

Group Actions, Invariants and Isomorphism Problems

Toward a Framework for Algebraic Attacks

Giuseppe D'Alconzo

Aug 15, 2026



Group Actions

Let G be a group, X a set and $\star : G \times X \rightarrow X$ be a map. We set $g \star x := \star(g, x)$.

A **group action** is a triple $(G, X, \star)$ such that

$$1) h \star (g \star x) = (hg) \star x, \quad \forall h, g \in G, x \in X;$$

$$2) e \star x = x, \quad \forall x \in X.$$

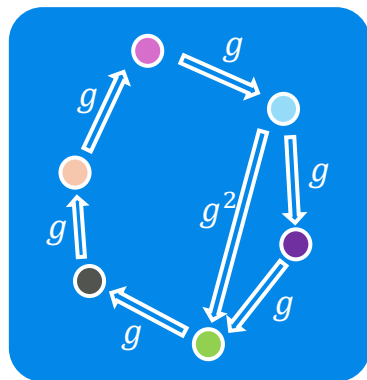
Group Actions

Let G be a group, X a set and $\star : G \times X \rightarrow X$ be a map. We set $g \star x := \star(g, x)$.

A **group action** is a triple $(G, X, \star)$ such that

$$1) h \star (g \star x) = (hg) \star x, \quad \forall h, g \in G, x \in X;$$

$$2) e \star x = x, \quad \forall x \in X.$$



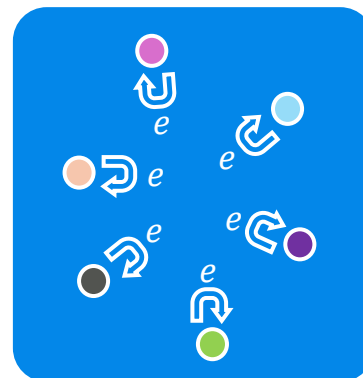
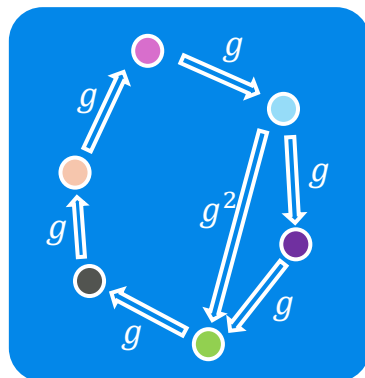
Group Actions

Let G be a group, X a set and $\star : G \times X \rightarrow X$ be a map. We set $g \star x := \star(g, x)$.

A **group action** is a triple $(G, X, \star)$ such that

$$1) h \star (g \star x) = (hg) \star x, \quad \forall h, g \in G, x \in X;$$

$$2) e \star x = x, \quad \forall x \in X.$$



Group Actions in Cryptography [ADMP20]

A group action $(G, X, \star)$ is **effective** if there are efficient algorithms for computing $\star$, products and inverses in the G , sampling and checking equality checks in G and X .

Group Actions in Cryptography [ADMP20]

A group action $(G, X, \star)$ is **effective** if there are efficient algorithms for computing $\star$, products and inverses in the G , sampling and checking equality checks in G and X .

A group action is said **one-way** if, given x and $g \star x$ for random $g \in G$ and $x \in X$, for any PPT adversary A the following probability is negligible

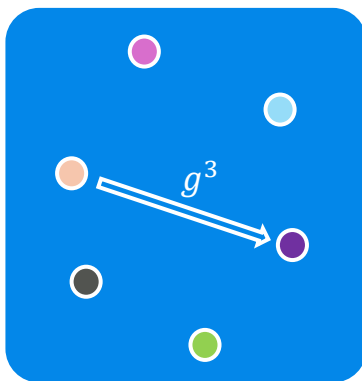
$$\Pr[A(x, g \star x) \star x = g \star x].$$

Group Actions in Cryptography [ADMP20]

A group action $(G, X, \star)$ is **effective** if there are efficient algorithms for computing $\star$, products and inverses in the G , sampling and checking equality checks in G and X .

A group action is said **one-way** if, given x and $g \star x$ for random $g \in G$ and $x \in X$, for any PPT adversary A the following probability is negligible

$$\Pr[A(x, g \star x) \star x = g \star x].$$

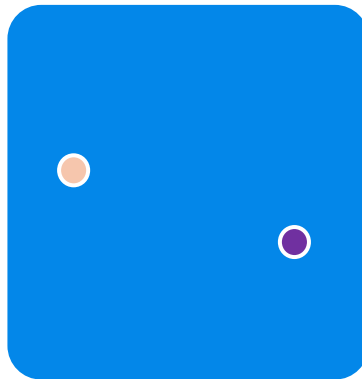


Group Actions in Cryptography [ADMP20]

A group action $(G, X, \star)$ is **effective** if there are efficient algorithms for computing $\star$, products and inverses in the G , sampling and checking equality checks in G and X .

A group action is said **one-way** if, given x and $g \star x$ for random $g \in G$ and $x \in X$, for any PPT adversary A the following probability is negligible

$$\Pr[A(x, g \star x) \star x = g \star x].$$



Examples

Let $(G, X, \star)$ be such that $G = \text{GL}(n) \times \text{GL}(m)$, $X = \text{Mat}(n \times m)$ and

$$\begin{aligned} \star : (\text{GL}(n) \times \text{GL}(m)) \times \text{Mat}(n \times m) &\rightarrow \text{Mat}(n \times m), \\ ((A, B), M) &\mapsto AMB. \end{aligned}$$

This action is effective but not one-way.

