A Note on Anemoi Gröbner Bases

Pierre Briaud

Simula UiB, Bergen, Norway

Abstract. This paper focuses on algebraic attacks on the Anemoi family of arithmetization-oriented permutations [BBC+23]. We consider a slight variation of the naive modeling of the CICO problem associated to the primitive, for which we can very easily obtain a Gröbner basis and prove the degree of the associated ideal. For inputs in $\mathbb{F}_q^2$ when q is an odd prime, we recover the same degree as conjectured for alternative polynomial systems used in other recent works [BBL+24, KLR24]. Furthermore, our approach can be adapted to cases which have not been studied there, i.e., even characteristic fields and inputs in $\mathbb{F}_q^{2\ell}$ for $\ell > 1$.

1 Introduction

A new type of symmetric cryptography motivated by applications in fully homomorphic encryption (FHE), multi-party computation (MPC) and zero-knowledge (ZK) proofs has emerged in very recent years. As part of this trend, the family of arithmetization-oriented (AO) permutations Anemoi [BBC+23] is taylored to ZK proof systems. The reason why classical block ciphers are not suited in this context is because the efficiency requirement is different. For instance, Anemoi as well as previous candidates such as Jarvis [AD18] and Rescue [AAB+20] aim at minimizing the number of multiplications over $\mathbb{F}_q$, where $\mathbb{F}_q$ is a large finite field. To achieve this, Anemoi relies on the notion of CCZ equivalence [CCZ98].

Algebraic cryptanalysis of symmetric schemes. The use of algebraic cryptanalysis in symmetric cryptography largely predates the advances in AO constructions. It dates back at least to [CP02], where it was employed on the AES [DR02]. Before moving on to these more recent ciphers, let us mention earlier findings arising from the study of classical ones. A first observation that highly differs from the public-key setting is that the cost of computing an arbitrary Gröbner basis should not always be taken as an indicator of the overall complexity. For instance, [BPW06] showed that the AES modeling of [MR02] is already a Gröbner basis for a "degree-then-lex" monomial order. The main analysis tool was the so-called Buchberger's second criterion (Proposition 1 in Section 2 below). Still, algebraic methods were not a threat because the cost of the FGLM algorithm [FGLM93] to obtain a lexicographic Gröbner basis (and therefore a univariate polynomial) was above the security level. The same idea was used to devise Flurry and Curry. The goal here was to give ciphers immune to linear and differential attacks but for which the polynomial modeling by introducing intermediate variables at each round was already a Gröbner basis.

A greater concern for AO ciphers. Algebraic techniques have gained a renewed interest with the recent arithmetization-oriented primitives. This is explained both by the low multiplicative complexity of these designs and the fact that classical symmetric cryptanalysis does not seem to perform extremely well. Concretely, these attacks are used to set the appropriate number of rounds in almost all these ciphers - and Anemoi is no

E-mail: pierre@simula.no (Pierre Briaud)

exception. For permutations used in sponge constructions, the focus is typically on the hardness of the CICO problem [BDPV11] with respect to these methods.

Related works on Anemoi. A preliminary analysis of algebraic attacks on the CICO problem was provided by the designers. They considered the naive modeling by introducing variables at each round (denoted by $\mathcal{F}_{\text{CICO}}$) and another one inspired by the analysis of Griffin [GHR+23] (denoted by $\mathcal{P}_{\text{CICO}}$). On the Anemoi version with inputs in $\mathbb{F}_q^2$ where q is an odd prime, subsequent works have significantly improved upon their results[1] [KLR24, BBL+24].

The experiments conducted in [KLR24] suggest that the complexity of FGLM is the limiting cost to solve the $\mathcal{P}_{\text{CICO}}$ system. The main contribution was to provide sharper bounds on the degree of the associated ideal, which is the main parameter to estimate the complexity of FGLM. These bounds follow from a clever use of the multihomogeneous Bézout bound, already employed by Faugère and Perret in the cryptographic context [BGL20]. The final estimate of [KLR24] assumes a generic change of order algorithm.

The approach of [BBL+24] was to consider polynomial systems that are already Gröbner bases for suitable weighted monomial orders, using once again Buchberger's second criterion. Referred to as "FreeLunch", such bases have leading monomials which are simply univariate. This technique is applied to various ciphers, including Anemoi. In this case, the authors cannot construct a FreeLunch Gröbner basis for the ideal generated by $\mathcal{P}_{\text{CICO}}$ but they can derive one for a subideal which is enough for their purposes. In contrast to [KLR24], another key contribution was a FGLM-type strategy taylored to FreeLunch Gröbner bases. The authors take advantage of the peculiar shape of the so-called multiplication matrices to produce a univariate polynomial in a faster way than with generic techniques. Their strategy works well when the input FreeLunch Gröbner basis contains one polynomial of very large degree, which was the case in the attacked ciphers.

