A Note on Anemoi Gröbner Bases

Pierre Briaud

Simula UiB, Bergen, Norway
pierre@simula.no

Abstract. Recently, [KLR24,BBL$^+$24] proposed two algebraic attacks on the Anemoi permutation [BBC$^+$23]. In this note, we construct a Gröbner basis for the ideal generated by the naive modeling of the CICO problem associated to Anemoi, in odd and in even characteristics, for one and several branches. We also infer the degree of the ideal from this Gröbner basis, while previous works relied on upper bounds [BBC$^+$23,KLR24,BBL$^+$24].

1 Introduction

In this note, we focus on algebraic techniques to solve the following version of the CICO problem [BDPV11].

Problem 1 (Constrained Input Constrained Output) *Given a permutation $P : \mathbb{F}_q^\ell \times \mathbb{F}_q^\ell \to \mathbb{F}_q^\ell \times \mathbb{F}_q^\ell$, the CICO problem consists in finding a pair $(y_{in}, y_{out}) \in \mathbb{F}_q^\ell \times \mathbb{F}_q^\ell$ such that $P(\mathbf{0}_\ell, y_{in}) = (\mathbf{0}_\ell, y_{out})$.*

1.1 Polynomial system solving

We refer to [CLO15] for notions related to Gröbner bases. We will mostly use the following definitions and results.

Definition 1. *Let $\prec$ be a monomial order on a polynomial ring R, let $f,\ g \in R$ be two non-zero polynomials and let $\mu \overset{def}{=} lcm(LM_\prec(f), LM_\prec(g))$. The S-polynomial of the polynomial pair $\{f, g\}$ with respect to $\prec$ is defined as*

$$S(f,g) \overset{def}{=} LC_\prec(g)\frac{\mu}{LM_\prec(f)}f - LC_\prec(f)\frac{\mu}{LM_\prec(g)}g.$$

Theorem 1 (Buchberger's first criterion, Theorem 6 p. 86, [CLO15]). *Let $I = \langle \mathcal{G} \rangle$ be an ideal of R. The set $\mathcal{G} = \{g_1, \ldots, g_\ell\}$ is a Gröbner basis of I if and only if for all $1 \le i < j \le \ell$, the S-polynomial $S(g_i, g_j)$ reduces to 0 modulo $\mathcal{G}$ (regardless of the order of the elements).*

Proposition 1 (Buchberger's second criterion, Prop. 4 p. 106, [CLO15]). *Let $\mathcal{G}$ be a finite set of polynomials in R and let $f,\ g \in \mathcal{G}$ whose leading monomials are coprime. Then, the S-polynomial $S(f, g)$ reduces to 0 modulo $\mathcal{G}$.*

Proposition 1 is known to be instrumental in the context of algebraic cryptanalysis of symmetric schemes [BPW06]. It was recently used in the cryptanalysis of several "arithmetization-oriented" primitives [BBL$^+$24,Ste24a,Ste24b].

1.2 Algebraic modelings of Anemoi

We refer to [BBC$^+$23] for a complete description of the Anemoi permutation. In this section, we detail its building blocks when the input is in $\mathbb{F}_q^2$. We denote the linear layer by $\mathcal{M}(x, y) = (2x+y, x+y)$ and the round constants by (c_i, d_i) for $i \in \{0..n-1\}$, where n is the number of rounds. The S-box components correspond to univariate polynomials $Q_\gamma(X)$, $Q_\delta(X)$ and X^α whose expression depends on the characteristic of the field. Using these notations, the naive modeling of the CICO problem adopted in [BBC$^+$23] is

Modeling 1 *We call $\mathcal{F}_{CICO}$ the system $\{f_0, g_0, \ldots, f_{n-1}, g_{n-1}, x_0, x_n\}$ in the polynomial ring $\mathbb{F}_q[x_0, y_0, \ldots, x_n, y_n]$, with*

$$\begin{cases} f_i & \overset{def}{=} (x_i + y_i + c_i + d_i - y_{i+1})^\alpha + Q_\gamma(x_i + y_i + c_i + d_i) \\ & - (2x_i + y_i + 2c_i + d_i), \\ g_i & \overset{def}{=} (x_i + y_i + c_i + d_i - y_{i+1})^\alpha + Q_\delta(y_{i+1}) - x_{i+1}. \end{cases}$$

Another basis for the $\langle \mathcal{F}_{CICO} \rangle$ ideal is $\{f_0, h_0, \ldots, f_{n-1}, h_{n-1}, x_0, x_n\}$, where

$$h_i \overset{def}{=} f_i - g_i = Q_\gamma(x_i + y_i + c_i + d_i) - (2x_i + y_i + 2c_i + d_i) - Q_\delta(y_{i+1}) + x_{i+1}.$$

In odd characteristic, the degree of $\langle \mathcal{F}_{\text{CICO}} \rangle$ was conjectured to be $(\alpha + 2)^n$ [BBC$^+$23, Conjecture 2 p. 34]. In even characteristic, this degree seems to correspond to a Bézout bound, applied to the generating set $\{f_0, h_0, \ldots, f_{n-1}, h_{n-1}\}$ in $\mathbb{F}_q[y_0, x_1, \ldots, x_{n-1}, y_{n-1}, y_n]$. The initial analysis also considers another modeling called $\mathcal{P}_{\text{CICO}}$. The $\mathcal{P}_{\text{CICO}}$ equations were later exploited in [BBL$^+$24] and [KLR24] to obtain more efficient attacks. There, the complexity of solving $\mathcal{P}_{\text{CICO}}$ was estimated to be the one of the change of ordering to produce a lexicographical Gröbner basis. The cost of this step is polynomial in the degree of the ideal.

1.3 Related works

Previous cryptanalysis of Anemoi. We briefly detail the content of [KLR24] and [BBL$^+$24] which is relevant for our purposes. In particular, we do not describe the contributions of [BBL$^+$24] that affect other schemes than Anemoi.

The point of [KLR24] was to provide sharper bounds on the degree of the ideal $\langle \mathcal{P}_{\text{CICO}} \rangle$. Their results follow from a clever use of the multihomogeneous Bézout bound, already employed by Faugère and Perret in the cryptographic context [BGL20]. The final estimate derived from such bounds assumes a change of order algorithm relying on fast linear algebra techniques [FM11,FGHR14].