Examples

Let $(G, X, \star)$ be such that $G = \text{GL}(n) \times \text{GL}(m)$, $X = \text{Mat}(n \times m)$ and

$$\begin{aligned} \star : (\text{GL}(n) \times \text{GL}(m)) \times \text{Mat}(n \times m) &\rightarrow \text{Mat}(n \times m), \\ ((A, B), M) &\mapsto AMB. \end{aligned}$$

This action is effective but not one-way.

A well-known group action is given by $G = (\mathbb{Z}_p^*, \cdot)$, $X = \{g^1, g^2, \dots, g^{p-1}\}$ and

$$\begin{aligned} \star : G \times X &\rightarrow X \\ (a, g^i) &\mapsto (g^i)^a = g^{ai} \pmod{p}. \end{aligned}$$

Examples

Let $(G, X, \star)$ be such that $G = \text{GL}(n) \times \text{GL}(m)$, $X = \text{Mat}(n \times m)$ and

$$\begin{aligned} \star : (\text{GL}(n) \times \text{GL}(m)) \times \text{Mat}(n \times m) &\rightarrow \text{Mat}(n \times m), \\ ((A, B), M) &\mapsto AMB. \end{aligned}$$

This action is effective but not one-way.

A well-known group action is given by $G = (\mathbb{Z}_p^*, \cdot)$, $X = \{g^1, g^2, \dots, g^{p-1}\}$ and

$$\begin{aligned} \star : G \times X &\rightarrow X \\ (a, g^i) &\mapsto (g^i)^a = g^{ai} \pmod{p}. \end{aligned}$$

This is effective too, and it is believed to be one-way, since computing $a \in \mathbb{Z}_p$ from g^i and g^{ai} means solving the discrete logarithm.

Our Goal

Given an action $(G, X, \star)$ and an instance $(x, y) \in X \times X$, where $y = g \star x$, we want to write a polynomial system with coefficients in a field $\mathbb{K}$

$$\mathcal{F}_{x,y}(Z) = \begin{cases} f_1(Z) = 0 \\ \vdots \\ f_m(Z) = 0 \end{cases}$$

such that a solution of $\mathcal{F}_{x,y}(Z)$ leads to an element $h \in G$ such that $y = h \star x$.

Our Goal

Given an action $(G, X, \star)$ and an instance $(x, y) \in X \times X$, where $y = g \star x$, we want to write a polynomial system with coefficients in a field $\mathbb{K}$

$$\mathcal{F}_{x,y}(Z) = \begin{cases} f_1(Z) = 0 \\ \vdots \\ f_m(Z) = 0 \end{cases}$$

such that a solution of $\mathcal{F}_{x,y}(Z)$ leads to an element $h \in G$ such that $y = h \star x$.

Cryptanalysis of
the one-wayness
of the action.

Our Goal

Given an action $(G, X, \star)$ and an instance $(x, y) \in X \times X$, where $y = g \star x$, we want to write a polynomial system with coefficients in a field $\mathbb{K}$

$$\mathcal{F}_{x,y}(Z) = \begin{cases} f_1(Z) = 0 \\ \vdots \\ f_m(Z) = 0 \end{cases}$$

such that a solution of $\mathcal{F}_{x,y}(Z)$ leads to an element $h \in G$ such that $y = h \star x$.

Cryptanalysis of
the one-wayness
of the action.

Analysis of the
multi-sample
setting.

Our Goal

Given an action $(G, X, \star)$ and an instance $(x, y) \in X \times X$, where $y = g \star x$, we want to write a polynomial system with coefficients in a field $\mathbb{K}$

$$\mathcal{F}_{x,y}(Z) = \begin{cases} f_1(Z) = 0 \\ \vdots \\ f_m(Z) = 0 \end{cases}$$

such that a solution of $\mathcal{F}_{x,y}(Z)$ leads to an element $h \in G$ such that $y = h \star x$.

Cryptanalysis of
the one-wayness
of the action.

Analysis of the
multi-sample
setting.

MPC/VOLE-ith
signatures

The multi-sample scenario [DD24]

Some protocols expose more than one instance, namely, for a fixed $g \in G$, the attacker has access to

$$(x^{(1)}, \dots, x^{(t)}), (y^{(1)}, \dots, y^{(t)})$$

where it holds that $y^{(i)} = g \star x^{(i)}$ for each i .

The multi-sample scenario [DD24]

Some protocols expose more than one instance, namely, for a fixed $g \in G$, the attacker has access to

$$(x^{(1)}, \dots, x^{(t)}), (y^{(1)}, \dots, y^{(t)})$$

where it holds that $y^{(i)} = g \star x^{(i)}$ for each i .

Assuming the existence of a polynomial system $\mathcal{F}_{x^{(i)}, y^{(i)}}(X) = (f_1^{(i)}(X), \dots, f_m^{(i)}(X))$, we can build a larger system in the same variables, sharing the same root g :

$$\mathcal{F}(X) = \begin{cases} \mathcal{F}_{x^{(1)}, y^{(1)}}(X) = 0 \\ \vdots \\ \mathcal{F}_{x^{(t)}, y^{(t)}}(X) = 0 \end{cases}.$$

We can compute the value of t for which we can easily solve the system (linearizing for example).

Algebraic Groups

An algebraic group G over a field $\mathbb{K}$ is an algebraic variety over $\mathbb{K}$ such that the group operations are morphisms of varieties.

Algebraic Groups

An algebraic group G over a field $\mathbb{K}$ is an algebraic variety over $\mathbb{K}$ such that the group operations are morphisms of varieties.