Finally, let us mention that using well-chosen weighted orders was also instrumental in the works of Steiner [Ste24a, Ste24b] on Rescue-XLIX [SAD20] and Poseidon [GKR+21]. For such orders, he showed that Gröbner bases could be obtained simply by performing linear transformations.

Contribution. We introduce an Anemoi encoding obtained from the original one $\mathcal{F}_{\text{CICO}}$ by applying a linear change of variables. Its advantage is that we can easily find a Gröbner basis for a monomial order that is less contrived than in [BBL+24]. The price to pay is that the leading monomials are not all univariate. Our approach also applies to cases not studied in [KLR24, BBL+24], i.e., the even characteristic case and a larger number of branches. From our Gröbner bases we can naturally deduce the degree of the ideal. In that respect, we would not need to rely on upper bounds as in [BBC+23, KLR24] in the final FGLM estimate.

Even though our Gröbner basis in odd characteristic is easier to produce than the FreeLunch one of [BBL+24] and even though our multiplication matrices are also cheaper to generate in practice (we provide experimental data to support this claim), it is unclear whether our approach will yield better results. We believe that further progress will require to leverage the structure of these matrices. In characteristic 2 and for a larger number of branches, the question is even more open. In particular, it would be interesting to adapt [BBL+24] to these settings.

2 Preliminaries

We will focus on the following version of the CICO problem.

[1] We will not elaborate on the recent preprint [YZY+24] which appeared later than the first version of this paper.

Problem 1 (Constrained Input Constrained Output)**.** *Let ℓ be a positive integer and let $\mathbb{F}_q$ be an arbitrary finite field. 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 of vectors $(\boldsymbol{y}_{in}, \boldsymbol{y}_{out}) \in \mathbb{F}_q^\ell \times \mathbb{F}_q^\ell$ such that $P(\mathbf{0}_\ell, \boldsymbol{y}_{in}) = (\mathbf{0}_\ell, \boldsymbol{y}_{out})$.*

2.1 Algebraic background

We refer to [CLO15] for notions related to Gröbner bases. We will write $\prec$ for a monomial order on a polynomial ring R and $\mathrm{LM}_\prec(f)$ (resp. $\mathrm{LC}_\prec(f)$) for the leading monomial (resp. coefficient) of a polynomial $f \in R$. We will use the following definitions and results, which all implicitly depend on the chosen monomial order.

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

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

Theorem 1 (Buchberger's first criterion, Theorem 6 p. 86, [CLO15])**.** *Let $\mathcal{G} = \{g_1, \dots, g_\ell\}$ be a finite set of polynomials and let $I = \langle \mathcal{G} \rangle$ be the ideal generated by $\mathcal{G}$. The set $\mathcal{G}$ is a Gröbner basis of I if and only if for all $1 \leq i < j \leq \ell$, 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 and let $f,\ g \in \mathcal{G}$ whose leading monomials are coprime. Then, the S-polynomial $S(f, g)$ reduces to 0 modulo $\mathcal{G}$.*

Details on multiplication matrices and FGLM-type algorithms will be given in Section 6 where we also present the results of our experiments.

2.2 Naive Anemoi encoding in odd characteristic

We refer to [BBC+23] for a complete description of the Anemoi permutation. In this subsection, we detail its building blocks for inputs in $\mathbb{F}_q^2$ when q is an odd prime and we introduce the $\mathcal{F}_{\mathrm{CICO}}$ polynomial system. Each of the n rounds R_i for $i \in \{0..n-1\}$ is defined as a composition

$$\mathsf{R}_i(x, y) = \mathcal{H} \circ \mathcal{M}(x + c_i, y + d_i),$$

where $\mathcal{H}$ is a non-linear map, where $\mathcal{M}(x, y) = (2x + y, x + y)$ is the linear layer and where $(c_i, d_i) \in \mathbb{F}_q^2$ are the round constants. The S-box components correspond to univariate polynomials $Q_\gamma(x) = gx^2 + g^{-1}$ and $Q_\delta(x) = gx^2$ where g generates the multiplicative subgroup of $\mathbb{F}_q$ as well as the monomial x^α for a rather small exponent α such that $x \mapsto x^\alpha$ is a permutation. Finally, the linear layer $\mathcal{M}$ is applied once again after these n rounds.

The naive modeling of Problem 1 with $\ell = 1$ adopted in [BBC+23] is the following set of polynomials.

