A Zero-Dimensional Gröbner Basis for Poseidon

Matthias Johann Steiner

Alpen-Adria-Universität Klagenfurt, Klagenfurt am Wörthersee, Austria
matthias.steiner@aau.at

Abstract. In this paper we construct dedicated weight orders $>$ so that a $>$-Gröbner bases of Poseidon can be found via linear transformations for the preimage as well as the CICO problem. In particular, with our Gröbner bases we can exactly compute the $\mathbb{F}_q$-vector space dimension of the quotient space for all possible Poseidon configurations. This in turn resolves previous attempts to assess the security of Poseidon against Gröbner basis attacks, since the vector space dimension quantifies the complexity of computing the variety of a zero-dimensional polynomial system.

Keywords: Gröbner basis · Sponge function · Substitution-Permutation Network · Poseidon

1 Introduction

The last years have seen a vast research effort to develop efficient symmetric cryptographic constructions for *Fully Homomorphic Encryption* (FHE), *Multi-Party Computation* (MPC) and *Zero-Knowledge* applications. These constructions are often summarized as *Arithmetization-Oriented* (AO) primitives. A common feature of AO primitives is that they are natively defined over prime fields $\mathbb{F}_p$, where $p \geq 2^{64}$, and that they use rather simple low degree polynomials at round level.

Due to the last feature, AO primitives often admit simple low degree polynomial models. Consequently, a lot of research effort has been dedicated to analyze the resistance of AO primitives against polynomial system solving techniques, in particular against Gröbner bases, e.g. [ACG+19, GKRS22, BBLP22, Ste24].

In this paper we analyze the hash function Poseidon [GKR+21] and its recent update Poseidon2 [GKS23] targeted for efficient ZK applications. Poseidon is a sponge function derived from the MPC cipher family Hades [GLR+20]. Aim of Hades was to improve the efficiency of Substitution-Permutation Networks (SPN) in MPC applications. To reduce the number of multiplications necessary to evaluate Hades, the classical SPN was split up into full rounds, where a power permutation is applied to all components, and partial rounds, where a power permutation is applied to only one component. Since their inception Hades and Poseidon have seen a lot of third party cryptanalysis to evaluate their security against various attack vectors [BCD+20, KR21, BBLP22, XCWW23, BBLP22, ABM23, Ste24]. Moreover, Poseidon has already been implemented in various zero-knowledge proof systems, e.g. [Wal21, Dus24, Pol24].

Gröbner basis cryptanalysis of Poseidon is typically performed as follows:

(1) A Poseidon polynomial system is set up for the preimage or Constrained-Input Constrained-Output (CICO) problem.

(2) A degree reverse lexicographic (DRL) Gröbner basis is computed.

To derive complexity estimates it is assumed that the Poseidon polynomial system satisfies a genericity condition.

(3) Term order conversion to a lexicographic (LEX) Gröbner basis is performed.

(4) A univariate polynomial in the LEX Gröbner basis is factored.

To estimate the complexities of Steps (3) and (4) one requires combinatorial knowledge about the DRL Gröbner basis of Poseidon, this will be discussed in more detail in Section 4. Since this is non-trivial information one usually assumes that computation of the DRL Gröbner basis already provides enough security to achieve a given security level. Though, the DRL complexity estimations are lacking mathematical rigor. To the best of our knowledge, for proven DRL complexity estimates the polynomial system has to be

(i) regular, semi-regular or cryptographically semi-regular [BFS04, BDND+21], or

(ii) in generic coordinates [CG21, Ste24].

In particular, the Poseidon designers [GKR+19, § C.2.2] assumed that their polynomial systems fall in category (i), but a formal proof is not provided. This assumption is typically justified by performing small scale experiments and observing that the polynomial systems indeed behave like regular or semi-regular ones. On the other hand, Steiner provided evidence that Poseidon polynomial systems cannot be in generic coordinates [Ste24, §6.3].

In this paper we take a fresh approach on Poseidon Gröbner basis cryptanalysis. Instead of sticking to the DRL and LEX term orders, we construct dedicated *weight orders* for Poseidon preimage as well as CICO polynomial systems. In particular, for our dedicated term orders Poseidon Gröbner bases can be found with rather simple linear transformations. This trivializes Step (2) of a Gröbner basis attack, after all every Gröbner basis is equally capable to describe the computational structure of a polynomial system. Moreover, it invalidates the underlying security assumption that Gröbner basis computations are difficult for Poseidon.

While term order conversion to LEX is the standard approach to compute the solutions of a zero-dimensional polynomial system, we discuss in Section 4 that linear algebra-based techniques [KR16, Chapter 6] are better suited to compute the solutions. One reason is that for state-of-the-art term order conversion algorithms [FGHR14, FM17] complexity analysis is only performed for the DRL term order. So one either has to redo the analysis for our weight orders or simply extrapolate the estimations. Second reason is that we do not care about the full variety of a polynomial system, all we care about are the $\mathbb{F}_p$-valued solutions of the input variables. Utilizing linear algebra-based techniques it turns out to be easier to extract the solutions of interest while maintaining the same complexity as state-of-the-art term order conversion.

As our main result, the $\mathbb{F}_p$-vector space dimension of Poseidon preimage as well as CICO polynomial system is

$$D_{\text{Poseidon}} = d^{2 \cdot r_{in} \cdot r_f + r_p}, \tag{1}$$

where d is the degree of the underlying power permutation, r_f is the number of full rounds, r_p is the number of partial rounds and r_{in} is the input rate of Poseidon.

1.1 Related Works

This paper has two spiritual predecessors. The first being *"A Zero-Dimensional Gröbner Basis for AES-128"* [BPW06] by Buchmann, Pyshkin and Weinmann who, as the title suggests, found a zero-dimensional DRL Gröbner basis for AES-128 through clever modeling. In their spirit we take a novel approach to term orders for SPN sponge functions to construct a zero-dimensional Gröbner basis. The second predecessor is *"Solving Degree Bounds for Iterated Polynomial Systems"* [Ste24] by Steiner who developed proven DRL Gröbner basis computation complexity estimates for the MiMC [AGR+16], GMiMC [AGP+19] and Hades [GLR+20] families. Unfortunately, he also provided evidence that his proving technique will always fail for SPN or Poseidon sponge functions [Ste24, §6.3]. Our work can be considered as resolution of this problem, since we find a Poseidon Gröbner basis via linear transformation, though at the cost of working with a non-standard term order.

It is worthwhile mentioning that analysis of sponge polynomial systems with respect to "weights" has already been performed in a previous work by Faugère and Perret [FP19]. In particular, they analyzed Poseidon [FP19, §10]. Essentially, their analysis is based on Bézout's theorem from algebraic geometry. Informally, for $f_1, \dots, f_m \in K[x_1, \dots, x_n]$, where K is an algebraically closed field, such that $I = (f_1, \dots, f_m)$ is zero-dimensional Bézout's theorem asserts that the ideal I has at most $\prod_{i=1}^{m} d_i$ solutions in K^n. Faugère and Perret further refined this bound via working with a multi-homogeneous generalization of Bézout's theorem, i.e. they assigned weights to the variables. Note that if the number of solutions is known, then one has a complexity estimate for Steps (3) and (4) in a Gröbner basis attack. We note that this approach has also recently been deployed to Gröbner basis cryptanalysis of `Anemoi` [BBC$^+$23] by Koschatko, Lüftenegger and Rechberger [KLR24]. While this approach might please our inner cryptographer, our inner algebraic geometer on the other hand might suffer a heart attack. First and foremost, to apply Bézout's theorem one has to ensure that the polynomial system in question is indeed zero-dimensional, this of course is obvious if one presents Bézout's theorem in its modern scheme theoretic formulation [EH16, §2.1.1]. In practice this means that we have outsourced the problem of computing a Gröbner basis to the problem of proving zero-dimensionality. To the best of our knowledge zero-dimensionality is not formally proven in the aforementioned works.

Note that for Poseidon our Gröbner basis also immediately resolves zero-dimensionality of the polynomial system via the *Finiteness Criterion* [KR00, Proposition 3.7.1]. Moreover, via the Finiteness Criterion we also obtain an estimate on the number of solutions of a Poseidon polynomial system. To the best of our knowledge this is the best generic estimate that can be derived using Gröbner basis techniques. Hence, we solve two of the aforementioned problems in one go.

Recently, Ashur, Buschman and Mahzoun interpolated the empirical DRL solving degree of Poseidon polynomial systems [ABM23]. In particular, they observed that the vector space dimension is given by Equation (1), see [ABM23, §4.3].

1.2 Organization of the Paper

In Section 2 we formally introduce the sponge construction, SPN permutations and Poseidon. In particular, in Section 2.4 we recall the notion of weight orders, the key technique in this paper, and the definition of Gröbner bases.

In Section 3 we develop Gröbner bases of preimage polynomial systems. We begin with a single round SPN sponge function, in the Horizontal Separation Lemma (Lemma 3.2) we will see that a Gröbner basis with respect to a weight order can be produced by separating input and output variables along a horizontal line. Next, in Section 2.2 we extend the Horizontal Separation Lemma to a multiple round SPN sponge function. Essentially, for every round we will set up a weight vector which separates the input and output variables of this round, but we have to ensure that the weight vector is trivial on all other rounds. In Section 3.2 we extend the technique to Poseidon, main difficulty is to balance the non-uniform degree growth in the partial rounds. Luckily, this can be achieved by adjusted weight vectors and linear transformations. In Section 3.3 we introduce an analog of the Horizontal Separation Lemma for single round SPN CICO problems. In addition, the preimage Gröbner bases for the SPN and Poseidon can be generalized in a straightforward manner to CICO, essentially one only has to introduce a slight modification for the last round. The CICO Gröbner bases for SPN and Poseidon sponge functions are formally recorded in Appendix B.

In Section 4 we discuss cryptanalytic implications of our Gröbner bases. Given any Gröbner basis of Poseidon, we discuss that the solutions of the polynomial systems can be found via eigenvalue computations of the so-called multiplication matrices. Moreover, Bariant et al. [BBLP22] introduced a trick to bypass two Poseidon rounds in the CICO model, we discuss that our Gröbner basis can be straight-forward generalized to this trick. In Table 1 we provide sample complexity estimations, and in Table 2 we reinvestigate the Ethereum Poseidon cryptanalysis challenge [Eth21]. Additionally, in Section 4.2 we show that the matrices of a concrete Poseidon2 instance satisfy the necessary conditions for the construction of our Gröbner bases.

We finish with a short discussion in Section 5. We provide a simple argument that any polynomial model $\mathcal{F}$ of Poseidon that can be generated by our Gröbner basis $\mathcal{G}$ can be ignored, since computing the solutions of $\mathcal{F}$ is at least as difficult as computing the ones for $\mathcal{G}$. Moreover, we discuss in Example 5.1 that weight orders might have applications beyond Poseidon by proving that the look-up table polynomial model for `Reinforced Concrete` [GKL+22] is already a zero-dimensional Gröbner basis.

2 Preliminaries

Let q be a prime power, we denote the finite field with q elements by $\mathbb{F}_q$. We denote matrices $\mathbf{M} \in \mathbb{F}_q^{m \times n}$ with bold capital letters and vectors $\mathbf{v} \in \mathbb{F}_q^n$ with bold lower letters. Matrix-vector products are denoted as $\mathbf{Mv}$ and analog for matrix-matrix products.

Let $k \leq n$ be integers, and let $\mathbf{v} = (v_1, \dots, v_n)^\intercal \in \mathbb{F}_q^n$. We denote with $\mathbf{v}|^k = (v_1, \dots, v_k)^\intercal$ the truncation to its first k elements, and by $\mathbf{v}|_k = (v_{n-k}, \dots, v_n)^\intercal$ the restriction to its last k elements.

We denote with $\mathbf{I}_{m \times n} \in \mathbb{F}_q^{m \times n}$ the identity matrix, and with $\mathbf{0}_{m \times n} \in \mathbb{F}_q^{m \times n}$ the zero matrix. Also, we denote $\mathbf{1}_n = (1, \dots, 1)^\intercal \in \mathbb{F}_q^n$ and $\mathbf{0}_n = (0, \dots, 0)^\intercal \in \mathbb{F}_q^n$.

We denote the standard inner product of vectors as

$$\langle \mathbf{x}, \mathbf{y} \rangle = \mathbf{x}^\intercal \mathbf{y} = \sum_{i=1}^{n} x_i \cdot y_i. \tag{2}$$

The natural logarithm will be denoted as $\log(x)$ and logarithms in base b as $\log_b(x)$.

2.1 Sponge Construction

The sponge construction [BDPV07, BDPV08] is a generic mode of operation to transform an arbitrary function, typically a permutation, into a hash function. Given $f : \mathbb{F}_2^n \to \mathbb{F}_2^n$ and $n = r + c$, where $n, r, c \in \mathbb{Z}_{\geq 1}$. The input of f is split into r *rate* and c *capacity* bits, and a finite message $m \in \mathbb{F}_2^*$ is split into blocks $m = (m_1, \dots, m_N)$, where $m_i \in \mathbb{F}_2^r$ for all N. (If necessary m is padded to have the appropriate length.) To digest the message m, we evaluate $f(m_1, \mathtt{IV})$, where $\mathtt{IV} \in F_2^c$ is some deterministic initial value, next we evaluate $f\big((m_2, \mathbf{0}) + f(m_1, \mathtt{IV})\big)$, i.e. m_2 is added to the first r bits of the output of $f(m_1, \mathtt{IV})$ and then again digested via f. This procedure is iterated, until all message parts have been digested. After the final digestion we return the first r bits of the output as hash value, if we need more bits we call f another time and return the first r output bits again. We visualize the sponge construction as directed graph in Figure 1.

Most noteworthy, the hash function `Keccak` [BDPA13] which has been selected in the third iteration of NIST's *Secure Hashing Algorithm* standardization (SHA-3) utilizes the sponge mode.

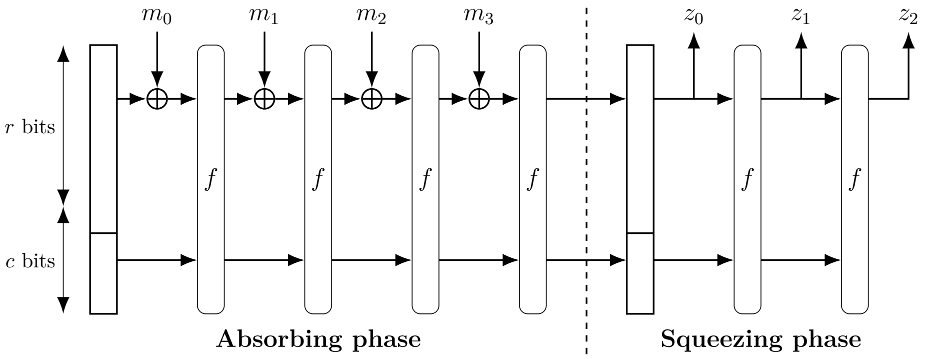

Figure 1: Visualization of the sponge construction, figure by [Jea16].

Over prime fields one cannot divide the output of a function into arbitrary bit lengths and be compatible with the field structure. Hence, over prime fields one must modify the sponge construction a bit.

Definition 2.1. *Let $\mathbb{F}_q$ be a finite field, let $n, r_{in}, r_{out}, c \in \mathbb{Z}_{\geq 1}$ be such that $n = r_{in} + c$ and $r_{out} < n$, and let $f : \mathbb{F}_q^n \to \mathbb{F}_q^n$ be a function. Let $\mathtt{IV} \in \mathbb{F}_q^c$ be an initial value, and let $\mathbf{m} = (\mathbf{m}_1, \ldots, \mathbf{m}_k) \in \mathbb{F}_q^{r_{in} \cdot k}$ be a message such that $\mathbf{m}_i \in \mathbb{F}_q^{r_{in}}$ for all i. To digest $\mathbf{m}$ via f in sponge mode one iterates through:*

(1) $\mathbf{y}_1 = f(\mathbf{m}_1, \mathtt{IV})$.

(2) For $2 \leq i \leq k$, $\mathbf{y}_i = f\big((\mathbf{m}_i, \mathbf{0}_c)^\intercal + \mathbf{y}_{i-1}\big)$.

To return an output in $\mathbb{F}_q^{(n-r_{out})\cdot l}$ one iterates through:

(1) $\mathbf{z}_1 = \mathbf{y}_k|^{n-r_{out}}$.

(2) For $2 \leq i \leq l$, $\mathbf{y}_{k+i} = f(\mathbf{y}_{k+i-1})$ *and* $\mathbf{z}_i = \mathbf{y}_{k+i}|^{n-r_{out}}$.

(3) Return $(\mathbf{z}_1, \ldots, \mathbf{z}_l)$.

From now on we will always denote with r_{in} the input rate of a sponge function and with r_{out} the "output rate" of the sponge, i.e. the size of the truncated output.

Also, for AO the sponge construction is a popular choice for compression respectively hash functions. E.g., Poseidon & Poseidon2 [GKR+21, GKS23], GMiMC [AGP+19], Anemoi [BBC+23] and Griffin [GHR+23].

2.1.1 Computational Problems for Sponge Functions

In this paper we will investigate polynomial systems for *preimage* and *Constrained-Input Constrained-Output* (CICO) [BDPV11, §8.2.4] problems of sponge functions. For a preimage problem, one is given an initial value $\boldsymbol{\alpha} \in \mathbb{F}_q^{n-r_{in}}$ and a hash value $\boldsymbol{\beta} \in \mathbb{F}_q^{n-r_{out}}$, then one asks for a solution to the equation

$$f \begin{pmatrix} \mathbf{x}_{in} \\ \boldsymbol{\alpha} \end{pmatrix} = \begin{pmatrix} \boldsymbol{\beta} \\ \mathbf{x}_{out} \end{pmatrix}, \tag{3}$$

where $\mathbf{x}_{in} = (x_{in,1}, \ldots, x_{in,r_{in}})^\intercal$ and $\mathbf{x}_{out} = (x_{out,1}, \ldots, x_{out,r_{out}})^\intercal$ are variables.

For a CICO problem, one is given two constants $\boldsymbol{\alpha} \in \mathbb{F}_q^{n-r_{in}}$ and $\boldsymbol{\beta} \in \mathbb{F}_q^{n-r_{out}}$, then one asks for a solution to the equation

$$f \begin{pmatrix} \mathbf{x}_{in} \\ \boldsymbol{\alpha} \end{pmatrix} = \begin{pmatrix} \mathbf{x}_{out} \\ \boldsymbol{\beta} \end{pmatrix}. \tag{4}$$

Note that these problems are only fully determined if $r_{in} + r_{out} \leq n$.

A third problem beyond the scope of this paper is the so-called *collision* problem. Let $\boldsymbol{\alpha} \in \mathbb{F}_q^{n-r_{in}}$ and $\boldsymbol{\beta} \in \mathbb{F}_q^{n-r_{in}}$ be initial values, then one asks for a solution to the equation

$$f \begin{pmatrix} \mathbf{x}_{in} \\ \boldsymbol{\alpha} \end{pmatrix} = f \begin{pmatrix} \mathbf{y}_{in} \\ \boldsymbol{\alpha} \end{pmatrix}, \tag{5}$$

where $\mathbf{x}_{in} = (x_{in,1}, \dots, x_{in,r_{in}})^\intercal$ and $\mathbf{y}_{in} = (y_{in,1}, \dots, y_{in,r_{in}})^\intercal$ are variables.

Obviously, any algorithm that solves one of these problems undermines the security of a sponge function.

2.2 Substitution-Permutation Network

The Substitution-Permutation Network (SPN) is one of the most widely adopted frameworks to construct cryptographic (keyed) permutations. Its idea is quite simple, to a state $\mathbf{x} \in \mathbb{F}_q^n$ apply a power permutation x^d to each component and then mix it via an affine transformation. E.g., the Advanced Encryption Standard (AES) [AES01, DR20] family are SPN ciphers.

Definition 2.2 (Substitution-Permutation Network)**.** *Let $\mathbb{F}_q$ be a finite field, let $n, d, r \in \mathbb{Z}_{\geq 1}^n$ be such that* $\gcd(d, q-1) = 1$*, let $\mathbf{M}_0, \dots, \mathbf{M}_r \in \mathbb{F}_q^n$ be invertible matrices, and let $\mathbf{c}_1, \dots, \mathbf{c}_r \in \mathbb{F}_q^n$ be constants.*

(1) The full Substitution Layer is defined as

$$\begin{aligned} \mathcal{S} : \mathbb{F}_q^n &\to \mathbb{F}_q^n, \\ (x_1, \dots, x_n)^\intercal &\mapsto \left(x_1^d, \dots, x_n^d\right)^\intercal. \end{aligned}$$

(2) For $1 \leq i \leq r$, the i^{th} Substitution-Permutation Network is defined as

$$\begin{aligned} \mathcal{R}_i : \mathbb{F}_q^n &\to \mathbb{F}_q^n, \\ \mathbf{x} &\mapsto \mathbf{M}_i \mathcal{S}(\mathbf{x}) + \mathbf{c}_i. \end{aligned}$$

(3) The Substitution-Permutation Network permutation is defined as

$$\begin{aligned} \mathrm{SPN} : \mathbb{F}_q^n &\to \mathbb{F}_q^n, \\ \mathbf{x} &\mapsto \mathcal{R}_r \circ \cdots \circ \mathcal{R}_1(\mathbf{M}_0 \mathbf{x}). \end{aligned}$$

Remark 2.3. For any $d \in \mathbb{Z}$, the power function $x \mapsto x^d$ induces a permutation over $\mathbb{F}_q$ if and only if $\gcd(d, q-1) = 1$, see [LN97, 7.8. Theorem].

For a SPN sponge function we can now define the preimage and CICO polynomial systems.

Definition 2.4. *Let $\mathbb{F}_q$ be a finite field, let $d, n, r, r_{in}, r_{out} \in \mathbb{Z}_{\geq 1}$ be integers such that $r_{in}, r_{out} < n$, let $\mathbf{M}_0, \dots, \mathbf{M}_r \in \mathbb{F}_q^{n \times n}$ be invertible matrices, let $\mathbf{c}_1, \dots, \mathbf{c}_r \in \mathbb{F}_q^n$ be constants, and let $\boldsymbol{\alpha} \in \mathbb{F}_q^{n-r_{in}}$ and $\boldsymbol{\beta} \in \mathbb{F}_q^{n-r_{out}}$. Let $\mathbf{x}_{in} = (x_{in,1}, \dots, x_{in,2})^\intercal$, $\mathbf{x}^{(i)} = \left(x_1^{(i)}, \dots, x_n^{(i)}\right)^\intercal$, where $1 \leq i \leq r$, and $\mathbf{x}_{out} = (x_{out,1}, \dots, x_{out,r_{out}})^\intercal$ be variables. In the polynomial ring $\mathbb{F}_q\left[\mathbf{x}_{in}, \mathbf{x}^{(1)}, \dots, \mathbf{x}^{(r)}, \mathbf{x}_{out}\right]$, let*

$$\mathbf{f}^{(i)} = \begin{cases} \mathbf{M}_0 \begin{pmatrix} \mathbf{x}_{in} \\ \boldsymbol{\alpha} \end{pmatrix} - \mathbf{x}^{(1)}, & i = 0, \\ \mathbf{M}_i \mathcal{S}\left(\mathbf{x}^{(i)}\right) + \mathbf{c}_i - \mathbf{x}^{(i+1)}, & 1 \leq i \leq r-1. \end{cases}$$

(1) Let

$$\mathbf{f}_{pre}^{(r)} = \mathbf{M}_r \mathcal{S}\left(\mathbf{x}^{(r)}\right) + \mathbf{c}_r - \begin{pmatrix} \boldsymbol{\beta} \\ \mathbf{x}_{out} \end{pmatrix}.$$

The polynomial system $\mathcal{F}_{pre} = \left\{\mathbf{f}^{(i)}\right\}_{0 \leq i \leq r-1} \cup \left\{\mathbf{f}_{pre}^{(r)}\right\}$ *is called the SPN sponge preimage polynomial system.*

(2) Let

$$\mathbf{f}_{CICO}^{(r)} = \mathbf{M}_r \mathcal{S}\left(\mathbf{x}^{(r)}\right) + \mathbf{c}_r - \begin{pmatrix} \mathbf{x}_{out} \\ \boldsymbol{\beta} \end{pmatrix}.$$

The polynomial system $\mathcal{F}_{CICO} = \left\{\mathbf{f}^{(i)}\right\}_{0 \leq i \leq r-1} \cup \left\{\mathbf{f}_{CICO}^{(r)}\right\}$ *is called the SPN sponge CICO polynomial system.*

2.3 Poseidon

For improved efficiency of SPNs in AO so-called *partial Substitution Layers* were first introduced in the cipher family Hades [GLR+20] and its derived sponge function Poseidon [GKR+21].