For our purposes, there are polynomials $f_1, \dots, f_s \in \mathbb{K}[X_1, \dots, X_n]$, $p_1, \dots, p_n \in \mathbb{K}[X_1, \dots, X_{2n}]$ and $i_1, \dots, i_n \in \mathbb{K}[X_1, \dots, X_n]$ such that

Algebraic Groups

An algebraic group G over a field $\mathbb{K}$ is an algebraic variety over $\mathbb{K}$ such that the group operations are morphisms of varieties.

For our purposes, there are polynomials $f_1, \dots, f_s \in \mathbb{K}[X_1, \dots, X_n]$, $p_1, \dots, p_n \in \mathbb{K}[X_1, \dots, X_{2n}]$ and $i_1, \dots, i_n \in \mathbb{K}[X_1, \dots, X_n]$ such that

$$1) G = \{ (a_1, \dots, a_n) \in \mathbb{K}^n \mid f_1(a_1, \dots, a_n) = \dots = f_s(a_1, \dots, a_n) = 0 \}$$

$$2) gh = (p_1(g, h), \dots, p_n(g, h)) \in G, \text{ for } g, h \in G$$

(product)

$$3) g^{-1} = (i_1(g), \dots, i_n(g)) \in G, \text{ for } g \in G$$

(inverse)

Example of an Algebraic Group

Consider $G = \text{GL}(n)$ over $\mathbb{F}_q$. Then, we can see that

$$G = \left\{ (a_{11}, \dots, a_{nn}, d) \in \mathbb{F}_q^{n^2+1} \mid d \cdot \det(a_{ij}) = 1 \right\}.$$

Example of an Algebraic Group

Consider $G = GL(n)$ over $\mathbb{F}_q$. Then, we can see that

$$G = \left\{ (a_{11}, \dots, a_{nn}, d) \in \mathbb{F}_q^{n^2+1} \mid d \cdot \det(a_{ij}) = 1 \right\}.$$

Moreover, if $A = (a_{11}, \dots, a_{nn}, d_A)$ and $B = (b_{11}, \dots, b_{nn}, d_B)$, we have that

$$AB = (\sum_k a_{1k} b_{k1}, \dots, \sum_k a_{nk} b_{kn}, d_A d_B)$$

and, since $A^{-1} = \frac{1}{\det(A)} \cdot adj(A)$, we have

$$A^{-1} = (d_A \cdot adj(A)_{11}, \dots, d_A \cdot adj(A)_{nn}, \det(A)).$$

Hence, $GL(n)$ is an algebraic group.

On the Degrees

Theorem

A finite group is an algebraic group over a (carefully chosen) field $\mathbb{K}$.

proof

A finite set is a variety, then just use Lagrange's interpolation for product and inverse.

On the Degrees

Theorem

A finite group is an algebraic group over a (carefully chosen) field $\mathbb{K}$.

proof

A finite set is a variety, then just use Lagrange's interpolation for product and inverse.

However, in this way the polynomials for product and inverse have degree of the order of the cardinality of the group G . Since in cryptography we have

On the Degrees

Theorem

A finite group is an algebraic group over a (carefully chosen) field $\mathbb{K}$.

proof

A finite set is a variety, then just use Lagrange's interpolation for product and inverse.

However, in this way the polynomials for product and inverse have degree of the order of the cardinality of the group G . Since in cryptography we have

$$|G| = \Omega(2^\lambda),$$

On the Degrees

Theorem

A finite group is an algebraic group over a (carefully chosen) field $\mathbb{K}$.

proof

A finite set is a variety, then just use Lagrange's interpolation for product and inverse.

However, in this way the polynomials for product and inverse have degree of the order of the cardinality of the group G . Since in cryptography we have

$$|G| = \Omega(2^\lambda),$$

we need something smaller.

On the Degrees

Theorem

A finite group is an algebraic group over a (carefully chosen) field $\mathbb{K}$.

proof

A finite set is a variety, then just use Lagrange's interpolation for product and inverse.

However, in this way the polynomials for product and inverse have degree of the order of the cardinality of the group G . Since in cryptography we have

$$|G| = \Omega(2^\lambda),$$

we need something smaller.

For this reason we need to start with groups that are *explicitly* algebraic groups.

Algebraic Group Actions

An algebraic group action over a field $\mathbb{K}$ is a triple $(G, X, \star)$ where G is an algebraic group, X an algebraic variety over $\mathbb{K}$ and $\star : G \times X \rightarrow X$ is a morphism of varieties.

Algebraic Group Actions

An algebraic group action over a field $\mathbb{K}$ is a triple $(G, X, \star)$ where G is an algebraic group, X an algebraic variety over $\mathbb{K}$ and $\star : G \times X \rightarrow X$ is a morphism of varieties.

This means that

- 1) $G \subset \mathbb{K}^n$;
- 2) $X \subset \mathbb{K}^\ell$;

Algebraic Group Actions

An algebraic group action over a field $\mathbb{K}$ is a triple $(G, X, \star)$ where G is an algebraic group, X an algebraic variety over $\mathbb{K}$ and $\star : G \times X \rightarrow X$ is a morphism of varieties.