The approach of [BBL$^+$24] was to build a polynomial system that is already a Gröbner basis for a suitable monomial order, thanks to Proposition 1. Such a Gröbner basis is referred to as *FreeLunch* and it has leading terms which are simply univariate. This technique is applied to various ciphers, in particular Anemoi. In this case, the authors cannot construct a FreeLunch Gröbner basis for $\langle \mathcal{P}_{\text{CICO}} \rangle$ but they can derive one for a subideal which is enough for their purposes. In turn they can obtain its degree, which is just slightly bigger than $(\alpha + 2)^n$. Finally, another key contribution of [BBL+24] is a change of order algorithm taylored to FreeLunch Gröbner bases. In the same way as the recent [BNSED22], this algorithm relies on linear algebra over polynomial matrices. This algorithm works very well when the input FreeLunch Gröbner basis contains one polynomial of very large degree. An efficient implementation is also provided.

Cryptanalysis of other schemes. Recently, Steiner showed that for well-chosen weighted orders, Gröbner bases for Rescue-XLIX [SAD20] and Poseidon [GKR+21] could be found simply by performing linear transformations [Ste24a,Ste24b].

1.4 Contribution

We show how to cheaply obtain Gröbner bases for polynomial modelings of the CICO problem on the Anemoi permutation derived from $\langle \mathcal{F}_{\text{CICO}} \rangle$. We consider cases that have not been studied in [KLR24,BBL+24], i.e., the even characteristic case and a larger number of branches.

From our Gröbner bases we can deduce the degree of the ideal, which allows us to improve the results of [KLR24] based on the multihomogeneous Bézout bound (here, we obtain the exact value). Even though these Gröbner bases are easier to produce than the FreeLunch ones of [BBL+24] and even if the ideal degree is smaller (as we consider the entire ideal), it is unclear whether the standard zero-dimensional solving method based on such Gröbner bases will yield better results. In addition to the efficient custom algorithm of [BBL+24], we note that FreeLunch Gröbner bases have a more lex-like shape.

2 Anemoi in odd characteristic when $\ell = 1$

Let q be a prime and let g be a generator of the multiplicative subgroup of $\mathbb{F}_q$. In odd characteristic, the S-box components are $Q_\gamma(X) = gX^2 + g^{-1}$, $Q_\delta(X) = gX^2$ and a monomial X^α such that the map $x \mapsto x^\alpha$ is a permutation. We start by rewriting the polynomials of Modeling 1:

$$\begin{aligned} f_i &= (x_i + y_i + c_i + d_i - y_{i+1})^\alpha + Q_\gamma(x_i + y_i + c_i + d_i) - (2x_i + y_i + 2c_i + d_i), \\ h_i &= f_i - g_i = Q_\gamma(x_i + y_i + c_i + d_i) - (2x_i + y_i + 2c_i + d_i) - Q_\delta(y_{i+1}) + x_{i+1}. \end{aligned}$$

Their shape suggests to adopt the change of variables

$$\begin{cases} X_i \overset{def}{=} x_i + y_i + c_i + d_i - y_{i+1} = -y_{i+1} + y_i + x_i + C_i \\ Y_i \overset{def}{=} x_i + y_i + c_i + d_i + y_{i+1} = y_{i+1} + y_i + x_i + C_i \end{cases}, \tag{1}$$

where $C_i \overset{def}{=} c_i + d_i$ for $i \in \{0..n-1\}$. Recalling that the two last equations in $\mathcal{F}_{\text{CICO}}$ correspond to fixing x_0 and x_n to zero, we can undo this change of variables by $y_0 = \frac{X_0+Y_0}{2} - C_0$, $y_{i+1} = \frac{Y_i - X_i}{2}$ and for $i \in \{0..n-2\}$:

$$\begin{aligned} x_{i+1} &= X_{i+1} + y_{i+2} - y_{i+1} - C_{i+1} \\ &= X_{i+1} + \frac{Y_{i+1} - X_{i+1}}{2} - \frac{Y_i - X_i}{2} - C_{i+1} \\ &= -\frac{1}{2}X_{i+1} + \frac{1}{2}Y_{i+1} + \frac{1}{2}X_i - \frac{1}{2}Y_i - C_{i+1}. \end{aligned}$$

Modeling 2 *We consider Modeling 1 with the change of variables given by Equation* (1)*, in the polynomial ring* $\mathbb{F}_q[X_0, \ldots, X_{n-1}, Y_0, \ldots, Y_{n-1}]$.

We can write

$$\begin{cases} f_i &= X_i^\alpha + g\left(\frac{X_i+Y_i}{2}\right)^2 + L_i(Y_i - X_i) + a_i \\ h_i &= gX_iY_i + M_i(Y_i - X_i) + b_i, \end{cases} \tag{2}$$

where $L_i,\ M_i$ are constants in $\mathbb{F}_q$ that we will not need to specify and where $a_i,\ b_i$ are degree 1 affine polynomials not involving X_i nor Y_i.

Gröbner basis of Modeling 2. For some appropriate monomial orders, the point is that we can obtain a Gröbner basis of Modeling 2 at a very low cost. We stress that this fact has already been observed on other schemes. As in [BBL$^+$24,Ste24a,Ste24b], we will consider a weighted ordering. However, its definition is not as contrived. Indeed, we do not necessarily look for a Gröbner basis with univariate, coprime leading terms as in [BBL$^+$24] and we also do not limit ourselves to applying linear transformations as in [Ste24a,Ste24b] (note that our change of variables can already be seen as a first linear transformation).

Ordering 1 *We denote by* $\prec$ *the weighted grevlex ordering on the polynomial ring* $\mathbb{F}_q[X_0, \ldots, X_{n-1}, Y_0, \ldots, Y_{n-1}]$ *with weight* 4 *on* X_i *for* $i \in \{0..n-1\}$ *and weight* $2\alpha + 1$ *on* Y_i *for* $i \in \{0..n-1\}$*. On variables, we have* $X_{n-1} \prec X_{n-2} \prec \cdots \prec X_0 \prec Y_{n-1} \prec Y_{n-2} \prec \cdots \prec Y_0$.

