universität
innsbruck

Gröbner basis Cryptanalysis of Anemoi

Luca Campa
(Joint work with Arnab Roy)

Department of Computer Science
University of Innsbruck

08 May, 2025

Table of Contents

Introduction

Context

- Advanced cryptographic protocols, e.g. ZK-Proofs: need efficient **hash functions over large fields**.
- **Arithmetization-Oriented Primitives (AOP)**
- Algebraic representation: **algebraic attacks are the main threat**.

Notation

- $\mathbb{K}$: a finite field
- $R = \mathbb{K}[x_1, \ldots, x_n]$: polynomial ring: the set of polynomials in n variables $x_1, \ldots, x_n$ with coefficients in $\mathbb{K}$.
- $I \subset R$ is an ideal iff:
  - $0 \in I$
  - $\forall a, b \in I \implies a \pm b \in I$
  - $r \in R, a \in I \implies r \cdot a \in I$ (simplification)
- $\mathbf{x}$ denotes the set of variables $x_1, \ldots, x_n$.

Gröbner basis background

Gröbner basis: Monomial ordering

Every monomial $m = \prod_{i=1}^{n} x_i^{\alpha_i} \in R$ can be identified with the corresponding vector of exponents $\alpha = (\alpha_1, \ldots, \alpha_n)$.

Monomial ordering

A monomial ordering $\prec$ on $\mathbb{K}[x_1, \ldots, x_n]$ is a relation $\prec$ on $\mathbb{Z}_{\geq 0}^n$, or rather a relation on the set of monomials x^α where $\alpha \in \mathbb{Z}_{\geq 0}^n$, satisfying the following conditions:

- $\prec$ is a total (or linear) order on $\mathbb{Z}_{\geq 0}^n$
- if $\alpha \prec \beta$ and $\gamma \in \mathbb{Z}_{\geq 0}^n$, then $\alpha + \gamma \prec \beta + \gamma$
- $\prec$ is a well-ordering on $\mathbb{Z}_{\geq 0}^n$, meaning that every non empty subset of $\mathbb{Z}_{\geq 0}^n$ has a smallest element under the relation $\prec$.

Gröbner basis: DRL Monomial ordering

DRL Monomial ordering

Let $\alpha, \beta \in \mathbb{Z}^n_{\geq 0}$. We say $\alpha >_{\text{DRL}} \beta$ if

$$|\alpha| = \sum_{i=1}^{n} \alpha_i > |\beta| = \sum_{i=1}^{n} \beta_i, \text{ or } |\alpha| = |\beta| \text{ and } \alpha >_{\text{RLEX}} \beta.$$

We say $x^\alpha >_{\text{DRL}} x^\beta$ if $\alpha >_{\text{DRL}} \beta$.

Gröbner basis: Weighted Monomial ordering

Weighted Monomial ordering

Given a weight vector $w = (w_1, \ldots, w_n) \in \mathbb{R}^n_{\geq 0}$, where $w_1 \neq 0$. We say that w is associated with the monomial ordering $\prec$, defined by:

$$\prod_{i=1}^{n} x_i^{\alpha_i} \prec \prod_{i=1}^{n} x_i^{\beta_i} \iff \begin{cases} \sum_{i=1}^{n} w_i \alpha_i > \sum_{i=1}^{n} w_i \beta_i \\ \sum_{i=1}^{n} w_i \alpha_i = \sum_{i=1}^{n} w_i \beta_i, \alpha \prec_M \beta \end{cases}$$

where M is another monomial order like LEX, RLEX.

Gröbner basis

Gröbner basis

Let $I = \langle f_1, \ldots, f_s \rangle$ be an ideal in $\mathbb{K}[x_1, \ldots, x_n]$ and let $\prec$ be a valid monomial ordering. A finite subset $G = \{g_1, \ldots, g_t\}$ of I different from $\{0\}$ is said to be a **Gröbner Basis** (or Standard Basis) w.r.t. $\prec$ if

$$\langle \mathrm{LM}(g_1), \ldots, \mathrm{LM}(g_t) \rangle = \langle \mathrm{LM}(I) \rangle.$$

Reduced Gröbner basis

Let G be a Gröbner basis for the ideal $I \subset \mathbb{K}[x_1, \ldots, x_n]$ with respect to a monomial ordering $\prec$, if

- $\mathrm{LC}(g) = 1$ for all $g \in G$
- for all $g \in G$, no monomial of g lies in $\langle \mathrm{LT}(G \setminus \{g\}) \rangle$

G is said to be a **reduced Gröbner basis**.

Gröbner basis: one criterion for computation

S-polynomial

Let $f, g \in R$ be nonzero polynomials. The S-polynomials of f and g, denoted as $\mathcal{S}(f, g)$ is defined as:

$$\frac{\mathrm{LCM}(\mathrm{LM}(f), \mathrm{LM}(g))}{\mathrm{LT}(f)} f - \frac{\mathrm{LCM}(\mathrm{LM}(f), \mathrm{LM}(g))}{\mathrm{LT}(g)} g$$

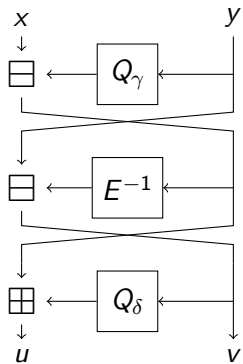
Buchberger criterion

Let I be a polynomial ideal. Then a basis $G = \{g_1, \ldots, g_t\}$ of I is a Gröbner basis of I if and only if for all pairs $i \neq j$, the remainder on division of $\mathcal{S}(g_i, g_j)$ by G (listed in some order) is zero.

