# A Note on the Rank Defect Phenomena in The Linearization Attack on Elisabeth-4

Antoine Bak[1,2]

[1] INRIA, Paris, France, antoine.bak@inria.fr
[2] Direction Générale de l'Armement (DGA), Paris, France

**Abstract.** This note gives an explanation for a phenomenon which appeared in the cryptanalysis of the Elisabeth-4 stream cipher, a stream cipher optimized for Torus Fully Homomorphic Encryption (TFHE). This primitive was broken in 2023 by a linearization attack. The authors of this attack made an observation on the rank of the linear system they generated, which was lower than expected. They have provided a partial explanation for it using some properties of the negacyclic lookup tables (NLUT), one of the potential building block of the ciphers optimized for TFHE. NLUTs are defined as functions over integers modulo $2^n$ such that for all $x$, $L(x+2^{n-1}) = -L(x)$. Their explanation of the rank defect of the linear system relies on the observation that the least significant bit of $L(x)$ does not depend on the most significant bit of $x$, which prevents some monomials from appearing in the algebraic normal form (ANF) of the system. In this note, we prove a stronger property of the ANF of NLUTs and use it to give a full proof of their observation on the rank of the system.

**Keywords:** linearization attack · Elisabeth-4 · algebraic normal form

## 1 Introduction

Torus Fully Homomorphic Encryption (TFHE) [CGGI20, CJP21] is a protocol allowing to perform fully homomorphic encryption on modular rings $\mathbb{Z}_t$, and features in particular some programmable bootstrapping (PBS) operations. Those allow to evaluate lookup tables on ring elements homomorphically. In the case where $t = 2t'$ is even, this operation is more efficient for negacyclic lookup tables (NLUT), that is, functions $L\colon \mathbb{Z}_t \to \mathbb{Z}_t$ such that $L(x + t') = -L(x)$. For practical applications, the TFHE protocol may be combined with symmetric primitives optimized for homomorphic evaluation following the *transciphering* framework. This implies that those primitives have to be natively defined over the ring $\mathbb{Z}_t$, and use the lookups allowed by the PBS operation. The first design for TFHE was Elisabeth-4 [CHMS22] and its followups [HMS24]. More recently, a second primitive named FRAST [CCH+24] was defined using some new operations allowed by TFHE, such as double blind rotation.

**Elisabeth-4 cryptanalysis.** The original Elisabeth-4 has been broken in [GHBJR23]. The authors made a linearization attack on the primitive: they wrote a sparse $\mathbb{F}_2$-linear system on some monomials depending on the key and solved it using the block Wiedermann algorithm [Wie86]. They also made an observation on the rank of the linear system they had to solve which was lower than expected. In an attempt to provide a formal proof for this phenomenon, they defined a family of functions named *Antler* whose properties are related to the rank of the system they have to solve. This allowed them to provide a partial explanation for the rank defect of their system in [GHBJR23, Appendix C].

**Our contribution.** In this work, we study the algebraic normal form (ANF) of NLUTs and give a characterization of them in Lemma 2. Using a known result on the algebraic properties of linear addition [BS05, HY24], we first give a simpler proof of the original bound from [GHBJR23]. Then, we use the property we identified on the ANF of NLUTs to give a full explanation for the rank defect.

**Outline.** The notations used in the paper, as well as the results on the ANF of NLUTs and modular addition are provided in Section 2. We give our proof of the original bound from Gilbert et al. in Section 3. Then, we give a full explanation for the rank defect in Section 4, before concluding in Section 5.

# 2 Preliminaries

## 2.1 Notations

In this paper, we denote the addition over the ring $\mathbb{Z}_{2^n}$ of the integers modulo $2^n$ by $\boxplus$. We denote the xor operation over the finite field $\mathbb{F}_2$ by $\oplus$. In the whole article, the element $x \in \mathbb{Z}_{2^n}$ is identified with $(x_n, \dots, x_1) \in \mathbb{F}_2^n$ using big endian notation. For $u \in \mathbb{Z}_{2^n}$, we denote by $x^u$ the monomial $\prod_{i=1}^{n} x_i^{u_i}$. We also denote by $[N]$ the interval $\{0, \dots, N-1\}$.

We recall the definition of negacyclic lookup tables over $\mathbb{Z}_{2^n}$, as they play an important role in TFHE.