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

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

Another generating set for $\langle \mathcal{F}_{\text{CICO}} \rangle$ is given by $\{f_0, h_0, \ldots, f_{n-1}, h_{n-1}, x_0, x_n\}$, where

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

In [BBC+23, Conjecture 2 p. 34], the ideal degree was conjectured to be equal to $(\alpha + 2)^n$.

2.3 Naive Anemoi encoding in even characteristic

When $q = 2^m$ for some odd integer m, the linear layer becomes $\mathcal{M}(x, y) = (y, x + y)$. This time, we have $Q_\gamma(x) = \beta x^3 + \gamma$ and $Q_\delta(x) = \beta x^3 + \delta$ for field elements $\gamma \neq \delta$ and $\beta \neq 0$. In this paper, we will only consider the monomial permutation x^3 but Anemoi can be defined for any value $\alpha = 2^i + 1$ such that i is coprime to m.

Using the same approach as in odd characteristic, the two polynomials obtained at round i for $\alpha = 3$ are

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

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

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

The polynomial expressions in Modeling 1 invite us to set

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

where $C_i \stackrel{def}{=} c_i + d_i$ is a public constant for $i \in \{0..n-1\}$. Recalling that the last two 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* $\mathbb{F}_q[X_0, \ldots, X_{n-1}, Y_0, \ldots, Y_{n-1}]$.

For $i \in \{0..n-1\}$, we can now 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 and M_i are constants in $\mathbb{F}_q$ that we will not need to specify and where a_i and b_i are degree 1 affine polynomials not involving X_i nor Y_i.

3.1 Easy Gröbner basis for 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 consider a weighted order. However, its definition is not as contrived as in these previous works. 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 performing 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 order on $\mathbb{F}_q[X_0, \dots, X_{n-1}, Y_0, \dots, Y_{n-1}]$ 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 $X_{n-1} \prec X_{n-2} \prec \cdots \prec X_0 \prec Y_{n-1} \prec Y_{n-2} \prec \cdots \prec Y_0$.*

It is easy to see that the leading monomial of f_i with respect to $\prec$ is equal to Y_i^2 while the one of h_i is X_iY_i. In the following, we will also consider the S-polynomial $s_i \stackrel{def}{=} S(f_i, h_i) = gX_if_i - \frac{g}{4}Y_ih_i$. By construction, its leading monomial is equal to $X_i^{\alpha+1}$.

Proposition 2. *The set*

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

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 $i \in \{0..n-1\}$ because we can then conclude by Proposition 1. To show that $\{f_i, h_i, s_i\}$ is a Gröbner basis, we use Theorem 1. We can restrict ourselves to studying the S-polynomial $S(h_i, s_i)$ as both polynomials $S(f_i, h_i)$ and $S(f_i, s_i)$ trivially reduce to zero. Finally, the fact that the polynomial $S(h_i, s_i)$ reduces to zero can be seen by symbolic computation since the expressions of $f_i,\ h_i$ and s_i are known. We will also give arguments in Appendix A. □

Obtaining the Gröbner basis $\mathcal{G}$ is very cheap as we only need to compute n S-polynomials in degree $\alpha+1$. These n computations can in fact be performed in parallel.

3.2 Ideal degree

We can deduce the degree of the ideal generated by Modeling 2 from the leading monomials in $\mathcal{G}$. This degree is clearly equal to the one of the former ideal $\langle \mathcal{F}_{\mathrm{CICO}} \rangle$ because we have simply applied a linear change of variables. Recall that for $i \in \{0..n-1\}$, we have $\mathrm{LM}_\prec(f_i) = Y_i^2,\ \mathrm{LM}_\prec(h_i) = X_iY_i$ 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". For any monomial

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

we will write $I \stackrel{def}{=} \{i \in \{0..n-1\},\ a_i \neq 0\}$ and $J \stackrel{def}{=} \{j \in \{0..n-1\},\ b_j \neq 0\}$ for the supports on the variable sets $\boldsymbol{Y}$ and $\boldsymbol{X}$ respectively. From the leading monomials in $\mathcal{G}$, a basis of the quotient space $\mathbb{F}_q[X_0, \dots, X_{n-1}, Y_0, \dots, Y_{n-1}]/\langle \mathcal{G} \rangle$ can be obtained as

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

Finally, its cardinality can be estimated by

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

□

4 Anemoi in odd characteristic when $\ell > 1$

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 Anemoi round in this case. We still denote by g a generator of the multiplicative group of $\mathbb{F}_q$ and we consider the matrices