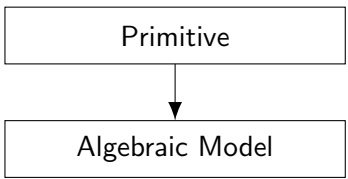
GB attack methodology

Gröbner basis attack walkthrough

Primitive

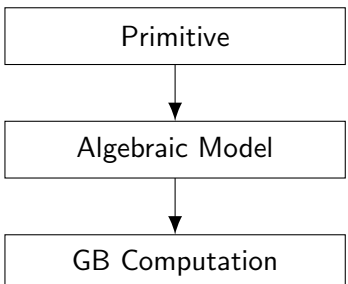


Gröbner basis attack walkthrough



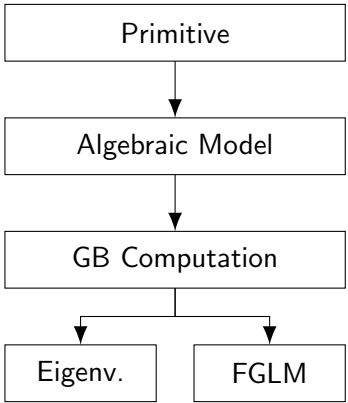
$$P = \begin{cases} p_1(x_1, \ldots, x_n) \\ p_2(x_1, \ldots, x_n) \\ p_3(x_1, \ldots, x_n) \\ \vdots \\ p_m(x_1, \ldots, x_n) \end{cases}$$

Gröbner basis attack walkthrough



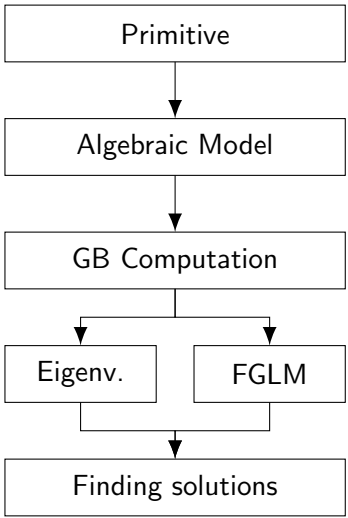
- Choose a monomial ordering
- Compute a GB G of $\langle P \rangle$ with well-known algorithms, e.g.:
  - Buchberger's algorithm [Buc85]
  - F4 [Fau99]
  - F5 [Fau02]

Gröbner basis attack walkthrough



- Univariate polynomial finding step
- Two main techniques:
  - basis conversion (e.g. `FGLM` [FM17])
  - determinant computation

Gröbner basis attack walkthrough



- Root finding for computing the variety (the solutions to the original system)

Existing problems (at least some of them)

- Degrees of the equations
- Sparse polynomial representation of the primitive
- High complexity algorithms [CG20; CLO15]:
  - GB computation
  - univariate polynomial finding
- Loose theoretical bounds

Anemoi

General overview

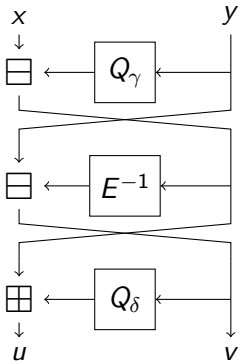
- ZK-friendly permutation [Bou+23] proposed in CRYPTO '23.
- Defined over $\mathbb{K} = \mathbb{F}_q$ where q is prime (or $q = 2^n, n \geq 32$).
- Two parameters: $\ell \geq 1$ and $\alpha \in \{3, 5, 7, 11\}$.
- $\texttt{Anemoi} : \mathbb{K}^{2\ell} \to \mathbb{K}^{2\ell}$
- Each round is composed by a:
  - Linear Layer
  - Non-linear layer: called Flystel

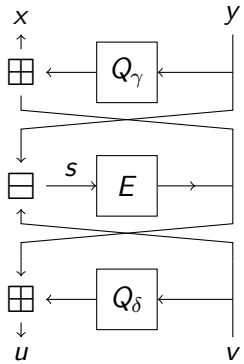
General overview

- ZK-friendly permutation [Bou+23] proposed in CRYPTO '23.
- Defined over $\mathbb{K} = \mathbb{F}_q$ where q is prime (or $q = 2^n, n \geq 32$).
- Two parameters: $\ell \geq 1$ and $\alpha \in \{3, 5, 7, 11\}$.
- $\texttt{Anemoi} : \mathbb{K}^{2\ell} \to \mathbb{K}^{2\ell}$
- Each round is composed by a:
  - Linear Layer
  - Non-linear layer: called Flystel

NOTE: we focused on $\mathbb{K} = \mathbb{F}_q$ where q is prime.

