ to conclude on the value of $\mathsf{res}(h)$. We use the expression of W_h in terms of W_f and W_g using the first item of Property 13, we separate $\mathsf{E}_{t,2t+3}$ based on the value of z:

– When $z = 1$, $a = (a', 1)$ where $a' \in \mathsf{E}_{t-1,2t+2}$ therefore $\mathsf{W}_h(a) = \mathsf{W}_f(a') - \mathsf{W}_g(a') = 0$ since both functions f and g are at least $(t-1)$-resilient.
– When $z = 0$, $a = (a', 0)$ where $a' \in \mathsf{E}_{t,2t+2}$, we use the expression of W_f in terms of W_{d_1} and W_{d_2} and W_g in terms of W_{d_3} and W_{d_4}. We separate $\mathsf{E}_{t,2t+2}$ based on the value of y:
  • When $y = 1$, $a = (a", 1, 0)$ where $a" \in \mathsf{E}_{t-1,2t+1}$ therefore:

$$\mathsf{W}_h(a) = \mathsf{W}_f(a') + \mathsf{W}_g(a') = \mathsf{W}_{d_1}(a") - \mathsf{W}_{d_2}(a") + \mathsf{W}_{d_3}(a") - \mathsf{W}_{d_4}(a") = 0$$

  since the d_i have resiliency order $t-1$.
  • For the last case, $y = 0$, it corresponds to $a = (a", 0, 0)$ where $a" \in \mathsf{E}_{t,2t+1}$ therefore $\mathsf{W}_h(a) = \mathsf{W}_f(a') + \mathsf{W}_g(a') = \mathsf{W}_{d_1}(a") + \mathsf{W}_{d_2}(a") + \mathsf{W}_{d_3}(a") + \mathsf{W}_{d_4}(a")$. Since we chose d_1, d_2, d_3 and d_4 such that $\forall a" \in \mathsf{E}_{t,2t+1}$, $\sum_{i=1}^{4} \mathsf{W}_{d_i}(a) = 0$, it concludes this part: $\forall a \in \mathsf{E}_{t,2t+3}, \mathsf{W}_h = 0$ and since previously we showed $\mathsf{res}(h) \geq t-1$ and $\mathsf{res}(h) \leq t$, finally $\mathsf{res}(h) = t$.

Then, we determine the algebraic immunity of h. We begin by focusing on the shape of the annihilators of f and g of minimal degree. Since f is obtained by Siegenthaler construction with components d_1 and d_2 the fourth item of Property 13 gives $\mathsf{AI}(f) = \mathsf{AI}(d_1) = \mathsf{AI}(d_2) = t+1$ (it cannot be higher since $f \in \mathcal{B}_{2t+2}$, Property 4 item 5). Let ϕ be an annihilator of f of degree $t+1$, then $\phi d_1 \cdot (y+1) = \phi y d_2$, and writing ϕ as $\phi_1 \cdot (y+1) + \phi_2 y$ with $\phi_1, \phi_2 \in \mathcal{B}_{2t+1}$ it forces ϕ_i to be an annihilator of d_i for $i \in [2]$. Since $\deg(\phi) = t+1$ it gives $\deg(\phi_1) \leq t+1$ and $\deg(\phi_1 + \phi_2) \leq t$. Since $\phi_1 d_1 = 0$ either $\phi_1 = 0$, either $\deg(\phi_1) = t+1$. In the first case, it would force ϕ_2 to have degree t, which is incompatible with $\phi_2 d_2 = 0$. In the second case, $\deg(\phi_1) = t+1$, and since d_1 is a function with optimal algebraic immunity in $2t+1$ variables $\mathcal{D}\mathsf{AN}(d_1)$ is maximal (Property 9) which means that for all $\psi \in \mathcal{H}_{t+1,2t+1}$ $\mathsf{an}_{d_1}(\psi)$ exists. Since $\deg(\phi_1 + \phi_2) \leq t$, when $\phi_1 = \mathsf{an}_{d_1}(\psi)$ the only possibility to comply with $\phi_2 d_2 = 0$ is $\phi_2 = \mathsf{an}_{d_2}(\psi)$ (which exists by using the same arguments since $d_2 \in \mathsf{Dahu}_{2t+1}$). The annihilators of f of degree $t+1$ are therefore $(1+y)\mathsf{an}_{d_1}(\psi) + y\mathsf{an}_{d_2}(\psi)$ for $\psi \in \mathcal{H}_{t+1,2t+1}$. By similar arguments since $1+d_1, 1+d_2, d_3, d_4, 1+d_3, 1+d_4 \in \mathsf{Dahu}_{2t+1}$ we determine the $(t+1)$-degree annihilators of $f+1$, g and $g+1$. Finally, we use the fourth item of Property 13 to determine $\mathsf{AI}(h)$. For $\varepsilon \in \mathbb{F}_2$ let consider any $(t+1)$-degree annihilator f' of $f+\varepsilon$ and any $(t+1)$-degree annihilator g' of $g+\varepsilon$, it leads to:

$$\begin{aligned} f' + g' &= (1+y)\mathsf{an}_{d_1+\varepsilon}(\psi) + y\mathsf{an}_{d_2+\varepsilon}(\psi) + (1+y)\mathsf{an}_{d_3+\varepsilon}(\psi') + y\mathsf{an}_{d_4+\varepsilon}(\psi'), \\ &= \mathsf{an}_{d_1+\varepsilon}(\psi) + \mathsf{an}_{d_3+\varepsilon}(\psi') + y(\mathsf{an}_{d_1+\varepsilon}(\psi) + \mathsf{an}_{d_2+\varepsilon}(\psi) + \mathsf{an}_{d_3+\varepsilon}(\psi') + \mathsf{an}_{d_4+\varepsilon}(\psi')). \end{aligned}$$

If $\psi \neq \psi'$ then $\deg(\mathsf{an}_{d_1+\varepsilon}(\psi)+\mathsf{an}_{d_3+\varepsilon}(\psi')) = t+1$ then $\deg(f'+g') = t+1$. If $\psi = \psi'$, since we chose d_1, d_2, d_3 and d_4 such that $\deg(\sum_{i=1}^{4} \mathsf{an}_{d_i}(\psi)) = \deg(\sum_{i=1}^{4} \mathsf{an}_{d_i+1}(\psi)) = t$, it gives $\deg(f' + g') = t + 1$. Consequently, $\mathsf{AI}(h) = 1 + \min\{\mathsf{AI}(f), \mathsf{AI}(g)\} = t + 2$. It allows to conclude: $h \in \mathsf{Dahu}_{2t+3}$.

□

Example 3. Let $t = 1$, the following functions satisfy the constraints of Proposition 5: $d_1 = x_1x_2 + x_1x_3 + x_2x_3$, $d_2 = x_1 + x_2 + x_3 + x_1x_2$, $d_3 = x_1 + x_2 + x_3 + x_2x_3$, and $d_4 = 1 + x_2 + x_1x_3$ and give a 5-variable dahu.

Corollary 4. *Let $t \in \mathbb{N}^*$, y, z two Boolean variables and $d_1, d_2, d_3 \in \mathsf{Dahu}_{2t+1}$. Let $\mathcal{H}_{d,n}$ denote the set of degree-d n-variable homogeneous functions and for $\psi \in \mathcal{H}_{d,n}$ let $\mathsf{an}_f(\psi)$ denote the degree-d annihilator of f with degree-d part being ψ if it exists. If the following constraints are satisfied:*

- *degree:* $\deg(d_1 + d_2) = t + 1$, $\deg(d_2 + d_3) < t + 1$,
- *Walsh transform:* $\forall a \in \mathsf{E}_{t,2t+1}$, $2\mathsf{W}_{d_1}(a) + \mathsf{W}_{d_2}(a) + \mathsf{W}_{d_3}(a) = 0$,
- *annihilators:* $\forall \psi \in \mathcal{H}_{t+1,2t+1}$, $\deg(\mathsf{an}_{d_2}(\psi) + \mathsf{an}_{d_3}(\psi)) = \deg(\mathsf{an}_{d_2+1}(\psi) + \mathsf{an}_{d_3+\varepsilon}(\psi)) = t$,

then $h = yz(d_2 + d_3) + y(d_1 + d_2) + d_1$ belongs to Dahu_{2t+3}.