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

In this section, the state before applying the i-th round for $i \in \{0..n-1\}$ will be denoted by $\begin{pmatrix} x_0^{(i)} & x_1^{(i)} & y_0^{(i)} & y_1^{(i)} \end{pmatrix}^\mathsf{T}$. The linear layer corresponds to the following steps

$$\begin{pmatrix} x_0^{(i)} \\ x_1^{(i)} \\ y_0^{(i)} \\ y_1^{(i)} \end{pmatrix} \mapsto^{\mathcal{M}_{\boldsymbol{x}},\ \mathcal{M}_{\boldsymbol{y}}} \begin{pmatrix} \mathcal{M}_{\boldsymbol{x}} \begin{pmatrix} x_0^{(i)} \\ x_1^{(i)} \end{pmatrix} \\ \mathcal{M}_{\boldsymbol{y}} \begin{pmatrix} y_0^{(i)} \\ y_1^{(i)} \end{pmatrix} \end{pmatrix} \mapsto \begin{pmatrix} x_0'' \\ x_1'' \\ y_0'' \\ y_1'' \end{pmatrix} = \begin{pmatrix} 2\mathcal{M}_{\boldsymbol{x}} \begin{pmatrix} x_0^{(i)} \\ x_1^{(i)} \end{pmatrix} + \mathcal{M}_{\boldsymbol{y}} \begin{pmatrix} y_0^{(i)} \\ y_1^{(i)} \end{pmatrix} \\ \mathcal{M}_{\boldsymbol{x}} \begin{pmatrix} x_0^{(i)} \\ x_1^{(i)} \end{pmatrix} + \mathcal{M}_{\boldsymbol{y}} \begin{pmatrix} y_0^{(i)} \\ y_1^{(i)} \end{pmatrix} \end{pmatrix}, \quad (3)$$

where the second step is the application of the Pseudo-Hadamard transform. In this description, round constants have been omitted. In practice, the whole map looks like

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

where the matrix $\boldsymbol{M} \in \mathbb{F}_q^{4\times 4}$ corresponds to the path of Equation (3) 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 non-linear map described in Section 3 that contains x^α, Q_γ and Q_δ.

To solve Problem 1 with $\ell = 2$, the i-th round polynomials 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 $x_0^{(n)} = x_1^{(n)} = 0$ (the linear layer applied at the very end should not affect our conclusions).

4.1 Change of variables

Following what has been done in Section 3, we consider the new variables

$$\begin{cases} X_0^{(i)} \stackrel{def}{=} y_0''^{(i)} - y_0^{(i+1)} \\ Y_0^{(i)} \stackrel{def}{=} y_0''^{(i)} + y_0^{(i+1)} \\ X_1^{(i)} \stackrel{def}{=} y_1''^{(i)} - y_1^{(i+1)} \\ Y_1^{(i)} \stackrel{def}{=} y_1''^{(i)} + y_1^{(i+1)} \end{cases}. \tag{4}$$

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

1. For $j \geq 1$, we express $y_0^{(j)}$ and $y_1^{(j)}$ in terms of the new variables as

$$y_0^{(j)} = \frac{Y_0^{(j-1)} - X_0^{(j-1)}}{2} \text{ and } y_1^{(j)} = \frac{Y_1^{(j-1)} - X_1^{(j-1)}}{2}.$$

2. For $j \geq 0$, we express $y_0''^{(j)}$ and $y_1''^{(j)}$ in terms of the new variables as

$$y_0''^{(j)} = \frac{Y_0^{(j)} + X_0^{(j)}}{2} \text{ and } y_1''^{(j)} = \frac{Y_1^{(j)} + X_1^{(j)}}{2}.$$

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 can write $x_0''^{(0)}$ and $x_1''^{(0)}$ linearly in terms of $y_0^{(0)}$ and $y_1^{(0)}$ and then use the values of $y_0^{(0)}$ and $y_1^{(0)}$ that have been 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 $x_1''^{(i)}$. Inverting this system 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 (4), in the polynomial ring*

$$\mathbb{F}_q[(X_0^{(i)}, X_1^{(i)})_{i \in \{0..n-1\}}, (Y_0^{(i)}, Y_1^{(i)})_{i \in \{0..n-1\}}].$$

4.2 Easy Gröbner basis for Modeling 3

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 the union

$$\bigcup_{i=0}^{n-1} \left\{ f_0^{(i)}, h_0^{(i)}, f_1^{(i)}, h_1^{(i)} \right\},$$

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*

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

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

Proof. For $i \in \{0..n-1\}$, we show that both sets $\{f_0^{(i)}, h_0^{(i)}, s_0^{(i)}\}$ and $\{f_1^{(i)}, h_1^{(i)}, s_1^{(i)}\}$ are Gröbner bases by using the same argument as in the $\ell = 1$ case (see Section 3 and Appendix A where we give more details). We can conclude by Proposition 1 as the leading monomials between any two of these Gröbner bases involve different variable sets. □

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

The proof of Proposition 3 is similar to the one of Proposition 2 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 $b_1^{(i)}$). This is the topic of the next lemma.