We can make a prior reduction of f_i modulo g_i in Equation (2) and start instead from the following two polynomials:

$$\begin{cases} f_i &= \frac{g}{4}Y_i^2 + X_i^\alpha + \frac{g}{4}X_i^2 + L_i'(Y_i - X_i) + a_i' \\ h_i &= gX_iY_i + M_i'(Y_i - X_i) + b_i'. \end{cases} \tag{3}$$

For $i \in \{0..n-1\}$, we consider the S-polynomial $s_i \overset{def}{=} S(f_i, h_i) = gX_if_i - \frac{g}{4}Y_ih_i$. Its leading monomial with respect to $\prec$ is equal to $X_i^{\alpha+1}$.

Proposition 2. *The set*

$$\mathcal{G} \overset{def}{=} \{f_0, h_0, \ldots, f_{n-1}, h_{n-1}\} \cup \{s_0, \ldots, s_{n-1}\}$$

is a $\prec$*-Gröbner basis for Modeling 2.*

Proof. We simply have to prove that $\{f_i, h_i, s_i\}$ is a Gröbner basis for any index $i \in \{0..n-1\}$ because we can then conclude by Proposition 1. To show that $\{f_i, h_i, s_i\}$ is a Gröbner basis, we can restrict ourselves to studying the S-polynomial $S(h_i, s_i)$ as both $S(f_i, h_i)$ and $S(f_i, s_i)$ trivially reduce to zero. The fact that $S(h_i, s_i)$ reduces to zero can already be seen by computation but we will prove it more formally in Appendix A. □

Obtaining this Gröbner basis is very cheap as we only need to compute n S-polynomials in degree $\alpha + 1$. In fact, each computation depends only on one round so we can do all of them in parallel.

Degree of the ideal. We can deduce the degree of the ideal generated by Modeling 2 by examining the leading terms in $\mathcal{G}$ (also, note that this degree is trivially equal to the one of Modeling 1). Recall that for $i \in \{0..n-1\}$, we have $\mathrm{LM}_{\prec}(f_i) = Y_i^2$, $\mathrm{LM}_{\prec}(h_i) = X_i Y_i$ and $\mathrm{LM}_{\prec}(s_i) = X_i^{\alpha+1}$.

Corollary 1 *The degree of the ideal generated by Modeling 2 is* $(\alpha+2)^n$.

Proof. We use the Gröbner basis given by Proposition 2 and we count monomials "under the staircase". Given a monomial

$$\mu \overset{def}{=} \prod_{i \in \{0..n-1\}} Y_i^{a_i} \prod_{j \in \{0..n-1\}} X_j^{b_j},$$

we will write $I \overset{def}{=} \{i \in \{0..n-1\},\ a_i \neq 0\}$ and $J \overset{def}{=} \{j \in \{0..n-1\},\ b_j \neq 0\}$ for the supports on the variable sets $\boldsymbol{Y}$ and $\boldsymbol{X}$ respectively. From the leading terms in $\mathcal{G}$, a basis of the quotient space is

$$\mathcal{B} \overset{def}{=} \left\{ \mu,\ \mu = \prod_{i \in I} Y_i \prod_{j \in J,\ b_j \in \{1..\alpha\}} X_j^{b_j},\ I \cap J = \emptyset \right\}.$$

Finally, its cardinality can be estimated by

$$\#\mathcal{B} = \sum_{i=0}^{n} \underbrace{\binom{n}{i}}_{\text{choice of } I} \underbrace{2^{n-i}}_{\text{choice of } J \text{ in } I^c} \underbrace{\alpha^i}_{\text{exponents } b_j} = (\alpha+2)^n.$$

□

3 Anemoi in odd characteristic with several branches

We now show that similar results hold for several branches. For the sake of clarity, we give details when $\ell = 2$ and we will sketch the general case at the end of the section. We start by recalling the definition of one round in this case.

For an element g that generates the multiplicative group of $\mathbb{F}_q$, we consider the matrices

$$\mathcal{M}_{\boldsymbol{x}} \overset{def}{=} \begin{pmatrix} 1 & g \\ g & g^2+1 \end{pmatrix} \text{ and } \mathcal{M}_{\boldsymbol{y}} \overset{def}{=} \mathcal{M}_{\boldsymbol{x}} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} g & 1 \\ g^2+1 & g \end{pmatrix}.$$

The linear layer corresponds to applying the following steps

$$\begin{pmatrix} x_0^{(i)} \\ x_1^{(i)} \\ y_0^{(i)} \\ y_1^{(i)} \end{pmatrix} \mapsto^{\mathcal{M}_{\boldsymbol{x}},\ \mathcal{M}_{\boldsymbol{y}}} \begin{pmatrix} \mathcal{M}_{\boldsymbol{x}} \begin{pmatrix} x_0^{(i)} \\ x_1^{(i)} \end{pmatrix} \\ \mathcal{M}_{\boldsymbol{y}} \begin{pmatrix} y_0^{(i)} \\ y_1^{(i)} \end{pmatrix} \end{pmatrix} \mapsto \begin{pmatrix} x_0'' \\ x_1'' \\ y_0'' \\ y_1'' \end{pmatrix} = \begin{pmatrix} 2\mathcal{M}_{\boldsymbol{x}} \begin{pmatrix} x_0^{(i)} \\ x_1^{(i)} \end{pmatrix} + \mathcal{M}_{\boldsymbol{y}} \begin{pmatrix} y_0^{(i)} \\ y_1^{(i)} \end{pmatrix} \\ \mathcal{M}_{\boldsymbol{x}} \begin{pmatrix} x_0^{(i)} \\ x_1^{(i)} \end{pmatrix} + \mathcal{M}_{\boldsymbol{y}} \begin{pmatrix} y_0^{(i)} \\ y_1^{(i)} \end{pmatrix} \end{pmatrix}, \tag{4}$$

where the second step refers to the Pseudo-Hadamard transform. In this description, round constants have been omitted. In practice, we may sum-up the whole map as