This means that

- 1) $G \subset \mathbb{K}^n$;
- 2) $X \subset \mathbb{K}^\ell$;
- 3) there are polynomials $s_1, \dots, s_\ell \in \mathbb{K}[Y_1, \dots, Y_n, Z_1, \dots, Z_\ell]$ such that, if $g = (a_1, \dots, a_n)$ and $x = (x_1, \dots, x_\ell)$, then

$$g \star x = (s_1(a_1, \dots, a_n, x_1, \dots, x_\ell), \dots, s_\ell(a_1, \dots, a_n, x_1, \dots, x_\ell)) \in X.$$

Example of an Algebraic Group Actions

Consider $(G, X, \star)$ be such that $G = \text{GL}(n)$, $X = \text{Mat}(n \times m)$ over $\mathbb{F}_q$, and

$$\begin{aligned} \star : \text{GL}(n) \times \text{Mat}(n \times m) &\rightarrow \text{Mat}(n \times m), \\ (B, A) &\mapsto BA. \end{aligned}$$

As before, we can see that

$$\begin{aligned} X &= \{(a_{11}, \dots, a_{nm}) \in \mathbb{F}_q^{n^2}\}. \\ G &= \{(b_{11}, \dots, b_{nn}, d) \in \mathbb{F}_q^{n^2+1} \mid d \cdot \det(b_{ij}) = 1\}. \end{aligned}$$

Example of an Algebraic Group Actions

Consider $(G, X, \star)$ be such that $G = \text{GL}(n)$, $X = \text{Mat}(n \times m)$ over $\mathbb{F}_q$, and

$$\begin{aligned} \star : \text{GL}(n) \times \text{Mat}(n \times m) &\rightarrow \text{Mat}(n \times m), \\ (B, A) &\mapsto BA. \end{aligned}$$

As before, we can see that

$$\begin{aligned} X &= \{(a_{11}, \dots, a_{nm}) \in \mathbb{F}_q^{n^2}\}. \\ G &= \{(b_{11}, \dots, b_{nn}, d) \in \mathbb{F}_q^{n^2+1} \mid d \cdot \det(b_{ij}) = 1\}. \end{aligned}$$

Moreover, if $A = (a_{11}, \dots, a_{nm})$ and $B = (b_{11}, \dots, b_{nn}, d_B)$, we have that

$$B \star A = BA = (\sum_i b_{ik} a_{i1}, \dots, \sum_i b_{ni} a_{im}).$$

Hence, it is an algebraic group action.

On the Degrees (again)

Theorem

A group action $(G, X, \star)$ with finite G and X is an algebraic group action over a (carefully chosen) field $\mathbb{K}$.

proof

As before!

On the Degrees (again)

Theorem

A group action $(G, X, \star)$ with finite G and X is an algebraic group action over a (carefully chosen) field $\mathbb{K}$.

proof

As before!

Even in this case, the polynomials for the action $\star$ would have degree of the order of

On the Degrees (again)

Theorem

A group action $(G, X, \star)$ with finite G and X is an algebraic group action over a (carefully chosen) field $\mathbb{K}$.

proof

As before!

Even in this case, the polynomials for the action $\star$ would have degree of the order of

$$|G| \cdot |X| = \Omega(2^\lambda).$$

On the Degrees (again)

Theorem

A group action $(G, X, \star)$ with finite G and X is an algebraic group action over a (carefully chosen) field $\mathbb{K}$.

proof

As before!

Even in this case, the polynomials for the action $\star$ would have degree of the order of

$$|G| \cdot |X| = \Omega(2^\lambda).$$

For the same reason we need to start with an *explicitly* algebraic group action.

The Polynomial System

Recall

$$X = \text{Mat}(n \times m) = \{(a_{11}, \dots, a_{nm}) \in \mathbb{F}_q^{n^2}\}.$$

$$G = \text{GL}(n) = \{(b_{11}, \dots, b_{nn}, d_B) \in \mathbb{F}_q^{n^2+1} \mid d_B \cdot \det((b_{ij})) = 1\}.$$

$$B \star A = (b_{11}, \dots, b_{nn}, d_B) \star (a_{11}, \dots, a_{nm}) = (\sum_i b_{1i} a_{i1}, \dots, \sum_i b_{ni} a_{im}).$$

The Polynomial System

Recall

$$\begin{aligned} X &= \text{Mat}(n \times m) = \{(a_{11}, \dots, a_{nm}) \in \mathbb{F}_q^{n^2}\}. \\ G &= \text{GL}(n) = \{(b_{11}, \dots, b_{nn}, d_B) \in \mathbb{F}_q^{n^2+1} \mid d_B \cdot \det((b_{ij})) = 1\}. \\ B \star A &= (b_{11}, \dots, b_{nn}, d_B) \star (a_{11}, \dots, a_{nm}) = (\sum_i b_{1i} a_{i1}, \dots, \sum_i b_{ni} a_{im}). \end{aligned}$$

Suppose to have $A_1, A_2 \in X$ such that there exists $B \in G$ for which $A_2 = BA_1$. Let

$$A_1 = (a_{11}^{(1)}, \dots, a_{nm}^{(1)}), A_2 = (a_{11}^{(2)}, \dots, a_{nm}^{(2)})$$

We can write

$$\mathcal{F}_{A_1, A_2}(z_{11}, \dots, z_{nn}, z) = \begin{cases} \sum_i z_{1i} a_{i1}^{(1)} = a_{11}^{(2)} \\ \vdots \\ \sum_i z_{ni} a_{im}^{(1)} = a_{nm}^{(2)} \\ z \cdot \det(z_{ij}) = 1 \end{cases}$$

A solution of the above system leads to an element $B = (z_{ij}) \in \text{GL}(n)$ such that $B \star A_1 = A_2$.