Lemma 1. *For $j \in \{0..1\}$ and for $i \in \{0..n-1\}$, 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 $y_1^{(0)}$. Thus, 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. above the definition of 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 $y_1''^{(i)}$. Finally, 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 $X_j^{(i)} + Y_j^{(i)}$.

4.3 Generalization to arbitrary ℓ

Our reasoning is not specific to the $\ell = 2$ case. If we keep a similar change of variables as the one given in Equation (4) for general ℓ, 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 $\ell = 2$. In particular, this means that the ideal degree is equal to $(\alpha + 2)^{\ell n}$ in the general case.

5 Anemoi in even characteristic

In even characteristic, we apply a similar change of variables and we arrive at the same conclusions. More precisely, we set

$$\begin{cases} X_i \overset{def}{=} y_{i+1} + x_i + y_i + C_i \\ Y_i \overset{def}{=} x_i + y_i + C_i \end{cases}, \tag{5}$$

where we still write $C_i \overset{def}{=} c_i + d_i$ for $i \in \{0..n-1\}$. To invert this change of variables, we use $y_0 = Y_0 + C_0,\ y_{i+1} = X_i + Y_i$ 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 (5), in the polynomial ring* $\mathbb{F}_q[X_0, \dots, X_{n-1}, Y_0, \dots, Y_{n-1}]$.

We obtain

$$\begin{cases} f_i &= \beta Y_i^3 + X_i^3 + \gamma + (y_i + d_i) \overset{def}{=} \beta Y_i^3 + X_i^3 + a_i, \\ h_i &= \beta Y_i^3 + \beta(X_i + Y_i)^3 + \gamma + (y_i + d_i) + \delta + x_{i+1} \\ &\overset{def}{=} \beta X_i Y_i^2 + \beta Y_i X_i^2 + \beta X_i^3 + Y_i + X_i + b_i, \end{cases} \tag{6}$$

where the polynomials a_i and b_i are affine of degree 1 and they do not involve X_i nor Y_i. We compute Gröbner bases with respect to the same monomial order as in odd characteristic.

Ordering 2. *We denote by* $\prec_2$ *the weighted grevlex order on* $\mathbb{F}_q[X_0, \dots, X_{n-1}, Y_0, \dots, Y_{n-1}]$ *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 this order, the monomials in f_i are sorted as $1 \prec_2 \cdots \prec_2 X_i^3 \prec_2 Y_i^3$ and the monomials in h_i are sorted as $1 \prec_2 \cdots \prec_2 X_i^3 \prec_2 X_i^2 Y_i \prec_2 X_i Y_i^2$, where … 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 the polynomial ρ_i does not contain cubic monomials (without considering weights).

Proposition 4. *The set*

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

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

Proof. Since $\mathrm{LM}_{\prec_2}(f_i) = Y_i^3$ and $\mathrm{LM}_{\prec_2}(\rho_i) = X_i^4$, 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 basis to obtain a Gröbner basis of the full ideal because the S-polynomials $S(h_i, \rho_i)$ reduce to zero. This follows from a computation similar to the one in Proposition 2 and we also give arguments in Appendix B. □

Using Proposition 4, we can deduce the degree of the ideal generated by Modeling 4. For $i \in \{0..n-1\}$, let us 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 equal to 3^{2n}.*

Proof. As in the proof of Corollary 1, we count the monomials "under the staircase". It will be convenient to write monomials 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 will call "overlaps" the indexes i for which μ_i involves both variables 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 $X_i Y_i$, $X_i^2 Y_i$ or $X_i^3 Y_i$. It remains to choose the other μ_i monomials that are 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 $\mathcal{B}$ of the quotient space $\mathbb{F}_q[X_0, \ldots, X_{n-1}, Y_0, \ldots, Y_{n-1}]/\langle \mathcal{G} \rangle$ that we obtain in this way is of size

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

□

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

6 Multiplication matrices

We have just seen that obtaining a first Gröbner basis is always cheap in the case of Anemoi. Therefore, we focus our attention on the end of the solving process which is the most costly part. This step typically corresponds to an application of FGLM or more efficient variants [FGHR14, FM17, BNSED22]. After constructing them, these algorithms proceed by linear algebra on the so-called multiplication matrices.