$$\begin{pmatrix} x_0''^{(i)} \\ x_1''^{(i)} \\ y_0''^{(i)} \\ y_1''^{(i)} \end{pmatrix} \overset{def}{=} \boldsymbol{M} \begin{pmatrix} x_0^{(i)} \\ x_1^{(i)} \\ y_0^{(i)} \\ y_1^{(i)} \end{pmatrix} + \boldsymbol{M}\boldsymbol{v}_i,$$

where the matrix $\boldsymbol{M} \in \mathbb{F}_q^{4\times 4}$ corresponds to the path of Equation (4) and where the vector $\boldsymbol{v}_i \in \mathbb{F}_q^4$ contains the round constants of the i-th round. Finally, we have $\mathcal{H}(x_0''^{(i)}, y_0''^{(i)}) = (x_0^{(i+1)}, y_0^{(i+1)})$ and $\mathcal{H}(x_1''^{(i)}, y_1''^{(i)}) = (x_1^{(i+1)}, y_1^{(i+1)})$, where $\mathcal{H}(.)$ is the Anemoi S-box containing the polynomials X^α, Q_γ and Q_δ described in Section 2. To solve Problem 1 with $\ell = 2$, the polynomials corresponding to the i-th round in the analogue of Modeling 1 are given by

$$\begin{aligned} f_0^{(i)} &= \left(y_0''^{(i)} - y_0^{(i+1)}\right)^\alpha + Q_\gamma(y_0''^{(i)}) - x_0''^{(i)}, \\ h_0^{(i)} &= Q_\gamma(y_0''^{(i)}) - x_0''^{(i)} - Q_\delta(y_0^{(i+1)}) + x_0^{(i+1)}, \\ f_1^{(i)} &= \left(y_1''^{(i)} - y_1^{(i+1)}\right)^\alpha + Q_\gamma(y_1''^{(i)}) - x_1''^{(i)}, \\ h_1^{(i)} &= Q_\gamma(y_1''^{(i)}) - x_1''^{(i)} - Q_\delta(y_1^{(i+1)}) + x_1^{(i+1)}, \end{aligned}$$

and the CICO constraints are $x_0^{(0)} = x_1^{(0)} = 0$ and $x_0^{(n)} = x_1^{(n)} = 0$ (note here that there may be a linear layer at the end but this should not affect the conclusion).

Change of variables. Following what has been done in Section 2, we consider the new variables

$$\begin{cases} X_0^{(i)} = y_0''^{(i)} - y_0^{(i+1)} \\ Y_0^{(i)} = y_0''^{(i)} + y_0^{(i+1)} \\ X_1^{(i)} = y_1''^{(i)} - y_1^{(i+1)} \\ Y_1^{(i)} = y_1''^{(i)} + y_1^{(i+1)}. \end{cases} \tag{5}$$

To undo this change of variables, we perform the following steps, in order.

1. For $j \geq 1$, we express $y_0^{(j)}$ and $y_1^{(j)}$ by
$$y_0^{(j)} = \frac{Y_0^{(j-1)} - X_0^{(j-1)}}{2} \text{ and } y_1^{(j)} = \frac{Y_1^{(j-1)} - X_1^{(j-1)}}{2}.$$
2. For $j \geq 0$, we express $y_0''^{(j)}$ and $y_1''^{(j)}$ by
$$y_0''^{(j)} = \frac{Y_0^{(j)} + X_0^{(j)}}{2} \text{ and } y_1''^{(j)} = \frac{Y_1^{(j)} + X_1^{(j)}}{2}.$$
3. Then, we write $y_0^{(0)}$ and $y_1^{(0)}$ linearly in terms of $y_0''^{(0)}$ and $y_1''^{(0)}$ from the CICO constraints $x_0^{(0)} = 0$ and $x_1^{(0)} = 0$, using coordinates 3 and 4 in
$$\begin{pmatrix} 0 \\ 0 \\ y_0^{(0)} \\ y_1^{(0)} \end{pmatrix} \mapsto \begin{pmatrix} x_0''^{(0)} \\ x_1''^{(0)} \\ y_0''^{(0)} \\ y_1''^{(0)} \end{pmatrix}.$$
Finally, we use the expressions of $y_0''^{(0)}$ and $y_1''^{(0)}$ that we have found in 2.
4. Similarly, we write $x_0''^{(0)}$ and $x_1''^{(0)}$ linearly in terms of $y_0^{(0)}$ and $y_1^{(0)}$ and we then use the values of $y_0^{(0)}$ and $y_1^{(0)}$ found in 3.
5. Finally, for any $i \geq 1$, we may view the transformation
$$\begin{pmatrix} x_0^{(i)} \\ x_1^{(i)} \\ y_0^{(i)} \\ y_1^{(i)} \end{pmatrix} \mapsto \begin{pmatrix} x_0''^{(i)} \\ x_1''^{(i)} \\ y_0''^{(i)} \\ y_1''^{(i)} \end{pmatrix}$$
as a system of 4 linear equations in the unknowns $x_0^{(i)}, x_1^{(i)}, x_0''^{(i)}$ and $x_1''^{(i)}$. Solving it allows to recover these values in terms of $y_0^{(i)}, y_1^{(i)}, y_0''^{(i)}$ and $y_1''^{(i)}$.

Modeling 3 *We consider the adaptation of Modeling 1 when $\ell = 2$ in which we apply the change of variables given by Equation* (5)*, in the polynomial ring* $\mathbb{F}_q[(X_0^{(i)}, X_1^{(i)})_{i \in \{0..n-1\}}, (Y_0^{(i)}, Y_1^{(i)})_{i \in \{0..n-1\}}]$.