The Framework

Let $(G, X, \star)$ be an algebraic group action over $\mathbb{K}$ with

- 1) $G = \{ (a_1, \dots, a_n) \in \mathbb{K}^n \mid f_1(a_1, \dots, a_n) = \dots = f_t(a_1, \dots, a_n) = 0 \};$
- 2) $X = \{ (x_1, \dots, x_\ell) \in \mathbb{K}^\ell \mid h_1(x_1, \dots, x_\ell) = \dots = h_l(x_1, \dots, x_\ell) = 0 \};$
- 3) $g \star x = (s_1(a_1, \dots, a_n, x_1, \dots, x_\ell), \dots, s_\ell(a_1, \dots, a_n, x_1, \dots, x_\ell)) \in X.$

The Framework

Let $(G, X, \star)$ be an algebraic group action over $\mathbb{K}$ with

- 1) $G = \{ (a_1, \dots, a_n) \in \mathbb{K}^n \mid f_1(a_1, \dots, a_n) = \dots = f_t(a_1, \dots, a_n) = 0 \}$;
- 2) $X = \{ (x_1, \dots, x_\ell) \in \mathbb{K}^\ell \mid h_1(x_1, \dots, x_\ell) = \dots = h_l(x_1, \dots, x_\ell) = 0 \}$;
- 3) $g \star x = (s_1(a_1, \dots, a_n, x_1, \dots, x_\ell), \dots, s_\ell(a_1, \dots, a_n, x_1, \dots, x_\ell)) \in X$.

Given two elements $x, y \in X$, with $x = (x_1, \dots, x_\ell), y = (y_1, \dots, y_\ell)$, for which there is $g \in G$ such that $y = g \star x$, we write

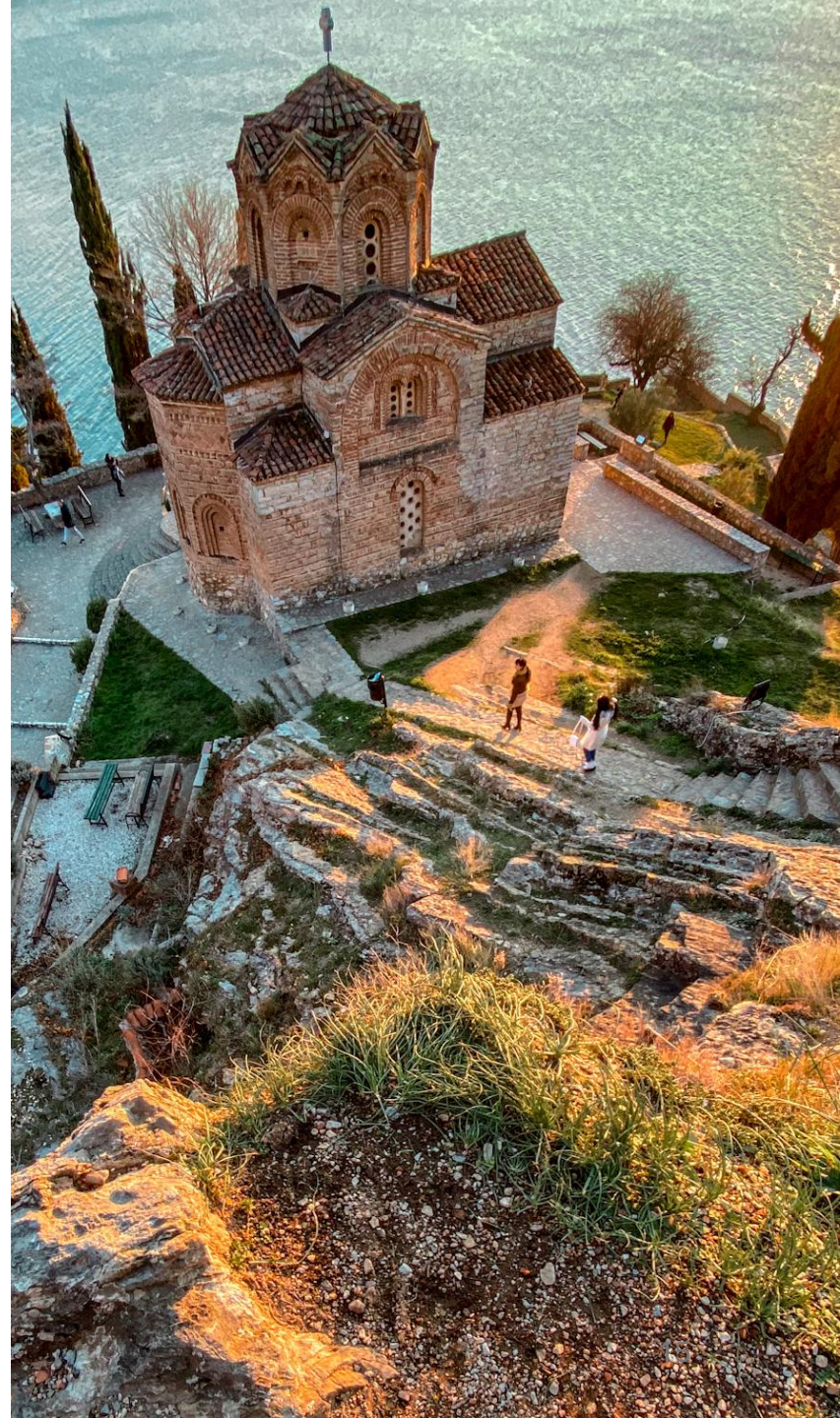
$$\mathcal{F}_{x,y}(z_1, \dots, z_n) = \begin{cases} s_1(z_1, \dots, z_n, x_1, \dots, x_\ell) = y_1 \\ \vdots \\ s_\ell(z_1, \dots, z_n, x_1, \dots, x_\ell) = y_\ell \\ f_1(z_1, \dots, z_n) = 0 \\ \vdots \\ f_t(z_1, \dots, z_n) = 0 \end{cases}.$$