**Definition 1** (Negacyclic lookup table (NLUT))**.** Let $L\colon \mathbb{Z}_{2^n} \to \mathbb{Z}_{2^n}$, we say that $L$ is a *Negacyclic LookUp Table* if for all $x \in \mathbb{Z}_{2^n}$, we have that

$$L(x \boxplus 2^{n-1}) = \boxminus L(x) \ .$$

In the following, as in [GHBJR23] we let $L_1, L_2, L_3$ be three NLUTs and denote by Antler the function $\mathrm{Antler}(x, y, z) = \mathrm{LSB} \circ L_3(L_1(x) \boxplus L_2(y) \boxplus z)$, where LSB is the least significant bit function. We denote $\tilde{x} = L_1(x)$ and $\tilde{y} = L_2(y)$. We denote by Span(Antler) the $\mathbb{F}_2$-vector space spanned by Antler functions when $L_1, L_2, L_3$ are arbitrary NLUTS.

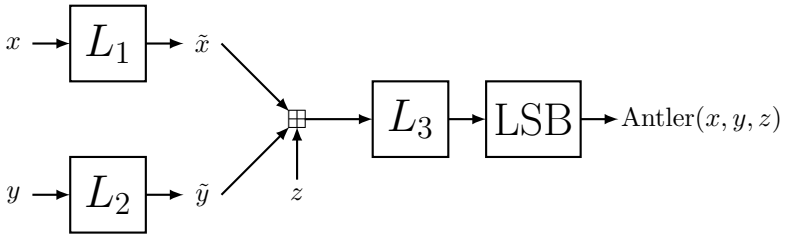


**Figure 1:** An Antler function.

## 2.2 Results on algebraic normal forms

We recall an important lemma in the study of ciphers combining modular addition over $\mathbb{Z}_{2^n}$ with nonlinear Boolean functions. A proof of the following result can be found in [HY24].

**Lemma 1** (Algebraic normal form and modular addition [BS05, HY24])**.** *Let $z = x \boxplus y$, we have that the monomial $x^u \cdot y^v$ is in the algebraic normal form of $z^w$ if and only if $u + v = w$ (without reduction modulo $2^n$).*

We prove the following lemma about the structure of NLUTs seen as Boolean functions.

**Lemma 2** (Algebraic normal form of an NLUT)**.** *Let $L\colon \mathbb{Z}_{2^n} \to \mathbb{Z}_{2^n}$ a NLUT, then, there exist $f_1, \dots, f_n\colon \mathbb{F}_2^{n-1} \to \mathbb{F}_2$ such that the algebraic normal form of the $i$-th component of $y = L(x)$ as a Boolean function has the following form:*

$$y_i = f_i(x_1, \dots, x_{n-1}) \oplus x_n \cdot \left(1 \oplus \prod_{k=1}^{i-1} (1 \oplus y_k)\right) .$$

*In the case $i = 1$, we use the convention that the product over the empty set is 1, and get $y_1 = f_1(x_1, \dots, x_{n-1})$.*

The intuition behind this lemma is that adding $2^{n-1}$ to $x$ is equivalent to flipping the value of $x_n$. In particular, we know that the $i$-th bit of $\boxminus y$ is the same as the $i$-th bit of $y$ only if the $i-1$ bits of lowest weight of $y$ equal 0. Combining those two observations allows us to study the influence of $x_n$ on the $i$-th bit of $y = L(x)$, and to deduce conditions on the algebraic normal form of $L$ for it to be negacyclic.

*Proof.* We denote by $L_{\restriction [2^{n-1}]}\colon \mathbb{F}_2^{n-1} \to \mathbb{F}_2^n$ the restriction of $L$ to the integers smaller than $2^{n-1}$. We let $f_i$ the $i$-th component of this function. In particular, $f_i(x_1, \dots, x_{n-1}) = y_i(x_1, \dots, x_{n-1}, 0)$.

For all $x \in [2^{n-1}]$, we know that $L(x \boxplus 2^{n-1}) = \boxminus L(x)$. The value of the $i$-th bit of $\boxminus L(x)$ (which equals $y_i(x_1 \dots x_{n-1}, 1)$) differs from the one of $L(x)$, except when $L(x) = 0 \pmod{2^i}$, that is $y_1 = \dots = y_{i-1} = 0$.