We will compute Gröbner bases with respect to the adaptation of Ordering 1 with weight 4 on all variables $X_0^{(i)}$ and $X_1^{(i)}$ and weight $2\alpha + 1$ on all variables $Y_0^{(i)}$ and $Y_1^{(i)}$, still denoted by $\prec$. Observe that we can write Modeling 3 as
$$\bigcup_{i=0}^{n-1} \left\{ f_0^{(i)}, h_0^{(i)}, f_1^{(i)}, h_1^{(i)} \right\},$$

where

$$\begin{aligned}
f_0^{(i)} &= \frac{g}{4}(Y_0^{(i)})^2 + (X_0^{(i)})^\alpha + \frac{g}{2}X_0^{(i)}Y_0^{(i)} + \frac{g}{4}(X_0^{(i)})^2 + a_0^{(i)},\\
h_0^{(i)} &= gX_0^{(i)}Y_0^{(i)} + b_0^{(i)},\\
f_1^{(i)} &= \frac{g}{4}(Y_1^{(i)})^2 + (X_1^{(i)})^\alpha + \frac{g}{2}X_1^{(i)}Y_1^{(i)} + \frac{g}{4}(X_1^{(i)})^2 + a_1^{(i)},\\
h_1^{(i)} &= gX_1^{(i)}Y_1^{(i)} + b_1^{(i)},
\end{aligned}$$

and where $a_0^{(i)}$, $a_1^{(i)}$, $b_0^{(i)}$ and $b_1^{(i)}$ are degree 1 polynomials which mix variables from both branches. For $j \in \{0,1\}$ and $i \in \{0..n-1\}$, we denote by $s_j^{(i)}$ the S-polynomial $S(f_j^{(i)}, h_j^{(i)})$.

Proposition 3. *The set*

$$\mathcal{G} \overset{def}{=} \bigcup_{i=0}^{n-1} \left\{f_0^{(i)}, h_0^{(i)}, f_1^{(i)}, h_1^{(i)}\right\} \cup \left\{s_0^{(i)}, s_1^{(i)}\right\}$$

is a $\prec$-Gröbner basis of the ideal generated by Modeling 3.

Proof. For $i \in \{0..n-1\}$, we show that both $\{f_0^{(i)}, h_0^{(i)}, s_0^{(i)}\}$ and $\{f_1^{(i)}, h_1^{(i)}, s_1^{(i)}\}$ are Gröbner bases by using the same argument as for $\ell = 1$, see Section 2 and Appendix A where we give more details. We conclude by Proposition 1. □

Corollary 2 *The degree of the ideal generated by Modeling 3 is $(\alpha+2)^{2n}$.*

We can use the same technique as in the $\ell = 1$ case due to the part in $\mathbb{F}_q[X_0^{(i)}, Y_0^{(i)}]$ of the polynomials $a_0^{(i)}$ and $b_0^{(i)}$ (resp. the part in $\mathbb{F}_q[X_1^{(i)}, Y_1^{(i)}]$ of the polynomials $a_1^{(i)}$ and $b_1^{(i)}$). Lemma 1 studies these degree 1 parts.

Lemma 1 *For $j \in \{0..1\}$ and for any $i \in \{0..n-1\}$, we have*

$$\begin{aligned}
x_j''^{(i)} &= L_{i,j}(X_j^{(i)} + Y_j^{(i)}) + a_{i,j},\\
x_j^{(i+1)} &= M_{i,j}(X_j^{(i)} + Y_j^{(i)}) + b_{i,j},
\end{aligned}$$

where $L_{i,j}$, $M_{i,j} \in \mathbb{F}_q$ and where $a_{i,j}$, $b_{i,j}$ are degree 1 affine polynomials not involving $X_j^{(i)}$ nor $Y_j^{(i)}$.

Proof. For $i = 0$, let us recall that $x_0''^{(0)}$ and $x_1''^{(0)}$ are expressed linearly in terms of $y_0^{(0)}$ and $y_1^{(0)}$. Therefore, it is enough to show the statement for both $y_0^{(0)}$ and $y_1^{(0)}$. Similarly, both $y_0^{(0)}$ and $y_1^{(0)}$ are obtained linearly from $y_0''^{(0)}$ and $y_1''^{(0)}$, whose expressions are given by

$$y_0''^{(0)} = \frac{Y_0^{(0)} + X_0^{(0)}}{2},\ y_1''^{(0)} = \frac{Y_1^{(0)} + X_1^{(0)}}{2}.$$

We can conclude from these expressions. For $i \geq 1$, item 5. in the text of above Modeling 3 shows that $x_0''^{(i)}$ and $x_1''^{(i)}$ are obtained linearly in terms of $y_0^{(i)}, y_1^{(i)}, y_0''^{(i)}$ and $y_1''^{(i)}$. As both $y_0^{(i)}$ and $y_1^{(i)}$ only involve variables $X_j^{(i-1)}$ or $Y_j^{(i-1)}$, we can once again conclude from the expressions of $y_0''^{(i)}$ and $y_1''^{(i)}$. The reasoning is similar for $x_j^{(i+1)}$. □

Since $a_j^{(i)} = -x_j''^{(i)}$ and $b_j^{(i)} = -x_j''^{(i)} + x_j^{(i+1)}$, Lemma 1 shows that the part in $\mathbb{F}_q[X_j^{(i)}, Y_j^{(i)}]$ in both equations is a degree 1 term in $X_j^{(i)} + Y_j^{(i)}$.

Generalization to arbitrary ℓ. This reasoning is not specific to $\ell = 2$. If we adopt a similar change of variables as in Equation (5) for general ℓ (still to solve the CICO problem given in the introduction), we can tackle in the same way the ℓ polynomials pairs $\{f_j^{(i)}, h_j^{(i)}\}$ for $j \in \{0..\ell - 1\}$ whose top degree parts only involve the two variables $X_j^{(i)}$ and $Y_j^{(i)}$. Note also that the proof of Lemma 1 does not depend on the precise definition of the linear layer when $\ell = 2$. Finally, in the same way as above, we can deduce that the ideal degree is equal to $(\alpha+2)^{\ell n}$.