Definition 2 (Multiplication matrix)**.** *Let I be a zero-dimensional ideal in a polynomial ring R, let $\prec$ be a monomial ordering and let $\mathcal{B} = \{\epsilon_1, \ldots, \epsilon_D\}$ be the canonical basis of the quotient ring R/I ordered with respect to $\prec$, where D is the ideal degree. The multiplication matrix of the variable x is the square matrix of size D whose columns are the normal forms of the $x\epsilon_i$'s with respect to a $\prec$-Gröbner basis of I.*

Instead of using these more efficient variants to obtain a lexicographic Gröbner basis, [BBL+24] directly produces a univariate equation by computing the characteristic polynomial of one of the multiplication matrices. If the input Gröbner basis is FreeLunch, these

matrices have a nice block structure [BBL+24, Lemma 1]. If furthermore the basis contains one polynomial with univariate leading monomial of high degree α_0, this is even more interesting. Indeed, the computation of the characteristic polynomial of the corresponding multiplication matrix reduces to the one of a determinant of size only D/α_0 instead of D [BBL+24, Lemma 2].

Even if our multiplication matrices do not exhibit such a block structure, we have tried to find a univariate polynomial by computing the characteristic polynomial of one of them or by applying the first steps of Sparse-FGLM [FM17, Algorithm 2] (our ideals seem to be in shape position). We present the results of our experiments in Section 6.1 while Section 6.2 contains further comments.

6.1 Experiments

Even if the difference was small (this is expected due to the shape of the Gröbner basis), considering the multiplication matrix of one X_i seemed a bit more efficient than taking that of one Y_i. The results in this section correspond to the multiplication matrix of X_0.

We keep the same notation as in [BBL+24] to facilitate comparison. In the following tables, matGen is the computation of the multiplication matrix and polyDet is the one of its characteristic polynomial. Finally, we consider a sparseFGLM approach whose goal is similar to that of polyDet. Once the multiplication matrix has been computed, it corresponds to applying steps 2 to 8 from the probabilistic version of FGLM in the shape position case [FM17, Algorithm 2]. If the univariate polynomial produced at step 8 is of degree D, then the ideal is indeed in shape position. This is what we observed in all our experiments (this might not always be the case, especially for much smaller field sizes than the ones used in Anemoi).

Our tests were performed in Magma [BCP97]. For the polyDet step, we used a build-in command[2]. For the sparseFGLM step, we stored the multiplication matrix as a sparse matrix[3] before computing the matrix-vector products. We give the time spent on these products as it corresponds to the dominant cost. In comparison, the final Berlekamp-Massey algorithm [Ber68, Mas69] of step 8 was negligible.

In Table 1, we see that we never improve upon the overall time complexity of [BBL+24]. However, the situation is reversed between the two steps. As expected, polyDet is much slower because we perform linear algebra on a matrix of size D and not smaller as in [BBL+24]. We also do not exploit any particular structure in the multiplication matrix. On the contrary, the time of matGen is reduced by a significant amount.

Table 1: Anemoi with $(q, \ell, \alpha) = (28407454060060787, 1, 3)$. All timings are in seconds.

n	matGen	polyDet	sparseFGLM	matGen [BBL+24]	polyDet [BBL+24]
3	<0.01	0.02	0.04	<0.01	0.02
4	0.03	2.50	1.51	0.34	0.24
5	0.54	197.8	94.0	23.3	7.6
6	11.3	19,528	5,722	2,127	292
7	541	aborted	aborted	156,348	10,725

Finally, Table 2 contains timings in even characteristic for future reference. When $\alpha = 3$, the ideal degree is 9^n while it was equal to $(3+2)^n = 5^n$ in odd characteristic. Due to the large memory demand, numbers of rounds $n \geq 6$ seemed completely out of reach.

[2]Several routines are available, see https://magma.maths.usyd.edu.au/magma/handbook/text/279. The default modular algorithm was by far the most efficient.

[3]See https://magma.maths.usyd.edu.au/magma/handbook/sparse_matrices.

Table 2: Anemoi with $(q, \ell, \alpha) = (2^{17}, 1, 3)$. All timings are in seconds.

n	matGen	polyDet	sparseFGLM
3	0.01	0.15	0.25
4	0.49	91.1	24.0
5	210.4	aborted	2,741

6.2 Matrix sparsity

From our experiments, sparseFGLM seems to give better results than computing the characteristic polynomial without relying on sparse linear algebra techniques. The cost of this method can be expressed as $\mathcal{O}(N_1 D + D \log(D))$, where N_1 is the number of non-zero entries in the multiplication matrix (see [FM17, §3.1.2]).