Definition 2.5 (Poseidon)**.** *Let* $\mathbb{F}_q$ *be a finite field, let* $n, d, r_f, r_p \in \mathbb{Z}_{\geq 1}^n$ *be such that* $\gcd(d, q-1) = 1$*, let* $\mathbf{M}_0, \ldots, \mathbf{M}_{2 \cdot r_f + r_p} \in \mathbb{F}_q^n$ *be invertible matrices, and let* $\mathbf{c}_1, \ldots, \mathbf{c}_{2 \cdot r_f + r_p} \in \mathbb{F}_q^n$ *be constants.*

(1) The partial Substitution Layer is defined as

$$\begin{aligned} \mathcal{P} : \mathbb{F}_q^n &\to \mathbb{F}_q^n, \\ (x_1, \ldots, x_n)^\intercal &\mapsto \left(x_1^d, x_2, \ldots, x_n\right)^\intercal. \end{aligned}$$

(2) For $1 \leq i \leq r_f$ *and* $r_f + r_p + 1 \leq i \leq 2 \cdot r_f + r_p$*, the* i^{th} *full Substitution-Permutation Network is defined as*

$$\begin{aligned} \mathcal{R}_i : \mathbb{F}_q^n &\to \mathbb{F}_q^n, \\ \mathbf{x} &\mapsto \mathbf{M}_i \mathcal{S}(\mathbf{x}) + \mathbf{c}_i. \end{aligned}$$

(3) For $r_f + 1 \leq i \leq r_f + r_p$*, the* i^{th} *partial Substitution-Permutation Network is defined as*

$$\begin{aligned} \mathcal{R}_i : \mathbb{F}_q^n &\to \mathbb{F}_q^n, \\ \mathbf{x} &\mapsto \mathbf{M}_i \mathcal{P}(\mathbf{x}) + \mathbf{c}_i. \end{aligned}$$

(4) The Poseidon *permutation is defined as*

$$\begin{aligned} \textsc{Poseidon} : \mathbb{F}_q^n &\to \mathbb{F}_q^n, \\ \mathbf{x} &\mapsto \mathcal{R}_{2 \cdot r_f + r_p} \circ \cdots \circ \mathcal{R}_1(\mathbf{M}_0 \mathbf{x}). \end{aligned}$$

For Poseidon, the designers [GKR+21, §2.3] proposed to set $\mathbf{M}_i = \mathbf{M}$ for all i, where $\mathbf{M}$ is an MDS matrix that resists various statistical as well as algebraic attack vectors. For Poseidon2, the designers [GKS23, §5.1] reused the matrices of Griffin [GHR+23] for the full rounds as well as efficient non-MDS matrices for the partial rounds. These matrices admit more efficient plain evaluation as well as more efficient Plonk [GWC19] prover circuits compared to standard Poseidon [GKS23, §8]. We list the Poseidon2 matrices in Appendix A.

Analog to the SPN, we can set up preimage and CICO polynomial systems for Poseidon.

Definition 2.6. *Let $\mathbb{F}_q$ be a finite field, let $d, n, r_f, r_p, r_{in}, r_{out} \in \mathbb{Z}_{\geq 1}$ be integers such that $r_{in}, r_{out} < n$, let $\mathbf{M}_0, \dots, \mathbf{M}_{2 \cdot r_f + r_p} \in \mathbb{F}_q^{n \times n}$ be invertible matrices, let $\mathbf{c}_1, \dots, \mathbf{c}_{2 \cdot r_f + r_p} \in \mathbb{F}_q^n$ be constants, and let $\boldsymbol{\alpha} \in \mathbb{F}_q^{n - r_{in}}$ and $\boldsymbol{\beta} \in \mathbb{F}_q^{n - r_{out}}$. Let $\mathbf{x}_{in} = (x_{in,1}, \dots, x_{in,2})^\intercal$, $\mathbf{x}^{(i)} = \left(x_1^{(i)}, \dots, x_n^{(i)} \right)^\intercal$, where $1 \leq i \leq 2 \cdot r_f + r_p$, and $\mathbf{x}_{out} = (x_{out,1}, \dots, x_{out,r_{out}})^\intercal$ be variables. In the polynomial ring $\mathbb{F}_q \left[\mathbf{x}_{in}, \mathbf{x}^{(1)}, \dots, \mathbf{x}^{(2 \cdot r_f + r_p)}, \mathbf{x}_{out} \right]$, let*

$$\mathbf{f}^{(i)} = \begin{cases} \mathbf{M}_0 \begin{pmatrix} \mathbf{x}_{in} \\ \boldsymbol{\alpha} \end{pmatrix} - \mathbf{x}^{(1)}, & i = 0, \\ \mathbf{M}_i \mathcal{S} \left(\mathbf{x}^{(i)} \right) + \mathbf{c}_i - \mathbf{x}^{(i+1)}, & \begin{cases} 1 \leq i \leq r_f, \\ r_f + r_p + 1 \leq i \leq 2 \cdot r_f + r_p - 1, \end{cases} \\ \mathbf{M}_i \mathcal{P} \left(\mathbf{x}^{(i)} \right) + \mathbf{c}_i - \mathbf{x}^{(i+1)}, & r_f + 1 \leq i \leq r_f + r_p. \end{cases}$$

(1) Let

$$\mathbf{f}_{pre}^{(2 \cdot r_f + r_p)} = \mathbf{M}_{2 \cdot r_f + r_p} \mathcal{S} \left(\mathbf{x}^{(2 \cdot r_f + r_p)} \right) + \mathbf{c}_{2 \cdot r_f + r_p} - \begin{pmatrix} \boldsymbol{\beta} \\ \mathbf{x}_{out} \end{pmatrix}.$$

The polynomial system $\mathcal{F}_{pre} = \left\{ \mathbf{f}^{(i)} \right\}_{0 \leq i \leq 2 \cdot r_f + r_p - 1} \cup \left\{ \mathbf{f}_{pre}^{(2 \cdot r_f + r_p)} \right\}$ is called the Poseidon preimage polynomial system.

(2) Let

$$\mathbf{f}_{CICO}^{(2 \cdot r_f + r_p)} = \mathbf{M}_{2 \cdot r_f + r_p} \mathcal{S} \left(\mathbf{x}^{(2 \cdot r_f + r_p)} \right) + \mathbf{c}_{2 \cdot r_f + r_p} - \begin{pmatrix} \mathbf{x}_{out} \\ \boldsymbol{\beta} \end{pmatrix}.$$

The polynomial system $\mathcal{F}_{CICO} = \left\{ \mathbf{f}^{(i)} \right\}_{0 \leq i \leq 2 \cdot r_f + r_p - 1} \cup \left\{ \mathbf{f}_{CICO}^{(2 \cdot r_f + r_p)} \right\}$ is called the Poseidon CICO polynomial system.

2.4 Term Orders & Gröbner Bases

Let $P = K[x_1, \dots, x_n]$, and let $m = \prod_{i=1}^n x_i^{a_i} \in P$ be a monomial. Obviously, we can then identify m with the integer vector $\mathbf{a} = (a_1, \dots, a_n)^\intercal \in \mathbb{Z}_{\geq 0}^n$. Via this identification we can define term orders on P, i.e. a binary relation to sort the monomials in P.

Definition 2.7 (cf. [CLO15, Chapter 2 §2 Definition 1])**.** *Let K be a field, a term order $>$ on $K[x_1, \dots, x_n]$ is a relation $>$ on $\mathbb{Z}_{\geq 0}^n$ such that*

(i) $>$ is a total ordering on $\mathbb{Z}_{\geq 0}$.

(ii) If $\mathbf{a} > \mathbf{b}$ and $\mathbf{c} \in \mathbb{Z}_{\geq 0}^n$, then $\mathbf{a} + \mathbf{c} > \mathbf{b} + \mathbf{c}$.

(iii) $>$ is a well-ordering on $\mathbb{Z}_{\geq 0}^n$, i.e. every non-empty subset of $\mathbb{Z}_{\geq 0}^n$ has a smallest element under $>$.

Let us recall the standard examples of term orders.

Example 2.8. Let $\mathbf{a} = (a_1, \dots, a_n)^\intercal, \mathbf{b} = (b_1, \dots, b_n)^\intercal \in \mathbb{Z}_{\geq 0}^n$.

(1) We say that lexicographically $\mathbf{a} >_{LEX} \mathbf{b}$ if the first non-zero entry of $\mathbf{a} - \mathbf{b}$ is positive. We denote this term order as LEX.

(2) We say that reverse lexicographically $\mathbf{a} >_{RLEX} \mathbf{b}$ if the last non-zero entry of $\mathbf{a} - \mathbf{b}$ is negative. We denote this term order as RLEX.

(3) We say that (degree) graded lexicographically $\mathbf{a} >_{DLEX} \mathbf{b}$ if $\sum_{i=1}^n a_i > \sum_{i=1}^n b_i$ or $\sum_{i=1}^n a_i = \sum_{i=1}^n b_i$ and $\mathbf{a} >_{LEX} \mathbf{b}$.

(4) We say that (degree) graded reverse lexicographically $\mathbf{a} >_{DRL} \mathbf{b}$ if $\sum_{i=1}^{n} a_i > \sum_{i=1}^{n} b_i$ or $\sum_{i=1}^{n} a_i = \sum_{i=1}^{n} b_i$ and $\mathbf{a} >_{RLEX} \mathbf{b}$. We denote this term order as DRL.

Another important class of term orders are so-called weight orders.

Definition 2.9. *Let $\mathbf{w} \in \mathbb{R}_{\geq 0}^{n}$, and let $>_\tau$ be a term order. For $\mathbf{a}, \mathbf{b} \in \mathbb{Z}_{\geq 0}^{n}$, the weight order $\mathbf{a} >_{\mathbf{w},\tau} \mathbf{b}$ is defined as*

(i) If $\langle \mathbf{w}, \mathbf{a} \rangle > \langle \mathbf{w}, \mathbf{b} \rangle$, then $\mathbf{a} >_{\mathbf{w},\tau} \mathbf{b}$.

(ii) If $\langle \mathbf{w}, \mathbf{a} \rangle = \langle \mathbf{w}, \mathbf{b} \rangle$, then $\mathbf{a} >_{\tau} \mathbf{b}$.

We call $\mathbf{w}$ the weight or weight vector, and $>_\tau$ the base order. The standard example of a weight order is the graded lexicographic order with weight $\mathbf{w} = (1, \dots, 1)^\intercal$.

Of course, $>_\tau$ can be a weight order itself, in that case we can write the weights into a $2 \times n$ matrix. Obviously, this generalizes to finite arbitrary sequences of weight orders, we will denote such an order as $>_{\mathbf{W},\tau}$, where $\mathbf{W} \in \mathbb{R}_{\geq 0}^{m \times n}$ and $>_\tau$ is again some arbitrary term order. Analog we call $\mathbf{W}$ the weight matrix. Given $\mathbf{a}, \mathbf{b} \in \mathbb{Z}_{\geq 0}^{n}$ we can then decide $\mathbf{a} >_{\mathbf{W},\tau} \mathbf{b}$ via the following iteration:

(1) Compute $\hat{\mathbf{a}} = \mathbf{W}\mathbf{a}$ and $\hat{\mathbf{b}} = \mathbf{W}\mathbf{b}$, and set $i = 1$.

(2) If $\hat{a}_i > \hat{b}_i$, then $\mathbf{a} >_{\mathbf{W},\tau} \mathbf{b}$.

(3) Else $i \mapsto i + 1$, if $i \leq m$ return to Step (2) else move to Step (4).

(4) Fall back to the base order $>_\tau$ to decide whether $\mathbf{a} >_\tau \mathbf{b}$ or not.

An easy example for such generalized a weight order is the LEX order, whose weight matrix is given by $\mathbf{W} = \mathbf{I}_{n \times n}$. Since LEX is already a term order we can then simply ignore the base order. In particular, all term orders from Example 2.8 can be represented via a weight matrix. We also note that in principle every term order on a polynomial ring can be constructed via an iteration of weight orders [Rob86].

For ease of writing, we will work with variable vectors most of the time in this paper, see e.g. Definitions 2.4 and 2.6. For a term order $>$, if we write $\mathbf{x} > \mathbf{y}$, then this shall be understood as $x_1 > \ldots > x_n > y_1 > \ldots > y_n$.

2.4.1 Gröbner Bases

Now let $f \in P = K[x_1, \dots, x_n]$ be a polynomial, and let $>$ be a term order on P. We denote the set of monomials that are present in f as $\mathcal{M}(f)$, if $f \in K \setminus \{0\}$, then we set $\mathcal{M}(f) = \{1\}$, and if $f = 0$, then $\mathcal{M}(f) = \{0\}$. Obviously, we can sort the monomials of f according to $>$, hence we obtain the notion of leading monomial of a polynomial

$$\mathrm{LM}_{>}(f) = \max_{m \in \mathcal{M}(f)} m. \tag{6}$$

Let $I \subset P$ be an ideal, then a $>$-Gröbner basis of I is a finite set $\mathcal{G} \subset I$ such that $I = (\mathcal{G})$ and

$$\big(\mathrm{LM}_{>}(f) \mid f \in I\big) = \big(\mathrm{LM}_{>}(g) \mid g \in \mathcal{G}\big). \tag{7}$$

Gröbner bases were first introduced in Bruno Buchberger's PhD thesis [Buc65]. With Gröbner bases one can solve many computational problems for ideals like the membership problem, computation of the radical, or computation of the set of zeros of a zero-dimensional ideal. For a general introduction into the theory of Gröbner bases we refer to [KR00, KR05, CLO15].

In general, to verify that a finite set of generators is a $>$-Gröbner basis requires application of Buchberger's criterion [CLO15, Chapter 2 §6 Theorem 6]. Though, for the polynomial systems in this paper we will always fall back to a special case.

Lemma 2.10. *Let K be a field, let $\mathcal{F} = \{f_1, \dots, f_m\} \subset P = K[x_1, \dots, x_n]$, and let $>$ be a term order on P. If for all $i \neq j$*

$$\gcd\big(\mathrm{LM}_>(f_i), \mathrm{LM}_>(f_j)\big) = 1,$$

then $\mathcal{F}$ is a $>$-Gröbner basis.

Proof. This is an immediate consequence of [CLO15, Chapter 2 §9 Theorem 3, Proposition 4]. □

Or in simpler language: Pairwise coprime leading monomials under $>$ implies being a $>$-Gröbner basis.

3 Gröbner Bases for Preimage Polynomial Systems

Recall the preimage problem from Equation (3), for a fully determined problem we require that $n = r_{in} + r_{out}$. Then, we can think of the input/output variables as lying along a horizontal line. The input variables lie above the line and the output variables lie below the line. Though, when using a term order like DRL we expect that only the variables $\mathbf{x}_{in}$ will be present in the leading monomials. To correct this dominance we have to increase the weights for the variables on the right-hand side.

As warm-up, we construct a Gröbner basis for a single round SPN with respect to a weighted term order via *horizontal separation.* Though, we also have to impose conditions on the matrix. For formalization of the necessary matrix condition we need to define a mapping.

Definition 3.1. *Let K be a field, let $k, l, m, n \in \mathbb{Z}_{\geq 1}$ be integers such that $k \leq m$ and $l \leq n$, and let*

$$\begin{aligned} \rho_{k,l} : K^{m \times n} &\to K^{k \times l}, \\ \mathbf{M} &\mapsto \begin{pmatrix} \mathbf{I}_{k \times l} & \mathbf{0}_{k \times (n-l)} \\ \mathbf{0}_{(m-k) \times l} & \mathbf{0}_{(m-k) \times (n-l)} \end{pmatrix} \mathbf{M}. \end{aligned}$$

Now let us investigate the single round SPN.

Lemma 3.2 (Horizontal Separation Lemma)**.** *Let K be a field, and let $d, n, r_{in}, r_{out} \in \mathbb{Z}_{\geq 1}$ be integers such that $n = r_{in} + r_{out}$. Let $\boldsymbol{\alpha} \in \mathbb{F}_q^{r_{out}}$ and $\boldsymbol{\beta} \in \mathbb{F}_q^{r_{in}}$, let $\mathbf{M} \in K^{n \times n}$ be a matrix such that* rank $\big(\rho_{r_{in}, r_{in}}(\mathbf{M})\big) = r_{in}$*, and let*

$$\mathcal{F} = \left\{ \mathbf{M} \begin{pmatrix} x_1^d \\ \vdots \\ x_{r_{in}}^d \\ \boldsymbol{\alpha} \end{pmatrix} - \begin{pmatrix} \boldsymbol{\beta} \\ y_1 \\ \vdots \\ y_{r_{out}} \end{pmatrix} \right\} \subset K[x_1, \dots, x_{r_{in}}, y_1, \dots, y_{r_{out}}].$$

Let $\mathbf{w} = (\mathbf{1}_{r_{in}}, d \cdot \mathbf{1}_{r_{out}})^\intercal \in \mathbb{Z}^n$, let $y_1 >_{LEX} \dots >_{LEX} y_{r_{out}} >_{LEX} x_1 >_{LEX} \dots >_{LEX} x_{r_{in}}$, and let $>_{\mathbf{w},LEX}$ be a weight order on the polynomial ring. Then

(1) A $>_{\mathbf{w},LEX}$-Gröbner basis of $\mathcal{F}$ can be computed via a linear transformation.

(2) $\dim_K(\mathcal{F}) = d^{r_{in}}$.

Proof. By the assumption $\operatorname{rank}\left(\rho_{r_{in},r_{in}}(\mathbf{M})\right) = r_{in}$, we can find an invertible matrix $\mathbf{N} \in K^{r_{in} \times r_{in}}$ such that

$$\mathcal{G} = \begin{pmatrix} \mathbf{N} & \mathbf{0}_{r_{in} \times r_{out}} \\ \mathbf{0}_{r_{out} \times r_{in}} & \mathbf{1}_{r_{out} \times r_{out}} \end{pmatrix} \mathcal{F} = \begin{pmatrix} \mathbf{1}_{r_{in} \times r_{in}} & \mathbf{A} \\ \mathbf{B} & \mathbf{C} \end{pmatrix} \begin{pmatrix} x_1^d \\ \vdots \\ x_{r_{in}}^d \\ \alpha_1 \\ \vdots \\ \alpha_{r_{out}} \end{pmatrix} - \begin{pmatrix} \gamma_1 \\ \vdots \\ \gamma_{r_{in}} \\ y_1 \\ \vdots \\ y_{r_{out}} \end{pmatrix},$$

for some matrices $\mathbf{A} \in K^{r_{in} \times r_{out}}$, $\mathbf{B} \in K^{r_{out} \times r_{in}}$, $\mathbf{C} \in K^{r_{out} \times r_{out}}$ and $\boldsymbol{\gamma} = \mathbf{N}\boldsymbol{\beta}$. The first r_{in} components then have leading monomials x_i^d since $(\boldsymbol{\gamma}, y_1, \dots, y_{r_{out}})^\intercal$ is constant on the first r_{in} entries. For the remaining components, y_j and x_i^d have weight d with respect to $\mathbf{w}$ for all i and j, hence we have to decide according to LEX which yields $y_j >_{\mathbf{w},LEX} x_i^d$. Thus, by Lemma 2.10 we have produced a Gröbner basis.

For the second claim

$$\left(\mathrm{LM}_{>_{\mathbf{w},LEX}}(f) \mid f \in \mathcal{F}\right) = \left(y_1, \dots, y_{r_{out}}, x_1^d, \dots, x_{r_{in}}^d\right). \tag{8}$$

It is well-known that the vector space dimension is equal to the number of monomials not contained in the ideal of leading terms, see [KR00, Theorem 1.5.7]. Therefore, only the monomials $\prod_{i=1}^{r_{in}} x_i^{d_i}$, where $0 \leq d_i \leq d-1$, generate the quotient ring as K-vector space, and it is well-known that this number is $d^{r_{in}}$. □

3.1 Substitution-Permutation Network

We will generalize the Horizontal Separation Lemma to multiple rounds by defining weight vectors $\mathbf{w}_0, \dots, \mathbf{w}_r$ such that $\mathbf{w}_i$ separates the variables in the i^{th} round or enforces a decision according to LEX. Though, to ensure that $\mathbf{w}_i$ decides for the i^{th} round the weight vectors $\mathbf{w}_0, \dots, \mathbf{w}_{i-1}, \mathbf{w}_{i+1}, \dots, \mathbf{w}_r$ have to produce ties. Moreover, to ensure ties the matrices of a SPN have to satisfy "non-singularity" conditions which we collect in the next definition.

Definition 3.3. *Let K be a field, let $k, n \in \mathbb{Z}_{\geq 1}$ be such that $k < n$, and let $\mathbf{M} \in K^{n \times n}$ be a matrix such that* $\operatorname{rank}\left(\rho_{k,k}(\mathbf{M})\right) = k$*. Then there exists an invertible matrix $\mathbf{N} \in K^{k \times k}$ such that*

$$\begin{pmatrix} \mathbf{N} & \mathbf{0}_{k \times (n-k)} \\ \mathbf{0}_{(n-k) \times k} & \mathbf{I}_{(n-k) \times (n-k)} \end{pmatrix} \mathbf{M} = \begin{pmatrix} \mathbf{I}_{k \times k} & \mathbf{A} \\ \mathbf{B} & \mathbf{C} \end{pmatrix},$$

where $\mathbf{A} \in K^{k \times (n-k)}$, $\mathbf{B} \in K^{(n-k) \times k}$ and $\mathbf{C} \in K^{(n-k) \times (n-k)}$.

(1) The matrix $\begin{pmatrix} \mathbf{N} & \mathbf{0}_{k \times (n-k)} \\ \mathbf{0}_{(n-k) \times k} & \mathbf{I}_{(n-k) \times (n-k)} \end{pmatrix}$ is called the $\rho_{k,k}$-transformation of $\mathbf{M}$.

(2) The matrix $\mathbf{M}$ is said to be in upper non-singular $\rho_{k,k}$-position if every row of $\mathbf{A}$ is non-zero.

(3) The matrix $\mathbf{M}$ is said to be in strong upper non-singular $\rho_{k,k}$-position if every row of $\mathbf{A}$ has at least two non-zero entries.

(4) The matrix $\mathbf{M}$ is said to be in lower non-singular $\rho_{k,k}$-position if every row of $\mathbf{B}$ is non-zero.

(5) The matrix $\mathbf{M}$ is said to be in strong lower non-singular $\rho_{k,k}$-position if every row of $\mathbf{B}$ has at least two non-zero entries.

Next we construct a Gröbner basis for the SPN with parameters $n > 2$ and $r_{in} < n - 1$.