4 Anemoi in even characteristic

In even characteristic, the linear layer becomes $(x, y) \mapsto (y, x + y)$ and the non-linear polynomials are $Q_\gamma(X) = \beta X^3 + \gamma$, $Q_\delta(X) = \beta X^3 + \delta$ for $\gamma \neq \delta$ and $\beta \neq 0$ (we will only consider the exponent $\alpha = 3$). We adopt the same notation as in odd characteristic, namely $C_i = c_i + d_i$ for $i \in \{0..n-1\}$. Using this notation, the two polynomials at round i are

$$\begin{cases} f_i & = (x_i + y_i + y_{i+1} + C_i)^3 + \beta(x_i + y_i + C_i)^3 + \gamma + (y_i + d_i), \\ h_i & = \beta(x_i + y_i + C_i)^3 + \gamma + \beta y_{i+1}^3 + \delta + (y_i + d_i) + x_{i+1}. \end{cases}$$

We still call Modeling 1 the system $\{f_0, h_0, \dots, f_{n-1}, h_{n-1}, x_0, x_n\}$ in even characteristic. According to [BBC+23, Lemma 1 p. 32], a grevlex Gröbner basis can be obtained in degree 5 for any value of n when $\ell = 1$. Thus, finding a first Gröbner basis is already known to be a non-issue in this case.

In this section, our goal is to apply the same change of variables as in Sections 2 and 3. More precisely, we will set

$$\begin{cases} X_i \overset{def}{=} y_{i+1} + x_i + y_i + C_i, \\ Y_i \overset{def}{=} x_i + y_i + C_i. \end{cases} \tag{6}$$

To invert this change of variables, simply note that $y_0 = Y_0 + C_0$, $y_{i+1} = X_i + Y_i$ and $x_{i+1} = Y_{i+1} + Y_i + X_i + C_{i+1}$ for $i \in \{0..n-1\}$.

Modeling 4 *We consider Modeling 1 with the change of variables given by Equation* (6)*, in the polynomial ring* $\mathbb{F}_q[X_0, \dots, X_{n-1}, Y_0, \dots, Y_{n-1}]$.

We obtain

$$\begin{cases} f_i &= \beta Y_i^3 + X_i^3 + \gamma + (y_i + d_i) \overset{def}{=} \beta Y_i^3 + X_i^3 + a_i, \\ h_i &= \beta Y_i^3 + \beta(X_i + Y_i)^3 + \gamma + (y_i + d_i) + \delta + x_{i+1} \\ &\overset{def}{=} \beta X_i Y_i^2 + \beta Y_i X_i^2 + \beta X_i^3 + Y_i + X_i + b_i, \end{cases} \tag{7}$$

where a_i, b_i are affine of degree 1 not involving X_i nor Y_i. We will compute Gröbner bases with respect to the same ordering as in odd characteristic.

Ordering 2 *We denote by $\prec_2$ the weighted grevlex order on the polynomial ring $\mathbb{F}_q[X_0, \ldots, X_{n-1}, Y_0, \ldots, Y_{n-1}]$ with weight 4 on X_i for $i \in \{0..n-1\}$ and weight $2\alpha + 1 = 7$ on Y_i for $i \in \{0..n-1\}$.*

With respect to $\prec_2$, the monomials in f_i are ordered as $Y_i^3 > X_i^3 > \cdots > 1$ and the monomials in h_i are ordered as $X_i Y_i^2 > X_i^2 Y_i > X_i^3 > \cdots > 1$, where $\ldots$ hide single variables. For $i \in \{0..n-1\}$, we introduce the S-polynomial

$$s_i \overset{def}{=} S(f_i, h_i) = \beta X_i f_i + \beta Y_i h_i,$$

whose leading monomial is equal to $X_i^2 Y_i^2$. Contrary to the odd characteristic case, the set $\{f_i, h_i, s_i\}$ is not a Gröbner basis. Thus, we naturally perform a reduction step and we define $\rho_i \overset{def}{=} s_i + \beta X_i h_i$. We have that $\mathrm{LM}_{\prec_2}(\rho_i) = X_i^4$ and that ρ_i does not contain cubic monomials (without considering weights).

Proposition 4. *The set*

$$\mathcal{G} \overset{def}{=} \{f_0, h_0, \ldots, f_{n-1}, h_{n-1}\} \cup \{\rho_0, \ldots, \rho_{n-1}\}$$

is a $\prec_2$-Gröbner basis for Modeling 4.

Proof. Since $\mathrm{LM}_{\prec_2}(f_i) = Y_i^3$ and $\mathrm{LM}_{\prec_2}(\rho_i) = X_i^4$ for $i \in \{0..n-1\}$, the set $\{f_0, \rho_0, \ldots, f_{n-1}, \rho_{n-1}\}$ is already a $\prec_2$-Gröbner basis for the subideal it generates (by Proposition 1). We can then append $\{h_0, \ldots, h_{n-1}\}$ to this Gröbner basis to obtain a Gröbner basis for the full ideal because the S-polynomials $S(h_i, \rho_i)$ reduce to zero for any $i \in \{0..n-1\}$. This follows from a computation similar to the one in Propositions 2 and 3 or from the same argument as above (by studying the system $\{f_i + a_i, h_i + b_i\}$ in $\mathbb{F}_q[X_i, Y_i]$ first, see Appendix B). □

Finally, we can deduce from $\mathcal{G}$ the degree of the ideal generated by Modeling 4. For $i \in \{0..n-1\}$, recall that $\mathrm{LM}_{\prec_2}(f_i) = Y_i^3$, $\mathrm{LM}_{\prec_2}(h_i) = X_i Y_i^2$ and $\mathrm{LM}_{\prec_2}(\rho_i) = X_i^4$.