Non-linear layer: Flystel



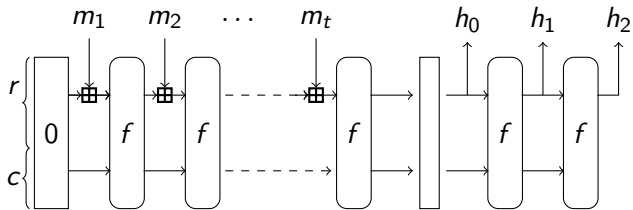


$$Q_\gamma = \beta x^2 + \gamma \quad \text{and} \quad Q_\delta = \beta x^2 + \delta$$

where $E^{-1} = x^{\frac{1}{\alpha}}$, $\beta = g$, $\gamma = 0$, $\delta = g^{-1}$

Anemoi Hashing

`Anemoi` is mainly used within **sponge constructions**.



The permutation function $f = \texttt{Anemoi}_{q,\alpha}(\mathbf{x}_0, \mathbf{y}_0)$ operating on $\mathbb{K}^{r+c}$.

Anemoi cryptanalysis

Example with $\ell = 1$ and $\alpha = 3$

CICO problem

The main problem on which algebraic attacks are based on is the CICO (Constrained Input Constrained Output) problem.

CICO for $\texttt{Anemoi}$ $\ell = 1$

Let $P : \mathbb{K}^2 \to \mathbb{K}^2$ be a permutation. The CICO problem consists in finding $(y_0, y_{N+1}) \in \mathbb{K}^2$ such that $\texttt{Anemoi}(0, y_0) = (0, y_{N+1})$.

Security Implications

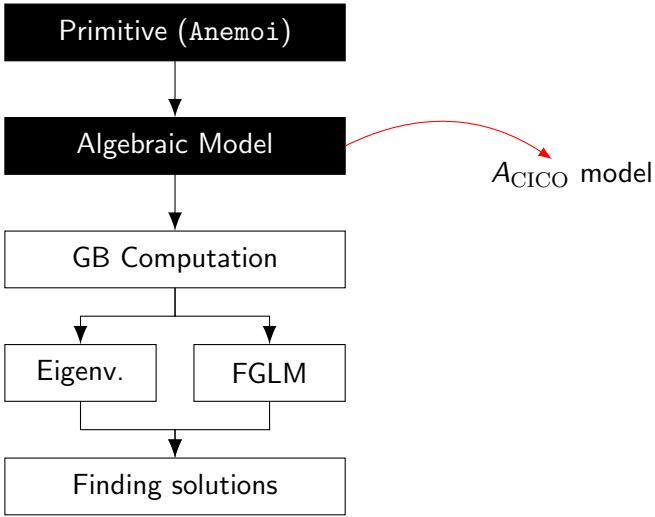
Hash functions rely on 3 main properties:

- Pre-Image Resistance
- Second Pre-Image Resistance
- Collision Resistance

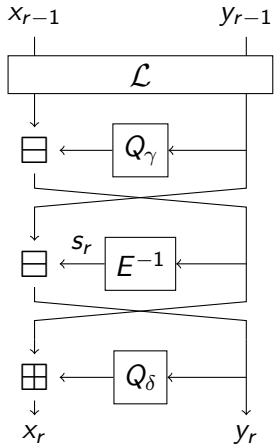
Finding the solutions to the system of polynomials means:

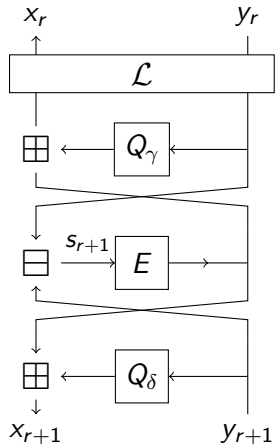
- Number of solutions $> 1 \implies$ breaking Collision resistance.
- Number of solutions $\geq 1 \implies$ breaking Pre-Image resistance.

Goals

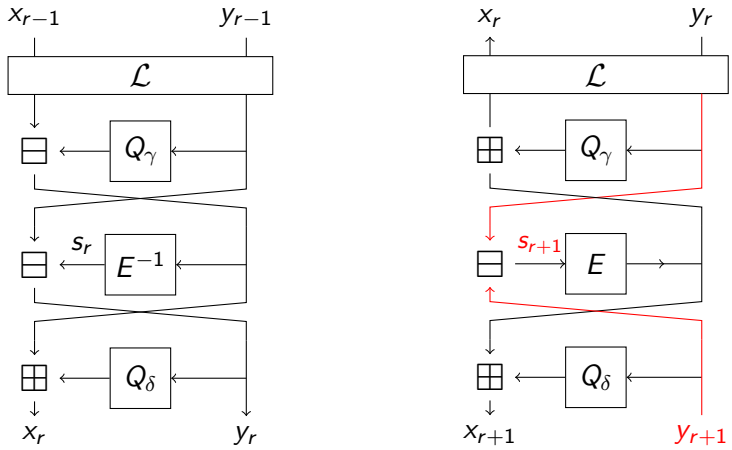

Primitive (Anemoi)
Algebraic Model
A_{CICO} model
GB Computation
Eigenv.
FGLM
Finding solutions