Theorem 3.4. *Let $\mathbb{F}_q$ be a finite field, let $d, n, r, r_{in}, r_{out} \in \mathbb{Z}_{\geq 1}$ be integers such that $n = r_{in} + r_{out}$, and let $\mathcal{F}_{pre} = \left\{ \mathbf{f}_{pre}^{(i)} \right\}_{0 \leq i \leq r} \subset \mathbb{F}_q \left[\mathbf{x}_{in}, \mathbf{x}^{(1)}, \dots, \mathbf{x}^{(r)}, \mathbf{x}_{out} \right]$ be a SPN sponge preimage polynomial system with the parameters d, n, r, r_{in} and r_{out}. Let $\mathbf{w}_0, \dots, \mathbf{w}_r \in \mathbb{Z}_{\geq 0}^{n \cdot (r+1)}$ be weight vectors defined as*

$$\mathbf{w}_0 = \begin{pmatrix} \mathbf{1}_{r_{in}} \\ \mathbf{0}_{r_{in}} \\ d \cdot \mathbf{1}_{r_{out}} \\ d^2 \cdot \mathbf{1}_n \\ \vdots \\ d^r \cdot \mathbf{1}_n \\ d^{r+1} \cdot \mathbf{1}_{r_{out}} \end{pmatrix}, \qquad \mathbf{w}_i = \begin{pmatrix} \mathbf{0}_{r_{in}} \\ \mathbf{0}_{n \cdot (i-1)} \\ \mathbf{1}_{r_{in}} \\ \mathbf{0}_{r_{out}} \\ \mathbf{0}_{r_{in}} \\ d \cdot \mathbf{1}_{r_{out}} \\ d^2 \cdot \mathbf{1}_n \\ \vdots \\ d^{r-i} \cdot \mathbf{1}_n \\ d^{r+1-i} \cdot \mathbf{1}_{r_{out}} \end{pmatrix}, \qquad \mathbf{w}_r = \begin{pmatrix} \mathbf{0}_{r_{in}} \\ \mathbf{0}_{n \cdot (r-1)} \\ \mathbf{1}_{r_{in}} \\ \mathbf{0}_{r_{out}} \\ d \cdot \mathbf{1}_{r_{out}} \end{pmatrix},$$

where $1 \leq i \leq r - 1$, and let $\mathbf{W} = \begin{pmatrix} \mathbf{w}_0 & \dots & \mathbf{w}_r \end{pmatrix}^\intercal \in \mathbb{Z}_{\geq 0}^{(r+1) \times n \cdot (r+1)}$. Let $\mathbf{x}_{out} >_{LEX} \mathbf{x}^{(r)} >_{LEX} \dots >_{LEX} \mathbf{x}^{(1)} >_{LEX} \mathbf{x}_{in}$, and let $>_{\mathbf{W},LEX}$ be a weight order on the SPN polynomial ring. Assume that

(i) $n > 2$,

(ii) $r_{in} < n - 1$,

(iii) $\operatorname{rank} \left(\rho_{r_{in}, r_{in}} (\mathbf{M}_0) \right) = r_{in}$,

(iv) $\mathbf{M}_i$ *is in upper non-singular $\rho_{r_{in}, r_{in}}$-position for all $1 \leq i \leq r - 1$, and*

(v) $\mathbf{M}_r$ *is in strong upper non-singular $\rho_{r_{in}, r_{in}}$-position.*

Then

(1) A $>_{\mathbf{W},LEX}$-Gröbner basis for $\mathcal{F}_{pre}$ can be computed via linear transformations.

(2) $\dim_{\mathbb{F}_q} \left(\mathcal{F}_{pre} \right) = d^{r_{in} \cdot r}$.

Proof. By the assumption of upper non-singular $\rho_{r_{in}, r_{in}}$-position, there exists an invertible matrix $\mathbf{N}_i \in \mathbb{F}_q^{r_{in} \times r_{in}}$ for all $1 \leq i \leq r$ such that

$$\begin{pmatrix} \mathbf{N}_i & \mathbf{0}_{r_{in} \times r_{out}} \\ \mathbf{0}_{r_{out} \times r_{in}} & \mathbf{I}_{r_{out} \times r_{out}} \end{pmatrix} \mathbf{M}_i = \begin{pmatrix} \mathbf{I}_{r_{in} \times r_{in}} & \mathbf{A}_i \\ \mathbf{B}_i & \mathbf{C}_i \end{pmatrix},$$

where $\mathbf{A}_i \in \mathbb{F}_q^{r_{in} \times r_{out}}$ has non-zero rows, $\mathbf{B}_i \in \mathbb{F}_q^{r_{out} \times r_{in}}$ and $\mathbf{C}_i \in \mathbb{F}_q^{r_{out} \times r_{out}}$. In addition, we can find such a block matrix for $\mathbf{M}_0$, but we do not impose any conditions on $\mathbf{A}_0$.

Now let

$$\mathcal{G} = \left\{ \mathbf{g}^{(i)} = \begin{pmatrix} \mathbf{N}_i & \mathbf{0}_{r_{in} \times r_{out}} \\ \mathbf{0}_{r_{out} \times r_{in}} & \mathbf{I}_{r_{out} \times r_{out}} \end{pmatrix} \mathbf{f}_{\text{pre}}^{(i)} \right\}_{0 \leq i \leq r},$$

we claim that $\mathcal{G}$ is the $>_{\mathbf{W},LEX}$-Gröbner basis of $\mathcal{F}_{\text{pre}}$.

- For $i = 0$, we have

$$\mathbf{g}^{(0)} = \begin{pmatrix} \mathbf{I}_{r_{in} \times r_{in}} & \mathbf{A}_0 \\ \mathbf{B}_0 & \mathbf{C}_0 \end{pmatrix} \begin{pmatrix} \mathbf{x}_{in} \\ \boldsymbol{\alpha} \end{pmatrix} - \begin{pmatrix} \mathbf{N}_0 \mathbf{x}^{(1)} |^{r_{in}} \\ \mathbf{x}^{(1)} |_{r_{out}} \end{pmatrix}.$$

By the choice of $\mathbf{w}_0$, the terms of $\mathbf{x}_{r_{in}}$ have weight 1, the ones of $\mathbf{x}^{(1)}|^{r_{in}}$ have weight 0 and the ones of $\mathbf{x}^{(1)}|_{r_{out}}$ have weight d. Therefore,

$$\mathrm{LM}_{>_{\mathbf{w},LEX}}\left(\mathbf{g}^{(0)}\right) = \begin{pmatrix} \mathbf{x}_{in} \\ \mathbf{x}^{(1)}\big|_{r_{out}} \end{pmatrix}.$$

- For $1 \leq i \leq r-1$, we have

$$\mathbf{g}^{(i)} = \begin{pmatrix} \mathbf{I}_{r_{in} \times r_{in}} & \mathbf{A}_i \\ \mathbf{B}_i & \mathbf{C}_i \end{pmatrix} \mathcal{S}\left(\mathbf{x}^{(i)}\right) + \hat{\mathbf{c}}_i - \begin{pmatrix} \mathbf{N}_i \mathbf{x}^{(i+1)}\big|^{r_{in}} \\ \mathbf{x}^{(i+1)}\big|_{r_{out}} \end{pmatrix},$$

where $\hat{\mathbf{c}}_i \in \mathbb{F}_q^n$. Let $0 \leq j < i-1$, by the choice of $\mathbf{w}_j$ the terms of $\mathcal{S}\left(\mathbf{x}^{(i)}\right)$ have weight $d \cdot d^{i-j}$ and the ones of $\mathbf{x}^{(i+1)}$ have weight d^{i-j+1}. Since $\mathbf{A}_i$ has all rows non-zero, at least two terms of equal weight are present in every component of $\mathbf{g}^{(i)}|^{r_{in}}$, so we have ties. If $\begin{pmatrix} \mathbf{B}_i & \mathbf{C}_i \end{pmatrix}$ has a zero row, then we have a trivial decision for a term of $\mathbf{x}^{(i+1)}|_{r_{out}}$, otherwise we have a tie.

For $\mathbf{w}_{i-1}$, the terms $\mathcal{S}\left(\mathbf{x}^{(i)}\right)|^{r_{in}}$ have weight 0, the ones of $\mathcal{S}\left(\mathbf{x}^{(i)}\right)|_{r_{out}}$ have weight $d \cdot d$, and the ones of $\mathbf{x}^{(i+1)}$ have weight d^2. The matrix $\mathbf{A}_i$ has all rows non-zero, hence at least two terms of weight d^2 are present in every component of $\mathbf{g}^{(i)}|^{r_{in}}$, so we have ties. If $\mathbf{C}_i$ has a zero row, then we have a trivial decision for a term of $\mathbf{x}^{(i+1)}$, otherwise we have a tie. Thus, all weight vectors $\mathbf{w}_0, \ldots, \mathbf{w}_{i-1}$ produce a tie, and we have to decide according to $\mathbf{w}_i$.

However, for $\mathbf{w}_i$, the terms of $\mathcal{S}\left(\mathbf{x}^{(i)}\right)|^{r_{in}}$ have weight d, the ones of $\mathcal{S}\left(\mathbf{x}^{(i)}\right)|_{r_{out}}$ have weight 0, the ones of $\mathbf{x}^{(i+1)}|^{r_{in}}$ have weight 0 and the ones of $\mathbf{x}^{(i+1)}|_{r_{out}}$ have weight d. Therefore,

$$\mathrm{LM}_{>_{\mathbf{w},LEX}}\left(\mathbf{g}^{(i)}\big|^{r_{in}}\right) = \mathcal{S}\left(\mathbf{x}^{(i)}\right)\Big|^{r_{in}}.$$

For $\mathbf{g}^{(i)}|_{r_{out}}$, if $\mathbf{B}_i$ has a zero row, then the leading term is coming from $\mathbf{x}^{(i+1)}|_{r_{out}}$, else we again have a tie. For $i+1 \leq j \leq r$, in the weight vector $\mathbf{w}_j$ the variables $\mathbf{x}_{in}, \mathbf{x}^{(1)}, \ldots, \mathbf{x}^{(i)}, \mathbf{x}^{(i+1)}|_{r_{out}}$ have weight 0. So we trivially produce ties, and we finally have to decide by LEX to conclude that

$$\mathrm{LM}_{>_{\mathbf{w},LEX}}\left(\mathbf{g}^{(i)}\big|_{r_{out}}\right) = \mathbf{x}^{(i+1)}\big|_{r_{out}}.$$

- For $i = r$, we have

$$\mathbf{g}^{(r)} = \begin{pmatrix} \mathbf{I}_{r_{in} \times r_{in}} & \mathbf{A}_r \\ \mathbf{B}_r & \mathbf{C}_r \end{pmatrix} \mathcal{S}\left(\mathbf{x}^{(r)}\right) + \hat{\mathbf{c}}_r - \begin{pmatrix} \mathbf{N}_r \boldsymbol{\beta} \\ \mathbf{x}_{out} \end{pmatrix},$$

where $\hat{\mathbf{c}}_r \in \mathbb{F}_q^n$. Let $0 \leq j < r-1$, by the choice of $\mathbf{w}_j$ the terms of $\mathcal{S}\left(\mathbf{x}^{(r)}\right)$ have weight $d \cdot d^{r-j}$ and the ones of $\mathbf{x}_{out}$ have weight d^{r-j+1}. Since $\mathbf{M}_r$ is in strong non-singular $\rho_{r_{in}, r_{in}}$-position, every row of $\mathbf{A}_i$ has at least two non-zero entries. Then, at least two terms of $\mathcal{S}\left(\mathbf{x}^{(r)}\right)|_{r_{out}}$ are present in every component of $\mathbf{g}^{(r)}|^{r_{in}}$, i.e. all $\mathbf{w}_0, \ldots, \mathbf{w}_{r-1}$ produce a tie. For $\mathbf{g}^{(r)}|_{r_{out}}$, if $\begin{pmatrix} \mathbf{B}_r & \mathbf{C}_r \end{pmatrix}$ has a zero row, then on $\mathbf{g}^{(r)}|_{r_{out}}$ we have a trivial decision for a term of $\mathbf{x}_{out}$ via $\mathbf{w}_0$, else we have a tie.

For $\mathbf{w}_{r-1}$, the terms $\mathcal{S}\left(\mathbf{x}^{(r)}\right)|^{r_{in}}$ have weight 0, the terms $\mathcal{S}\left(\mathbf{x}^{(r)}\right)|_{r_{out}}$ have weight d^2 and the terms $\mathbf{x}_{out}$ have weight 0. Since $\mathbf{A}_r$ has two non-zero entries on every row we have a tie on $\mathbf{g}^{(r)}|^{r_{in}}$. If $\mathbf{C}_r$ has a zero row, then we have a trivial decision for a term of $\mathbf{x}_{out}$, otherwise we have a tie.

However, for $\mathbf{w}_r$, the terms of $\mathcal{S}\left(\mathbf{x}^{(r)}\right)|^{r_{in}}$ have weight d, the ones of $\mathcal{S}\left(\mathbf{x}^{(i)}\right)|_{out}$ have weight 0 and the ones of $\mathbf{x}_{out}$ have weight d. Therefore,

$$\mathrm{LM}_{>_{\mathbf{W},LEX}}\left(\mathbf{g}^{(r)}|^{r_{in}}\right) = \mathcal{S}\left(\mathbf{x}^{(r)}\right)\Big|^{r_{in}}.$$

For $\mathbf{g}^{(r)}|_{r_{out}}$, if $\mathbf{B}_r$ has a zero row, then the leading term is coming from $\mathbf{x}_{out}$, else we again have a tie. In the latter case we have to decide according to LEX and conclude that

$$\mathrm{LM}_{>_{\mathbf{W},LEX}}\left(\mathbf{g}^{(r)}\Big|_{r_{out}}\right) = \mathbf{x}_{out}.$$

Hence, the leading monomials of $\mathcal{G}$ are pairwise coprime and the claim follows from Lemma 2.10.

For the vector space dimension of the quotient space let us compute the generators of the ideal of leading terms of $(\mathcal{F}_{\text{pre}})$

$$\begin{aligned}\left(\mathrm{LM}_{>_{\mathbf{W},LEX}}(f) \mid f \in (\mathcal{F}_{\text{pre}})\right) &= \left(\mathrm{LM}_{>_{\mathbf{W},LEX}}(g) \mid g \in \mathcal{G}\right)\\ &= \left(\mathbf{x}_{in}, \mathbf{x}^{(i)}\Big|_{r_{out}}, \mathcal{S}\left(\mathbf{x}^{(i)}\right)\Big|^{r_{in}}, \mathbf{x}_{out} \;\middle|\; 1 \leq i \leq r\right)\\ &= \left(\mathbf{x}_{in}, \mathbf{x}^{(i)}\Big|_{r_{out}}, {x_j^{(i)}}^{d}, \mathbf{x}_{out} \;\middle|\; 1 \leq i \leq r,\ 1 \leq j \leq r_{in}\right).\end{aligned}$$

It is well-known that the vector space dimension is equal to the number of monomials not contained in the ideal of leading terms, see [KR00, Theorem 1.5.7]. Only the monomials $\prod_{i=1}^{r}\prod_{j=1}^{r_{in}} {x_j^{(i)}}^{k_{i,j}}$, where $0 \leq k_{i,j} \leq d-1$, are not contained in the ideal of leading terms, and it is well-known that the total number of such monomials is $d^{r_{in}\cdot r}$. □

Obviously, the argument for the last round will fail for $r_{in} = n-1$ since $\mathbf{A}_i \in \mathbb{F}_q^{(r_{in}-1)\times 1}$, i.e. strong upper non-singular $\rho_{r_{in},r_{in}}$-position is impossible. For this scenario we have to modify the weights a bit.

Proposition 3.5. *Let $\mathbb{F}_q$ be a finite field, let $d, n, r, r_{in}, r_{out} \in \mathbb{Z}_{\geq 1}$ be integers such that $n = r_{in} + r_{out}$, and let $\mathcal{F}_{pre} = \left\{\mathbf{f}_{pre}^{(i)}\right\}_{0 \leq i \leq r} \subset \mathbb{F}_q\left[\mathbf{x}_{in}, \mathbf{x}^{(1)}, \dots, \mathbf{x}^{(r)}, \mathbf{x}_{out}\right]$ be a SPN sponge preimage polynomial system with the parameters d, n, r, r_{in} and r_{out}. Let $\mathbf{w}_0, \dots, \mathbf{w}_r \in \mathbb{Z}_{\geq 0}^{n\cdot(r+1)}$ be weight vectors defined as*

$$\mathbf{w}_0 = \begin{pmatrix} \mathbf{1}_{r_{in}} \\ \mathbf{0}_n \\ d^2 \cdot \mathbf{1}_n \\ \vdots \\ d^r \cdot \mathbf{1}_n \\ d^{r+1} \cdot \mathbf{1}_{r_{out}} \end{pmatrix}, \qquad \mathbf{w}_i = \begin{pmatrix} \mathbf{0}_{r_{in}} \\ \mathbf{0}_{n\cdot(i-1)} \\ \mathbf{1}_{r_{in}} \\ \mathbf{0}_{r_{out}} \\ \mathbf{0}_n \\ d^2 \cdot \mathbf{1}_n \\ \vdots \\ d^{r-i} \cdot \mathbf{1}_n \\ d^{r+1-i} \cdot \mathbf{1}_{r_{out}} \end{pmatrix}, \qquad \mathbf{w}_r = \begin{pmatrix} \mathbf{0}_{r_{in}} \\ \mathbf{0}_{n\cdot(r-1)} \\ \mathbf{1}_{r_{in}} \\ \mathbf{0}_{r_{out}} \\ \mathbf{0}_{r_{out}} \end{pmatrix},$$

where $1 \leq i \leq r-1$, and let $\mathbf{W} = \begin{pmatrix}\mathbf{w}_0 & \dots & \mathbf{w}_r\end{pmatrix}^\intercal \in \mathbb{Z}_{\geq 0}^{(r+1)\times n\cdot(r+1)}$. Let $x_{out} >_{LEX} \mathbf{x}^{(r)} >_{LEX} \dots >_{LEX} \mathbf{x}^{(1)} >_{LEX} \mathbf{x}_{in}$, and let $>_{\mathbf{W},LEX}$ be a weight order on the SPN polynomial ring. Assume that

(i) $n > 2$,

(ii) $r_{in} = n - 1$,

(iii) the matrix $\mathbf{M}_0$ is in strong lower non-singular $\rho_{r_{in},r_{in}}$-position,

(iv) for all $1 \leq i \leq r-1$:

(a) $\operatorname{rank}\left(\rho_{r_{in},r_{in}}(\mathbf{M}_i)\right) = r_{in}$,

(b) let $\mathbf{N}_i \in \mathbb{F}_q^{r_{in} \times r_{in}}$ be the matrix of the $\rho_{r_{in},r_{in}}$-transformation of $\mathbf{M}_i$, then $\mathbf{N}_i$ has at least two non-zero entries in every row, and

(v) $\operatorname{rank}\left(\rho_{r_{in},r_{in}}(\mathbf{M}_r)\right) = r_{in}$.

Then

(1) A $>_{\mathbf{w},LEX}$-Gröbner basis for $\mathcal{F}_{pre}$ can be computed via linear transformations.

(2) $\dim_{\mathbb{F}_q}(\mathcal{F}_{pre}) = d^{r_{in} \cdot r}$.

Proof. We consider the same $\mathcal{G}$ as in the proof of Theorem 3.4, we claim that it is the $>_{\mathbf{w},LEX}$-Gröbner basis.

- For $i = 0$, trivially have that
$$\mathrm{LM}_{>_{\mathbf{w},LEX}}\left(\mathbf{g}^{(0)}\big|^{r_{in}}\right) = \mathbf{x}_{in}.$$
For $\mathbf{w}_0$, the variables $\mathbf{x}_{in}$ have weight 1 and the ones of $\mathbf{x}^{(1)}|_{r_{out}}$ have weight 0. By the assumption of strong lower non-singular $\rho_{r_{in},r_{in}}$-position of $\mathbf{M}_0$, every row of $\mathbf{B}_0$ has at least two non-zero entries, hence two terms of $\mathbf{x}_{in}$ are present in every component of $\mathbf{g}^{(0)}|_{r_{out}}$, so we have a tie. But for $\mathbf{w}_1$ we then trivially have that
$$\mathrm{LM}_{>_{\mathbf{w},LEX}}\left(\mathbf{g}^{(0)}\big|^{r_{out}}\right) = \mathbf{x}^{(1)}\Big|_{r_{out}}.$$

- For $1 \leq i \leq r-1$, we recall that
$$\mathbf{g}^{(i)} = \begin{pmatrix} \mathbf{I}_{r_{in} \times r_{in}} & \mathbf{A}_i \\ \mathbf{B}_i & \mathbf{C}_i \end{pmatrix} \mathcal{S}\left(\mathbf{x}^{(i)}\right) + \hat{\mathbf{c}}_i - \begin{pmatrix} \mathbf{N}_i \mathbf{x}^{(i+1)}\big|^{r_{in}} \\ \mathbf{x}^{(i+1)}\Big|_{r_{out}} \end{pmatrix}.$$
The term orders $\mathbf{w}_0, \ldots \mathbf{w}_{i-2}$ produce ties analog to Theorem 3.4.

  For $\mathbf{w}_{i-1}$, the variables $\mathbf{x}^{(i)}$ have weight 0 but the ones of $\mathbf{x}^{(i+1)}$ have weight d^2, so we directly have that
$$\mathrm{LM}_{>_{\mathbf{w},LEX}}\left(\mathbf{g}^{(i)}\Big|_{r_{out}}\right) = \mathbf{x}^{(i+1)}|_{r_{out}}.$$
By the assumption that $\mathbf{N}_i$ has at least two non-zero entries on every row, $\mathbf{g}^{(i)}|^{r_{in}}$ has at least two non-constant terms coming from $\mathbf{x}^{(i+1)}|^{r_{in}}$ in every component, so we have ties.

  So we have to decide via $\mathbf{w}_i$ which yields
$$\mathrm{LM}_{>_{\mathbf{w},LEX}}\left(\mathbf{g}^{(i)}\big|^{r_{in}}\right) = \mathcal{S}\left(\mathbf{x}^{(i)}\right)\Big|^{r_{in}}.$$

- For $i = r$, for $\mathbf{g}^{(r)}|^{r_{in}}$ depending on whether $\mathbf{A}_r$ has a zero row or not, we either have a trivial decision for a term of $\mathcal{S}\left(\mathbf{x}^{(r)}\right)\Big|^{r_{in}}$, or the weights $\mathbf{w}_1, \ldots, \mathbf{w}_{r-2}$ produce ties analog to the previous case. For $\mathbf{w}_{r-1}$, all terms in $\mathbf{g}^{(r)}|^{r_{in}}$ have weight 0, so we have to decide via $\mathbf{w}_r$ which yields
$$\mathrm{LM}_{>_{\mathbf{w},LEX}}\left(\mathbf{g}^{(r)}\big|^{r_{in}}\right) = \mathcal{S}\left(\mathbf{x}^{(r)}\right)\Big|^{r_{in}}.$$

For $\mathbf{g}^{(r)}|_{r_{out}}$, the weights $\mathbf{w}_1, \dots, \mathbf{w}_{r-2}$ produce ties analog to the previous case, but for $\mathbf{w}_{r-1}$ the variables $\mathbf{x}^{(r)}$ have weights 0 but x_{out} has weight d^2. So we trivially have that

$$\mathrm{LM}_{>_{\mathbf{W},LEX}} \left(\mathbf{g}^{(r)}|_{r_{out}} \right) = x_{out}.$$

Since the polynomials in $\mathcal{G}$ have pairwise coprime leading monomials, we have found a $>_{\mathbf{W},LEX}$-Gröbner basis by Lemma 2.10.

Counting the number of monomials not contained in the ideal of leading terms is analog to Theorem 3.4. □

Obviously, the arguments of Theorem 3.4 and Proposition 3.5 will fail for $n = 2$ since $\mathbf{M}_i$ cannot be in strong upper/lower non-singular $\rho_{r_{in}, r_{in}}$-position and $\mathbf{N}_i$ is only a single field element. Though, we can reuse the weights of Theorem 3.4, we just have to modify LEX ordering and the polynomials in the last round a bit.

Corollary 3.6. *Let $\mathbb{F}_q$ be a finite field, let $d, n, r, r_{in}, r_{out} \in \mathbb{Z}_{\geq 1}$ be integers such that $n = 2$, $r_{in} = 1$ and $n = r_{in} + r_{out}$, and let $\mathcal{F}_{pre} = \left\{ \mathbf{f}_{pre}^{(i)} \right\}_{0 \leq i \leq r} \subset \mathbb{F}_q \left[x_{in}, \mathbf{x}^{(i)}, x_{out} \mid 1 \leq i \leq r \right]$ be a SPN sponge preimage polynomial system with the parameters d, n, r, r_{in} and r_{out}. Let $\mathbf{W} \in \mathbb{Z}_{\geq 0}^{(r+1) \times n \cdot (r+1)}$ be the weight matrix from Theorem 3.4, let $x_1^{(r)} >_{LEX} x_{out} >_{LEX} x_2^{(r)} >_{LEX} \mathbf{x}^{(r-1)} >_{LEX} \ldots >_{LEX} \mathbf{x}^{(1)} >_{LEX} x_{in}$, and let $>_{\mathbf{W},LEX}$ be a weight order on the SPN polynomial ring. Assume that $\mathbf{M}_i$ is in upper non-singular $\rho_{r_{in}, r_{in}}$-position for all $0 \leq i \leq r$. Then*

(1) A $>_{\mathbf{W},LEX}$-Gröbner basis for $\mathcal{F}_{pre}$ can be computed via linear transformations.