The trivial columns in the multiplication matrix of x (i.e., the ones that contain only one non-zero entry) are associated to the elements $\epsilon_i \in \mathcal{B}$ such that $x\epsilon_i \in \mathcal{B}$. In our case, the number of such columns is known since we have the expression of $\mathcal{B}$. However, a precise estimate for N_1 requires further study. In general, the column weight depends on (i) the number of polynomial reductions to compute the normal form of $x\epsilon_i$ (ii) the shape of the reductors, i.e., the elements of $\mathcal{G}$. In our Gröbner bases, the polynomials contain very few terms and this lets us think that the multiplication matrices are sparser than the average.

We give experimental results in Tables 3 and 4 but a finer-grained analysis of the matrix sparsity is left for future work. We can already notice that the matrix becomes sparser as the number of rounds increases and also for larger values of α. This second observation might be due to the fact that the elements of $\mathcal{G}$ have the same number of monomials regardless of the value of α (and thus they can be seen as sparser when α increases). It is also in line with what was shown for generic systems: for fixed number of equations of degree d, the multiplication matrix is sparser when d increases [FM17, Corollary 6.10]. However, the dependency with respect to the number of rounds is not encompassed by [FM17, Corollary 6.10].

Table 3: Sparsity of the multiplication matrix of the variable X_0 when $(q, \ell) = (28407454060060787, 1)$ and $\alpha \in \{3, 5, 7\}$.

n	Sparsity $\alpha = 3$	Sparsity $\alpha = 5$	Sparsity $\alpha = 7$
3	0.099	0.045	0.026
4	0.038	0.017	0.010
5	0.013	0.006	0.003
6	0.004	0.002	aborted

Table 4: Sparsity of the multiplication matrix of the variable X_0 when $(q, \ell, \alpha) = (2^{17}, 1, 3)$.

n	Sparsity
3	0.007
4	9×10^{-4}
5	1×10^{-4}

References

[AAB+20] Abdelrahaman Aly, Tomer Ashur, Eli Ben-Sasson, Siemen Dhooghe, and Alan Szepieniec. Design of Symmetric-Key Primitives for Advanced Cryptographic Protocols. *IACR Trans. Symmetric Cryptol.*, 2020:1–45, 2020.

[AD18] Tomer Ashur and Siemen Dhooghe. MARVELlous: a STARK-Friendly Family of Cryptographic Primitives. Cryptology ePrint Archive, Paper 2018/1098, 2018. URL: https://eprint.iacr.org/2018/1098.

[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. URL: https://eprint.iacr.org/2024/347.

[BCP97] Wieb Bosma, John Cannon, and Catherine Playoust. The Magma algebra system. I. The user language. *J. Symbolic Comput.*, 24(3-4):235–265, 1997. Computational algebra and number theory (London, 1993).

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

[Ber68] Elwyn Berlekamp. Nonbinary BCH decoding (Abstr.). *IEEE Transactions on Information Theory*, 14(2):242–242, 1968.

[BGL20] Eli Ben-Sasson, Lior Goldberg, and David Levit. STARK Friendly Hash – Survey and Recommendation. Cryptology ePrint Archive, Paper 2020/948, 2020. URL: 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. A Zero-Dimensional Gröbner Basis for AES-128. In Matthew Robshaw, editor, *Fast Software Encryption*, pages 78–88, Berlin, Heidelberg, 2006. Springer Berlin Heidelberg.

[CCZ98] Claude Carlet, Pascale Charpin, and Victor Zinoviev. Codes, Bent Functions and Permutations Suitable For DES-like Cryptosystems. *Designs, Codes and Cryptography*, 15:125–156, 1998.

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

[CP02] Nicolas T. Courtois and Josef Pieprzyk. Cryptanalysis of Block Ciphers with Overdefined Systems of Equations. In Yuliang Zheng, editor, *Advances in Cryptology — ASIACRYPT 2002*, pages 267–287, Berlin, Heidelberg, 2002. Springer Berlin Heidelberg.

[DR02] Joan Daemen and Vincent Rijmen. *The Design of Rijndael: AES - The Advanced Encryption Standard (Information Security and Cryptography)*. Springer, 1 edition, 2002.

[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.

[FGLM93] Jean-Charles Faugère, Patrizia M. Gianni, Daniel Lazard, and Teo Mora. Efficient Computation of Zero-Dimensional Gröbner Bases by Change of Ordering. 16(4):329–344, 1993.

[FM17] Jean-Charles Faugère and Chenqi Mou. Sparse FGLM algorithms. *Journal of Symbolic Computation*, 80:538–569, 2017.