On the Polynomial System

$$\mathcal{F}_{x,y}(z_1, \dots, z_n) = \begin{cases} s_1(z_1, \dots, z_n, x_1, \dots, x_\ell) = y_1 \\ \vdots \\ s_\ell(z_1, \dots, z_n, x_1, \dots, x_\ell) = y_\ell \\ f_1(z_1, \dots, z_n) = 0 \\ \vdots \\ f_t(z_1, \dots, z_n) = 0 \end{cases}.$$

It has $\ell + t$ equations (equations for G and $\star$),
 n variables (for G) and has degree

$$\max\{\deg_{(z_1, \dots, z_n)}(s_1), \dots, \deg_{(z_1, \dots, z_n)}(s_\ell), \\ \deg(f_1), \dots, \deg(f_t)\}$$



More Equations

Given $x, y \in X$, with $x = (x_1, \dots, x_\ell), y = (y_1, \dots, y_\ell)$, for which there is $g = (g_1, \dots, g_n) \in G$ such that

$$y = g \star x,$$

then it holds also that

$$g^{-1} \star y = x.$$

More Equations

Given $x, y \in X$, with $x = (x_1, \dots, x_\ell)$, $y = (y_1, \dots, y_\ell)$, for which there is $g = (g_1, \dots, g_n) \in G$ such that

$$y = g \star x,$$

then it holds also that

$$g^{-1} \star y = x.$$

Hence, using the fact that G is an algebraic group, we can write

$$g^{-1} = (i_1(g_1, \dots, g_n), \dots, i_n(g_1, \dots, g_n))$$

and consider the additional equations

$$\mathcal{F}_{x,y}^{(\text{inv})}(z_1, \dots, z_n) = \begin{cases} s_1(i_1(z_1, \dots, z_n), \dots, i_n(z_1, \dots, z_n), y_1, \dots, y_\ell) = x_1 \\ \vdots \\ s_\ell(i_1(z_1, \dots, z_n), \dots, i_n(z_1, \dots, z_n), y_1, \dots, y_\ell) = x_\ell \end{cases}$$

Linear Code Equivalence

Linear Code Equivalence problem (LCE)

Given $M_1, M_2 \in \text{Mat}_k(k \times n)$ such that they generate linearly equivalent linear codes, find $(S, Q) \in \text{GL}(k) \times \text{Mon}(n)$ such that $M_2 = SM_1Q$.

Linear Code Equivalence

Linear Code Equivalence problem (LCE)

Given $M_1, M_2 \in \text{Mat}_k(k \times n)$ such that they generate linearly equivalent linear codes, find $(S, Q) \in \text{GL}(k) \times \text{Mon}(n)$ such that $M_2 = SM_1Q$.

Observe that LCE can be reformulated as a group actions problem:

$$\begin{aligned} G &= \text{GL}(k) \times \text{Mon}(n), \\ X &= \text{Mat}_k(k \times n) = \{ M \in \text{Mat}(k \times n) \mid \text{rk}(M) = k \} \\ \star_{\text{LCE}}: G \times X &\rightarrow X, \quad ((S, Q), M) \mapsto SMQ. \end{aligned}$$

LCE as an Algebraic Group Action

Consider $\mathbb{F}_q = \{0, a_1, \dots, a_{q-1}\}$ and observe that, from [Saeed17],

$$\begin{aligned} \text{GL}(k) &= \left\{ (S_{11}, \dots, S_{kk}, d_S) \in \mathbb{F}_q^{k^2+1} \mid d_S \cdot \det(s_{ij}) = 1 \right\} \\ \text{Mon}(n) &= \left\{ (Q_{11}, \dots, Q_{nn}) \in \mathbb{F}_q^{n^2} \mid \begin{array}{l} Q_{i'j} Q_{ij} = 0 \quad \forall 1 \leq i' < i \leq n, 1 \leq j \leq n \\ \Pi_l(\Sigma_j (Q_{ij} - a_l)) = 0 \quad \forall 1 \leq i \leq n \end{array} \right\} \\ X &= \left\{ (M_{11}, \dots, M_{kn}) \in \mathbb{F}_q^{kn} \mid \text{not all minors vanish} \right\} \end{aligned}$$

The polynomials for $\star_{\text{LCE}}$ are given by

$$\left((S, Q) \star_{\text{LCE}} M \right)_{ij} = (SMQ)_{ij} = \sum_{u,v} S_{iu} M_{uv} Q_{vj}.$$

The Polynomial System for LCE

Let $M, N \in \text{Mat}_k(k \times n)$ such that $N = SMQ$, we write the system

$$\mathcal{F}_{M,N}(Y_{11}, \dots, Y_{nn}, d_Y, Z_{11}, \dots, Z_{nn}) = \begin{cases} \sum_{u,v} Y_{1u} M_{uv} Z_{v1} = N_{11} \\ \vdots \\ \sum_{u,v} Y_{ku} M_{uv} Z_{vn} = N_{kn} \\ Z_{i'j} Z_{ij} = 0 \quad \forall 1 \leq i' < i \leq n, 1 \leq j \leq n. \\ \Pi_l(\sum_j (Z_{ij} - a_l)) = 0 \quad \forall 1 \leq i \leq n \\ d_Y \cdot \det(Y) = 1 \end{cases}$$

The number of variables is $k^2 + n^2 + 1$ and the degree in Y and Z of the polynomial system is

$$\max\{n + 1, q - 1, 2\}.$$

A (not so) little workaround [DMS26]

As we saw, the degrees may be too high for a practical cryptanalysis.

We can use a technique initially developed to shorten the signatures length.

A (not so) little workaround [DMS26]

As we saw, the degrees may be too high for a practical cryptanalysis.

We can use a technique initially developed to shorten the signatures length.