(2) $\dim_{\mathbb{F}_q} \left(\mathcal{F}_{pre} \right) = d^r$.

Proof. Let $\mathbf{g}^{(0)}, \dots \mathbf{g}^{(r)}$ be as in Theorem 3.4, we have to slightly modify the polynomials for the last round

$$\begin{aligned}
\hat{\mathbf{g}}^{(r)} &= \begin{pmatrix} 1 & \gamma \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ -B_r & 1 \end{pmatrix} \begin{pmatrix} N_r & 0 \\ 0 & 1 \end{pmatrix} \mathbf{g}^{(r)} \\
&= \begin{pmatrix} 1 & \gamma \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ -B_r & 1 \end{pmatrix} \begin{pmatrix} N_r & 0 \\ 0 & 1 \end{pmatrix} \left(\mathbf{M}_r \mathcal{S} \left(\mathbf{x}^{(r)} \right) + \mathbf{c}_r - \begin{pmatrix} \beta \\ x_{out} \end{pmatrix} \right) \\
&= \begin{pmatrix} 1 & \gamma \\ 0 & 1 \end{pmatrix} \left(\begin{pmatrix} 1 & 0 \\ -B_r & 1 \end{pmatrix} \begin{pmatrix} 1 & A_r \\ B_r & C_r \end{pmatrix} \mathcal{S} \left(\mathbf{x}^{(r)} \right) + \hat{\mathbf{c}}_r - \begin{pmatrix} N_r & 0 \\ -B_r \cdot N_r & 1 \end{pmatrix} \begin{pmatrix} \beta \\ x_{out} \end{pmatrix} \right) \\
&= \begin{pmatrix} 1 & \gamma \\ 0 & 1 \end{pmatrix} \left(\begin{pmatrix} 1 & A_r \\ 0 & C_r - B_r \cdot A_r \end{pmatrix} \mathcal{S} \left(\mathbf{x}^{(r)} \right) + \hat{\mathbf{c}}_r - \begin{pmatrix} \beta \cdot N_r \\ x_{out} - B_r \cdot N_r \end{pmatrix} \right),
\end{aligned}$$

where $\gamma \in \mathbb{F}_q^\times$ is chosen such that the coefficient of ${x_2^{(r)}}^d$ in $\hat{g}_1^{(r)}$ is non-zero. Then, ${x_1^{(r)}}^d$, ${x_2^{(r)}}^d$ and x_{out} are present in $g_1^{(r)}$, but only ${x_2^{(r)}}^d$ and x_{out} are present in $g_2^{(r)}$. We claim that

$$\mathcal{G} = \left\{ \mathbf{g}^{(i)} \right\}_{0 \leq i \leq r-1} \cup \left\{ \hat{\mathbf{g}}^{(r)} \right\}$$

is the $>_{\mathbf{W},LEX}$-Gröbner basis of $\mathcal{F}_{\text{pre}}$.

- For $0 \leq i \leq r - 1$, the argument is identical to Theorem 3.4.
- For $i = r$, the term orders $\mathbf{w}_0, \dots, \mathbf{w}_{r-2}$ produce ties for $\hat{\mathbf{g}}^{(r)}$ analog to Theorem 3.4.

  For $\mathbf{w}_{r-1}$, $x_1^{(r)}$ has weight 0, ${x_2^{(r)}}^d$ has weight $d \cdot d$ and x_{out} has weight d^2. By the construction of $\hat{\mathbf{g}}^{(r)}$, ${x_2^{(r)}}^d$ is present in both components, so we again produced ties.

For $\mathbf{w}_r$, ${x_1^{(r)}}^d$ has weight d, $x_2^{(r)}$ has weight 0 and x_{out} has weight d. So trivially, we have that

$$\mathrm{LM}_{>_{\mathbf{w},LEX}}\left(g_2^{(r)}\right) = x_{out}.$$

For the first component we again have a tie, so we have to make the final decision via LEX which yields

$$\mathrm{LM}_{>_{\mathbf{w},LEX}}\left(g_1^{(r)}\right) = {x_1^{(r)}}^d.$$

We have constructed pairwise coprime leading monomial, so by Lemma 2.10 we have found a $>_{\mathbf{w},LEX}$-Gröbner basis.

Counting the number of monomials not contained in the ideal of leading terms is analog to Theorem 3.4. □

3.2 Poseidon

To construct Gröbner bases for Poseidon we have to reflect on the proof strategy a bit. For the SPN we utilized that the degree growth of $\mathcal{S}(\mathbf{x})$ is uniform among the components, but this will fail for partial rounds of Poseidon because $\mathcal{P}(\mathbf{x})$ applies the power permutation only to the first component. Luckily, we can correct non-uniform degree growth by adjusting the weights for partial rounds. Conceptually, within full or partial rounds we reduce to the SPN case with possibly adjusted weights. But we have to take a special look at the rounds r_f and $r_f + r_p$, for these rounds full SPN variables are connected with partial SPN variables and vice verse. This will require another slight adjustment of the weights for the connecting rounds. Moreover, for simpler description of partial rounds the Poseidon Gröbner basis inverts the matrices of the partial rounds.

To formalize necessary conditions for the inverse partial round matrices, we need another map analog to Definitions 3.1 and 3.3.

Definition 3.7. *Let K be a field, let $k, l, m, n \in \mathbb{Z}_{\geq 1}$ be integers such that $k \leq m$ and $l \leq n$, and let*

$$\begin{aligned} \sigma_{k,l} : K^{m \times n} &\to K^{k \times l}, \\ \mathbf{M} &\mapsto \begin{pmatrix} \mathbf{0}_{(m-k)\times(n-l)} & \mathbf{0}_{(m-k)\times l} \\ \mathbf{0}_{k\times(n-l)} & \mathbf{I}_{k\times l} \end{pmatrix} \mathbf{M}. \end{aligned}$$

If in addition $m = n$ and $k = l$ and $\mathrm{rank}\left(\sigma_{k,k}(\mathbf{M})\right) = k$*, then there exists an invertible matrix $\mathbf{N} \in K^{k \times k}$ such that*

$$\begin{pmatrix} \mathbf{I}_{(n-k)\times(n-k)} & \mathbf{0}_{(n-k)\times k} \\ \mathbf{0}_{k\times(n-k)} & \mathbf{N} \end{pmatrix} \mathbf{M} = \begin{pmatrix} \mathbf{A} & \mathbf{B} \\ \mathbf{C} & \mathbf{I}_{k \times k} \end{pmatrix},$$

where $\mathbf{A} \in K^{(n-k)\times(n-k)}$, $\mathbf{B} \in K^{k\times(n-k)}$ and $\mathbf{C} \in K^{k\times(n-k)}$.
The matrix $\begin{pmatrix} \mathbf{I}_{(n-k)\times(n-k)} & \mathbf{0}_{(n-k)\times k} \\ \mathbf{0}_{k\times(n-k)} & \mathbf{N} \end{pmatrix}$ is called the $\sigma_{k,k}$-transformation of $\mathbf{M}$.

Now we have all necessary tools to generalize Theorem 3.4 to Poseidon.

Theorem 3.8. *Let $\mathbb{F}_q$ be a finite field, let $d, n, r_f, r_p, r_{in}, r_{out} \in \mathbb{Z}_{\geq 1}$ be integers such that $n = r_{in} + r_{out}$, and let $\mathcal{F}_{pre} = \left\{\mathbf{f}_{pre}^{(i)}\right\}_{0 \leq i \leq r} \subset \mathbb{F}_q\left[\mathbf{x}_{in}, \mathbf{x}^{(1)}, \ldots, \mathbf{x}^{(2\cdot r_f + r_p)}, \mathbf{x}_{out}\right]$ be a Poseidon preimage polynomial system with the parameters d, n, r_f, r_p, r_{in} and r_{out}. Let*

$\mathbf{w}_0, \dots, \mathbf{w}_{2 \cdot r_f + r_p} \in \mathbb{Z}_{\geq 0}^{n \cdot (2 \cdot r_f + r_p + 1)}$ *be weight vectors defined as*

$$\mathbf{w}_0 = \begin{pmatrix} \mathbf{1}_{r_{in}} \\ \mathbf{0}_{r_{in}} \\ d \cdot \mathbf{1}_{r_{out}} \\ d^2 \cdot \mathbf{1}_n \\ \vdots \\ d^{2 \cdot r_f + r_p} \cdot \mathbf{1}_n \\ d^{2 \cdot r_f + r_p + 1} \cdot \mathbf{1}_{r_{out}} \end{pmatrix}, \qquad \mathbf{w}_i = \begin{pmatrix} \mathbf{0}_{r_{in}} \\ \mathbf{0}_{n \cdot (i-1)} \\ \mathbf{1}_{r_{in}} \\ \mathbf{0}_{r_{out}} \\ \mathbf{0}_{r_{in}} \\ d \cdot \mathbf{1}_{r_{out}} \\ d^2 \cdot \mathbf{1}_n \\ \vdots \\ d^{2 \cdot r_f + r_p - i} \cdot \mathbf{1}_n \\ d^{2 \cdot r_f + r_p + 1 - i} \cdot \mathbf{1}_{r_{out}} \end{pmatrix},$$

$$\mathbf{w}_{r_f} = \begin{pmatrix} \mathbf{0}_{r_{in}} \\ \mathbf{0}_{n \cdot (r_f - 1)} \\ \mathbf{1}_{r_{in}} \\ \mathbf{0}_{r_{out}} \\ \mathbf{0}_{r_{in}} \\ d^2 \cdot \mathbf{1}_{r_{out}} \\ d^2 \cdot \mathbf{1}_n \\ \vdots \\ d^{r_f + r_p} \cdot \mathbf{1}_n \\ d^{r_f + r_p + 1} \cdot \mathbf{1}_n \end{pmatrix}, \qquad \mathbf{w}_j = \begin{pmatrix} \mathbf{0}_{r_{in}} \\ \mathbf{0}_{n \cdot (j-1)} \\ 1 \\ d \cdot \mathbf{1}_{r_{in} - 1} \\ \mathbf{0}_{r_{out}} \\ \mathbf{0}_{r_{in}} \\ d^2 \cdot \mathbf{1}_{r_{out}} \\ d^2 \cdot \mathbf{1}_n \\ \vdots \\ d^{2 \cdot r_f + r_p - j} \cdot \mathbf{1}_n \\ d^{2 \cdot r_f + r_p + 1 - j} \cdot \mathbf{1}_{r_{out}} \end{pmatrix},$$

$$\mathbf{w}_{r_f + r_p} = \begin{pmatrix} \mathbf{0}_{r_{in}} \\ \mathbf{0}_{n \cdot (r_f + r_p - 1)} \\ 1 \\ d \cdot \mathbf{1}_{r_{in} - 1} \\ \mathbf{0}_{r_{out}} \\ \mathbf{0}_{r_{in}} \\ d \cdot \mathbf{1}_{r_{out}} \\ d^2 \cdot \mathbf{1}_n \\ \vdots \\ d^{r_f + r_p} \cdot \mathbf{1}_n \\ d^{r_f + r_p + 1} \cdot \mathbf{1}_{r_{out}} \end{pmatrix}, \qquad \mathbf{w}_{2 \cdot r_f + r_p} = \begin{pmatrix} \mathbf{0}_{r_{in}} \\ \mathbf{0}_{n \cdot (2 \cdot r_f + r_p - 1)} \\ \mathbf{1}_{r_{in}} \\ \mathbf{0}_{r_{out}} \\ d \cdot \mathbf{1}_{r_{out}} \end{pmatrix},$$

where $1 \leq i \leq r_f - 1$ *or* $r_f + r_p + 1 \leq i \leq 2 \cdot r_f + r_p - 1$ *and* $r_f + 1 \leq j \leq r_f + r_p - 1$*, and let* $\mathbf{W} = \begin{pmatrix} \mathbf{w}_0 & \dots & \mathbf{w}_{2 \cdot r_f + r_p} \end{pmatrix}^\intercal \in \mathbb{Z}_{\geq 0}^{(2 \cdot r_f + r_p + 1) \times n \cdot (2 \cdot r_f + r_p + 1)}$*. Let* $\mathbf{x}_{out} >_{LEX} \mathbf{x}^{(2 \cdot r_f + r_p)} >_{LEX} \dots >_{LEX} \mathbf{x}^{(1)} >_{LEX} \mathbf{x}_{in}$*, and let* $>_{\mathbf{W}, LEX}$ *be a weight order on the* Poseidon *polynomial ring. Assume that*

(i) $n > 2$,

(ii) $1 < r_{in} < n - 1$,

(iii) $\operatorname{rank}\left(\rho_{r_{in}, r_{in}}(\mathbf{M}_0)\right) = r_{in}$,

(iv) $\mathbf{M}_i$ *is in upper non-singular* $\rho_{r_{in}, r_{in}}$*-position for all* $1 \leq i \leq r_f$ *and* $r_f + r_p + 1 \leq 2 \cdot r_f + r_p - 1$,

(v) for all $r_f + 1 \leq j \leq r_f + r_p$:

  (a) $\operatorname{rank}\left(\sigma_{r_{out}, r_{out}}\left(\mathbf{M}_j^{-1}\right)\right) = r_{out}$,

(b) let $\mathbf{A}_j \in \mathbb{F}_q^{r_{in} \times r_{in}}$, $\mathbf{B}_j \in \mathbb{F}_q^{r_{in} \times r_{out}}$ and $\mathbf{C}_j \in \mathbb{F}_q^{r_{out} \times r_{in}}$ be the matrices of the $\sigma_{r_{out}, r_{out}}$-position of $\mathbf{M}_j^{-1}$, then $\mathbf{A}_j - \mathbf{B}_j \mathbf{C}_j$ has at least two non-zero entries on every row, and

(vi) $\mathbf{M}_{2 \cdot r_f + r_p}$ is in strong upper non-singular $\rho_{r_{in}, r_{in}}$-position.

Then

(1) A $>_{\mathbf{W}, LEX}$-Gröbner basis for $\mathcal{F}_{pre}$ can be computed via linear transformations.

(2) $\dim_{\mathbb{F}_q}(\mathcal{F}_{pre}) = d^{2 \cdot r_{in} \cdot r_f + r_p}$.

Proof. Let $\mathbf{N}_i$ denote the matrices to transform $\mathbf{M}_i$ / $\mathbf{M}_j^{-1}$ in $\rho_{r_{in}, r_{in}} / \sigma_{r_{out}, r_{out}}$-position, and let

$$\mathcal{G} = \left\{ \begin{matrix} \mathbf{g}^{(i)} = \begin{pmatrix} \mathbf{N}_i & \mathbf{0}_{r_{in} \times r_{out}} \\ \mathbf{0}_{r_{out} \times r_{in}} & \mathbf{I}_{r_{out} \times r_{out}} \end{pmatrix} \mathbf{f}_{\text{pre}}^{(i)}, \\ \mathbf{g}^{(j)} = \begin{pmatrix} \mathbf{I}_{r_{in} \times r_{in}} & -\mathbf{B}_j \mathbf{N}_j \\ \mathbf{0}_{r_{out} \times r_{in}} & \mathbf{N}_j \end{pmatrix} \mathbf{M}_j^{-1} \mathbf{f}_{\text{pre}}^{(j)} \end{matrix} \;\middle|\; \begin{matrix} 0 \leq i \leq r_f, \\ r_f + r_p + 1 \leq i \leq 2 \cdot r_f + r_p, \\ r_f + 1 \leq j \leq r_f + r_p \end{matrix} \right\}.$$

We claim that $\mathcal{G}$ is the $>_{\mathbf{W}, LEX}$-Gröbner basis of $\mathcal{F}_{\text{pre}}$.

- For $0 \leq i \leq r_f - 1$ and $r_f + r_p + 1 \leq i \leq 2 \cdot r_f + r_p$, the argument is identical to Theorem 3.4.
- For $i = r_f$, the weights $\mathbf{w}_0, \ldots, \mathbf{w}_{r_f - 1}$ produce ties analog to Theorem 3.4. For $\mathbf{g}^{(r_f)}|^{r_{in}}$ the weight vector $\mathbf{w}_{r_f}$ follows the structure of full SPN rounds, so we also have that
$$\mathrm{LM}_{>_{\mathbf{W}, LEX}} \left(\mathbf{g}^{(r_f)} \middle|^{r_{in}} \right) = \mathcal{S}\left(\mathbf{x}^{(r_f)} \right) \Big|^{r_{in}}.$$
For $\mathbf{g}^{(r_f)}|_{r_{out}}$, by definition of $\mathbf{w}_{r_f}$ the terms $\mathcal{S}\left(\mathbf{x}^{(r_f)} \right) \Big|^{r_{in}}$ have weight d, the terms $\mathcal{S}\left(\mathbf{x}^{(r_f)} \right) \Big|_{r_{out}}$ have weight 0, and the terms $\mathbf{x}^{(r_f+1)}|_{r_{out}}$ have weight d^2. Therefore,
$$\mathrm{LM}_{>_{\mathbf{W}, LEX}} \left(\mathbf{g}^{(r_f)} \Big|_{r_{out}} \right) = \mathbf{x}^{(r_f+1)} \Big|_{r_{out}}.$$
- For $r_f + 1 \leq i \leq r_f + r_p - 1$, we have that
$$\begin{pmatrix} \mathbf{I}_{r_{in} \times r_{in}} & -\mathbf{B}_i \\ \mathbf{0}_{r_{out} \times r_{in}} & \mathbf{I}_{r_{out} \times r_{out}} \end{pmatrix} \begin{pmatrix} \mathbf{I}_{r_{in} \times r_{in}} & \mathbf{0}_{r_{in} \times r_{out}} \\ \mathbf{0}_{r_{out} \times r_{in}} & \mathbf{N}_i \end{pmatrix} = \begin{pmatrix} \mathbf{I}_{r_{in} \times r_{in}} & -\mathbf{B}_i \mathbf{N}_i \\ \mathbf{0}_{r_{out} \times r_{in}} & \mathbf{N}_i \end{pmatrix},$$
and therefore
$$\begin{aligned} \mathbf{g}^{(i)} &= \begin{pmatrix} \mathbf{I}_{r_{in} \times r_{in}} & -\mathbf{B}_i \mathbf{N}_i \\ \mathbf{0}_{r_{out} \times r_{in}} & \mathbf{N}_i \end{pmatrix} \begin{pmatrix} {x_1^{(i)}}^d \\ x_2^{(i)} \\ \vdots \\ x_n^{(i)} \end{pmatrix} + \hat{\mathbf{c}}_i - \begin{pmatrix} \mathbf{A}_i & -\mathbf{B}_i \mathbf{N}_i \\ \mathbf{0}_{r_{out} \times r_{in}} & \mathbf{N}_i \end{pmatrix} \mathbf{M}_i^{-1} \mathbf{x}^{(i+1)} \\ &= \begin{pmatrix} \mathbf{I}_{r_{in} \times r_{in}} & -\mathbf{B}_i \mathbf{N}_i \\ \mathbf{0}_{r_{out} \times r_{in}} & \mathbf{N}_i \end{pmatrix} \begin{pmatrix} {x_1^{(i)}}^d \\ x_2^{(i)} \\ \vdots \\ x_n^{(i)} \end{pmatrix} + \hat{\mathbf{c}}_i - \begin{pmatrix} \mathbf{A}_i - \mathbf{B}_i \mathbf{C}_i & \mathbf{0}_{r_{in} \times r_{out}} \\ \mathbf{C}_i & \mathbf{I}_{r_{out} \times r_{out}} \end{pmatrix} \mathbf{x}^{(i+1)}, \end{aligned}$$
where $\hat{\mathbf{c}}_i \in \mathbb{F}_q^n$.

- Let us first consider $\mathbf{g}^{(i)}|^{r_{in}}$. For $0 \leq j < r_f - 1$ and $\mathbf{w}_j$, the term ${x_1^{(i)}}^d$ has weight d^{i+1-j}, the terms $\mathbf{x}^{(i)}|_{n-1}$ have weight d^{i-j} and the terms $\mathbf{x}^{(i+1)}$ have weight d^{i+1-j}. Moreover, by assumption $\mathbf{A}_i - \mathbf{B}_i\mathbf{C}_i$ has at least two non-zero entries on every row, so every component of $\mathbf{g}^{(i)}|^{r_{in}}$ has at least two terms of weight d^{i+1-j}, so we have produced ties.

  For $r_f \leq j < i - 1$, the terms $\mathcal{P}\left(\mathbf{x}^{(i)}\right)|^{r_{in}}$ have weight $d \cdot d^{i-j}$ and the terms $\mathbf{x}^{(i+1)}$ have weight d^{i-j+1}, so we have ties.

  For $\mathbf{w}_{i-1}$, the terms $\mathcal{P}\left(\mathbf{x}^{(i)}\right)\Big|^{r_{in}}$ have weight 0 but the terms $\mathbf{x}^{(i)}|_{r_{out}}$ and $\mathbf{x}^{(i+1)}$ have weight d^2. By assumption $\mathbf{A}_i - \mathbf{B}_i\mathbf{C}_i$ has at least two non-zero entries on every row, so we again produced ties.

  Now we have to decide according to $\mathbf{w}_i$, but then trivially

  $$\mathrm{LM}_{>_{\mathbf{W},LEX}}\left(\mathbf{g}^{(i)}\Big|^{r_{in}}\right) = \mathcal{P}\left(\mathbf{x}^{(i)}\right)\Big|^{r_{in}}.$$

- Now we consider $\mathbf{g}^{(i)}|_{r_{out}}$. For $0 \leq j \leq i - 1$ and $\mathbf{w}_j$, the terms $\mathbf{x}^{(i)}|_{r_{out}}$ have weight d^{i-j} but the terms $\mathbf{x}^{(i+1)}$ have weight d^{i+1-j}. Depending on $\mathbf{C}_i$ there are either at least two terms of weight d^{i+1-j} present, one is coming from $\mathbf{x}^{(i+1)}|^{r_{in}}$ and one from $\mathbf{x}^{(i+1)}|_{r_{out}}$, or only one from $\mathbf{x}^{(i+1)}|_{r_{out}}$. The second case forces a trivial decision, so let us assume that one term from $\mathbf{x}^{(i+1)}|^{r_{in}}$ is present.

  For $\mathbf{w}_i$, the terms $\mathbf{x}^{(i)}|_{r_{out}}$ and $\mathbf{x}^{(i+1)}|^{r_{in}}$ have weight 0 but the terms $\mathbf{x}^{(i+1)}|_{r_{out}}$ have weight d^2. So,

  $$\mathrm{LM}_{>_{\mathbf{W},LEX}}\left(\mathbf{g}^{(i)}\Big|_{r_{out}}\right) = \mathbf{x}^{(i+1)}|_{r_{out}}.$$

- For $i = r_f + r_p$, analog to the previous case the weights $\mathbf{w}_0, \dots, \mathbf{w}_{r_f+r_p-1}$ produce ties on $\mathbf{g}^{(r_f+r_p)}|^{r_{in}}$. So we have to decide via $\mathbf{w}_{r_f+r_p}$ which yields

  $$\mathrm{LM}_{>_{\mathbf{W},LEX}}\left(\mathbf{g}^{(i)}\Big|^{r_{in}}\right) = \mathcal{P}\left(\mathbf{x}^{(i)}\right)\Big|^{r_{in}}.$$

  For $\mathbf{g}^{(r_f+r_p)}|_{r_{out}}$, analog to the previous case we either have a trivial decision for a term of $\mathbf{x}^{(r_f+r_p+1)}|_{r_{out}}$, or we have to decide via $\mathbf{w}_{r_f+r_p}$ analog to the previous case which yields

  $$\mathrm{LM}_{>_{\mathbf{W},LEX}}\left(\mathbf{g}^{(r_f+r_p)}\Big|_{r_{out}}\right) = \mathbf{x}^{(r_f+r_p+1)}|_{r_{out}}.$$

Hence, the leading monomials of $\mathcal{G}$ are pairwise coprime, and the claim follows again from Lemma 2.10.