Modelling phase: obtaining the equations



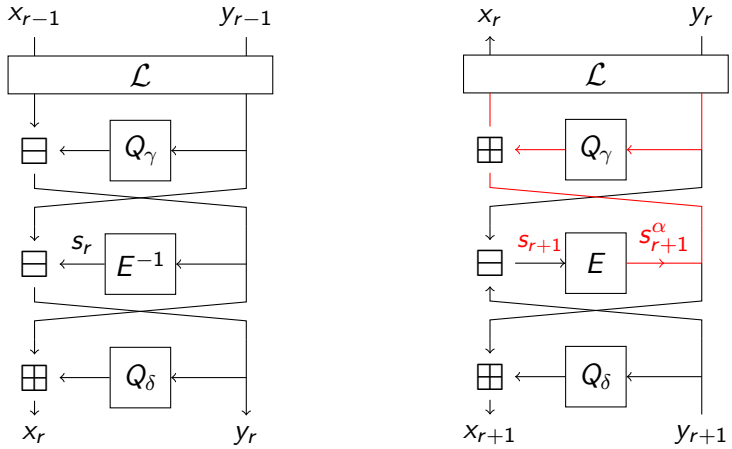


Modelling phase: obtaining the equations



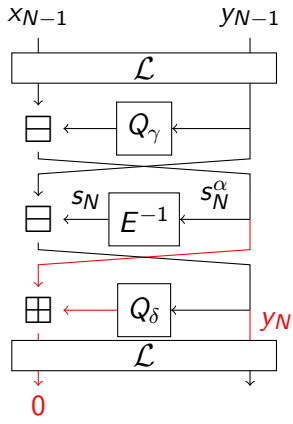
$$b_{r+1} = \mathcal{L}^{(2)}(x_r, y_r) - s_{r+1} - y_{r+1}$$

Modelling phase: obtaining the equations



$$a_{r+1} = Q_\gamma(\mathcal{L}^{(2)}(x_r, y_r)) - s^\alpha_{r+1} - \mathcal{L}^{(1)}(x_r, y_r)$$

Modelling phase: obtaining the equations



$$f_{N+1} = \mathcal{L}^{(1)}(x_N, y_N)$$

New model for Anemoi : A_{CICO}

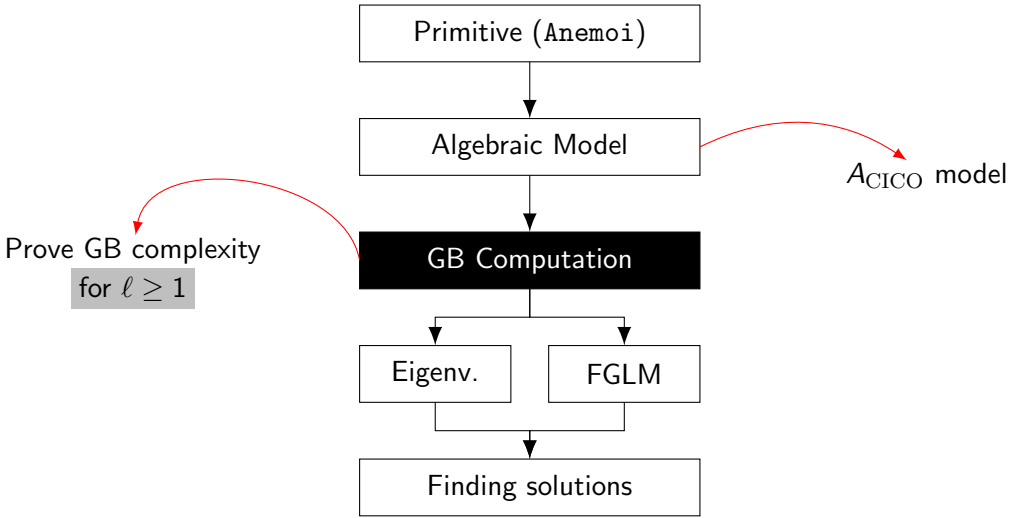
Definition (A_{CICO} model for $\ell \geq 1$)

An algebraic model of the Anemoi permutation $A_\pi : \mathbb{K}^{2\ell} \to \mathbb{K}^{2\ell}$ applied for N rounds, under the *CICO* constraints, is given by the system

$$A_{\mathrm{CICO}} = \{\mathbf{a}_1, \ldots, \mathbf{a}_N, \mathbf{b}_1, \ldots, \mathbf{b}_N, \mathbf{f}_{N+1}\}$$

where $A_{\mathrm{CICO}} \subset \mathbb{K}[\mathbf{y}_0, \ldots \mathbf{y}_N, \mathbf{s}_1, \ldots, \mathbf{s}_N]$. The generated system contains $\ell(2N+1)$ equations in $\ell(2N+1)$ variables.