Proof. The result is obtained by taking $d_1 = d_3$ and renaming d_4 by d_3. □

Remark 7. The condition $\deg(d_2 + d_3) < t + 1$ in Corollary 4 forces to choose two dahus with the same degree $t + 1$ part. Nevertheless the condition on the annihilators prevents taking $d_2 = d_3$ or $d_2 = d_3 + 1$.

A.4 Necessary conditions

In the next proposition, we consider necessary conditions to obtain a dahu in an odd number of variables through Siegenthaler's construction (outlined in Definition 12 and detailed in Section A.1). Since any function can be written through this construction, the following result shows what are the prerequisites on the sets of even-variable Boolean functions to the existence of odd-variable dahus. If for an even $n \geq 4$ such conditions could not be satisfied then it would invalidate Conjecture 1.

Proposition 6. *Let $t \in \mathbb{N}, t \geq 2$. Let $h \in \mathcal{B}_{2t}$ written as the Siegenthaler construction with components f and g where $f, g \in \mathcal{B}_{2t}$ (see Definition 12). If $h \in \mathsf{Dahu}_{2t+1}$ then*

1. $\mathcal{D}\mathsf{AN}(f) = \mathcal{D}\mathsf{AN}(g) = \binom{2t}{t}/2$,
2. $\mathsf{AI}(f) = \mathsf{AI}(g) = t$,
3. *for $\varepsilon \in \{0, 1\}$ the highest degree part of the degree t annihilators of $f + \varepsilon$ and $g + \varepsilon$ are different.*

In addition, ***exactly one*** *of the following holds:*

4.a. $f, g \in \mathsf{Dahu}_{2t}$,

4.b. $\mathsf{res}(f) = \mathsf{res}(g) = t-2$, $\deg(f) = \deg(g) = t+1$, $\deg(f+g) < t+1$ *and for* $a \in \mathsf{E}_{t-1,2t}$ $\mathsf{W}_f(a) = -\mathsf{W}_g(a)$,

4.c. $\mathsf{res}(f) = \mathsf{res}(g) = t-2$, $\deg(f) = \deg(g) = t$, $\deg(f+g) = t$, *for* $a \in \mathsf{E}_{t-1,2t}$ $\mathsf{W}_f(a) = -\mathsf{W}_g(a)$, *and* $|\mathsf{Wsupp}_f| \leq 2^{2t-2}$, $|\mathsf{Wsupp}_g| \leq 2^{2t-2}$, *and* $|\mathsf{Wsupp}_h| \leq 2^{2t} - 1$.

Proof. The different constraints on f and g are obtained by combining Property 13 and the parameters of a dahu in an odd number of variables (Lemma 13).

- **Algebraic immunity.** $\mathsf{AI}(h) = t + 1$ by Definition 14 and f and g have algebraic immunity at most t since they are $2t$-variable functions (Property 4 item 6). Hence using Property 13 item 4, f and g must have AI equal to t and that for $\varepsilon \in \{0, 1\}$ no degree-t annihilator of $f + \varepsilon$ have the same degree-t monomials as a degree-t annihilator of $g + \varepsilon$. It proves the items 2 and 3 in the proposition.

- $\mathcal{D}\mathsf{AN}(f)$**.** The latter condition implies[10], since the dimension of the vector space of homogeneous degree-t $2t$-variable functions is $\binom{2t}{t}$. More precisely, both f and g have a dimension of annihilators of degree at most t of at least $\binom{2t}{t}/2$ by Property 9. Focusing on the vector space V_t of homogeneous functions of degree t, the degree t part of the annihilators of degree at most t of f form a sub-space of dimension at least $\binom{2t}{t}/2$, that we denote $V_t(f)$. The condition of f and g having no annihilator of degree t with the same degree-t part is equivalent to having $V_t(f) \cap V_t(g) = 0$. With f and g with such $\mathcal{D}\mathsf{AN}$, the only possibility is when $V_t(f)$ and $V_t(g)$ are complementary (*i.e.* the direct sum of vector spaces $V_t(f) \oplus V_t(g)$ is equal to V_t). It forces both $\mathcal{D}\mathsf{AN}$ to be exactly $\binom{2t}{t}/2$. It proves the item 1 in the proposition.
- **Resiliency order.** $\mathsf{res}(h) = t-1$ by Definition 14 then from Property 13 item 2, there are two possibilities:
  1. $\min(\mathsf{res}(f), \mathsf{res}(g)) = t-1$.
  2. $\mathsf{res}(f) = \mathsf{res}(g) = t-2$ and $\forall a \in \mathsf{E}_{t-1,2t}$, $\mathsf{W}_f(a) = -\mathsf{W}_g(a)$.