For the vector space dimension, we note that the only non-linear monomials in the ideal of leading terms are $\mathcal{S}\left(\mathbf{x}^{(i)}\right)\Big|^{r_{in}}$ and ${x_1^{(j)}}^d$, where $1 \leq i \leq r_f$ or $r_f + r_p + 1 \leq i \leq 2 \cdot r_f + r_p$ and $r_f + 1 \leq j \leq r_f + r_p$. So the claim follows. □

Obviously, Assumption (v) (b) cannot be satisfied for $r_{in} = 1$, since $\mathbf{A}_i$ is a 1×1 matrix then. Nevertheless, the proof of Theorem 3.8 trivially extends to this case.

Corollary 3.9. *Let $\mathbb{F}_q$ be a finite field, let $d, n, r_f, r_p, r_{in}, r_{out} \in \mathbb{Z}_{\geq 1}$ be integers such that $n = r_{in} + r_{out}$, and let $\mathcal{F}_{pre} = \left\{\mathbf{f}_{pre}^{(i)}\right\}_{0 \leq i \leq r} \subset \mathbb{F}_q\left[\mathbf{x}_{in}, \mathbf{x}^{(1)}, \dots, \mathbf{x}^{(2 \cdot r_f + r_p)}, \mathbf{x}_{out}\right]$ be a* Poseidon *preimage polynomial system with the parameters d, n, r_f, r_p, r_{in} and r_{out}. Let $>_{\mathbf{W},LEX}$ be the weight order from Theorem 3.8. Assume that*

(i) $n > 2$,

(ii) $r_{in} = 1$,

(iii) $\operatorname{rank}\left(\rho_{r_{in},r_{in}}(\mathbf{M}_0)\right) = r_{in}$,

(iv) $\mathbf{M}_i$ *is in upper non-singular* $\rho_{r_{in},r_{in}}$*-position for all* $1 \leq i \leq r_f$ *and* $r_f + r_p + 1 \leq 2 \cdot r_f + r_p - 1$,

(v) *for all* $r_f + 1 \leq j \leq r_f + r_p$*:*

  (a) $\operatorname{rank}\left(\sigma_{r_{out},r_{out}}\left(\mathbf{M}_j^{-1}\right)\right) = r_{out}$,

  (b) *let* $\mathbf{N}_j \in \mathbb{F}_q^{r_{out} \times r_{out}}$*,* $\mathbf{A}_j \in \mathbb{F}_q^{r_{in} \times r_{in}}$*,* $\mathbf{B}_j \in \mathbb{F}_q^{r_{in} \times r_{out}}$ *and* $\mathbf{C}_j \in \mathbb{F}_q^{r_{out} \times r_{in}}$ *be the matrices of the* $\sigma_{r_{out},r_{out}}$*-position of* $\mathbf{M}_j^{-1}$*, then* $\mathbf{B}_j\mathbf{N}_j$ *and* $\mathbf{A}_j - \mathbf{B}_j\mathbf{C}_j$ *are non-zero, and*

(vi) $\mathbf{M}_{2 \cdot r_f + r_p}$ *is in strong upper non-singular* $\rho_{r_{in},r_{in}}$*-position.*

Then

(1) A $>_{\mathbf{W},LEX}$*-Gröbner basis for* $\mathcal{F}_{pre}$ *can be computed via linear transformations.*

(2) $\dim_{\mathbb{F}_q}(\mathcal{F}_{pre}) = d^{2 \cdot r_f + r_f}$.

Proof. Let $\mathcal{G}$ as in the proof of Theorem 3.8. The assumption that $\mathbf{A}_i - \mathbf{B}_i\mathbf{C}_i$ has at least two non-zero entries was used to compute the leading monomials of $\mathcal{P}\big(\mathbf{x}^{(i)}\big)\Big|^{r_{in}}$, so let us replace it by our new assumption.

Let $r_f + 1 \leq i \leq r_f + r_p$, recall that

$$\mathbf{g}^{(i)} = \begin{pmatrix} \mathbf{I}_{1 \times 1} & -\mathbf{B}_i\mathbf{N}_i \\ \mathbf{0}_{r_{out} \times 1} & \mathbf{N}_i \end{pmatrix} \begin{pmatrix} {x_1^{(i)}}^d \\ x_2^{(i)} \\ \vdots \\ x_n^{(i)} \end{pmatrix} + \hat{\mathbf{c}}_i - \begin{pmatrix} \mathbf{A}_i - \mathbf{B}_i\mathbf{C}_i & \mathbf{0}_{1 \times r_{out}} \\ \mathbf{C}_i & \mathbf{I}_{r_{out} \times r_{out}} \end{pmatrix} \mathbf{x}^{(i+1)}.$$

Now let $0 \leq j < i - 1$, $\mathcal{P}\big(\mathbf{x}^{(i)}\big)\Big|^{r_{in}} = \left({x_1^{(i)}}^d\right)$ so the term orders $\mathbf{w}_0, \dots, \mathbf{w}_{i-2}$ trivially produce ties. For $\mathbf{w}_{i-1}$, the term $x_1^{(i)}$ has weight 0 but the terms $\mathbf{x}^{(i)}|_{r_{out}}$ and $\mathbf{x}^{(i+1)}$ have weight d^2. By assumption $\mathbf{B}_i\mathbf{N}_i$ and $\mathbf{A}_i - \mathbf{B}_i\mathbf{C}_i$ are non-zero, so there are always to terms of weight d^2 present, and we have to decide according to $\mathbf{w}_i$. □

Analog to Proposition 3.5, we need a minor correction of the weight vectors for $r_{in} = n - 1$.

Proposition 3.10. *Let* $\mathbb{F}_q$ *be a finite field, let* $d, n, r_f, r_p, r_{in}, r_{out} \in \mathbb{Z}_{\geq 1}$ *be integers such that* $n = r_{in} + r_{out}$*, and let* $\mathcal{F}_{pre} = \left\{\mathbf{f}_{pre}^{(i)}\right\}_{0 \leq i \leq r} \subset \mathbb{F}_q\big[\mathbf{x}_{in}, \mathbf{x}^{(1)}, \dots, \mathbf{x}^{(2 \cdot r_f + r_p)}, \mathbf{x}_{out}\big]$ *be a* POSEIDON *preimage polynomial system with the parameters* d, n, r_f, r_p, r_{in} *and* r_{out}*. Let* $\mathbf{w}_0, \dots, \mathbf{w}_{2 \cdot r_f + r_p} \in \mathbb{Z}_{\geq 0}^{n \cdot (2 \cdot r_f + r_p + 1)}$ *be weight vectors defined as*

$$\mathbf{w}_0 = \begin{pmatrix} \mathbf{1}_{r_{in}} \\ \mathbf{0}_n \\ d^2 \cdot \mathbf{1}_n \\ \vdots \\ d^{2 \cdot r_f + r_p} \cdot \mathbf{1}_n \\ d^{2 \cdot r_f + r_p + 1} \cdot \mathbf{1}_{r_{out}} \end{pmatrix}, \qquad \mathbf{w}_i \quad = \begin{pmatrix} \mathbf{0}_{r_{in}} \\ \mathbf{0}_{n \cdot (i-1)} \\ \mathbf{1}_{r_{in}} \\ \mathbf{0}_{r_{out}} \\ \mathbf{0}_n \\ d^2 \cdot \mathbf{1}_n \\ \vdots \\ d^{2 \cdot r_f + r_p - i} \cdot \mathbf{1}_n \\ d^{2 \cdot r_f + r_p + 1 - i} \cdot \mathbf{1}_{r_{out}} \end{pmatrix},$$

$$\mathbf{w}_{r_f} = \begin{pmatrix} \mathbf{0}_{r_{in}} \\ \mathbf{0}_{n \cdot (r_f - 1)} \\ \mathbf{1}_{r_{in}} \\ \mathbf{0}_{r_{out}} \\ \mathbf{0}_{r_{in}} \\ d^2 \cdot \mathbf{1}_{r_{out}} \\ d^2 \cdot \mathbf{1}_n \\ \vdots \\ d^{r_f + r_p} \cdot \mathbf{1}_n \\ d^{r_f + r_p + 1} \cdot \mathbf{1}_n \end{pmatrix}, \qquad \mathbf{w}_j = \begin{pmatrix} \mathbf{0}_{r_{in}} \\ \mathbf{0}_{n \cdot (j - 1)} \\ 1 \\ d \cdot \mathbf{1}_{r_{in} - 1} \\ \mathbf{0}_{r_{out}} \\ \mathbf{0}_{r_{in}} \\ d^2 \cdot \mathbf{1}_{r_{out}} \\ d^2 \cdot \mathbf{1}_n \\ \vdots \\ d^{2 \cdot r_f + r_p - j} \cdot \mathbf{1}_n \\ d^{2 \cdot r_f + r_p + 1 - j} \cdot \mathbf{1}_{r_{out}} \end{pmatrix},$$

$$\mathbf{w}_{r_f + r_p} = \begin{pmatrix} \mathbf{0}_{r_{in}} \\ \mathbf{0}_{n \cdot (r_f + r_p - 1)} \\ 1 \\ d \cdot \mathbf{1}_{r_{in} - 1} \\ \mathbf{0}_{r_{out}} \\ \mathbf{0}_n \\ d^2 \cdot \mathbf{1}_n \\ \vdots \\ d^{r_f + r_p} \cdot \mathbf{1}_n \\ d^{r_f + r_p + 1} \cdot \mathbf{1}_{r_{out}} \end{pmatrix}, \qquad \mathbf{w}_{2 \cdot r_f + r_p} = \begin{pmatrix} \mathbf{0}_{r_{in}} \\ \mathbf{0}_{n \cdot (2 \cdot r_f + r_p - 1)} \\ \mathbf{1}_{r_{in}} \\ \mathbf{0}_{r_{out}} \\ \mathbf{0}_{r_{out}} \end{pmatrix},$$

where $1 \leq i \leq r_f - 1$ *or* $r_f + r_p + 1 \leq i \leq 2 \cdot r_f + r_p - 1$ *and* $r_f + 1 \leq j \leq r_f + r_p - 1$, *and let* $\mathbf{W} = \begin{pmatrix} \mathbf{w}_0 & \dots & \mathbf{w}_{2 \cdot r_f + r_p} \end{pmatrix}^\intercal \in \mathbb{Z}_{\geq 0}^{(2 \cdot r_f + r_p + 1) \times n \cdot (2 \cdot r_f + r_p + 1)}$. *Let* $x_{out} >_{LEX} \mathbf{x}^{(2 \cdot r_f + r_p)} >_{LEX} \ldots >_{LEX} \mathbf{x}^{(1)} >_{LEX} \mathbf{x}_{in}$, *and let* $>_{\mathbf{W}, LEX}$ *be a weight order on the* Poseidon *polynomial ring. Assume that*

(i) $n > 2$,

(ii) $r_{in} = n - 1$,

(iii) the matrix $\mathbf{M}_0$ *is in strong lower non-singular* $\rho_{r_{in}, r_{in}}$*-position,*

(iv) for all $1 \leq i \leq r_f$ *and* $r_f + r_p + 1 \leq i \leq 2 \cdot r_f + r_p - 1$*:*

- *(a)* $\operatorname{rank}\left(\rho_{r_{in}, r_{in}}(\mathbf{M}_i)\right) = r_{in}$,
- *(b) let* $\mathbf{N}_i \in \mathbb{F}_q^{r_{in} \times r_{in}}$ *be the matrix of the* $\rho_{r_{in}, r_{in}}$*-transformation of* $\mathbf{M}_i$*, then* $\mathbf{N}_i$ *has at least two non-zero entries in every row,*

(v) $\operatorname{rank}\left(\rho_{r_{in}, r_{in}}(\mathbf{M}_{2 \cdot r_f + r_p})\right) = r_{in}$,

(vi) for all $r_f + 1 \leq j \leq r_f + r_p$*:*

- *(a)* $\operatorname{rank}\left(\sigma_{r_{out}, r_{out}}\left(\mathbf{M}_j^{-1}\right)\right) = r_{out}$, *and*
- *(b) let* $\mathbf{A}_j \in \mathbb{F}_q^{r_{in} \times r_{in}}$, $\mathbf{B}_j \in K^{r_{in} \times r_{out}}$ *and* $\mathbf{C}_j \in K^{r_{out} \times r_{in}}$ *be the matrices of the* $\sigma_{r_{out}, r_{out}}$*-position of* $\mathbf{M}_j$*, then* $\mathbf{A}_j - \mathbf{B}_j \mathbf{C}_j$ *has at least two non-zero entries on every row.*

Then

(1) A $>_{\mathbf{W}, LEX}$*-Gröbner basis for* $\mathcal{F}_{pre}$ *can be computed via linear transformations.*

(2) $\dim_{\mathbb{F}_q}\left(\mathcal{F}_{pre}\right) = d^{2 \cdot r_{in} \cdot r_f + r_f}$.

Proof. Let $\mathcal{G}$ be as in the proof of Theorem 3.8.

- For $0 \leq i \leq r_f - 1$ and $r_f + r_p + 1 \leq i \leq 2 \cdot r_f + r_p$, follows analog to Proposition 3.5.
- For $i = r_f$, the weights $\mathbf{w}_0, \dots, \mathbf{w}_{r_f - 1}$ produce ties analog to Proposition 3.5, and $\mathbf{w}_{r_f}$ decides as in Theorem 3.8.
- For $r_f + 1 \leq i \leq r_f + r_p$, let $0 \leq j < i - 1$. Then $\mathbf{w}_j$ produces ties on the terms of $\mathbf{g}^{(i)}$ analog to Theorem 3.8.

  For $\mathbf{w}_{i-1}$, on $\mathbf{g}^{(i)}|^{r_{in}}$ the terms $\mathcal{P}\left(\mathbf{x}^{(i)}\right)$ have weight 0 but the ones of $\mathbf{x}^{(i+1)}$ have weight d^2. Since by assumption the matrix $\mathbf{A}_j - \mathbf{B}_j \mathbf{C}_j$ has at least two non-zero entries on every row, at least two terms of $\mathbf{x}^{(i+1)}|^{r_{in}}$ are present in every component of $\mathbf{g}^{(i)}|^{r_{in}}$, so we have a tie.

  Then we have to decide with $\mathbf{w}_i$ which yields

  $$\mathrm{LM}_{>_{\mathbf{W},LEX}}\left(\mathbf{g}^{(i)}|^{r_{in}}\right) = \mathcal{P}\Big(\mathbf{x}^{(i)}\Big)\Big|^{r_{in}}.$$

  For $\mathbf{g}^{(i)}|_{r_{out}}$ and $\mathbf{w}_{i-1}$, the terms $\mathbf{x}^{(i)}|_{r_{out}}$ have weight 0 but the ones $\mathbf{x}^{(i+1)}$ have weight d^2, so we again have

  $$\mathrm{LM}_{>_{\mathbf{W},LEX}}\left(\mathbf{g}^{(i)}\big|_{r_{out}}\right) = \mathbf{x}^{(i+1)}|^{r_{out}}.$$

- For $i = r_f + r_p$, the weights $\mathbf{w}_0, \dots, \mathbf{w}_{r_f + r_p - 1}$ produce ties analog to the previous case, but decision with $\mathbf{w}_{r_f + r_p}$ yields that

  $$\mathrm{LM}_{>_{\mathbf{W},LEX}}\left(\mathbf{g}^{(r_f + r_p)}|^{r_{in}}\right) = \mathcal{P}\Big(\mathbf{x}^{(r_f + r_p)}\Big)\Big|^{r_{in}}.$$

  For $\mathbf{g}^{(r_f + r_p)}|_{r_{out}}$ we either have a trivial decision for a term of $\mathbf{x}^{(r_f + r_p + 1)}|_{r_{out}}$ analog to Theorem 3.8, or we have to decide via $\mathbf{w}_{r_f + r_p}$ which yields

  $$\mathrm{LM}_{>_{\mathbf{W},LEX}}\left(\mathbf{g}^{(r_f + r_p)}\big|_{r_{out}}\right) = \mathbf{x}^{(r_f + r_p + 1)}\big|_{r_{out}}.$$

Again, we have pairwise coprime leading monomials, so being a Gröbner basis follows from Lemma 2.10.

Counting the number of monomials not contained in the ideal of leading terms follows analog to Theorem 3.8. □

Analog to Corollary 3.6, we also need a minor correction for $n = 2$.

Corollary 3.11. *Let $\mathbb{F}_q$ be a finite field, let $d, n, r_f, r_p, r_{in}, r_{out} \in \mathbb{Z}_{\geq 1}$ be integers such that $n = 2$, $r_{in} = 2$ and $n = r_{in} + r_{out}$, and let $\mathcal{F}_{pre} = \left\{\mathbf{f}_{pre}^{(i)}\right\}_{0 \leq i \leq r} \subset \mathbb{F}_q\big[x_{in}, \mathbf{x}^{(i)}, x_{out} \mid 1 \leq i \leq 2 \cdot r_f + r_p\big]$ be a* Poseidon *preimage polynomial system with the parameters d, n, r_f, r_p, r_{in} and r_{out}. Let $\mathbf{W} \in \mathbb{Z}^{(2 \cdot r_f + r_p + 1) \times n \cdot (2 \cdot r_f + r_p)}$ be the weight matrix from Theorem 3.8, let $x_1^{(2 \cdot r_f + r_p)} >_{LEX} x_{out} >_{LEX} x_2^{(2 \cdot r_f + r_p)} >_{LEX} \ldots >_{LEX} \mathbf{x}^{(1)} >_{LEX} x_{in}$, and let $>_{\mathbf{W},LEX}$ be a weight order on the* Poseidon *polynomial ring. Assume that*

(i) $\mathbf{M}_i$ is in upper non-singular $\rho_{r_{in}, r_{in}}$-position for all $0 \leq i \leq r_f$ and $r_f + r_p + 1 \leq i \leq 2 \cdot r_f + r_p$, and

(ii) for all $r_f + 1 \leq j \leq r_f + r_p$:

(a) $\mathrm{rank}\left(\sigma_{r_{out}, r_{out}}\left(\mathbf{M}_j^{-1}\right)\right) = r_{out}$, and

(b) let $\mathbf{N}_j \in \mathbb{F}_q^{r_{out} \times r_{out}}$*,* $\mathbf{A}_j \in \mathbb{F}_q^{r_{in} \times r_{in}}$*,* $\mathbf{B}_j \in \mathbb{F}_q^{r_{in} \times r_{out}}$ *and* $\mathbf{C}_j \in \mathbb{F}_q^{r_{out} \times r_{in}}$ *be the matrices of the* $\sigma_{r_{out}, r_{out}}$*-position of* $\mathbf{M}_j^{-1}$*, then* $\mathbf{B}_j \mathbf{N}_j$ *and* $\mathbf{A}_j - \mathbf{B}_j \mathbf{C}_j$ *are non-zero.*

Then

(1) A $>_{\mathbf{W}, LEX}$*-Gröbner basis for* $\mathcal{F}_{pre}$ *can be computed via linear transformations.*

(2) $\dim_{\mathbb{F}_q} \left(\mathcal{F}_{pre} \right) = d^{2 \cdot r_f + r_p}$.

Proof. Let $\mathcal{G}$ be as in Theorem 3.8. Analog to Corollary 3.6, we replace $\mathbf{g}^{(2 \cdot r_f + r_p)}$ by

$$\hat{\mathbf{g}}^{(r)} = \begin{pmatrix} 1 & \gamma \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ B_r & 1 \end{pmatrix} \mathbf{g}^{(r)},$$

where $\gamma \in \mathbb{F}_q^\times$ is chosen such that the coefficient of ${x_2^{(r)}}^d$ in $\hat{g}_1^{(2 \cdot r_f + r_p)}$ is non-zero. Now the claim follows analog to Corollary 3.6, Theorem 3.8 and Corollary 3.9. □

3.3 Horizontal Separation for CICO Polynomial Systems

Lastly, let us give an outlook how the Gröbner bases from Sections 2.2 and 3.2 can be extended to CICO polynomial systems. Recall that in the Horizontal Separation Lemma (Lemma 3.2) we exploited that input variables lie above, and output variables lie below the horizontal line. In CICO problems on the other hand, input as well as output variables lie above the line, see Equation (4). Luckily, for a single round SPN the variable position can easily be corrected by inverting the matrix and applying an additional linear transformation to separate the output variables along a horizontal line.

To formalize the transformation we need another map analog to Definitions 3.1 and 3.7.

Definition 3.12. *Let* K *be a field, let* $k, l, m, n \in \mathbb{Z}_{\geq 1}$ *be integers such that* $k \leq m$ *and* $l \leq n$*, and let*

$$\begin{aligned} \tau_{k,l} : K^{m \times n} &\to K^{k \times l}, \\ \mathbf{M} &\mapsto \begin{pmatrix} \mathbf{0}_{(m-k) \times l} & \mathbf{0}_{(m-k) \times (n-l)} \\ \mathbf{I}_{k \times l} & \mathbf{0}_{k \times (n-l)} \end{pmatrix} \mathbf{M}. \end{aligned}$$

Note that for the CICO Horizontal Separation Lemma we can work with the DRL term order.

Lemma 3.13 (CICO Horizontal Separation Lemma)**.** *Let* K *be a field, and let* $d, n, r_{in}, r_{out} \in \mathbb{Z}_{\geq 1}$ *be integers such that* $r_{in} < n$ *and* $n = r_{in} + r_{out}$*. Let* $\boldsymbol{\alpha} \in \mathbb{F}_q^{r_{out}}$ *and* $\boldsymbol{\beta} \in \mathbb{F}_q^{r_{in}}$*, let* $\mathbf{M} \in K^{n \times n}$ *be a matrix such that* $\operatorname{rank}\left(\tau_{r_{out}, r_{out}} \left(\mathbf{M}^{-1} \right) \right) = r_{out}$*, and let*

$$\mathcal{F} = \left\{ \mathbf{M} \begin{pmatrix} x_1^d \\ \vdots \\ x_{r_{in}}^d \\ \boldsymbol{\alpha} \end{pmatrix} - \begin{pmatrix} y_1 \\ \vdots \\ y_{r_{out}} \\ \boldsymbol{\beta} \end{pmatrix} \right\} \subset K[x_1, \dots, x_{r_{in}}, y_1, \dots, y_{r_{out}}].$$

Then a $>_{DRL}$*-Gröbner basis of* $\mathcal{F}$ *can be computed via a linear transformation.*

Proof. By the assumption $\operatorname{rank}\left(\tau_{r_{out}, r_{out}} \left(\mathbf{M}^{-1} \right) \right) = r_{out}$, we can find an invertible matrix

$\mathbf{N} \in K^{r_{out} \times r_{out}}$ such that

$$\mathcal{G} = \begin{pmatrix} \mathbf{I}_{r_{in} \times r_{in}} & \mathbf{0}_{r_{in} \times r_{out}} \\ \mathbf{0}_{r_{out} \times r_{in}} & \mathbf{N} \end{pmatrix} \mathcal{F} = \begin{pmatrix} x_1^d \\ \vdots \\ x_{r_{in}}^d \\ \gamma_1 \\ \vdots \\ \gamma_{r_{out}} \end{pmatrix} - \begin{pmatrix} \mathbf{A} & \mathbf{B} \\ \mathbf{I}_{r_{out} \times r_{out}} & \mathbf{C} \end{pmatrix} \begin{pmatrix} y_1 \\ \vdots \\ y_{r_{out}} \\ \beta_1 \\ \vdots \\ \beta_{r_{in}} \end{pmatrix},$$

for some matrices $\mathbf{A} \in K^{r_{in} \times r_{out}}$, $\mathbf{B} \in K^{r_{out} \times r_{in}}$, $\mathbf{C} \in K^{r_{in} \times r_{out}}$ and $\boldsymbol{\gamma} = \mathbf{N}\boldsymbol{\alpha}$. The first r_{in} components then have DRL leading monomials x_i^d, and the last r_{out} components have leading monomials y_j. Therefore, the components of $\mathcal{G}$ have pairwise coprime leading monomials, so by [CLO15, Chapter 2 §9 Theorem 3, Proposition 4] $\mathcal{G}$ is a $>_{DRL}$-Gröbner basis. □

We record the Gröbner bases for SPN and Poseidon CICO problems in Appendix B. Essentially, they differ from their preimage counterparts only in the last round, where we invert the matrix and apply a linear transformation relative to $\tau_{r_{out}, r_{out}}$ for horizontal separation.