Let $(G, X, \star)$ such that $G = G_1 \rtimes G_2$. Then, we define the following equivalence on X

$$x \sim y \Leftrightarrow \exists g_1 \in G_1 : y = g_1 \star x.$$

We can then define

$$X_2 = \{ [x]_{G_1} \mid x \in X \}.$$

A (not so) little workaround [DMS26]

As we saw, the degrees may be too high for a practical cryptanalysis.

We can use a technique initially developed to shorten the signatures length.

Let $(G, X, \star)$ such that $G = G_1 \rtimes G_2$. Then, we define the following equivalence on X

$$x \sim y \Leftrightarrow \exists g_1 \in G_1 : y = g_1 \star x.$$

We can then define

$$X_2 = \{ [x]_{G_1} \mid x \in X \}.$$

If there is a polynomial-time algorithm to choose a representative for a given $[x]_{\sim}$ (a Canonical Form), then the following action is effective

$$\begin{aligned} & (G_2, X_2, \star_2) \\ \star_2: G_2 \times X_2 & \rightarrow X_2, (g, [x]_{G_1}) \mapsto [g \star x]_{G_1}. \end{aligned}$$

In our Framework

Working with G_2 instead of G leads to lower degrees in the polynomials defining the algebraic group G_2 .

However, we need X_2 to be an algebraic variety. Luckily, in our case we have the following

In our Framework

Working with G_2 instead of G leads to lower degrees in the polynomials defining the algebraic group G_2 .

However, we need X_2 to be an algebraic variety. Luckily, in our case we have the following

Theorem (informal)

Consider the action $(G_1, X, \star)$ where X is an algebraic variety over a field $\mathbb{K}$. Then

$$X_2 = \{ [x]_{G_1} \mid x \in X, y \in [x]_{G_1} \Leftrightarrow \exists g_1 \in G_1 : y = g_1 \star x \}$$
 is an algebraic variety over $\mathbb{K}$.

On X_2 (1/2)

To present the structure of X_2 , we need to introduce the ring of invariant polynomials.

Definition

Given the action $(G_1, X, \star)$, where X is an algebraic variety over a field $\mathbb{K}$, the **ring of polynomials over X invariant under the action of G_1** is

$$\mathbb{K}[X]^{G_1} = \{f \in \mathbb{K}[X] \mid f(x) = f(g_1 \star x) \ \forall x \in X, \ g_1 \in G_1\}.$$

On X_2 (1/2)

To present the structure of X_2 , we need to introduce the ring of invariant polynomials.

Definition

Given the action $(G_1, X, \star)$, where X is an algebraic variety over a field $\mathbb{K}$, the **ring of polynomials over X invariant under the action of G_1** is

$$\mathbb{K}[X]^{G_1} = \{f \in \mathbb{K}[X] \mid f(x) = f(g_1 \star x) \ \forall x \in X, \ g_1 \in G_1\}.$$

And we have the following result.

Theorem [Noether1916]

If G_1 is finite, then $\mathbb{K}[X]^{G_1}$ is a **finitely-generated** $\mathbb{K}$ -algebra.

On X_2 (2/2)

Hence, let

$$\mathbb{K}[X]^{G_1} = \mathbb{K}[b_1, \dots, b_m],$$

with algebraically independent $b_1, \dots, b_m \in \mathbb{K}[X]$.

On X_2 (2/2)

Hence, let

$$\mathbb{K}[X]^{G_1} = \mathbb{K}[b_1, \dots, b_m],$$

with algebraically independent $b_1, \dots, b_m \in \mathbb{K}[X]$.

We know that we can identify elements in X_2 as the image of the map

$$\phi : X \rightarrow \mathbb{K}^m, (x_1, \dots, x_\ell) \mapsto (b_1(x_1, \dots, x_\ell), \dots, b_m(x_1, \dots, x_\ell)).$$

In other words, two elements of X are in the same orbit if and only if their images under ϕ are equal

$$y \in [x]_{G_1} \Leftrightarrow \phi(y) = \phi(x).$$

Back to the System

Let $b_1, \dots, b_m \in \mathbb{K}[X]$ be such that $\mathbb{K}[X]^{G_1} = \mathbb{K}[b_1, \dots, b_m]$.

Consider the action $(G_2, X_2, \star_2)$ where

$$G_2 = \{ (a_1, \dots, a_n) \in \mathbb{K}^n \mid f_1(a_1, \dots, a_n) = \dots = f_t(a_1, \dots, a_n) = 0 \}$$

and let $x, y \in X$ such that there is $g_2 \in G_2$ for which

$$[y]_{G_1} = [g_2 \star x]_{G_1} = g_2 \star_2 [x]_{G_1}.$$

Back to the System

Let $b_1, \dots, b_m \in \mathbb{K}[X]$ be such that $\mathbb{K}[X]^{G_1} = \mathbb{K}[b_1, \dots, b_m]$.