Goals


Primitive (Anemoi)
Algebraic Model
A_{CICO} model
Prove GB complexity
for $\ell \geq 1$
GB Computation
Eigenv.
FGLM
Finding solutions

Gröbner basis computation

$$G_{\mathrm{DRL}} = \begin{cases} g_{i,0} := y_{i,0} + Q(\mathbf{y}_1, \mathbf{s}_1) \\ g'_{i,j} := y^{\alpha}_{i,j} + Q(s_{i,j}, \mathbf{s}_{j+1}, \mathbf{y}_{j-1}, \mathbf{y}_j, \mathbf{y}_{j+1}) \\ g_{i,j} := s^{\alpha}_{i,j} + Q(\mathbf{y}_j, \mathbf{y}_{j+1}, \mathbf{s}_{j+1}) \\ g''_{i,j} := y_{i,j} s_{i,j} + Q(s_{i,j}, \mathbf{s}_{j+1}, \mathbf{y}_{j-1}, \mathbf{y}_j, \mathbf{y}_{j+1}) \end{cases}$$

$$G_{\mathrm{W}_{DRL}} = \begin{cases} g_{i,0} := y_{i,0} + Q(\mathbf{y}_1, \mathbf{s}_1) \\ g'_{i,j} := s^{\alpha+1}_{i,j} + Q(s_{i,j}, \mathbf{s}_{j+1}, \mathbf{y}_{j-1}, \mathbf{y}_j, \mathbf{y}_{j+1}) \\ g_{i,j} := y^{2}_{i,j} + Q(s^{\alpha}_{i,j}, y_{l-i-1,j}, \mathbf{y}_{j+1}, \mathbf{s}_{j+1}) \\ g''_{i,j} := y_{i,j} s_{i,j} + Q(s_{i,j}, \mathbf{s}_{j+1}, \mathbf{y}_{j-1}, \mathbf{y}_j, \mathbf{y}_{j+1}) \end{cases}$$

where $1 \leq i \leq \ell, 1 \leq j \leq N$.
Complexity and structure of the GB: proven by following the steps of the Buchberger's Algorithm.

Why a weighted monomial ordering?

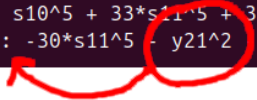
```
4: s10^5 + 3*s11^5 + 3*y20^2 + 9*y21^2 + 3*y20 + y21 - y30 - s20 - 12
5: s10^5 + 33*s11^5 + 3*y20^2 + 10*y21^2 + 33*y20 + y21 - 30*y31 - 30*s21 + 10
16: -30*s11^5 - y21^2 - 30*y20 - y30 + 30*y31 - s20 + 30*s21 - 22
```

Why a weighted monomial ordering?

```
4: s10^5 + 3*s11^5 + 3*y20^2 + 9*y21^2 + 3*y20 + y21 - y30 - s20 - 12
5: s10^5 + 33*s11^5 + 3*y20^2 + 10*y21^2 + 33*y20 + y21 - 30*y31 - 30*s21 + 10
16: -30*s11^5 - y21^2 - 30*y20 - y30 + 30*y31 - s20 + 30*s21 - 22
```

Why a weighted monomial ordering?

```
4: s10^5 + 3*s11^5 + 3*y20^2 + 9*y21^2 + 3*y20 + y21 - y30 - s20 - 12
5: s10^5 + 33*s11^5 + 3*y20^2 + 10*y21^2 + 33*y20 + y21 - 30*y31 - 30*s21 + 10
16: -30*s11^5 - y21^2 - 30*y20 - y30 + 30*y31 - s20 + 30*s21 - 22
```



$$2\mathrm{wt}(y) \geq \alpha \mathrm{wt}(s)$$

Why a weighted monomial ordering?

```
4: s10^5 + 3*s11^5 + 3*y20^2 + 9*y21^2 + 3*y20 + y21 - y30 - s20 - 12
5: s10^5 + 33*s11^5 + 3*y20^2 + 10*y21^2 + 33*y20 + y21 - 30*y31 - 30*s21 + 10
16: -30*s11^5 - y21^2 - 30*y20 - y30 + 30*y31 - s20 + 30*s21 - 22
```

$$2\mathrm{wt}(y) \geq \alpha \mathrm{wt}(s)$$

```
4: y20^2 + 3*y21^2 + 30*s10^5 + s11^5 + y20 + 30*y21 - 30*y30 - 30*s20 - 4
5: y20^2 + 33*y21^2 + 30*s10^5 + 11*s11^5 + 11*y20 + 30*y21 - 10*y31 - 10*s21 + 33
18: -30*y21^2 - 10*s11^5 - 10*y20 - 30*y30 + 10*y31 - 30*s20 + 10*s21 - 37
```

Gröbner basis computation: experimental results

Small scale experiments with a 31-bit prime: 1481823929.

		$\alpha = 3$	$\alpha = 5$	$\alpha = 7$	$\alpha = 11$
$\ell = 1$	$T_{GB}[ms]$	2.16 (21)	2.33 (21)	2.12 (20)	1.94 (19)
	d_{solv}	9	30	42	66
$\ell = 2$	$T_{GB}[ms]$	4.57 (14)	4.39 (14)	3.83 (13)	4.02 (13)
	d_{solv}	9	30	42	66
$\ell = 3$	$T_{GB}[ms]$	11.0 (12)	8.79 (12)	8.74 (12)	8.49 (11)
	d_{solv}	9	30	42	66

Table: For $\ell = 1, 2, 3$, the G_{DRL} (if $\alpha = 3$) and $G_{\mathrm{W}_{DRL}}$ (if $\alpha = 5, 7, 11$) computation time in millisecond and the solving degree d_{solv}. We present the GB results with respect to the number of rounds of `Anemoi` (in brackets), but we were able to compute the Gröbner basis for more than 100 rounds.