4 Cryptanalytic Applications

Now that we have found Poseidon Gröbner bases, let us discuss how we can extract the cryptographically relevant solutions. Recall from the introduction that we could use a term order conversion algorithm to convert to a LEX Gröbner basis, and then factor a univariate polynomial. Let $I \subset P = K[x_1, \dots, x_n]$ be a zero-dimensional ideal, and let $D = \dim_K(I)$ be the K-vector space dimension of the quotient ring P/I. Moreover, for (arbitrary) polynomial ideals I we denote the variety of I, i.e. its set of zeros, as

$$\mathcal{V}(I) = \{\mathbf{x} \in K^n \mid \forall f \in I \colon f(\mathbf{x}) = 0\}. \tag{9}$$

It is well known that $D < \infty$ if and only if $|\mathcal{V}(I)| < \infty$, and that $D = |\mathcal{V}(I)|$ for radical ideals over algebraically closed fields.

The original FGLM algorithm [FGLM93] performs term order conversion in $\mathcal{O}\left(n \cdot D^3\right)$. An improved probabilistic version [FGHR14] achieves $\mathcal{O}(n \cdot D^\omega)$, where $2 \leq \omega < 2.37286$ [AW21] is a linear-algebra constant, and an improved sparse linear algebra a variant [FM17] achieves $\mathcal{O}\left(\sqrt{n} \cdot D^{2 + \frac{n-1}{n}}\right)$. To the best of our knowledge complexity analysis of [FGHR14, FM17] is only performed for the DRL term order.

Moreover, if $K = \mathbb{F}_q$, then extraction of the $\mathbb{F}_q$-valued solutions of the univariate polynomial can be done via the greatest common divisor (GCD) with the field equation [BBLP22, §3.1]. The complexity of this GCD computation[1] is

$$\mathcal{O}\Big(D \cdot \log(D) \cdot \log\big(\log(D)\big) \cdot \big(\log(D) + \log(q)\big)\Big), \tag{10}$$

for $D \leq q$, else D and q have to be exchanged in the complexity estimate.

As already mentioned, for our custom term orders we would either have to redo the FGLM complexity analysis or extrapolate the DRL complexities. Luckily, this analysis can be bypassed via linear algebra-based techniques.

In [KR16, Chapter 6] Kreuzer & Robbiano discuss how to compute the variety $\mathcal{V}(I)$ in case a vector space basis $\mathcal{B}$ of the quotient space is known. In particular, if a $>$-Gröbner

[1] The method applies an auxiliary division by remainder step to reduce the field equation to a polynomial of degree $\leq D - 1$, hence the complexity differs from the standard GCD.

basis $\mathcal{G} \subset I$ is known, then we can easily compute the ideal of $>$-leading terms, and the K-vector space basis $\mathcal{B}$ are simply the monomials not contained in the ideal of leading terms. Now let us fix some $f \in P$, we can set up a multiplication map for f in P/I, see [KR16, Definition 4.1.4]

$$\theta_f : P/I \to P/I, \qquad x \mapsto f \cdot x. \tag{11}$$

Since P/I is a finite dimensional K-vector space and the map is K-linear, θ_f can be represented as matrix. This is called the multiplication matrix $\mathbf{M}_f$ of f in R/I. Given a $>$-Gröbner basis $\mathcal{G} \subset I$ computation of the multiplication matrix $\mathbf{M}_f$ is straight-forward: First index the columns of the matrix by the elements of $\mathcal{B}$, and rows by $f \cdot b$, where $b \in \mathcal{B}$. Now compute $f \cdot b \mod \mathcal{G}$, extract its coefficient vector with respect to $\mathcal{B}$ and fill it into the row $b \cdot f$. In particular over the algebraic closure $\bar{K}$ of K, if we pick a variable x_i, then the i^{th} coordinate of a point $\mathbf{x} \in \mathcal{V}_{\bar{K}}(I)$ is an eigenvalue of the multiplication matrix $\mathbf{M}_{x_i}$, see [KR16, Corollary 6.2.3]. Hence, we can compute the variety $\mathcal{V}_{\bar{K}}(I)$ by computing the eigenvalues of $\mathbf{M}_{x_1}, \dots, \mathbf{M}_{x_n}$, taking all possible combinations of the eigenvalues, and finally verifying whether a combination is indeed a point in the variety. This approach is known as the *Eigenvalue Method* [KR16, Algorithm 6.2.7]. The complexity of eigenpolynomial computations is equivalent to the complexity of determinant computations, and via fast matrix multiplication the determinant of an $\mathbf{M} \in K^{N \times N}$ matrix can be computed in, see [AHU74, Theorem 6.6], $\mathcal{O}(N^\omega)$, where again $2 \leq \omega < 2.37286$. Therefore, the complexity of the computation of the eigenpolynomials is

$$\mathcal{O}(n \cdot D^\omega), \tag{12}$$

i.e. it is identical to the complexity of the probabilistic FGLM algorithm [FGHR14]. This is no coincidence, the probabilistic FGLM utilizes the multiplication matrices $\mathbf{M}_{x_1}, \dots, \mathbf{M}_{x_n}$ to construct the LEX Gröbner basis.

Moreover, Equation (12) can be improved. First, we only care about solutions for the input variables $\mathbf{x}_{in}$. Moreover, our sponge functions are given by permutations, so alternatively we could solve for $\mathbf{x}_{out}$ and simply invert the permutation. Hence, we can estimate the construction of the eigenpolynomials as

$$\mathcal{O}(\min\{r_{in}, r_{out}\} \cdot D^\omega). \tag{13}$$

Lastly, we only care about $\mathbb{F}_q$-valued solutions, therefore we can again estimate the complexity of eigenpolynomial factoring via Equation (10). In total, we yield the complexities

$$\mathcal{O}\Bigg(\min\{r_{in}, r_{out}\} \cdot \Big(D^\omega + D \cdot \log(D) \cdot \log\big(\log(D)\big) \cdot \big(\log(D) + \log(q)\big)\Big)\Bigg), \tag{14}$$

if $D \leq q$, and

$$\mathcal{O}\Bigg(\min\{r_{in}, r_{out}\} \cdot \Big(D^\omega + q \cdot \log(q) \cdot \log\big(\log(q)\big) \cdot \big(\log(q) + \log(D)\big)\Big)\Bigg), \tag{15}$$

if $D > q$, to solve the preimage or CICO problem if a Gröbner basis is known.

Readers should keep in mind that these are generic estimations, i.e. they do not take the structure of the Gröbner basis into account. If we take a closer look onto the bases of Section 3 and Appendix B we realize that the Gröbner basis elements are rather sparse. For the round $0 < i < r$, a basis element only contains variables coming from $\mathbf{x}^{(i)}$ and $\mathbf{x}^{(i+1)}$, and analog for the 0th and r^{th} round. Let us take the variable $x_{in,1}$ and some $b \in \mathcal{B}$, when does a non-trivial reduction $x_{in,1} \cdot b \mod \mathcal{G}$ occur? Of course, one reduction takes place with respect to $x_{in,1}$ but if $\gcd\left(b, \mathbf{x}^{(1)}\right) = 1$, then no more reductions occur. As consequence, almost all entries of the row $x_{in,1} \cdot b$ are going to be zero. Therefore, we can develop the determinant via *Laplace expansion* and cut almost all summands. Of course, we can recursively iterate this expansion for all coprime basis elements until we end up with smaller but dense matrices.

We leave the precise estimation of the potential complexity gain as problem for future work. But we use this observation to justify our complexity estimations on Poseidon. For a given κ-bit security level, we say that the instance resist generic eigenpolynomial computation if

$$\log_2\big(\min\{r_{in}, r_{out}\}\big) + \omega \cdot \log_2(D) \geq \kappa, \tag{16}$$

and we say the instance resists root extraction if

$$\left.\begin{cases} D \cdot \log(D) \cdot \log\big(\log(D)\big) \cdot \big(\log(D) + \log(q)\big), & D \leq q \\ q \cdot \log(q) \cdot \log\big(\log(q)\big) \cdot \big(\log(q) + \log(D)\big), & D > q \end{cases}\right\} \geq 2^{\kappa}. \tag{17}$$

I.e., for root extraction we assume that construction for the eigenpolynomials is either for free or can be done below the root extraction complexity.

4.1 Poseidon Complexity Estimation

In this subsection we assume that a Poseidon instance satisfies the necessary matrix conditions for the Gröbner bases. Summarizing our results from Section 3.2 and Appendix B.2, for a Poseidon Gröbner basis we have that

$$D_{\text{Poseidon}} = \dim_{\mathbb{F}_q}\left(\mathcal{F}_{\text{pre}}\right) = \dim_{\mathbb{F}_q}\left(\mathcal{F}_{\text{CICO}}\right) = d^{2 \cdot r_{in} \cdot r_f + r_p}, \tag{18}$$

which obviously becomes optimal for $r_{in} = 1$.

Therefore, for a Poseidon CICO problem, see Equation (4), with $r_{in} + r_{out} > n$, one is best advise guessing input variables until $n = \tilde{r}_{in} + r_{out}$. In theory, we could further improve the theoretical complexity by guessing other input variables until $\tilde{r}_{in} = 1$ and leaving some prespecified output constants as open variables, i.e. $\tilde{r}_{out} = n - 1$. Though, we have to stress that for the further guessing there is no guarantee that a $\mathbb{F}_q$-valued solution exists.

In principle, one can proceed in an analog manner for the Poseidon preimage problem, see Equation (3). In particular, if $\log_2(q) \geq 250$, then a Poseidon sponge could return just one field element as output and still achieve 125 bits of birthday security, i.e. $r_{out} = n - 1$. Then, we have to guess input variables until $\tilde{r}_{in} = 1$, else the polynomial system is always undetermined.

Summarizing, for both problems if $n > r_{in} + r_{out}$, then we have to guess some input/output variables or leave some input/output constants as variables until $n = \tilde{r}_{in} + \tilde{r}_{out}$, then solve for the solutions, and finally filter with respect to the ignored input/output constants.

In Table 1 we provide complexity estimations for Poseidon and various parameter sets, round numbers are taken from [GKS23, Table 1]. Note that for all estimates we neglected the term $\log_2\big(\min\{r_{in}, r_{out}\}\big)$. Except one parameter set, all instances achieve 128 bits of security for eigenpolynomial construction. But for root extraction, only instances over a 256 bit prime field achieve 128 bits of security.

Table 1: POSEIDON complexity estimations for eigenpolynomial computation and $\mathbb{F}_q$-valued root extraction. All estimations use $\omega = 2$.

$\log_2(q)$	d	r_{in}	r_f	r_p	Eigenpolynomial (bits)	Root extraction (bits)
31	5	1	4	14	103	43
31	5	2	4	14	140	44
31	5	4	4	14	214	44
31	5	8	4	14	363	45
31	5	1	4	22	140	44
31	5	2	4	22	177	44
31	5	4	4	22	251	44
31	5	8	4	22	400	45
64	7	1	4	22	169	79
64	7	2	4	22	214	79
64	7	4	4	22	304	79
256	5	1	4	56	298	166
256	5	2	4	56	335	185

4.1.1 Ethereum Challenge

In 2021 Ethereum foundation hosted a CICO cryptanalysis challenge [Eth21] for various AO hash functions among them POSEIDON. For the challenge one had to solve the CICO problem

$$\text{POSEIDON}\begin{pmatrix} x_{in,1} \\ x_{in,2} \\ 0 \end{pmatrix} = \begin{pmatrix} x_{out,1} \\ x_{out,2} \\ 0 \end{pmatrix} \tag{19}$$

over the prime $p = 18446744073709551557$ with $d = 3$ for various parameter sets. This polynomial system is not fully determined, hence we have to guess one variable. By Equation (18) we are best advised to guess a value for $x_{in,2}$. We note that Bariant et al. [BBLP22, §4.3] also investigated the POSEIDON challenge and claimed a break of some parameter sets. Utilizing our Gröbner basis we present the complexities of a Gröbner basis attack on the POSEIDON challenge in Table 2. The first two parameter sets do not achieve the claimed security level for eigenpolynomial construction, and no parameter set achieves the security level for root extraction.

Bariant et al. found a trick [BBLP22, §4.2] to bypass the first two SPN rounds of POSEIDON. By their analysis, one can consider the input state of the third full round to be of the form

$$\mathbf{x}^{(3)} = \begin{pmatrix} a_1 \cdot x \\ a_2 \cdot x \\ b \end{pmatrix} = \begin{pmatrix} a_1 & 0 & 0 \\ a_2 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} x \\ 0 \\ b \end{pmatrix}, \tag{20}$$

where x is a new variable and $a_1, a_2, b \in \mathbb{F}_q$ are such that $a_1 \cdot a_2 \neq 0$. Obviously, our POSEIDON CICO Gröbner basis from Theorem B.5 can be extended to this trick. After all, we just cut off two rounds and formulated a smaller CICO problem. In particular, the quotient space dimension becomes

$$\hat{D}_{\text{POSEIDON}} = \dim_{\mathbb{F}_q}\left(\hat{\mathcal{F}}_{\text{CICO}}\right) = d^{2\cdot(r_f - 1) + r_p}. \tag{21}$$

Utilizing our Gröbner basis we present the complexities of a Gröbner basis attack on the POSEIDON challenge in Table 2. With the first two rounds bypassed, the third instance achieves exactly the security level for eigenpolynomial construction.

Table 2: Poseidon Ethereum challenge [Eth21] complexity estimation. The challenge is defined over the prime $p = 18446744073709551557$ and $d = 3$. All estimations use $r_{in} = 1$ and $\omega = 2$.

r_f	r_p	Eigenpolynomial (bits)	Root extraction (bits)	Security level (bits)
		Full model		
4	3	35	29	45
4	8	51	37	53
4	13	67	46	61
4	19	86	56	69
4	24	102	64	77
		First two rounds bypassed		
4	3	29	25	45
4	8	45	34	53
4	13	61	43	61
4	19	80	53	69
4	24	96	61	77

4.2 A Concrete Poseidon2 Instance

In Section 4.1 we implicitly assumed that the necessary conditions on the matrices are satisfied. Next let us showcase that the conditions are indeed satisfied for a concrete Poseidon2 instance over the prime

$$\text{BN256} = 0x30644e72e131a029b85045b68181585d2833e84879b97709143e1f593f0000001. \tag{22}$$

We utilize rational representations of the matrices. This has the convenient benefit that we can lift our findings to all primes strictly larger than the largest denominator in our analysis.

For $n = 3$ the matrices full and partial rounds are, see Appendix A,

$$\mathbf{M}_f = \begin{pmatrix} 2 & 1 & 1 \\ 1 & 2 & 1 \\ 1 & 1 & 2 \end{pmatrix}, \qquad \mathbf{M}_p = \begin{pmatrix} 2 & 1 & 1 \\ 1 & 2 & 1 \\ 1 & 1 & 3 \end{pmatrix}. \tag{23}$$

Then, for $\mathbf{M}_f$ we have that

$$\left(\begin{array}{c|cc} \frac{1}{2} & 0 & 0 \\ \hline 0 & 1 & 0 \\ 0 & 0 & 1 \end{array}\right) \mathbf{M}_f = \left(\begin{array}{c|cc} 1 & \frac{1}{2} & \frac{1}{2} \\ \hline 1 & 2 & 1 \\ 1 & 1 & 2 \end{array}\right), \tag{24}$$

$$\left(\begin{array}{cc|c} \frac{2}{3} & -\frac{1}{3} & 0 \\ -\frac{1}{3} & \frac{2}{3} & 0 \\ \hline 0 & 0 & 1 \end{array}\right) \mathbf{M}_f = \left(\begin{array}{cc|c} 1 & 0 & \frac{1}{3} \\ 0 & 1 & \frac{1}{3} \\ \hline 1 & 1 & 2 \end{array}\right) \tag{25}$$

We can directly see that

- for $r_{in} = 1$, $\mathbf{M}_f$ is in strong upper non-singular $\rho_{r_{in}, r_{in}}$-position, and
- for $r_{in} = 2$, $\mathbf{M}_f$ is in strong lower non-singular $\rho_{r_{in}, r_{in}}$-position and the matrix $\mathbf{N}$ of the $\rho_{r_{in}, r_{in}}$-transformation has two non-zero entries in every row.

So the necessary conditions of Corollary 3.9 and Proposition 3.10 for $\mathbf{M}_f$ are satisfied.

Now let us look at the inverse

$$\mathbf{M}_f^{-1} = \begin{pmatrix} \frac{3}{4} & -\frac{1}{4} & -\frac{1}{4} \\ -\frac{1}{4} & \frac{3}{4} & -\frac{1}{4} \\ -\frac{1}{4} & -\frac{1}{4} & \frac{3}{4} \end{pmatrix}, \tag{26}$$

then

$$\left(\begin{array}{c|cc} 1 & 0 & 0 \\ \hline 0 & -1 & -3 \\ 0 & 1 & -1 \end{array}\right) \mathbf{M}_f^{-1} = \left(\begin{array}{cc|c} \frac{3}{4} & -\frac{1}{4} & -\frac{1}{4} \\ \hline 1 & 0 & -2 \\ 0 & 1 & -1 \end{array}\right), \tag{27}$$

$$\left(\begin{array}{cc|c} 1 & 0 & 0 \\ 0 & 1 & 0 \\ \hline 0 & 0 & -4 \end{array}\right) \mathbf{M}_f^{-1} = \left(\begin{array}{c|cc} \frac{3}{4} & -\frac{1}{4} & -\frac{1}{4} \\ -\frac{1}{4} & \frac{3}{4} & -\frac{1}{4} \\ \hline 1 & 1 & -3 \end{array}\right). \tag{28}$$

We can directly see that $\operatorname{rank}\left(\tau_{r_{out}, r_{out}}\left(\mathbf{M}_f^{-1}\right)\right) = r_{out}$, and for $r_{in} = 1 \Leftrightarrow r_{out} = 2$, the matrix

$$\mathbf{AN} = \begin{pmatrix} \frac{3}{4} & -\frac{1}{4} \end{pmatrix} \begin{pmatrix} -1 & -3 \\ 1 & -1 \end{pmatrix} = \begin{pmatrix} -1 & -2 \end{pmatrix} \tag{29}$$

has two non-zero entries. So the necessary conditions of Corollary B.6 and Proposition B.7 for $\mathbf{M}_f^{-1}$ are satisfied.

For the matrix of the partial rounds, we have that

$$\mathbf{M}_p^{-1} = \begin{pmatrix} \frac{5}{7} & -\frac{2}{7} & -\frac{1}{7} \\ -\frac{2}{7} & \frac{5}{7} & -\frac{1}{7} \\ -\frac{1}{7} & -\frac{1}{7} & \frac{3}{7} \end{pmatrix}, \tag{30}$$

then

$$\left(\begin{array}{cc|c} 1 & 0 & 0 \\ 0 & 1 & 0 \\ \hline 0 & 0 & \frac{7}{3} \end{array}\right) \mathbf{M}_p^{-1} = \left(\begin{array}{cc|c} \frac{5}{7} & -\frac{2}{7} & -\frac{1}{7} \\ -\frac{2}{7} & \frac{5}{7} & -\frac{1}{7} \\ \hline -\frac{1}{3} & -\frac{1}{3} & 1 \end{array}\right), \tag{31}$$

$$\left(\begin{array}{c|cc} 1 & 0 & 0 \\ \hline 0 & \frac{3}{2} & \frac{1}{2} \\ 0 & \frac{1}{2} & \frac{5}{2} \end{array}\right) \mathbf{M}_f^{-1} = \left(\begin{array}{c|cc} \frac{5}{7} & -\frac{2}{7} & -\frac{1}{7} \\ \hline -\frac{1}{2} & 1 & 0 \\ -\frac{1}{2} & 0 & 1 \end{array}\right). \tag{32}$$

We can directly see that $\operatorname{rank}\left(\sigma_{r_{out}, r_{out}}\left(\mathbf{M}_p^{-1}\right)\right) = r_{out}$, and

- for $r_{in} = 1 \Leftrightarrow r_{out} = 2$, the matrices

$$\mathbf{BN} = \begin{pmatrix} \frac{3}{2} & \frac{1}{2} \\ \frac{1}{2} & \frac{5}{2} \end{pmatrix} \begin{pmatrix} -\frac{2}{7} & -\frac{1}{7} \end{pmatrix} = \begin{pmatrix} -\frac{1}{2} & -\frac{1}{2} \end{pmatrix}, \tag{33}$$

$$\mathbf{A} - \mathbf{BC} = \begin{pmatrix} \frac{5}{7} \end{pmatrix} - \begin{pmatrix} -\frac{2}{7} & -\frac{1}{7} \end{pmatrix} \begin{pmatrix} -\frac{1}{2} \\ -\frac{1}{2} \end{pmatrix} = \begin{pmatrix} \frac{1}{2} \end{pmatrix} \tag{34}$$

  are non-zero, and

- for $r_{in} = 2 \Leftrightarrow r_{out} = 1$, the matrix

$$\mathbf{A} - \mathbf{BC} = \begin{pmatrix} \frac{5}{7} & -\frac{2}{7} \\ -\frac{2}{7} & \frac{5}{7} \end{pmatrix} - \begin{pmatrix} -\frac{1}{7} \\ -\frac{1}{7} \end{pmatrix} \begin{pmatrix} -\frac{1}{3} & -\frac{1}{3} \end{pmatrix} = \begin{pmatrix} \frac{2}{3} & -\frac{1}{3} \\ -\frac{1}{3} & \frac{2}{3} \end{pmatrix} \tag{35}$$

  has two non-zero entries on every row.

So the necessary conditions of Corollaries 3.9 and B.6 and Propositions 3.10 and B.7 for the matrix $\mathbf{M}_p^{-1}$ are satisfied.

Overall, for all primes $p > 7$, $n = 3$, $d \geq 2$ and the matrices of Equation (23) we have computed Poseidon2 Gröbner bases for the preimage as well as the CICO problem.

5 Discussion

In this paper, we developed Gröbner bases for preimage and CICO Poseidon polynomial systems for all possible parameters d, n, r_f, r_p, r_{in} and r_{out}. Moreover, even if the power permutation x^d is replaced by some non-linear permutation polynomial $f(x)$, our Gröbner bases generalize in a straight-forward manner. Obviously, the necessary conditions on the matrices could fail for a concrete instantiation, a trivial example is the identity matrix. In such a scenario, we still expect that our Gröbner bases can be extended via a dedicated analysis. However, experimentally we never came across a random matrix that failed these conditions.

Since we have now Gröbner bases for Poseidon and Hades at hand, see [Ste24, §6.1], we can now quantify the trade-off between the keyed version and the sponge mode in terms of the $\mathbb{F}_q$-vector space dimension

$$D_{\text{Hades}} = d^{2 \cdot n \cdot r_f + r_p}, \tag{36}$$

$$D_{\text{Poseidon}} = d^{2 \cdot r_{in} \cdot r_f + r_p}. \tag{37}$$

Hence, for the Hades strategy the sponge mode is always weaker than the keyed mode. Moreover, as discussed in Section 4.1 by guessing input variables and ignoring output constants we have control over r_{in} in Poseidon polynomial system. In particular, the extremal case $r_{in} = 1$ is achievable.

For completeness, one could also consider pseudo-preimage and pseudo-CICO problems

$$f \begin{pmatrix} \boldsymbol{\alpha} \\ \mathbf{x}_{in} \end{pmatrix} = f \begin{pmatrix} \mathbf{y}_{in} \\ \boldsymbol{\beta} \end{pmatrix}, \tag{38}$$

$$f \begin{pmatrix} \boldsymbol{\alpha} \\ \mathbf{x}_{in} \end{pmatrix} = \begin{pmatrix} \boldsymbol{\beta} \\ \mathbf{y}_{in} \end{pmatrix}. \tag{39}$$

(Pseudo because we are not aware of any Poseidon instance that uses the lower blocks as input and output.) Obviously, these problems are symmetric to Equations (3) and (4), and it is easy to see that the Horizontal Separation Lemmas (Lemmas 3.2 and 3.13) as well as our techniques to construct SPN/Poseidon Gröbner bases (Section 3 and Appendix B) can be generalized to these problems albeit with new conditions on the matrices.