Corollary 3 *The degree of the ideal generated by Modeling 4 is 3^{2n}.*

Proof. As in the proof of Corollary 1, we compute the number of monomials "under the staircase". We may write monomials μ as $\mu = \prod_{i=0}^{n-1} \mu_i$, where μ_i is a monomial in $\mathbb{F}_q[X_i, Y_i]$ for $i \in \{0..n-1\}$. We call "overlaps" the indexes i for which μ_i involves both X_i and Y_i. Any monomial μ under the staircase can be constructed by fixing the set of overlaps first (denoted by A) and then by choosing the corresponding μ_i's, whose representatives are among X_iY_i, $X_i^2Y_i$ or $X_i^3Y_i$. It remains to choose the other μ_i monomials, univariate in X_i or Y_i. Let B be the subset of $\{0..n-1\} \setminus A$ such that the μ_i monomials are univariate in Y_i and different from the constant monomial. The only possibility for these monomials is Y_i or Y_i^2. Finally, for $i \in \{0..n-1\} \setminus (A \cup B)$, we can choose μ_i univariate in X_i, possibly constant (i.e., 1, X_i, X_i^2 or X_i^3). The basis $\mathcal{B}$ that we obtain in this way has cardinality

$$\begin{aligned}\#\mathcal{B} &= \sum_{a=0}^{n} \binom{n}{a} 3^a \left(\sum_{b=0}^{n-a} \binom{n-a}{b} 2^b 4^{n-a-b} \right) \\ &= \sum_{a=0}^{n} \binom{n}{a} 3^a 6^{n-a} = 9^n = 3^{2n}.\end{aligned}$$

□

Remark 1 *Using the same argument, the value of the degree could actually be inferred from [BBC+23, Lemma 1 p. 32].*

5 Open questions

We obtained the value of the ideal degree for encodings of the CICO problem associated to Anemoi. The next step for more crucial progress would be to devise change of order algorithms taylored to the Gröbner bases we found. Another route would be to first study the relationship with potential FreeLunch Gröbner bases in order to apply the custom techniques of [BBL+24].

Acknowledgements. We would like to warmly thank Katharina Koschatko as well as the other authors of [KLR24] for sharing their preprint. We would also like to thank Morten Øygarden for the numerous discussions and for proof-reading an earlier version of this note.

References

BBC+23. Clémence Bouvier, Pierre Briaud, Pyrros Chaidos, Léo Perrin, Robin Salen, Vesselin Velichkov, and Danny Willems. New Design Techniques For Efficient Arithmetization-Oriented Hash Functions: Anemoi Permutations And Jive Compression Mode. In *CRYPTO 2023*, volume 14085 of *LNCS*, page 507–539. Springer, 2023.

BBL+24. Augustin Bariant, Aurélien Boeuf, Axel Lemoine, Irati Manterola Ayala, Morten Øygarden, Léo Perrin, and Håvard Raddum. The Algebraic Freelunch Efficient Gröbner Basis Attacks Against Arithmetization-Oriented Primitives. Cryptology ePrint Archive, Paper 2024/347, 2024. `https://eprint.iacr.org/2024/347`.

BDPV11. Guido Bertoni, Joan Daemen, Michaël Peeters, and Gilles Van Assche. Cryptographic sponge functions. `https://keccak.team/files/CSF-0.1.pdf`, 2011.

BGL20. Eli Ben-Sasson, Lior Goldberg, and David Levit. STARK Friendly Hash – Survey and Recommendation. Cryptology ePrint Archive, Paper 2020/948, 2020. `https://eprint.iacr.org/2020/948`.

BNSED22. Jérémy Berthomieu, Vincent Neiger, and Mohab Safey El Din. Faster change of order algorithm for Gröbner bases under shape and stability assumptions. In *2022 International Symposium on Symbolic and Algebraic Computation*, Lille, France, July 2022.

BPW06. Johannes Buchmann, Andrei Pyshkin, and Ralf-Philipp Weinmann. Block Ciphers Sensitive to Gröbner Basis Attacks. In David Pointcheval, editor, *Topics in Cryptology – CT-RSA 2006*, pages 313–331, Berlin, Heidelberg, 2006. Springer Berlin Heidelberg.

CLO15. David A. Cox, John Little, and Donal O'Shea. *Ideals, Varieties, and Algorithms*. Springer International Publishing, 2015.

FGHR14. Jean-Charles Faugère, Pierrick Gaudry, Louise Huot, and Guénaël Renault. Sub-cubic change of ordering for gröbner basis: a probabilistic approach. In *Proceedings of the 39th International Symposium on Symbolic and Algebraic Computation*, ISSAC '14, page 170–177, New York, NY, USA, 2014. Association for Computing Machinery.

FM11. Jean-Charles Faugère and Chenqi Mou. Fast algorithm for change of ordering of zero-dimensional gröbner bases with sparse multiplication matrices. In *Proceedings of the 36th International Symposium on Symbolic and Algebraic Computation*, ISSAC '11, page 115–122, New York, NY, USA, 2011. Association for Computing Machinery.

GKR$^+$21. Lorenzo Grassi, Dmitry Khovratovich, Christian Rechberger, Arnab Roy, and Markus Schofnegger. Poseidon: A new hash function for Zero-Knowledge proof systems. In *30th USENIX Security Symposium (USENIX Security 21)*, pages 519–535. USENIX Association, August 2021.

KLR24. Katharina Koschatko, Reinhard Lüftenegger, and Christian Rechberger. Exploring the Six Worlds of Gröbner Basis Cryptanalysis: Application to Anemoi. Cryptology ePrint Archive, Paper 2024/250, 2024. `https://eprint.iacr.org/2024/250`.

SAD20. Alan Szepieniec, Tomer Ashur, and Siemen Dhooghe. Rescue-prime: a standard specification (sok). Cryptology ePrint Archive, Paper 2020/1143, 2020. `https://eprint.iacr.org/2020/1143`.

Ste24a. Matthias Johann Steiner. A Zero-Dimensional Gröbner Basis for Poseidon. Cryptology ePrint Archive, Paper 2024/310, 2024. `https://eprint.iacr.org/2024/310`.

Ste24b. Matthias Johann Steiner. Zero-Dimensional Gröbner Bases for Rescue-XLIX. Cryptology ePrint Archive, Paper 2024/468, 2024. `https://eprint.iacr.org/2024/468`.

A More arguments in odd characteristic

We will prove Proposition 2 by using Lemma 2 below. More generally, we will tackle polynomial systems of the form $\{f_i, h_i\}$, where

$$\begin{cases} f_i &= Y_i^2 + UX_i^\alpha + X_i^2 + V(Y_i - X_i) + \ell_i \\ h_i &= X_iY_i + W(Y_i - X_i) + \mu_i, \end{cases} \tag{8}$$

and where $\ell_i,\ \mu_i$ are degree 1 polynomials not involving X_i nor Y_i. Equation (3) above the statement of the proposition clearly appears as a particular case of Equation (8).