As $y_i(x_1, \dots, x_{n-1}, 0) \oplus y_i(x_1, \dots, x_{n-1}, 1) = 0$ if and only if $y_1 = \dots = y_{i-1} = 0$ we have that $y_i = f_i(x_1, \dots, x_{n-1}) \oplus x_n \cdot \left(1 \oplus \prod_{k=1}^{i-1}(1 \oplus y_k)\right)$. □

In particular, the least significant bit $y_1$ only depends on $x_1, \dots, x_{n-1}$, which was already proven in [GHBJR23] and used to deduce a first bound on the rank of the space of Antler functions. Our result shows that the second most significant bit of $y$ has the form $y_2 = f_2(x_1, \dots, x_{n-1}) \oplus x_n f_1(x_1, \dots, x_{n-1})$. This fact will be used in Section 4 to explain the rank defect.

## 3 Monomials present in an Antler function

We start by proving the following result, which only relies on the observation that the least significant bit of an NLUT does not depend on the most significant bit of its input. This result is very close to the upper bounds derived in the case $n = 4$ in [GHBJR23]. We provide in this section a generalization of this result to any $n \geq 3$, along with a more compact proof thanks to Lemma 1.

**Theorem 1** (Monomials in the ANF of Antler functions)**.** *Let $n \geq 3$, the monomials contained in the ANF of an Antler function can only be of the following forms:*

1. $z^{2^{n-1}-1}$,
2. $z^{2^{n-1}-2}x^u$, $z^{2^{n-1}-2}y^v$ $(0 \leq u, v < 2^{n-1})$,
3. $z^{2^{n-1}-3}x^u y^v$ $(0 < u, v < 2^{n-1})$, $z^{2^{n-1}-3}x^u$, $z^{2^{n-1}-3}y^v$ $(0 \leq u, v < 2^n)$,
4. $z^{2^{n-1}-4}x_n x^u y^v$, $z^{2^{n-1}-4}x^u y_n y^v$, $z^{2^{n-1}-4}x^u y^v$ $(0 \leq u, v < 2^{n-1})$, *or*
5. $z^w x^u y^v$ $(0 \leq w \leq 2^{n-1} - 5,\ 0 \leq u, v < 2^n)$.

*Proof.* Using the case $i = 1$ of Lemma 2, we know that $\mathrm{LSB} \circ L_3$ does not depend on the most significant bit of its input. Thus, the ANF of $\mathrm{LSB} \circ L_3(x)$ can only contain monomials of the form $x^u$ where $0 \leq u < 2^{n-1}$. Applying Lemma 1 to $\mathrm{Antler}(x, y, z) = \mathrm{LSB} \circ L_3(\tilde{x} \boxplus \tilde{y} \boxplus z)$, we get that its ANF can only contain monomials of the form $z^w \tilde{x}^u \tilde{y}^v$, where $0 \leq u + v + w < 2^{n-1}$. Hence for some values of $w$, the values of $u, v$ are constrained. Moreover, the monomial $\tilde{x}^1$ (resp. $\tilde{y}^1$) corresponds to the least significant bit of $L_1(x)$ (resp. $L_2(y)$) and thus, does not depend on $x_n$ (resp. $y_n$).

Using these two observations, we can prove the theorem:

1. Let $w = 2^{n-1} - 1$, then $u + v \leq 0$ and we can only have the monomial $z^{2^{n-1}-1}$.
2. Let $w = 2^{n-1} - 2$, then $u + v \leq 1$, we have either $z^{2^{n-1}-2}\tilde{x}^1$ or $z^{2^{n-1}-2}\tilde{y}^1$. Those terms do not depend on $x_n, y_n$, and thus this variable does not appear in their ANF.
3. Let $w = 2^{n-1}-3$, then $u+v \leq 2$ and either $u, v \leq 1$, $u = 2, v = 0$ or $u = 0, v = 2$. The first case corresponds to the $z^{2^{n-1}-3}x^u y^v$ terms, while the last two cases correspond to the $z^{2^{n-1}-3}x^u$, $z^{2^{n-1}-3}y^v$ terms.
4. Let $w = 2^{n-1} - 4$, then $u + v \leq 3$ and we cannot have terms of the form $z^{2^{n-1}-4}\tilde{x}^u\tilde{y}^v$ with $u, v \geq 2$. As a consequence, we do not have monomials of the form $z^{2^{n-1}-4}x_n x^u y_n u^v$.