Gröbner basis computation complexity

DRL GB for $\alpha = 3$

$$\mathcal{O}\left(\frac{poly_1(\ell)N - poly_2(\ell)}{2}\right)$$

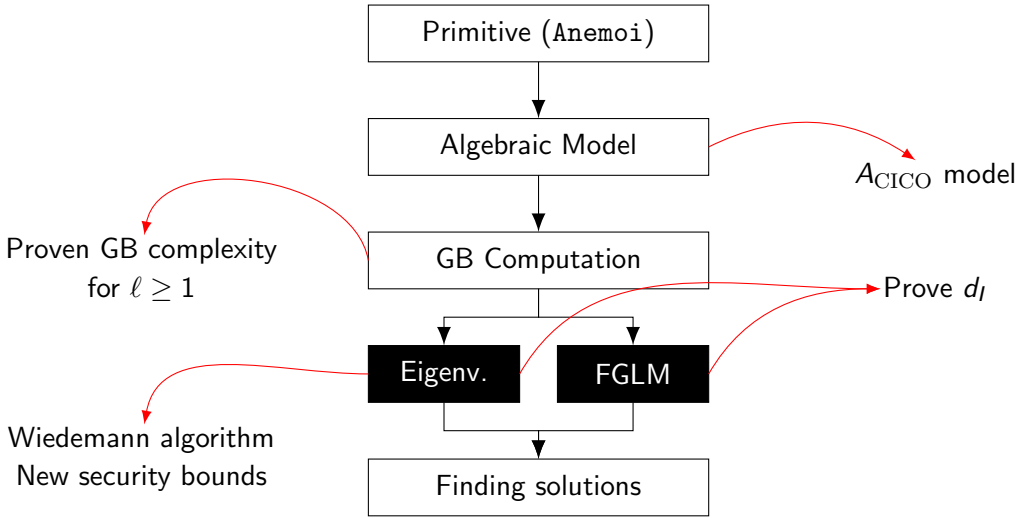
field operations where $poly_1(\ell) = \ell^2(24\ell^4 + 40\ell^3 + 32\ell^2 + 29\ell - 1)$ and $poly_2(\ell) = \ell^2(17\ell^4 + 4\ell^3 + 27\ell^2 + 15\ell + 1)$.

W_{DRL} GB for $\alpha = 5, 7, 11$

$$\mathcal{O}\left(\frac{poly_1(\ell)N + poly_2(\ell)}{2}\right)$$

field operations where $poly_1(\ell) = \ell^2(24\ell^3 + 6\ell^2 + 7\ell - 1)$ and $poly_2(\ell) = \ell^2(4\ell^4 - 6\ell^3 + 18\ell^2 + 11\ell - 1)$.

Goals


Primitive (Anemoi)
Algebraic Model
A_{CICO} model
Proven GB complexity
for $\ell \geq 1$
GB Computation
Prove d_I
Eigenv.
FGLM
Wiedemann algorithm
New security bounds
Finding solutions

Univariate polynomial finding

Main methods:

- Basis conversion: e.g. `SparseFGLM` [FM17] ($\mathcal{O}(d_I(\mathcal{Z} + n_v \log(d_I)))$)
- Eigenvalue methods:
  - Determinant computation [Bar+24; LNZ17]: $\mathcal{O}(\ell \cdot d_I^\omega)$
  - **Wiedemann algorithm** [FM17; Wie86]: $\mathcal{O}(\ell d_I(\mathcal{Z} + \log(d_I)))$

Depend on:

- $\mathcal{Z}$: number of non-zero entries in the multiplication matrices
- d_I: quotient ring dimension

The quotient ring dimension

Conjectured in [KLR24; Bar+24].

Quotient ring dimension for `Anemoi`

Let N be the number of rounds of `Anemoi` for $\ell \geq 1$ and $\alpha = 3$ (resp. $\alpha = 3, 5, 7, 11$). The dimension of the quotient ring basis of the DRL Gröbner basis (resp. W_{DRL} Gröbner basis) w.r.t `Anemoi`(N, α, ℓ) is:

$$d_I = |B_{G_{\mathrm{DRL}}}| = |B_{G_{\mathrm{W}_{DRL}}}| := (\alpha + 2)^{N\ell}$$

Proof idea: the proven GB structure of `Anemoi` $\implies$ proving d_I.

Applying the Wiedemann algorithm: why?