Lemma 2 *Let $(U, V, W) \in \mathbb{F}_q^3$ and let $\{f, h\} \subset \mathbb{F}_q[x, y]$ the system defined by*

$$\begin{cases} f = y^2 + Ux^\alpha + x^2 + V(y - x) \\ h = xy + W(y - x). \end{cases}$$

Let $\prec$ be the grevlex weighted ordering with weight 4 on x and weight $2\alpha + 1$ on y and let $s = (x + W)f - yh$. Then, the S-polynomial $t = S(s, h) = ys - Ux^\alpha h$ is such that

$$t = ((V + W)x + VW)f - Vs + (x^2 - Vx)h. \tag{9}$$

From this identity we deduce that the set $\{f, h, s\}$ is a $\prec$-Gröbner basis of the ideal $\langle f, h\rangle$. Also, the set $\{f, h, A^{-1}s\}$ is the reduced Gröbner basis.

Proof. The restriction to the S-polynomial $t = S(s, h) = ys - Ux^\alpha h$ in our proof is due to the fact that the polynomials $S(f, h)$ and $S(f, s)$ trivially reduce to zero (for $S(f, s)$, we apply Proposition 1). Finally, using Equation (9) and the fact that $\mathrm{LM}_\prec(f) = y^2,\ \mathrm{LM}_\prec(h) = xy$ and $\mathrm{LM}_\prec(s) = x^{\alpha+1}$, we see that t reduces to zero modulo $[f, s, h]$. □

We now study the Gröbner basis computation on the system given by Equation (8), rewritten as

$$\begin{cases} f_i = f + \ell_i \\ h_i = h + \mu_i, \end{cases}$$

where both f and h are in $\mathbb{F}_q[X_i, Y_i]$. We will apply Lemma 2 to $\{f, h\}$ and keep some notation from this lemma. We have

$$\begin{aligned} s_i &= s + (X_i\ell_i - Y_i\mu_i) + W\ell_i \\ t_i &= t \underbrace{- UX_i^\alpha\mu_i + Y_iW\ell_i + \big(X_iY_i\ell_i - Y_i^2\mu_i\big)}_{\overset{def}{=}\ \lambda_i} = t + \lambda_i. \end{aligned}$$

As above, the fact that $\{f_i, h_i, s_i\}$ is a Gröbner basis can be proven by checking that t_i reduces to zero. For that purpose, we will reduce both summands t and λ_i. For λ_i, we have to kill the terms $X_iY_i\ell_i$ and $-Y_i^2\mu_i$. We obtain

$$\begin{aligned} \lambda_i &\equiv \lambda_i - h_i\ell_i + f_i\mu_i \\ &= -UX_i^\alpha\mu_i + WY_i\ell_i + (-W(Y_i - X_i)\ell_i - \ell_i\mu_i) + \big(UX_i^\alpha\mu_i + X_i^2\mu_i + V(Y_i - X_i)\mu_i + \ell_i\mu_i\big) \\ &= WX_i\ell_i + X_i^2\mu_i + V(Y_i - X_i)\mu_i. \end{aligned}$$

For t, we rely on the identity given by Equation (9).

$$\begin{aligned} t &\equiv -\ell_i((V + W)X_i + VW) - \mu_i(X_i^2 - VX_i) + V(X_i\ell_i - Y_i\mu_i) + VW\ell_i \\ &= -\ell_iX_iW - \mu_i(X_i^2 - VX_i) - VY_i\mu_i \\ &= -WX_i\ell_i - X_i^2\mu_i + VX_i\mu_i - VY_i\mu_i. \end{aligned}$$

Therefore, the polynomial t_i reduces to zero and we can conclude from there.

Several branches. We can use a similar argument to prove Proposition 3. Indeed, Lemma 1 shows Equation (8) encompasses the case of $\{f_j^{(i)}, h_j^{(i)}\}$ in Modeling 3 for $j \in \{0..1\}$ (there, the variables $-X_j^{(i)}$ and $Y_j^{(i)}$ play the role of X_i and Y_i respectively).

B More arguments in even characteristic

As in odd characteristic, the system given by Equation (7) can be written in the form

$$\begin{cases} f_i &= \beta Y_i^3 + X_i^3 + a_i, \\ h_i &= \beta X_i Y_i^2 + \beta Y_i X_i^2 + \beta X_i^3 + Y_i + X_i + b_i, \end{cases}$$

where what matters is that both a_i and b_i are degree 1 affine polynomials not involving X_i nor Y_i. In Lemma 3, we study the Gröbner basis computation on the system $\{f_i + a_i, h_i + b_i\}$.

Lemma 3 *Let $\mathbb{F}_q$ be a finite extension of $\mathbb{F}_2$, let $U \in \mathbb{F}_q$ and let $\{f, h\} \subset \mathbb{F}_q[x, y]$ be the system defined by*

$$\begin{cases} f = Uy^3 + x^3 \\ h = Uxy^2 + Ux^2y + Ux^3 + y + x. \end{cases}$$

Let $\prec$ be the grevlex weighted order with weight 4 on x and weight 7 on y and let

$$\rho = Uxf + U(x + y)h = (U^2 + U)x^4 + Uy^2 + Ux^2,$$

which can be seen as the S-polynomial $S(f, h)$ reduced modulo h. Then, the set $\{f, h, \rho\}$ is a $\prec$-Gröbner basis of the ideal $\langle f, h\rangle$.

Proof. As above, we conclude by focusing on the S-polynomial $t = S(\rho, h)$, whose expression is given by $Uy^2\rho + (U^2 + U)x^3h$. First, we have that

$$t = (Ux^2 + Uxy + 1)\rho + (Ux + Uy)h + Uyf.$$

Using this second expression, the reduction of t modulo ρ will kill the first term and it will add $U(U + 1)^{-1}\rho$ due to the Uxh term. Then, the reduction modulo h will kill $(Ux + Uy)h$ but leave the rest unchanged. At this stage we are left with $U(U + 1)^{-1}\rho + Uyf$, which reduces to zero modulo $[f, \rho]$. □

Finally, we can conclude for the genuine set of polynomials $\{f_i, h_i\}$ by an argument similar to the one below Lemma 2.