□

Using those conditions on the monomials in the algebraic normal form, we get the following corollary:

**Corollary 1.** *Let $n \geq 3$, the number of monomials in an Antler function is at most*

$$2^{3n-1} - 3 \cdot 2^{2n} + 2^{n+1} \ .$$

*Proof.* A simple enumeration of all possible cases from Theorem 1 gives:

1. 1 monomial for $z^{2^{n-1}-1}$,
2. $2 \cdot 2^{n-1} - 1$ monomials for $z^{2^{n-1}-2}x^u$, $z^{2^{n-1}-2}y^v$ $(0 \leq u, v < 2^{n-1})$,
3. $(2^{n-1} - 1)^2$ monomials for $z^{2^{n-1}-3}x^u y^v$ $(0 < u, v < 2^{n-1})$, and $2 \cdot 2^n - 1$ monomials for $z^{2^{n-1}-3}x^u$, $z^{2^{n-1}-3}y^v$ $(0 \leq u, v < 2^n)$,
4. $3 \cdot 2^{2n-2}$ monomials for $z^{2^{n-1}-4}x_n x^u y^v$, $z^{2^{n-1}-4}x^u y_n y^v$, $z^{2^{n-1}-4}x^u y^v$ $(0 \leq u, v < 2^{n-1})$, and
5. $2^{2n}(2^{n-1} - 4)$ monomials for $z^w x^u y^v$ $(0 \leq w \leq 2^{n-1} - 5,\ 0 \leq u, v < 2^n)$.

By taking the sum over all cases, we get at most:

$$1 + (2 \cdot 2^{n-1} - 1) + (2^{n-1} - 1)^2 + (2 \cdot 2^n - 1) + 3 \cdot 2^{2n-2} + 2^{2n}(2^{n-1} - 4) = 2^{3n-1} - 3 \cdot 2^{2n} + 2^{n+1}$$

monomials. □

We checked experimentally[1] for $n = 3, 4$ that this upper bound corresponds to the actual number of monomials in the Antler function. This bound gives 80 monomials for $n = 3$ and 1312 monomials for $n = 4$.

[1] https://github.com/AntoineBak/Elisabeth4-rank-defect

# 4 Explaining the rank defect phenomena

We prove in this section the results observed in [GHBJR23] on the rank of the space of Antler functions. The proof crucially relies on Lemma 2, as the second most significant bit $\tilde{x}_2$ is related to its least significant bit $\tilde{x}_1$ through the relation $\tilde{x}_2 = f_2(x_1, \dots, x_{n-1}) \oplus x_n \tilde{x}_1$. As a consequence, we will see that among the monomials identified in Theorem 1, some of them can only appear at the same time. This means that Span(Antler) admits a nontrivial but smaller basis than explained simply by the constraints of Theorem 1.

**Theorem 2** (Rank of the space of Antler functions)**.** *The rank of the space of Antler functions equals:*

- 56 *when* $n = 3$,
- 1088 *when* $n = 4$.

In the following proofs, we give an explicit basis of Span(Antler) and use it to deduce its dimension.

### Case n=3

*Proof.* The grouping of the monomials from Theorem 1 that implies a rank defect is as follows:

- $(z_2 \oplus z_1 x_3)x^u$, $(z_2 \oplus z_1 y_3)y^v$ for $0 < u, v < 4$,
- $(x_3 \oplus y_3 \oplus z_1)x^u y^v$ for $0 < u, v < 4$, and
- the other monomials are not necessarily grouped in the ANF of Antler.

Indeed, let a monomial of the form $z_2 x^u, u > 0$ in the algebraic normal form of the Antler function, then this monomial can only come from a $z^2\tilde{x}^1 = z_2 f_1^{(x)}(x_1, x_2)$ term. Other terms of weight 3 must be in the algebraic normal form, and in particular the term $z^1\tilde{x}^2 = z_1(f_2^{(x)}(x_1, x_2) \oplus x_3 f_1^{(x)}(x_1, x_2))$ imply the presence of $z_1 x_3 f_1^{(x)}(x_1, x_2)$. Hence the $z_2 x^u$ terms are grouped with $z_1 x_3 x^u$, and we get $(z_2 \oplus z_1 x_3)x^u$ in the basis. The same argument goes for $y$.