  In the first case, since we proved above that $\mathsf{AI}(f) = \mathsf{AI}(g) = t$, then their resiliency order is at most $t-1$ (see Lemma 2), hence $\mathsf{res}(f) = \mathsf{res}(g) = t-1$ and they both belong to Dahu_{2t}. It corresponds to the case $(4.a)$ of the proposition.

  In the second case, the degree of such functions is upper bounded by $t+1$ (Siegenthaler's bound), and lower bounded by t due to the AI value. Since $\mathsf{deg}(h) = t+1$ (Lemma 13) Property 13 item 3 gives two possibilities:
  a. $\mathsf{deg}(f) = \mathsf{deg}(g) = t+1$ and $\mathsf{deg}(f+g) < t+1$ (case $4.b$ in the proposition).
  b. $\mathsf{deg}(f) = \mathsf{deg}(g) = t$ and $\mathsf{deg}(f+g) = t$ (case $4.c$ in the proposition).
- **Walsh support.** Property 11 allows to derive the constraints on the Wash support of f, g and h. Since $\mathsf{deg}(f) \geq t \geq 2$, f is non constant hence the property gives $2^{\mathsf{res}(f)+2+\lfloor(2t-\mathsf{res}(f)-2)/\mathsf{deg}(f)\rfloor}$ divides $\mathsf{W}_f(a)$. Hence, if both functions have degree t (respectively $t+1$) it gives 2^{t+1} divides $\mathsf{W}_f(a)$ (respectively 2^t) which gives an upper bound of 2^{2t-2} (respectively 2^{2t}) for the cardinality of the Walsh support (following the proof of Lemma 13 item 4). Since the cardinal of the Walsh support is always at most 2^{2t} for a $2t$-variable function, we get an improvement only in the case (b) (*i.e.* case $4.c$ in the proposition). Finally, from Property 13 item 1, by construction $|\mathsf{Wsupp}_{(}h)| \leq 2|\mathsf{Wsupp}_f| + 2|\mathsf{Wsupp}_g|$ and here the upper bound cannot be reached. Since for all $a \in \mathsf{E}_{t-1,2t}$ we saw that $\mathsf{W}_f(a) = -\mathsf{W}_g(a)$, and $\mathsf{E}_{t-1,2t} \cap \mathsf{Wsupp}_f \neq \emptyset$ since $\mathsf{res}(f) = t-2$, using Property 13 item 1 there exists at least one element $b \in \mathsf{E}_{t-1,2t} \cap \mathsf{Wsupp}_f$ hence $(b, 0) \notin \mathsf{Wsupp}_h$ and:

$$|\mathsf{Wsupp}_h| \leq 2|\mathsf{Wsupp}_f| + 2|\mathsf{Wsupp}_g| - 1.$$

  Therefore the case (b) implies $|\mathsf{Wsupp}_f| \leq 2^{2t-2}$, $|\mathsf{Wsupp}_g| \leq 2^{2t-2}$, and $|\mathsf{Wsupp}_h| \leq 2^{2t} - 1$.

□

Note that the existence of a $(2t+1)$-variable dahus shows that two $2t$-variable functions satisfy one of the three possibilities of Proposition 6. For $t = 2$, we remarked that no 5-variable dahu can be obtained from Siegenthaler's construction with two 4-variable dahus, which means that all the elements of Dahu_5 come from the case $4.b.$ or $4.c.$ If such behavior happens to be general, the sufficient conditions could be narrowed to the cases $4.b$ or $4.c$, which would be a next step towards (dis)proving Conjecture 1.

[10] Note that this condition is stronger that the bound proven on the $\mathcal{D}\mathsf{AN}$ of $(2t)$-variables dahus in Lemma 13 $\mathcal{D}\mathsf{AN}(f) = \mathcal{D}\mathsf{AN}(g) = \binom{2t}{t}/2$: either the bound can be reduced to an equality, either some $(2t)$-variables dahus cannot produce $(2t+1)$-variables dahus