Of course the iterated polynomial model is not the only modeling that has been studied for Poseidon. Another choice is to substitute all rounds into $n - r_{out}$ equations in r_{in} variables, i.e. the truncated branches of the sponge are ignored, and we do not need r_{out} auxiliary variables for the output. Obviously, in terms of ideals we always have that

$$(\text{Substituted Model}) \subset (\text{Iterated Model}). \tag{40}$$

Moreover, for any polynomial ideals $I, J \subset P$ one always has that

$$I \subset J \Rightarrow \mathcal{V}(J) \subset \mathcal{V}(I). \tag{41}$$

I.e., the substituted model has at least as many solutions as the iterated model. In addition, by the isomorphism theorem of rings we have that

$$I \subset J \Rightarrow \big(P/I\big)/\big(J/I\big) \cong P/J. \tag{42}$$

In particular, for zero-dimensional ideals I and J we have a surjection $P/I \twoheadrightarrow P/J$ of finite dimensional K-vector spaces, i.e. $\dim_K(J) \leq \dim_K(I)$. Or in more cryptographic terms: Solving the substituted model is at least as hard as solving the iterated model once a Gröbner basis for both systems is known. This has an important consequence: We can do not need to perform Gröbner basis computations for any Poseidon polynomial model that is contained in the iterated model, because solving for the variety is at least as hard as for the iterated model, and we already have a Gröbner basis for the iterated model at hand.

As another convenient consequence, we do not rely on small scale experiments and extrapolation as done in [GKR+21, GKS23, ABM23] anymore to assess the resistance of Poseidon against Gröbner basis attacks.

One problem that has not been discussed in this paper is the collision problem for Poseidon, see Equation (5). Setting up the collision polynomial model is straight-forward: First we set up two preimage polynomial systems in distinct variables, then we connect the outputs of the last round. Of course, we would be interested to know whether our approach can transform the iterated collision model via linear transformation into a Gröbner basis. Even if that is the case, such a Gröbner basis will hardly have a cryptographic impact, after all one still would have $2 \cdot (2 \cdot r_f - 1 + r_p)$ rounds that act like in the preimage polynomial system and one additional collision round. Hence, if the approach is successful the collision vector space dimension will always exceed the preimage one for practical round numbers.

Besides Poseidon, many other sponge functions for ZK applications have been proposed in the past years, e.g. `Reinforced Concrete` [GKL+22], `Anemoi` [BBC+23] and Griffin [GHR+23]. Though, these designs deviated heavily from classical Feistel and SPN constructions. Hence, it is also of interest whether Gröbner bases with respect to a weight order can be constructed for these designs for all possible parameter sets.

Moreover, `Reinforced Concrete` introduced a look-up table permutation. In general, no polynomial representation in the specified prime field $\mathbb{F}_p$ of the look-up table permutation is known. Hence, one has to resort to a different modeling. Interestingly, the look-up table polynomial model proposed in [BGK+21, §B.3] is already a zero-dimensional Gröbner basis with respect to a weight order.

Example 5.1 (Look-Up Table Gröbner Basis)**.** Let $n \in \mathbb{Z}_{\geq 1}$, let $p_i, L_i \in \mathbb{F}_q[x]$ be non-constant univariate polynomials, and let $b_1, \dots, b_n \in \mathbb{F}_q \setminus \{0\}$. In $\mathbb{F}_q[x, x_1, \dots, x_n, y, y_1, \dots, y_n]$ the look-up polynomial system is defined as

$$x = \sum_{i=1}^{n} b_i \cdot x_i, \tag{43}$$

$$0 = p_i(x_i), \qquad 1 \leq i \leq n, \tag{44}$$

$$y_i = L_i(x_i), \qquad 1 \leq i \leq n, \tag{45}$$

$$y = \sum_{i=1}^{n} b_i \cdot y_i. \tag{46}$$

Let $y >_{LEX} y_1 >_{LEX} \dots >_{LEX} y_n >_{LEX} x >_{LEX} >_{LEX} x_1 >_{LEX} \dots >_{LEX} x_n$, and let

$$\mathbf{w} = \begin{pmatrix} 1 & 1 & \dots & 1 & \max_{1 \leq i \leq n} \deg(L_i) & \deg(L_1) & \dots & \deg(L_n) \end{pmatrix}^\intercal. \tag{47}$$

Then, the look-up polynomial system has pairwise coprime leading monomials under $>_{\mathbf{w},LEX}$, so by Lemma 2.10 it is a Gröbner basis. Moreover, by [KR00, Proposition 3.7.1] this Gröbner basis is zero-dimensional.

Acknowledgments

Matthias Steiner has been supported in part by the European Research Council (ERC) under the European Union's Horizon 2020 research and innovation program (grant agreement No. 725042) and the enCRYPTON project (grant agreement No. 101079319).

A Poseidon2 Matrices

Poseidon2 matrices for the full rounds are constructed via (block) circulant matrices.[2] For $n \in \{3, 4, 4 \cdot t\}$, where $t \in \mathbb{Z}_{\geq 2}$ the full round matrix is defined as

$$\mathbf{M}_f = \begin{cases} \operatorname{circ}(2, 1, 1), & n = 3, \\ \begin{pmatrix} 5 & 7 & 1 & 3 \\ 4 & 6 & 1 & 1 \\ 1 & 3 & 5 & 7 \\ 1 & 1 & 4 & 6 \end{pmatrix}, & n = 4, \\ \operatorname{circ}(2 \cdot \mathbf{M}_4, \mathbf{M}_4, \dots, \mathbf{M}_4), & n > 4,\ n \equiv 0 \mod 4. \end{cases} \tag{48}$$

For the partial Poseidon2 rounds, the matrix is defined as

$$\mathbf{M}_p = \begin{pmatrix} \mu_1 & 1 & \dots & 1 \\ 1 & \mu_2 & \dots & 1 \\ \vdots & \vdots & \ddots & \vdots \\ 1 & 1 & \dots & \mu_n \end{pmatrix}, \tag{49}$$

where $\mu_1, \dots, \mu_n \in \mathbb{F}_q \setminus \{0, 1\}$ are such that the matrix is invertible. E.g., in [Wal21] over the prime BN256 and $n = 3$ the diagonal entries $\mu_1 = \mu_2 = 2$ and $\mu_3 = 3$ have been used.

B Gröbner Bases for CICO Polynomial Systems

For the CICO Horizontal separation we introduced a third map τ, hence we can get an analog of Definitions 3.3 and 3.7

Definition B.1. *Let K be a field, let $k, n \in \mathbb{Z}_{\geq 1}$ be such that $k < n$, and let $\mathbf{M} \in K^{n \times n}$ be a matrix such that* $\operatorname{rank}\big(\tau_{k,k}(\mathbf{M})\big) = k$. *Then there exists an invertible matrix $\mathbf{N} \in K^{k \times k}$ such that*

$$\begin{pmatrix} \mathbf{I}_{(n-k) \times (n-k)} & \mathbf{0}_{(n-k) \times k} \\ \mathbf{0}_{k \times (n-k)} & \mathbf{N} \end{pmatrix} \mathbf{M} = \begin{pmatrix} \mathbf{A} & \mathbf{B} \\ \mathbf{I}_{k \times k} & \mathbf{C} \end{pmatrix},$$

where $\mathbf{A} \in K^{(n-k) \times k}$, $\mathbf{B} \in K^{(n-k) \times (n-k)}$ and $\mathbf{C} \in K^{k \times (n-k)}$.
The matrix $\begin{pmatrix} \mathbf{I}_{(n-k) \times (n-k)} & \mathbf{0}_{(n-k) \times k} \\ \mathbf{0}_{k \times (n-k)} & \mathbf{N} \end{pmatrix}$ is called the $\tau_{k,k}$-transformation of $\mathbf{M}$.

[2] We define circulant matrices via a right shift, i.e.

$$\operatorname{circ}(a_1, \dots, a_n) = \begin{pmatrix} a_1 & a_2 & \dots & a_{n-1} & a_n \\ a_n & a_1 & \dots & a_{n-2} & a_{n-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ a_2 & a_3 & \dots & a_n & a_1 \end{pmatrix}.$$

B.1 Substitution-Permutation Network

Let us start with the analog for Theorem 3.4, as already indicated only the last round has to be modified.

Theorem B.2. *Let $\mathbb{F}_q$ be a finite field, let $d, n, r, r_{in}, r_{out} \in \mathbb{Z}_{\geq 1}$ be integers such that $n = r_{in} + r_{out}$, and let $\mathcal{F}_{pre} = \left\{ \mathbf{f}_{pre}^{(i)} \right\}_{0 \leq i \leq r} \subset \mathbb{F}_q \left[\mathbf{x}_{in}, \mathbf{x}^{(1)}, \dots, \mathbf{x}^{(r)}, \mathbf{x}_{out} \right]$ be a SPN sponge CICO polynomial system with the parameters d, n, r, r_{in} and r_{out}. Let $>_{\mathbf{w}, LEX}$ be the weight order from Theorem 3.4. Assume that*

(i) $n > 2$,

(ii) $r_{in} < n - 1$,

(iii) $\operatorname{rank}\left(\rho_{r_{in}, r_{in}}(\mathbf{M}_0) \right) = r_{in}$,

(iv) $\mathbf{M}_i$ *is in upper non-singular* $\rho_{r_{in}, r_{in}}$*-position for all* $1 \leq i \leq r - 1$,

(v) for $\mathbf{M}_r$*:*

(a) $\operatorname{rank}\left(\tau_{r_{out}, r_{out}}\left(\mathbf{M}_r^{-1} \right) \right) = r_{out}$*, and*

(b) let $\mathbf{A}_r \in \mathbb{F}_q^{r_{in} \times r_{out}}$ *and* $\mathbf{N}_r \in \mathbb{F}_q^{r_{out} \times r_{out}}$ *be the matrices of the* $\tau_{r_{out}, r_{out}}$ *transformation of* $\mathbf{M}_r^{-1}$*, then* $\mathbf{A}_r \mathbf{N}_r$ *has at least two non-zero entries on every row.*

Then

(1) A $>_{\mathbf{w}, LEX}$*-Gröbner basis for* $\mathcal{F}_{pre}$ *can be computed via linear transformations.*

(2) $\dim_{\mathbb{F}_q}\left(\mathcal{F}_{pre} \right) = d^{r_{in} \cdot r}$.

Proof. Let $\mathbf{g}^{(0)}, \dots, \mathbf{g}^{(r)}$ be as in Theorem 3.4, we have to slightly modify the polynomials for the last round

$$
\begin{aligned}
\hat{\mathbf{g}}^{(r)} &= \begin{pmatrix} \mathbf{I}_{r_{in} \times r_{in}} & -\mathbf{A}_r \\ \mathbf{0}_{r_{out} \times r_{in}} & \mathbf{I}_{r_{out} \times r_{out}} \end{pmatrix} \begin{pmatrix} \mathbf{I}_{r_{in} \times r_{in}} & \mathbf{0}_{r_{in} \times r_{out}} \\ \mathbf{0}_{r_{out} \times r_{in}} & \mathbf{N}_r \end{pmatrix} \mathbf{M}_r^{-1} \mathbf{g}^{(r)} \\
&= \begin{pmatrix} \mathbf{I}_{r_{in} \times r_{in}} & -\mathbf{A}_r \mathbf{N}_r \\ \mathbf{0}_{r_{out} \times r_{out}} & \mathbf{N}_r \end{pmatrix} \mathcal{S}\left(\mathbf{x}^{(r)} \right) + \hat{\mathbf{c}}_r - \begin{pmatrix} \mathbf{0}_{r_{in} \times r_{in}} & \mathbf{B}_r - \mathbf{A}_r \mathbf{C}_r \\ \mathbf{I}_{r_{out} \times r_{out}} & \mathbf{C}_r \end{pmatrix} \begin{pmatrix} \mathbf{x}_{out} \\ \boldsymbol{\beta} \end{pmatrix},
\end{aligned}
$$

which is possible due to $\operatorname{rank}\left(\tau_{r_{out}, r_{out}}\left(\mathbf{M}_r^{-1} \right) \right) = r_{out}$. We claim that

$$
\mathcal{G} = \left\{ \mathbf{g}^{(i)} \right\}_{0 \leq i \leq r-1} \cup \left\{ \hat{\mathbf{g}}^{(r)} \right\}
$$

is the $>_{\mathbf{w}, LEX}$-Gröbner basis.

- For $0 \leq i \leq r - 1$, computation of the leading monomials is identical to Theorem 3.8.
- For $i = r$, due to the assumption that $\mathbf{A}_r \mathbf{N}_r$ has two non-zero entries on every row, the weights $\mathbf{w}_0, \dots, \mathbf{w}_{r-1}$ produce ties for $\mathbf{g}^{(r)}|^{r_{in}}$.

  Also, the weights $\mathbf{w}_0, \dots, \mathbf{w}_{r-1}$ produce ties on $\mathbf{g}^{(r)}|_{r_{out}}$ since $\mathbf{N}_r$ is an invertible matrix.

  Therefore, we have to decide via $\mathbf{w}_r$ which yields

$$
\mathrm{LM}_{>_{\mathbf{w}, LEX}}\left(\hat{\mathbf{g}}^{(r)} \right) = \begin{pmatrix} \mathcal{S}\left(\mathbf{x}^{(r)} \right) \Big|^{r_{in}} \\ \mathbf{x}_{out} \end{pmatrix}.
$$

So we have pairwise coprime leading monomials and henceforth also a Gröbner basis by Lemma 2.10.

Counting the number of monomials not contained in the ideal of leading terms is analog to Theorem 3.8. □

If $r_{in} = n - 1$, then $\mathbf{A}_r \mathbf{N}_r$ is an $r_{in} \times 1$ matrix, hence the assumptions of Theorem B.2 can never be satisfied. So we also need an analog of Proposition 3.5.

Proposition B.3. *Let $\mathbb{F}_q$ be a finite field, let $d, n, r, r_{in}, r_{out} \in \mathbb{Z}_{\geq 1}$ be integers such that $n = r_{in} + r_{out}$, and let $\mathcal{F}_{pre} = \left\{ \mathbf{f}_{pre}^{(i)} \right\}_{0 \leq i \leq r} \subset \mathbb{F}_q \left[\mathbf{x}_{in}, \mathbf{x}^{(i)}, x_{out} \mid 1 \leq i \leq r \right]$ be a SPN sponge CICO polynomial system with the parameters d, n, r, r_{in} and r_{out}. Let $>_{\mathbf{W}, LEX}$ be the weight order from Proposition 3.5. Assume that*

(i) $n > 2$,

(ii) $r_{in} = n - 1$,

(iii) *for all* $1 \leq i \leq r - 1$*:*

  (a) $\operatorname{rank}\left(\rho_{r_{in}, r_{in}}(\mathbf{M}_i)\right) = r_{in}$,

  (b) let $\mathbf{N}_i \in \mathbb{F}_q^{r_{in} \times r_{in}}$ be the matrix of the $\rho_{r_{in}, r_{in}}$-transformation of $\mathbf{M}_i$, then $\mathbf{N}_i$ has at least two non-zero entries in every row, and

(iv) $\operatorname{rank}\left(\tau_{r_{out}, r_{out}}\left(\mathbf{M}_r^{-1}\right)\right) = r_{out}$.

Then

(1) A $>_{\mathbf{W}, LEX}$-Gröbner basis for $\mathcal{F}_{pre}$ can be computed via linear transformations.

(2) $\dim_{\mathbb{F}_q}\left(\mathcal{F}_{pre}\right) = d^{r_{in} \cdot r}$.

Proof. Let $\mathcal{G}$ as in Theorem B.2, we claim that this is the $>_{\mathbf{W}, LEX}$-Gröbner basis.

- For $0 \leq i \leq r - 1$, computation of the leading monomials is analog to Proposition 3.5.
- For $i = r$, let $0 \leq j \leq r - 2$, if the matrix $\mathbf{A}_r \mathbf{N}_r$ has a zero row, then we have a trivial decision for a term of $\mathcal{S}\left(\mathbf{x}^{(r)}\right) |^{r_{in}}$ on that row of $\mathbf{g}^{(r)}|^{r_{in}}$. Otherwise, we have two terms present of weight $d \cdot d^{i-j}$, so we have a tie.

  In case of a tie, for $\mathbf{w}_{r-1}$ all terms in $\mathbf{g}^{(r)}|^{r_{in}}$ have weight 0, so we have a trivial tie.

  Finally, decision by $\mathbf{w}_r$ yields

  $$\mathrm{LM}_{>_{\mathbf{W}, LEX}}\left(\mathbf{g}^{(r)}\Big|^{r_{in}}\right) = \mathcal{S}\left(\mathbf{x}^{(r)}\right)\Big|^{r_{in}}.$$

  Analog for $\mathbf{g}^{(r)}|_{r_{out}}$, the weights $\mathbf{w}_0, \ldots, \mathbf{w}_{r-2}$ produce ties since $\mathbf{N}_r$ is invertible, but for $\mathbf{w}_{r-1}$ the terms $\mathcal{S}\left(\mathbf{x}^{(r)}\right)$ have weight 0 and the ones of $\mathbf{x}_{out}$ have weight d^2, so

  $$\mathrm{LM}_{>_{\mathbf{W}, LEX}}\left(\mathbf{g}^{(r)}\Big|_{r_{out}}\right) = \mathbf{x}_{out}.$$

So, we have pairwise coprime leading monomials and being a Gröbner basis follows from Lemma 2.10.

Counting the number of monomials not contained in the ideal of leading terms is analog to Proposition 3.5. □

Finally, for $n = 2$ we need an analog of Corollary 3.6.

Corollary B.4. *Let $\mathbb{F}_q$ be a finite field, let $d, n, r, r_{in}, r_{out} \in \mathbb{Z}_{\geq 1}$ be integers such that $n = 2$, $r_{in} = 1$ and $n = r_{in} + r_{out}$, and let $\mathcal{F}_{pre} = \left\{ \mathbf{f}_{pre}^{(i)} \right\}_{0 \leq i \leq r} \subset \mathbb{F}_q \big[x_{in}, \mathbf{x}^{(i)}, x_{out} \mid 1 \leq i \leq r \big]$ be a SPN sponge CICO polynomial system with the parameters d, n, r, r_{in} and r_{out}. Let $>_{\mathbf{W},LEX}$ be the weight order from Corollary 3.6. Assume that*

(i) $\mathbf{M}_i$ *is in upper non-singular $\rho_{r_{in},r_{in}}$-position for all $0 \leq i \leq r - 1$, and*

(ii) $\operatorname{rank}\left(\tau_{r_{out},r_{out}} \left(\mathbf{M}_r^{-1} \right) \right) = r_{out}$.

Then

(1) A $>_{\mathbf{W},LEX}$-Gröbner basis for $\mathcal{F}_{pre}$ can be computed via linear transformations.

(2) $\dim_{\mathbb{F}_q} \left(\mathcal{F}_{pre} \right) = d^r$.

Proof. Let $\mathbf{g}^{(0)}, \dots, \mathbf{g}^{(r)}$ be as in Theorem 3.4, we have to slightly modify the polynomials for the last round

$$\begin{aligned}
\hat{\mathbf{g}}^{(r)} &= \begin{pmatrix} 1 & \gamma \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & -A_r \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & N_r \end{pmatrix} \mathbf{M}_r^{-1} \mathbf{g}^{(r)} \\
&= \begin{pmatrix} 1 & \gamma \\ 0 & 1 \end{pmatrix} \left(\begin{pmatrix} 1 & -A_r \cdot N_r \\ 0 & N_r \end{pmatrix} \mathcal{S} \left(\mathbf{x}^{(r)} \right) + \hat{\mathbf{c}}_r - \begin{pmatrix} 1 & -A_r \\ 0 & 1 \end{pmatrix} \begin{pmatrix} A_r & B_r \\ 1 & C_r \end{pmatrix} \begin{pmatrix} x_{out} \\ \beta \end{pmatrix} \right) \\
&= \begin{pmatrix} 1 & \gamma \\ 0 & 1 \end{pmatrix} \left(\begin{pmatrix} 1 & -A_r \cdot N_r \\ 0 & N_r \end{pmatrix} \mathcal{S} \left(\mathbf{x}^{(r)} \right) + \hat{\mathbf{c}}_r - \begin{pmatrix} 0 & B_r - A_r \cdot C_r \\ 1 & C_r \end{pmatrix} \begin{pmatrix} x_{out} \\ \beta \end{pmatrix} \right),
\end{aligned}$$

where $\gamma \in \mathbb{F}_q^\times$ is chosen such that the coefficient of ${x_2^{(r)}}^d$ in $\hat{g}_1^{(r)}$ is non-zero. Then, ${x_1^{(r)}}^d$, ${x_2^{(r)}}^d$ and x_{out} are present in $g_1^{(r)}$, but only ${x_2^{(r)}}^d$ and x_{out} are present in $g_2^{(r)}$. Proving that

$$\mathcal{G} = \left\{ \mathbf{g}^{(i)} \right\}_{0 \leq i \leq r-1} \cup \left\{ \hat{\mathbf{g}}^{(r)} \right\}$$

is the $>_{\mathbf{W},LEX}$-Gröbner basis of $\mathcal{F}_{\text{pre}}$ is then identical to Corollary 3.6. □

B.2 Poseidon

Next we combine Theorems 3.8 and B.2 to compute a Gröbner basis for the Poseidon CICO polynomial system.

Theorem B.5. *Let $\mathbb{F}_q$ be a finite field, let $d, n, r_f, r_p, r_{in}, r_{out} \in \mathbb{Z}_{\geq 1}$ be integers such that $n = r_{in} + r_{out}$, and let $\mathcal{F}_{pre} = \left\{ \mathbf{f}_{pre}^{(i)} \right\}_{0 \leq i \leq r} \subset \mathbb{F}_q \big[\mathbf{x}_{in}, \mathbf{x}^{(1)}, \dots, \mathbf{x}^{(2 \cdot r_f + r_p)}, \mathbf{x}_{out} \big]$ be a Poseidon CICO polynomial system with the parameters d, n, r_f, r_p, r_{in} and r_{out}. Let $>_{\mathbf{W},LEX}$ be the weight order from Theorem 3.8. Assume that*

(i) $n > 2$,

(ii) $1 < r_{in} < n - 1$,

(iii) $\operatorname{rank} \big(\rho_{r_{in},r_{in}} (\mathbf{M}_0) \big) = r_{in}$,

(iv) $\mathbf{M}_i$ *is in upper non-singular $\rho_{r_{in},r_{in}}$-position for all $1 \leq i \leq r_f$ and $r_f + r_p + 1 \leq 2 \cdot r_f + r_p - 1$,*

(v) for all $r_f + 1 \leq j \leq r_f + r_p$:

(a) $\operatorname{rank}\left(\sigma_{r_{out},r_{out}}\left(\mathbf{M}_j^{-1}\right)\right) = r_{out}$,

(b) let $\mathbf{A}_j \in \mathbb{F}_q^{r_{in} \times r_{in}}$, $\mathbf{B}_j \in \mathbb{F}_q^{r_{in} \times r_{out}}$ *and* $\mathbf{C}_j \in \mathbb{F}_q^{r_{out} \times r_{in}}$ *be the matrices of the* $\sigma_{r_{out},r_{out}}$*-position of* $\mathbf{M}_j$*, then* $\mathbf{A}_j - \mathbf{B}_j \mathbf{C}_j$ *has at least two non-zero entries on every row,*

(vi) for $\mathbf{M}_{2 \cdot r_f + r_p}$*:*

(a) $\operatorname{rank}\left(\tau_{r_{out},r_{out}}\left(\mathbf{M}_{2 \cdot r_f + r_p}^{-1}\right)\right) = r_{out}$*, and*

(b) let $\mathbf{A}_{2 \cdot r_f + r_p} \in \mathbb{F}_q^{r_{in} \times r_{out}}$ *and* $\mathbf{N}_{2 \cdot r_f + r_p} \in \mathbb{F}_q^{r_{out} \times r_{out}}$ *be the matrices of the* $\tau_{r_{out},r_{out}}$ *transformation of* $\mathbf{M}_{2 \cdot r_f + r_p}^{-1}$*, then* $\mathbf{A}_{2 \cdot r_f + r_p} \mathbf{N}_{2 \cdot r_f + r_p}$ *has at least two non-zero entries on every row.*

Then

(1) A $>_{\mathbf{w},LEX}$*-Gröbner basis for* $\mathcal{F}_{pre}$ *can be computed via linear transformations.*

(2) $\dim_{\mathbb{F}_q}\left(\mathcal{F}_{pre}\right) = d^{2 \cdot r_{in} \cdot r_f + r_f}$.