In the second case, a term $z_1 x^u y^v, u, v > 0$ implies a $z^1\tilde{x}^1\tilde{y}^1 = z_1 f_1^{(x)}(x_1, x_2) f_1^{(y)}(y_1, y_2)$ term. As this term is of weight 3, there must also be terms corresponding to

$$\tilde{x}^2\tilde{y}^1 = (f_2^{(x)}(x_1, x_2) \oplus x_3 f_1^{(x)}(x_1, x_2)) f_1^{(y)}(y_1, y_2)$$

and

$$\tilde{x}^1\tilde{y}^2 = f_1^{(x)}(x_1, x_2)(f_2^{(y)}(y_1, y_2) \oplus y_3 f_1^{(y)}(y_1, y_2)) \ .$$

Hence the only monomials of the form $z_1 x^u y^v, u, v > 0$ can come from $(x_3 \oplus y_3 \oplus z_1) f_1^{(x)}(x_1, x_2) f_1^{(y)}(y_1, y_2)$.

Counting the number of vectors in this basis gives rank $80 - 2 \cdot 3 - 2 \cdot 3^2 = 56$.

□

### Case n=4

*Proof.* The grouping of the monomials from Theorem 1 that implies a rank defect is as follows:

- $z_3(z_2 \oplus z_1 x_4)x^u$, $z_3(z_2 \oplus z_1 y_4)y^v$ for $0 < u, v < 8$,
- $(z_3 \oplus z_2 x_4 y_4)x^u y^v$ for $0 < u, v < 8$,

- $(z_3 \oplus z_2z_1x_4)x^uy^v$, $(z_3 \oplus z_2z_1y_4)x^uy^v$ for $0 < u, v < 8$,
- $y_4(z_3 \oplus z_2z_1x_4)x^u$, $x_4(z_3 \oplus z_2z_1y_4)y^v$ for $0 < u, v < 8$,
- $(z_3z_1 \oplus z_3x_4 \oplus z_3y_4 \oplus z_2z_1x_4y_4)x^uy^v$ for $0 < u, v < 8$, and
- the other monomials are not necessarily grouped in the ANF of Antler.

We explain in the following where those terms come from:

- $z_3(z_2 \oplus z_1x_4)x^u, 0 < u < 8$: a term $z_3z_2x^u$ can only come from $z^6\tilde{x}^1$, which is present if and only if $z^5\tilde{x}^2$ is present. On the other hand, $z_3z_1x_4x^u$ can only come from $z^5\tilde{x}^2$. As $z^6\tilde{x}^1 \oplus z^5\tilde{x}^2 = z_3(z_2f_1^{(x)} \oplus z_1(x_4f_1^{(x)} \oplus f_2^{(x)})) = z_3(z_2 \oplus x_4z_1)f_1^{(x)} \oplus z_3z_1f_2^{(x)}$, the coefficients in front of $z_3z_2x_4x^u$ and $z_3z_1x_4x^u$ are necessarily the same. The case of $z_3(z_2 \oplus z_1y_4)y^v$ is analogous.
- The term of degree 7 of $L_3$ contains the following sum. The terms in **bold** are the ones corresponding to the basis we described at the start of the proof:

$$
\begin{aligned}
&z^5\tilde{x}^1\tilde{y}^1 \oplus z^4\tilde{x}^2\tilde{y}^1 \oplus z^4\tilde{x}^1\tilde{y}^2 \oplus z^3\tilde{x}^2\tilde{y}^2\\
=&(z_3z_1 \oplus z_3x_4 \oplus z_3y_4 \oplus z_2z_1x_4y_4)f_1^{(x)}f_1^{(y)} \oplus (z_3 \oplus z_2z_1x_4)f_1^{(x)}f_2^{(y)}\\
&\oplus (z_3 \oplus z_2z_1y_4)f_2^{(x)}f_1^{(y)} \oplus z_2z_1f_2^{(x)}f_2^{(y)}\\
=&(\mathbf{z_3z_1 \oplus z_3x_4 \oplus z_3y_4 \oplus z_2z_1x_4y_4})(\mathbf{f_1^{(x)} \oplus f_1^{(x)}(0)})(\mathbf{f_1^{(y)} \oplus f_1^{(y)}(0)})\\
&\oplus (\mathbf{z_3 \oplus z_2z_1x_4})\mathbf{f_1^{(x)}f_2^{(y)}} \oplus (\mathbf{z_3 \oplus z_2z_1y_4})\mathbf{f_2^{(x)}f_1^{(y)}}\\
&\oplus \mathbf{y_4}(\mathbf{z_3 \oplus z_2z_1x_4})(\mathbf{f_1^{(x)} \oplus f_1^{(x)}(0)})\mathbf{f_1^{(y)}(0)}\\
&\oplus \mathbf{x_4}(\mathbf{z_3 \oplus z_2z_1y_4})\mathbf{f_1^{(x)}(0)}(\mathbf{f_1^{(y)} \oplus f_1^{(y)}(0)})\\
&\oplus z_2z_1f_2^{(x)}f_2^{(y)} \oplus (z_3z_1 \oplus z_3x_4)(f_1^{(x)} \oplus f_1^{(x)}(0))f_1^{(y)}(0)\\
&\oplus (z_3z_1 \oplus z_3y_4)f_1^{(x)}(0)(f_1^{(y)} \oplus f_1^{(y)}(0))\\
&\oplus (z_3z_1 \oplus z_3x_4 \oplus z_3y_4 \oplus z_2z_1x_4y_4)f_1^{(x)}(0)f_1^{(y)}(0)\ ,
\end{aligned}
$$