Conjecture: Sparsity of the multiplication matrices

Sparseness of the multiplication matrices w.r.t the input variables computed as $\mathcal{Z}/d_I^2$:

$$Sparsity(T_i) \approx \begin{cases} 0.9e^{-1.148N}/\ell & \text{for } \alpha = 3 \\ 0.32e^{-1.06N}/\ell & \text{for } \alpha = 5 \end{cases}$$

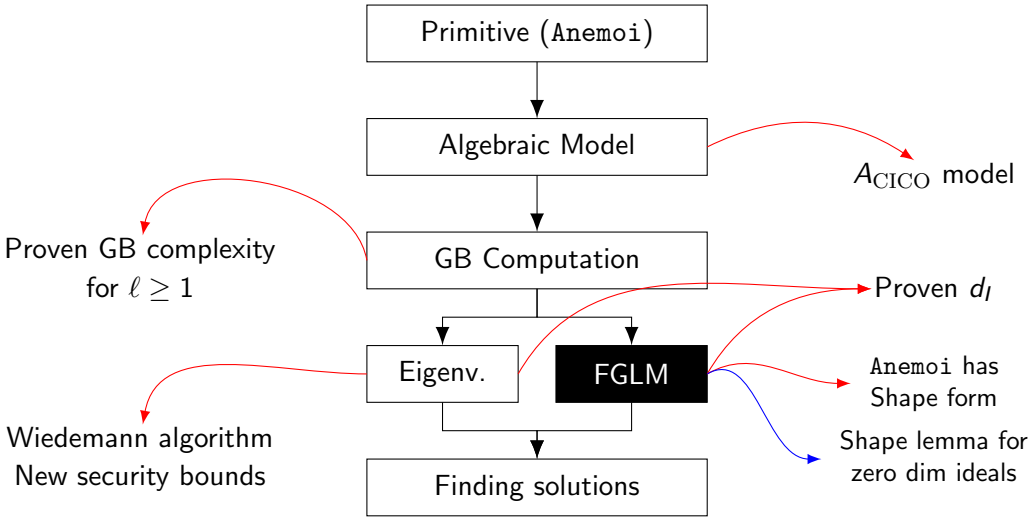
Applying the Wiedemann algorithm: results

Security	128		256	
α	3	5	3	5
$\ell = 1$	111 (21)	143 (21)	196 (37)	253 (37)
	111 (21)	122 (18)	196 (37)	253 (37)
$\ell = 2$	171 (14)	212 (14)	269 (22)	335 (22)
	122 (10)	120 (8)	245 (20)	243 (16)
$\ell = 3$	230 (12)	283 (12)	326 (17)	401 (17)
	115 (6)	117 (5)	249 (13)	235 (10)

bits : security of full rounds instances

bits : security of reduced rounds instances

Goals


Primitive (Anemoi)
Algebraic Model
A_{CICO} model
Proven GB complexity
for $\ell \geq 1$
GB Computation
Proven d_I
Eigenv.
FGLM
Anemoi has
Shape form
Wiedemann algorithm
New security bounds
Shape lemma for
zero dim ideals
Finding solutions

Basis conversion: is it useful for Anemoi?

- Common *modus operandi*: converting the GB from a graded monomial ordering to lexicographic
- In cryptanalysis, *Shape lemma is often assumed.*

Shape lemma

Let I be a zero-dimensional radical ideal such that the x_n coordinate of the points in $\mathbb{V}(I)$ are distinct. Let G be a reduced Gröbner basis for I relative to a LEX monomial order with x_n as the last variable. G consists of n polynomials

$$\{x_1 - g_1(x_n), x_2 - g_2(x_n), \ldots, g_n(x_n)\}$$

where $\deg(g_i) < \deg(g_n)$ for each $1 \leq i < n$ and $\deg(g_n) = dim_{\mathbb{K}}(\mathbb{K}[x_1, \ldots, x_n]/I)$. We say, equivalently, that the ideal I has shape lemma or shape form.

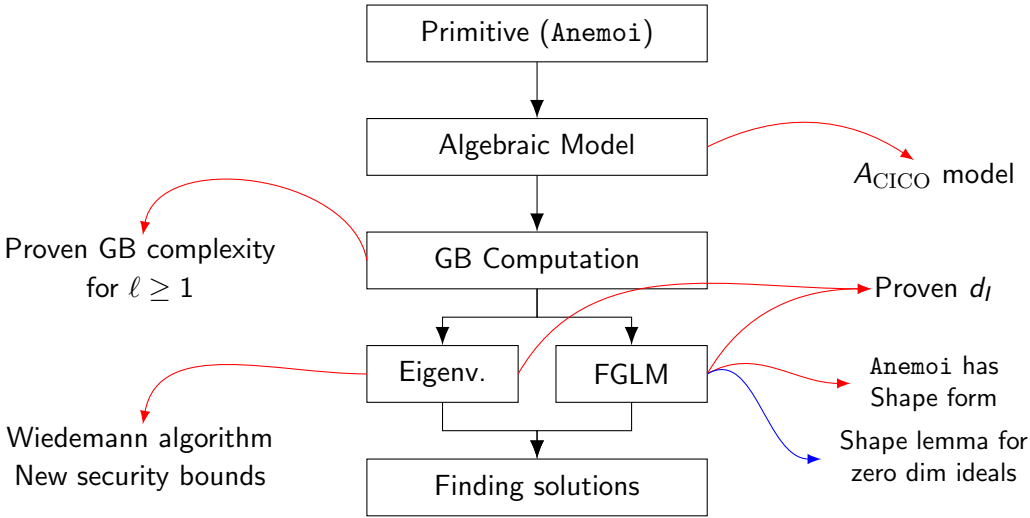
Shape lemma for zero dimensional ideals

Theorem

Let $I \subset \mathbb{K}[x_1, \ldots, x_n]$ be a zero-dimensional ideal and let G be its Gröbner basis (w.r.t a generic monomial ordering $\prec$) which contains elements f_i such that $\mathrm{LM}(f_i) = x_i^{\alpha_i}$ for each $1 \leq i \leq n$. If I has no solutions at ∞, then the ideal I has a Shape Form in the reduced LEX Gröbner basis.