Proof. For the last round use the same transformation as in Theorem B.2, then the proof follows from synthesizing the proofs of Theorems 3.8 and B.2. □

Analog to Corollary 3.9, we need a slightly modified argument for $r_{in} = 1$.

Corollary B.6. *Let* $\mathbb{F}_q$ *be a finite field, let* $d, n, r_f, r_p, r_{in}, r_{out} \in \mathbb{Z}_{\geq 1}$ *be integers such that* $n = r_{in} + r_{out}$*, and let* $\mathcal{F}_{pre} = \left\{\mathbf{f}_{pre}^{(i)}\right\}_{0 \leq i \leq r} \subset \mathbb{F}_q\left[\mathbf{x}_{in}, \mathbf{x}^{(1)}, \dots, \mathbf{x}^{(2 \cdot r_f + r_p)}, \mathbf{x}_{out}\right]$ *be a* Poseidon *CICO polynomial system with the parameters* d, n, r_f, r_p, r_{in} *and* r_{out}*. Let* $>_{\mathbf{w},LEX}$ *be the weight order from Corollary 3.9. Assume that*

(i) $n > 2$,

(ii) $r_{in} = 1$,

(iii) $\operatorname{rank}\left(\rho_{r_{in},r_{in}}\left(\mathbf{M}_0\right)\right) = r_{in}$,

(iv) $\mathbf{M}_i$ *is in upper non-singular* $\rho_{r_{in},r_{in}}$*-position for all* $1 \leq i \leq r_f$ *and* $r_f + r_p + 1 \leq 2 \cdot r_f + r_p$,

(v) For all $r_f + 1 \leq j \leq r_f + r_p$*:*

(a) $\operatorname{rank}\left(\sigma_{r_{out},r_{out}}\left(\mathbf{M}_j^{-1}\right)\right) = r_{out}$,

(b) let $\mathbf{N}_j \in \mathbb{F}_q^{r_{out} \times r_{out}}$, $\mathbf{A}_j \in \mathbb{F}_q^{r_{in} \times r_{in}}$, $\mathbf{B}_j \in \mathbb{F}_q^{r_{in} \times r_{out}}$ *and* $\mathbf{C}_j \in \mathbb{F}_q^{r_{out} \times r_{in}}$ *be the matrices of the* $\sigma_{r_{out},r_{out}}$*-position of* $\mathbf{M}_j^{-1}$*, then* $\mathbf{B}_j \mathbf{N}_j$ *and* $\mathbf{A}_j - \mathbf{B}_j \mathbf{C}_j$ *are non-zero, and*

(vi) for $\mathbf{M}_{2 \cdot r_f + r_p}$*:*

(a) $\operatorname{rank}\left(\tau_{r_{out},r_{out}}\left(\mathbf{M}_{2 \cdot r_f + r_p}^{-1}\right)\right) = r_{out}$*, and*

(b) let $\mathbf{A}_{2 \cdot r_f + r_p} \in \mathbb{F}_q^{r_{in} \times r_{out}}$ *and* $\mathbf{N}_{2 \cdot r_f + r_p} \in \mathbb{F}_q^{r_{out} \times r_{out}}$ *be the matrices of the* $\tau_{r_{out},r_{out}}$ *transformation of* $\mathbf{M}_{2 \cdot r_f + r_p}^{-1}$*, then* $\mathbf{A}_{2 \cdot r_f + r_p} \mathbf{N}_{2 \cdot r_f + r_p}$ *has at least two non-zero entries on every row.*

Then

(1) A $>_{\mathbf{w},LEX}$*-Gröbner basis for* $\mathcal{F}_{pre}$ *can be computed via linear transformations.*

(2) $\dim_{\mathbb{F}_q}\left(\mathcal{F}_{pre}\right) = d^{2 \cdot r_f + r_f}$.

Proof. For the last round use the same transformation as in Theorem B.2, then the proof follows from synthesizing the proofs of Theorem 3.8 and Corollary 3.9. □

The case $r_{in} = n - 1$ follows from a combination of Propositions 3.10 and B.3.

Proposition B.7. *Let $\mathbb{F}_q$ be a finite field, let $d, n, r_f, r_p, r_{in}, r_{out} \in \mathbb{Z}_{\geq 1}$ be integers such that $n = r_{in} + r_{out}$, and let $\mathcal{F}_{pre} = \left\{ \mathbf{f}_{pre}^{(i)} \right\}_{0 \leq i \leq r} \subset \mathbb{F}_q\left[\mathbf{x}_{in}, \mathbf{x}^{(1)}, \dots, \mathbf{x}^{(2 \cdot r_f + r_p)}, \mathbf{x}_{out}\right]$ be a* Poseidon *CICO polynomial system with the parameters d, n, r_f, r_p, r_{in} and r_{out}. Let $>_{\mathbf{w}, LEX}$ be the weight order from Proposition 3.10. Assume that*

(i) $n > 2$,

(ii) $r_{in} = n - 1$,

(iii) the matrix $\mathbf{M}_0$ is in strong lower non-singular $\rho_{r_{in}, r_{in}}$-position,

(iv) for all $1 \leq i \leq r_f$ and $r_f + r_p + 1 \leq i \leq 2 \cdot r_f + r_p$:

  (a) $\operatorname{rank}\left(\rho_{r_{in}, r_{in}}(\mathbf{M}_i)\right) = r_{in}$,

  (b) let $\mathbf{N}_i \in \mathbb{F}_q^{r_{in} \times r_{in}}$ be the matrix of the $\rho_{r_{in}, r_{in}}$-transformation of $\mathbf{M}_i$, then $\mathbf{N}_i$ has at least two non-zero entries in every row,

(v) for all $r_f + 1 \leq j \leq r_f + r_p$:

  (a) $\operatorname{rank}\left(\sigma_{r_{out}, r_{out}}\left(\mathbf{M}_j^{-1}\right)\right) = r_{out}$,

  (b) let $\mathbf{A}_j \in \mathbb{F}_q^{r_{in} \times r_{in}}$, $\mathbf{B}_j \in K^{r_{in} \times r_{out}}$ and $\mathbf{C}_j \in K^{r_{out} \times r_{in}}$ be the matrices of the $\sigma_{r_{out}, r_{out}}$-position of $\mathbf{M}_j$, then $\mathbf{A}_j - \mathbf{B}_j \mathbf{C}_j$ has at least two non-zero entries on every row, and

(vi) $\operatorname{rank}\left(\tau_{r_{out}, r_{out}}\left(\mathbf{M}_{2 \cdot r_f + r_p}^{-1}\right)\right) = r_{out}$.

Then

(1) A $>_{\mathbf{w}, LEX}$-Gröbner basis for $\mathcal{F}_{pre}$ can be computed via linear transformations.

(2) $\dim_{\mathbb{F}_q}\left(\mathcal{F}_{pre}\right) = d^{2 \cdot r_{in} \cdot r_f + r_f}$.

Proof. For the last round use the same transformation as in Theorem B.2, then the proof follows from synthesizing the proofs of Propositions 3.10 and B.3. □

Finally, the case $n = 2$ is follows from combination of Corollaries 3.11 and B.4.

Corollary B.8. *Let $\mathbb{F}_q$ be a finite field, let $d, n, r_f, r_p, r_{in}, r_{out} \in \mathbb{Z}_{\geq 1}$ be integers such that $n = 2$, $r_{in} = 2$ and $n = r_{in} + r_{out}$, and let $\mathcal{F}_{pre} = \left\{ \mathbf{f}_{pre}^{(i)} \right\}_{0 \leq i \leq r} \subset \mathbb{F}_q\left[x_{in}, \mathbf{x}^{(i)}, x_{out} \mid 1 \leq i \leq 2 \cdot r_f + r_p\right]$ be a* Poseidon *preimage polynomial system with the parameters d, n, r_f, r_p, r_{in} and r_{out}. Let $>_{\mathbf{w}, LEX}$ be the weight order from Corollary 3.11 Assume that*

(i) $\mathbf{M}_i$ is in upper non-singular $\rho_{r_{in}, r_{in}}$-position for all $0 \leq i \leq r_f$ and $r_f + r_p + 1 \leq i \leq 2 \cdot r_f + r_p - 1$,

(ii) for all $r_f + 1 \leq j \leq r_f + r_p$:

  (a) $\operatorname{rank}\left(\sigma_{r_{out}, r_{out}}\left(\mathbf{M}_j^{-1}\right)\right) = r_{out}$,

(b) let $\mathbf{N}_j \in \mathbb{F}_q^{r_{out} \times r_{out}}$, $\mathbf{A}_j \in \mathbb{F}_q^{r_{in} \times r_{in}}$, $\mathbf{B}_j \in \mathbb{F}_q^{r_{in} \times r_{out}}$ *and* $\mathbf{C}_j \in \mathbb{F}_q^{r_{out} \times r_{in}}$ *be the matrices of the* $\sigma_{r_{out}, r_{out}}$*-position of* $\mathbf{M}_j^{-1}$*, then* $\mathbf{B}_j \mathbf{N}_j$ *and* $\mathbf{A}_j - \mathbf{B}_j \mathbf{C}_j$ *are non-zero, and*

(iii) $\operatorname{rank}\left(\tau_{r_{out}, r_{out}}\left(\mathbf{M}_{2 \cdot r_f + r_p}^{-1}\right)\right) = r_{out}$.

Then

(1) A $>_{\mathbf{w}, LEX}$*-Gröbner basis for* $\mathcal{F}_{pre}$ *can be computed via linear transformations.*

(2) $\dim_{\mathbb{F}_q}\left(\mathcal{F}_{pre}\right) = d^{2 \cdot r_f + r_p}$.

Proof. For the last round use the same transformation as in Corollary B.4, then the proof follows from synthesizing the proofs of Corollaries 3.11 and B.4. □

References

[ABM23] Tomer Ashur, Thomas Buschman, and Mohammad Mahzoun. Algebraic cryptanalysis of HADES design strategy: Application to POSEIDON and Poseidon2. Cryptology ePrint Archive, Paper 2023/537, 2023. Version: 20230704:143237. URL: https://eprint.iacr.org/2023/537.

[ACG+19] Martin R. Albrecht, Carlos Cid, Lorenzo Grassi, Dmitry Khovratovich, Reinhard Lüftenegger, Christian Rechberger, and Markus Schofnegger. Algebraic cryptanalysis of STARK-friendly designs: Application to MARVELlous and MiMC. In Steven D. Galbraith and Shiho Moriai, editors, *ASIACRYPT 2019, Part III*, volume 11923 of *LNCS*, pages 371–397. Springer, Heidelberg, December 2019. doi:10.1007/978-3-030-34618-8_13.

[AES01] Advanced Encryption Standard (AES). National Institute of Standards and Technology, NIST FIPS PUB 197, U.S. Department of Commerce, November 2001.

[AGP+19] Martin R. Albrecht, Lorenzo Grassi, Léo Perrin, Sebastian Ramacher, Christian Rechberger, Dragos Rotaru, Arnab Roy, and Markus Schofnegger. Feistel structures for MPC, and more. In Kazue Sako, Steve Schneider, and Peter Y. A. Ryan, editors, *ESORICS 2019, Part II*, volume 11736 of *LNCS*, pages 151–171. Springer, Heidelberg, September 2019. doi:10.1007/978-3-030-29962-0_8.

[AGR+16] Martin R. Albrecht, Lorenzo Grassi, Christian Rechberger, Arnab Roy, and Tyge Tiessen. MiMC: Efficient encryption and cryptographic hashing with minimal multiplicative complexity. In Jung Hee Cheon and Tsuyoshi Takagi, editors, *ASIACRYPT 2016, Part I*, volume 10031 of *LNCS*, pages 191–219. Springer, Heidelberg, December 2016. doi:10.1007/978-3-662-53887-6_7.

[AHU74] Alfred V. Aho, John E. Hopcroft, and Jeffrey D. Ullman. *The Design and Analysis of Computer Algorithms*. Addison-Wesley Longman Publishing Co., Inc., USA, 1st edition, 1974.

[AW21] Josh Alman and Virginia Vassilevska Williams. A refined laser method and faster matrix multiplication. In Dániel Marx, editor, *32nd SODA*, pages 522–539. ACM-SIAM, January 2021. doi:10.1137/1.9781611976465.32.

[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 Helena Handschuh and Anna Lysyanskaya, editors, *CRYPTO 2023, Part III*, volume 14083 of *LNCS*, pages 507–539. Springer, Heidelberg, August 2023. doi:10.1007/978-3-031-38548-3_17.

[BBLP22] Augustin Bariant, Clémence Bouvier, Gaëtan Leurent, and Léo Perrin. Algebraic attacks against some arithmetization-oriented primitives. *IACR Trans. Symm. Cryptol.*, 2022(3):73–101, 2022. doi:10.46586/tosc.v2022.i3.73-101.

[BCD$^+$20] Tim Beyne, Anne Canteaut, Itai Dinur, Maria Eichlseder, Gregor Leander, Gaëtan Leurent, María Naya-Plasencia, Léo Perrin, Yu Sasaki, Yosuke Todo, and Friedrich Wiemer. Out of oddity - new cryptanalytic techniques against symmetric primitives optimized for integrity proof systems. In Daniele Micciancio and Thomas Ristenpart, editors, *CRYPTO 2020, Part III*, volume 12172 of *LNCS*, pages 299–328. Springer, Heidelberg, August 2020. doi:10.1007/978-3-030-56877-1_11.

[BDND$^+$21] Mina Bigdeli, Emanuela De Negri, Manuela Muzika Dizdarevic, Elisa Gorla, Romy Minko, and Sulamithe Tsakou. Semi-regular sequences and other random systems of equations. In Alina Carmen Cojocaru, Sorina Ionica, and Elisa Lorenzo García, editors, *Women in Numbers Europe III: Research Directions in Number Theory*, pages 75–114, Cham, 2021. Springer International Publishing. doi:10.1007/978-3-030-77700-5_3.

[BDPA13] Guido Bertoni, Joan Daemen, Michaël Peeters, and Gilles Van Assche. Keccak. In Thomas Johansson and Phong Q. Nguyen, editors, *EUROCRYPT 2013*, volume 7881 of *LNCS*, pages 313–314. Springer, Heidelberg, May 2013. doi:10.1007/978-3-642-38348-9_19.

[BDPV07] Guido Bertoni, Joan Daemen, Michaël Peeters, and Gilles Van Assche. Sponge functions. Ecrypt Hash Workshop, 2007. URL: https://keccak.team/files/SpongeFunctions.pdf.

[BDPV08] Guido Bertoni, Joan Daemen, Michaël Peeters, and Gilles Van Assche. On the indifferentiability of the sponge construction. In Nigel P. Smart, editor, *EUROCRYPT 2008*, volume 4965 of *LNCS*, pages 181–197. Springer, Heidelberg, April 2008. doi:10.1007/978-3-540-78967-3_11.

[BDPV11] Guido Bertoni, Joan Daemen, Michaël Peeters, and Gilles Van Assche. Cryptographic sponge functions. NIST SHA-3 competition (round 3), 2011. URL: https://keccak.team/files/CSF-0.1.pdf.

[BFS04] Magali Bardet, Jean-Charles Faugère, and Bruno Salvy. On the complexity of Gröbner basis computation of semi-regular overdetermined algebraic equations. In *Proceedings of the International Conference on Polynomial System Solving*, pages 71–74, 2004.

[BGK$^+$21] Mario Barbara, Lorenzo Grassi, Dmitry Khovratovich, Reinhard Lueftenegger, Christian Rechberger, Markus Schofnegger, and Roman Walch. Reinforced concrete: Fast hash function for zero knowledge proofs and verifiable computation. Cryptology ePrint Archive, Report 2021/1038, 2021. https://eprint.iacr.org/2021/1038.

[BPW06] Johannes Buchmann, Andrei Pyshkin, and Ralf-Philipp Weinmann. A zero-dimensional Gröbner basis for AES-128. In Matthew J. B. Robshaw, editor, *FSE 2006*, volume 4047 of *LNCS*, pages 78–88. Springer, Heidelberg, March 2006. doi:10.1007/11799313_6.

[Buc65] Bruno Buchberger. *Ein Algorithmus zum Auffinden der Basiselemente des Restklassenringes nach einem nulldimensionalen Polynomideal*. PhD thesis, Universität Innsbruck, 1965.

[CG21] Alessio Caminata and Elisa Gorla. Solving multivariate polynomial systems and an invariant from commutative algebra. In Jean-Claude Bajard and Alev Topuzoğlu, editors, *Arithmetic of Finite Fields - 8th International Workshop, WAIFI 2020, Rennes, France, July 6-8, 2020, Revised Selected and Invited Papers*, volume 12542 of *Lecture Notes in Computer Science*, pages 3–36, Cham, 2021. Springer International Publishing. doi:10.1007/978-3-030-68869-1_1.

[CLO15] David A. Cox, John Little, and Donal O'Shea. *Ideals, Varieties, and Algorithms: An Introduction to Computational Algebraic Geometry and Commutative Algebra*. Undergraduate Texts in Mathematics. Springer International Publishing, 4 edition, 2015. doi:10.1007/978-3-319-16721-3.

[DR20] Joan Daemen and Vincent Rijmen. *The Design of Rijndael: AES - The Advanced Encryption Standard*. Information Security and Cryptography. Springer Berlin, Heidelberg, 2 edition, 2020. doi:10.1007/978-3-662-60769-5.

[Dus24] Dusk Network. Dusk-Poseidon, 2024. Version: 0.34.0. URL: https://github.com/dusk-network/Poseidon252.

[EH16] David Eisenbud and Joe Harris. *3264 and All That: A Second Course in Algebraic Geometry*. Cambridge University Press, Cambridge, 2016. doi:10.1017/CBO9781139062046.

[Eth21] The Ethereum Foundation. ZK Hash Function Cryptanalysis Bounties 2021. https://www.zkhashbounties.info/, 2021. Accessed: 2024-02-21.

[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. doi:10.1145/2608628.2608669.

[FGLM93] Jean-Charles Faugère, Patrizia Gianni, Daniel Lazard, and Teo Mora. Efficient computation of zero-dimensional Gröbner bases by change of ordering. *J. Symb. Comput.*, 16(4):329–344, 1993. doi:10.1006/jsco.1993.1051.

[FM17] Jean-Charles Faugère and Chenqi Mou. Sparse FGLM algorithms. *J. Symb. Comput.*, 80:538–569, 2017. doi:10.1016/j.jsc.2016.07.025.

[FP19] Jean-Charles Faugère and Ludovic Perret. Algebraic attacks against `stark`-friendly ciphers. Appearing as Appendix A in https://eprint.iacr.org/2020/948, 2019. Version 1.2.

[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 Helena Handschuh and Anna Lysyanskaya, editors, *CRYPTO 2023, Part III*, volume 14083 of *LNCS*, pages 573–606. Springer, Heidelberg, August 2023. doi:10.1007/978-3-031-38548-3_19.

[GKL+22] Lorenzo Grassi, Dmitry Khovratovich, Reinhard Lüftenegger, Christian Rechberger, Markus Schofnegger, and Roman Walch. Reinforced concrete: A fast hash function for verifiable computation. In Heng Yin, Angelos Stavrou, Cas Cremers, and Elaine Shi, editors, *ACM CCS 2022*, pages 1323–1335. ACM Press, November 2022. doi:10.1145/3548606.3560686.

[GKR+19] Lorenzo Grassi, Dmitry Khovratovich, Christian Rechberger, Arnab Roy, and Markus Schofnegger. Poseidon: A new hash function for zero-knowledge proof systems. Cryptology ePrint Archive, Paper 2019/458, 2019. URL: https://eprint.iacr.org/2019/458.

[GKR+21] Lorenzo Grassi, Dmitry Khovratovich, Christian Rechberger, Arnab Roy, and Markus Schofnegger. Poseidon: A new hash function for zero-knowledge proof systems. In Michael Bailey and Rachel Greenstadt, editors, *USENIX Security 2021*, pages 519–535. USENIX Association, August 2021.

[GKRS22] Lorenzo Grassi, Dmitry Khovratovich, Sondre Rønjom, and Markus Schofnegger. The Legendre symbol and the modulo-2 operator in symmetric schemes over $\mathbb{F}_p^n$: Preimage attack on full Grendel. *IACR Trans. Symm. Cryptol.*, 2022(1):5–37, 2022. doi:10.46586/tosc.v2022.i1.5-37.

[GKS23] Lorenzo Grassi, Dmitry Khovratovich, and Markus Schofnegger. Poseidon2: A faster version of the poseidon hash function. In Nadia El Mrabet, Luca De Feo, and Sylvain Duquesne, editors, *AFRICACRYPT 23*, volume 14064 of *LNCS*, pages 177–203. Springer Nature, July 2023. doi:10.1007/978-3-031-37679-5_8.

[GLR+20] Lorenzo Grassi, Reinhard Lüftenegger, Christian Rechberger, Dragos Rotaru, and Markus Schofnegger. On a generalization of substitution-permutation networks: The HADES design strategy. In Anne Canteaut and Yuval Ishai, editors, *EUROCRYPT 2020, Part II*, volume 12106 of *LNCS*, pages 674–704. Springer, Heidelberg, May 2020. doi:10.1007/978-3-030-45724-2_23.

[GWC19] Ariel Gabizon, Zachary J. Williamson, and Oana Ciobotaru. PLONK: Permutations over lagrange-bases for oecumenical noninteractive arguments of knowledge. Cryptology ePrint Archive, Report 2019/953, 2019. https://eprint.iacr.org/2019/953.

[Jea16] Jérémy Jean. TikZ for Cryptographers. https://www.iacr.org/authors/tikz/, 2016.

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

[KR00] Martin Kreuzer and Lorenzo Robbiano. *Computational Commutative Algebra 1*. Springer Berlin Heidelberg, Berlin, Heidelberg, 1 edition, 2000. doi:10.1007/978-3-540-70628-1.

[KR05] Martin Kreuzer and Lorenzo Robbiano. *Computational Commutative Algebra 2*. Springer Berlin Heidelberg, Berlin, Heidelberg, 1 edition, 2005. doi:10.1007/3-540-28296-3.

[KR16] Martin Kreuzer and Lorenzo Robbiano. *Computational Linear and Commutative Algebra*. Springer International Publishing, Cham, 1 edition, 2016. doi:10.1007/978-3-319-43601-2.

[KR21] Nathan Keller and Asaf Rosemarin. Mind the middle layer: The HADES design strategy revisited. In Anne Canteaut and François-Xavier Standaert, editors, *EUROCRYPT 2021, Part II*, volume 12697 of *LNCS*, pages 35–63. Springer, Heidelberg, October 2021. doi:10.1007/978-3-030-77886-6_2.

[LN97] Rudolf Lidl and Harald Niederreiter. *Finite fields*. Encyclopedia of mathematics and its applications. Cambridge Univ. Press, Cambridge, 2 edition, 1997.

[Pol24] Polygon Zero. Plonky2, 2024. Version: 0.2.0. URL: https://github.com/0xPolygonZero/plonky2.

[Rob86] Lorenzo Robbiano. On the theory of graded structures. *J. Symb. Computat.*, 2(2):139–170, 1986. doi:10.1016/S0747-7171(86)80019-0.

[Ste24] Matthias Johann Steiner. Solving degree bounds for iterated polynomial systems. *IACR Trans. Symm. Cryptol.*, 2024(1):357–411, Mar. 2024. doi:10.46586/tosc.v2024.i1.357-411.

[Wal21] Roman Walch. Hash functions for zero-knowledge applications zoo. https://extgit.iaik.tugraz.at/krypto/zkfriendlyhashzoo, aug 2021. IAIK, Graz University of Technology.

[XCWW23] Zeyu Xu, Shiyao Chen, Meiqin Wang, and Puwen Wei. Linear cryptanalysis and its variants with fast fourier transformation technique on MPC/FHE/ZK-friendly $\mathbb{F}_p$-based ciphers. In Leonie Simpson and Mir Ali Rezazadeh Baee, editors, *ACISP 23*, volume 13915 of *LNCS*, pages 25–52. Springer, Heidelberg, July 2023. doi:10.1007/978-3-031-35486-1_2.