  where we replaced $f_1^{(x)}$ (resp. $f_1^{(y)}$) with $f_1^{(x)} \oplus f_1^{(x)}(0) \oplus f_1^{(x)}(0)$ (resp.$f_1^{(y)} \oplus f_1^{(y)}(0) \oplus f_1^{(y)}(0)$) to obtain the terms in $y_4(z_3 \oplus z_2z_1x_4)x^u$ (resp. $x_4(z_3 \oplus z_2z_1y_4)y^v$). As terms in $z_3z_1x^uy^v, 0 < u, v < 8$, $z_2z_1x_4y_4x^uy^v, z_3y_4x^uy^v, 0 \leq v < 8, 0 < u < 8$ and $z_2z_1x_4y_4x^uy^v, z_3x_4x^uy^v, 0 \leq u < 8, 0 < v < 8$ can only come from degree 7 terms in $L_3$, this explains where the terms in $(z_3z_1 \oplus z_3x_4 \oplus z_3y_4 \oplus z_2z_1x_4y_4)x^uy^v, y_4(z_3 \oplus z_2z_1x_4)x^u, x_4(z_3 \oplus z_2z_1y_4)y^v, 0 < u, v < 8$ come from.
- The only terms left all contain a $z_3x^uy^v$ monomial with $0 < u, v < 8$. Such a monomial can only come from $z^4\tilde{x}^2\tilde{y}^1, z^4\tilde{x}^1\tilde{y}^2, z^4\tilde{x}^1\tilde{y}^1$. The cases of $z^4\tilde{x}^2\tilde{y}^1$ and $z^4\tilde{x}^1\tilde{y}^2$ have already been treated and imply the presence of the $(z_3 \oplus z_2z_1x_4)x^uy^v$, $(z_3 \oplus z_2z_1y_4)x^uy^v$ terms. The term $z^4\tilde{x}^1\tilde{y}^1$ is of weight 6, and hence is present if and only if $z^3\tilde{x}^2\tilde{y}^1, z^3\tilde{x}^1\tilde{y}^2, z^2\tilde{x}^2\tilde{y}^2$ are present. As:

$$
\begin{aligned}
&z^4\tilde{x}^1\tilde{y}^1 \oplus z^3\tilde{x}^2\tilde{y}^1 \oplus z^3\tilde{x}^1\tilde{y}^2 \oplus z^2\tilde{x}^2\tilde{y}^2\\
=&z_3f_1^{(x)}f_1^{(y)} \oplus z_2z_1(x_4f_1^{(x)} \oplus f_2^{(x)})f_1^{(y)} \oplus z_2z_1f_1^{(x)}(y_4f_1^{(y)} \oplus f_2^{(y)})\\
&\oplus z_2(x_4f_1^{(x)} \oplus f_2^{(x)})(y_4f_1^{(y)} \oplus f_2^{(y)})\\
=&(\mathbf{z_3 \oplus z_2z_1x_4 \oplus z_2z_1y_4 \oplus z_2x_4y_4})\mathbf{f_1^{(x)}f_1^{(y)}}\\
&\oplus z_2(z_1 \oplus x_4)f_1^{(x)}f_2^{(y)} \oplus z_2(z_1 \oplus y_4)f_2^{(x)}f_1^{(y)} \oplus z_2f_2^{(x)}f_2^{(y)}
\end{aligned}
$$