Proof uses a recent result by Cox and D'Andrea [CD23].

Summary of the results



Thanks for your attention!

Questions?

Bibliography I

[Bar+24] Augustin Bariant et al. "The Algebraic FreeLunch: Efficient Gröbner Basis Attacks Against Arithmetization-Oriented Primitives". In: *Advances in Cryptology - CRYPTO 2024, Proceedings, Part IV*. Ed. by Leonid Reyzin and Douglas Stebila. Vol. 14923. Lecture Notes in Computer Science. Springer, 2024, pp. 139–173. DOI: 10.1007/978-3-031-68385-5_5.

[Bou+23] Clémence Bouvier et al. "New Design Techniques for Efficient Arithmetization-Oriented Hash Functions: ttAnemoi Permutations and ttJive Compression Mode". In: *Advances in Cryptology - CRYPTO 2023 - 43rd Annual International Cryptology Conference, CRYPTO 2023, Santa Barbara, CA, USA, August 20-24, 2023, Proceedings, Part III*. Ed. by Helena Handschuh and Anna Lysyanskaya. Vol. 14083. Lecture Notes in Computer Science. Springer, 2023, pp. 507–539. DOI: 10.1007/978-3-031-38548-3_17. URL: https://doi.org/10.1007/978-3-031-38548-3%5C_17.

Bibliography II

[Buc85] Bruno Buchberger. "Gröbner Bases: An Algorithmic Method in Polynomial Ideal Theory". In: Jan. 1985, pp. 184–232. ISBN: 978-1-4020-0328-8. DOI: 10.1007/978-94-009-5225-6_6.

[CD23] David Cox and Carlos D'andrea. "Subresultants and the Shape Lemma". In: *Math. Comput.* 92.343 (2023), pp. 2355–2379. DOI: 10.1090/MCOM/3840.

[CG20] Alessio Caminata and Elisa Gorla. "Solving Multivariate Polynomial Systems and an Invariant from Commutative Algebra". In: *Arithmetic of Finite Fields - 8th International Workshop, WAIFI 2020, Revised Selected and Invited Papers*. Ed. by Jean-Claude Bajard and Alev Topuzoglu. Vol. 12542. Lecture Notes in Computer Science. Springer, 2020, pp. 3–36. DOI: 10.1007/978-3-030-68869-1_1.

Bibliography III

[CLO15] David A. Cox, John Little, and Donal O'Shea. *Ideals, Varieties, and Algorithms*. Fourth. Undergraduate Texts in Mathematics. Springer, 2015. ISBN: 978-3-319-16720-6. DOI: 10.1007/978-3-319-16721-3.

[Fau02] Jean Charles Faugère. "A new efficient algorithm for computing Gröbner bases without reduction to zero (F5)". In: *Proceedings of the 2002 International Symposium on Symbolic and Algebraic Computation*. ISSAC '02. Association for Computing Machinery, 2002, pp. 75–83. ISBN: 1581134843. DOI: 10.1145/780506.780516.

[Fau99] Jean-Charles Faugére. "A new efficient algorithm for computing Gröbner bases (F4)". In: *Journal of Pure and Applied Algebra* 139.1 (1999), pp. 61–88. ISSN: 0022-4049. DOI: https://doi.org/10.1016/S0022-4049(99)00005-5.

Bibliography IV

[FM17] Jean-Charles Faugère and Chenqi Mou. "Sparse FGLM algorithms". In: *J. Symb. Comput.* 80 (2017), pp. 538–569. DOI: 10.1016/J.JSC.2016.07.025.

[KLR24] Katharina Koschatko, Reinhard Lüftenegger, and Christian Rechberger. "Exploring the Six Worlds of Gröbner Basis Cryptanalysis: Application to Anemoi". In: *IACR Trans. Symmetric Cryptol.* 2024.4 (2024), pp. 138–190. DOI: 10.46586/TOSC.V2024.I4.138-190.

[LNZ17] George Labahn, Vincent Neiger, and Wei Zhou. "Fast, deterministic computation of the Hermite normal form and determinant of a polynomial matrix". In: *J. Complex.* 42 (2017), pp. 44–71. DOI: 10.1016/J.JCO.2017.03.003.

Bibliography V

[Wie86] Douglas H. Wiedemann. “Solving sparse linear equations over finite fields”. In: *IEEE Trans. Inf. Theory* 32.1 (1986), pp. 54–62. DOI: 10.1109/TIT.1986.1057137.