[GHR+23] Lorenzo Grassi, Yonglin Hao, Christian Rechberger, Markus Schofnegger, Roman Walch, and Qingju Wang. Horst Meets Fluid-SPN: Griffin for Zero-Knowledge Applications. In *Advances in Cryptology – CRYPTO 2023: 43rd Annual International Cryptology Conference, CRYPTO 2023, Santa Barbara, CA, USA, August 20–24, 2023, Proceedings, Part III*, page 573–606, Berlin, Heidelberg, 2023. Springer-Verlag.

[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. URL: https://eprint.iacr.org/2024/250.

[Mas69] James Massey. Shift-register synthesis and BCH decoding. *IEEE Transactions on Information Theory*, 15(1):122–127, 1969.

[MR02] Sean Murphy and Matthew J. B. Robshaw. Essential Algebraic Structure within the AES. In *Advances in Cryptology - CRYPTO 2002, 22nd Annual International Cryptology Conference, Santa Barbara, California, USA, August 18-22, 2002, Proceedings*, volume 2442 of *Lecture Notes in Computer Science*, pages 1–16. Springer, 2002.

[SAD20] Alan Szepieniec, Tomer Ashur, and Siemen Dhooghe. Rescue-Prime: a Standard Specification (SoK). Cryptology ePrint Archive, Paper 2020/1143, 2020. URL: https://eprint.iacr.org/2020/1143.

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

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

[YZY+24] Hong-Sen Yang, Qun-Xiong Zheng, Jing Yang, Quan feng Liu, and Deng Tang. A New Security Evaluation Method Based on Resultant for Arithmetic-Oriented Algorithms. Cryptology ePrint Archive, Paper 2024/886, 2024. URL: https://eprint.iacr.org/2024/886.

A Arguments for Proposition 2

We will prove Proposition 2 thanks to Lemma 2 below. Our reasoning actually applies to any polynomial system $\{\widetilde{f}_i, \widetilde{h}_i\}$ of the form

$$\begin{cases} \widetilde{f}_i &= Y_i^2 + U_i X_i^\alpha + X_i^2 + V_i(Y_i - X_i) + \ell_i \\ \widetilde{h}_i &= X_i Y_i + W_i(Y_i - X_i) + \mu_i, \end{cases} \tag{7}$$

where U_i, V_i and W_i are constants in $\mathbb{F}_q$ and where ℓ_i and μ_i are degree 1 polynomials not involving X_i nor Y_i. Note that the system $\{\widetilde{f}_i, \widetilde{h}_i\}$ where $\widetilde{h}_i = h_i$ and where $\widetilde{f}_i$ is the reduction of f_i by h_i in Equation (2) is clearly a particular case of Equation (7).

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

$$t = ((V + W)x + VW)f - Vs + (x^2 - Vx)h. \tag{8}$$

From this identity we deduce that the set $\{f, h, s\}$ is a $\prec$-Gröbner basis of the ideal $\langle f, h\rangle$. Furthermore, 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 the S-polynomial $S(f, s)$, we apply Proposition 1). Finally, by Equation (8) and using 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 the polynomial t reduces to zero after reduction by f, s and then h. □

We now study the Gröbner basis computation on the system given by Equation (7), rewritten as

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

where both polynomials f and h are in $\mathbb{F}_q[X_i, Y_i]$. We apply Lemma 2 to $\{f, h\}$ and we keep notation from the proof of this lemma, namely the polynomials s and t. We have

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

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

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

For the t summand, we rely on the identity given by Equation (8). We get

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

which is the opposite of what has just been obtained for λ_i. Therefore, the polynomial t_i reduces to zero and we can conclude from there.

Several branches ($\ell > 1$). We can use a similar argument to prove Proposition 3. Indeed, Lemma 1 shows that Equation (7) 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 Arguments for Proposition 4

As in odd characteristic, the system given by Equation (6) 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 polynomials a_i and b_i are affine of degree 1 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

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

This polynomial 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 can 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 by the polynomial ρ will naturally kill the first term which is divisible by ρ and it will add $U(U+1)^{-1}\rho$ due to the Uxh term. Similarly, the reduction of the result by h will kill the term $(Ux + Uy)h$ but it will leave the rest unchanged. At this stage we are left with $U(U+1)^{-1}\rho + Uyf$, which reduces to zero by the quotients f and eventually ρ. □

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

Remark 2. *The proofs of Lemma 2 and Lemma 3 are just given for the sake of completeness. These statements can also be checked by using a computer algebra system (we simply have 2 equations in 2 variables). In order not to create a dependency with respect to the coefficients, we have to introduce symbolic ones instead of sampling fixed $\mathbb{F}_q$ values.*