we have terms in $(z_3 \oplus z_2 z_1 x_4 \oplus z_2 z_1 y_4 \oplus z_2 x_4 y_4) x^u y^v$. In the weight 7 sum, we found $(z_3 \oplus z_2 z_1 x_4) f_1^{(x)} f_2^{(y)}$ and $(z_3 \oplus z_2 z_1 y_4) f_2^{(x)} f_1^{(y)}$ terms, where $f_1^{(x)} f_2^{(y)}$ and $f_2^{(x)} f_1^{(y)}$ are a priori independent from $f_1^{(x)} f_1^{(y)}$. Hence we only get polynomials of the form $(z_3 \oplus z_2 z_1 x_4) x^u y^v, (z_3 \oplus z_2 z_1 y_4) x^u y^v, (z_3 \oplus z_2 x_4 y_4) x^u y^v, 0 < u, v < 8$ in the basis.

Using Theorem 1, we get at most 1312 monomials in the algebraic normal form. Moreover, counting the ones that are grouped gives the following upper bound for the dimension of Span(Antler):

$$1312 - 2 \cdot 7 - 7^2 - 2 \cdot 7 - 3 \cdot 7^2 = 1088$$

which corresponds to the dimension observed experimentally.

□

## 5 Conclusion

Negacyclicity being a strong property for a lookup table, it is not that surprising that we find meaningful structures in its algebraic normal form. In this note, we provided a deeper understanding of those, which allowed us to prove a conjecture by Gilbert et al. [GHBJR23].

## Acknowledgment

This work is funded in part by the ERC grant ReSCALE (number 101041545), and by the French DGA. We also thank Léo Perrin for proof-reading a first draft of this note.

## References

[BS05] An Braeken and Igor Semaev. The ANF of the composition of addition and multiplication mod $2^n$ with a Boolean function. In Henri Gilbert and Helena Handschuh, editors, *FSE 2005*, volume 3557 of *LNCS*, pages 112–125, Paris, France, February 21–23, 2005. Springer Berlin Heidelberg, Germany.

[CCH+24] Mingyu Cho, Woohyuk Chung, Jincheol Ha, Jooyoung Lee, Eun-Gyeol Oh, and Mincheol Son. FRAST: TFHE-friendly cipher based on random S-boxes. *IACR Transactions on Symmetric Cryptology*, 2024(3):1–43, 2024.

[CGGI20] Ilaria Chillotti, Nicolas Gama, Mariya Georgieva, and Malika Izabachène. TFHE: fast fully homomorphic encryption over the torus. *Journal of Cryptology*, 33(1):34–91, 2020.

[CHMS22] Orel Cosseron, Clément Hoffmann, Pierrick Méaux, and François-Xavier Standaert. Towards case-optimized hybrid homomorphic encryption. In Shweta Agrawal and Dongdai Lin, editors, *Advances in Cryptology – ASIACRYPT 2022*, pages 32–67, Cham, 2022. Springer Nature Switzerland.

[CJP21] Ilaria Chillotti, Marc Joye, and Pascal Paillier. Programmable bootstrapping enables efficient homomorphic inference of deep neural networks. In *Cyber Security Cryptography and Machine Learning: 5th International Symposium, CSCML 2021, Be'er Sheva, Israel, July 8–9, 2021, Proceedings 5*, pages 1–19. Springer, 2021.

[GHBJR23] Henri Gilbert, Rachelle Heim Boissier, Jérémy Jean, and Jean-René Reinhard. Cryptanalysis of Elisabeth-4. In Jian Guo and Ron Steinfeld, editors, *Advances in Cryptology – ASIACRYPT 2023*, pages 256–284, Singapore, 2023. Springer Nature Singapore.

[HMS24] Clément Hoffmann, Pierrick Méaux, and François-Xavier Standaert. The patching landscape of Elisabeth-4 and the mixed filter permutator paradigm. In Anupam Chattopadhyay, Shivam Bhasin, Stjepan Picek, and Chester Rebeiro, editors, *Progress in Cryptology – INDOCRYPT 2023*, pages 134–156, Cham, 2024. Springer Nature Switzerland.

[HY24] Kai Hu and Trevor Yap. Perfect monomial prediction for modular addition. *IACR Transactions on Symmetric Cryptology*, 2024(3):177–199, Sep. 2024.

[Wie86] Douglas Wiedemann. Solving sparse linear equations over finite fields. *IEEE transactions on information theory*, 32(1):54–62, 1986.