Consider the action $(G_2, X_2, \star_2)$ where

$$G_2 = \{ (a_1, \dots, a_n) \in \mathbb{K}^n \mid f_1(a_1, \dots, a_n) = \dots = f_t(a_1, \dots, a_n) = 0 \}$$

and let $x, y \in X$ such that there is $g_2 \in G_2$ for which

$$[y]_{G_1} = [g_2 \star x]_{G_1} = g_2 \star_2 [x]_{G_1}.$$

The polynomial system associated to $x = (x_1, \dots, x_\ell)$ and $y = (y_1, \dots, y_\ell)$ is given by

$$\mathcal{F}_{x,y}(z_1, \dots, z_n) = \begin{cases} b_1(s_1(z_1, \dots, z_n, x_1, \dots, x_\ell), \dots, s_\ell(z_1, \dots, z_n, x_1, \dots, x_\ell)) = b_1(y_1, \dots, y_\ell) \\ \vdots \\ b_t(s_1(z_1, \dots, z_n, x_1, \dots, x_\ell), \dots, s_\ell(z_1, \dots, z_n, x_1, \dots, x_\ell)) = b_t(y_1, \dots, y_\ell) \\ f_1(z_1, \dots, z_n) = 0 \\ \vdots \\ f_t(z_1, \dots, z_n) = 0 \end{cases}.$$

Our Example on LCE: a First Step

Recall the Linear Code Equivalence action:

$$G = \mathrm{GL}(k) \times \mathrm{Mon}(n), X = \mathrm{Mat}_k(k \times n) \\ \star_{\mathrm{LCE}}: G \times X \rightarrow X, \quad ((S, Q), M) \mapsto SMQ.$$

Our Example on LCE: a First Step

Recall the Linear Code Equivalence action:

$$G = \mathrm{GL}(k) \times \mathrm{Mon}(n), X = \mathrm{Mat}_k(k \times n) \\ \star_{\mathrm{LCE}}: G \times X \rightarrow X, \quad ((S, Q), M) \mapsto SMQ.$$

The group is already splitted: $G = \mathrm{GL}(k) \times \mathrm{Mon}(n)$ and we can apply or workaround.

We define the relation on $\mathrm{Mat}_k(k \times n)$

$$M_1 \sim M_2 \Leftrightarrow \exists S \in \mathrm{GL}(k) : M_2 = SM_1$$

obtaining the quotient action

$$G_2 = \mathrm{Mon}(n), X = \mathrm{Gr}(k, n) \cong \{ \mathrm{RREF}(M) \in \mathrm{Mat}_k(k \times n) \mid M \in \mathrm{Mat}_k(k \times n) \} \\ \star_{\mathrm{Mon}}: \mathrm{Mon}(n) \times \mathrm{Gr}(k, n) \rightarrow \mathrm{Gr}(k, n), (Q, M) \mapsto \mathrm{RREF}(Q \star_{\mathrm{LCE}} M).$$

Plücker Coordinates

Theorem [Every AG book]

$\text{Gr}(k, n)$ is an irreducible projective variety.

Plücker Coordinates

Theorem [Every AG book]

$\text{Gr}(k, n)$ is an irreducible projective variety.

Let $V \in \text{Gr}(k, n)$ and let M be a generator matrix. Let J be a subset of cardinality k of $\{1, \dots, n\}$ and define the **Plücker coordinates**
$$p_J : \text{Gr}(k, n) \rightarrow \mathbb{K}, V \mapsto \det(M_J).$$

Plücker Coordinates

Theorem [Every AG book]

$\text{Gr}(k, n)$ is an irreducible projective variety.

Let $V \in \text{Gr}(k, n)$ and let M be a generator matrix. Let J be a subset of cardinality k of $\{1, \dots, n\}$ and define the **Plücker coordinates**
 $p_J : \text{Gr}(k, n) \rightarrow \mathbb{K}, V \mapsto \det(M_J).$

Then, the **Plücker embedding** is given by

$$\iota : \text{Gr}(k, n) \rightarrow \mathbb{P}(\mathbb{K})^{\binom{n}{k}-1}, V \mapsto \left(p_{J_1}(V) : \dots : p_{J_{\binom{n}{k}}}(V) \right).$$

The Algebraic Group Action

How $\text{Mon}(n)$ acts on the Plücker coordinates?

A generator matrix of $Q \star_{\text{Mon}} V$ is given by MQ , where M spans V .

Let $Q = P_\sigma D$ such that $D = \text{diag}(d_1, \dots, d_n)$. Therefore, the Plücker coordinates change as

$$Q : p_J(M) \mapsto p_J(MQ) = \det\left((MQ)_J\right) = (-1)^{\sigma|_J} \cdot \left(\prod_{i \in J} d_i\right) p_{\sigma(J)}(V).$$

The Algebraic Group Action

How $\text{Mon}(n)$ acts on the Plücker coordinates?

A generator matrix of $Q \star_{\text{Mon}} V$ is given by MQ , where M spans V .

Let $Q = P_\sigma D$ such that $D = \text{diag}(d_1, \dots, d_n)$. Therefore, the Plücker coordinates change as

$$Q : p_J(M) \mapsto p_J(MQ) = \det((MQ)_J) = (-1)^{\sigma|_J} \cdot (\prod_{i \in J} d_i) p_{\sigma(J)}(V).$$

The polynomials defining the action are

$$s_J \in \mathbb{K} [Q_{11}, \dots, Q_{nn}, p_{J_1}, \dots, p_{J_{\binom{n}{k}}}]$$

with

$$s_J (Q_{11}, \dots, Q_{nn}, p_{J_1}, \dots, p_{J_{\binom{n}{k}}}) = \sum_{I \subset \{1, \dots, n\}, |I|=k} Q_{I,J} p_I$$

for $J \subset \{1, \dots, n\}, |J| = k$.

The New System

Consider $\mathbb{F}_q = \{0, a_1, \dots, a_{q-1}\}$, then from [Saeed17]

$$\text{Mon}(n) = \left\{ (Q_{11}, \dots, Q_{nn}) \in \mathbb{K}^{n^2} \mid \begin{array}{l} Q_{i'j}Q_{ij} = 0 \quad \forall 1 \leq i' < i \leq n, 1 \leq j \leq n \\ \Pi_l(\Sigma_j (Q_{ij} - a_l)) = 0 \quad \forall 1 \leq i \leq n \end{array} \right\},$$

The New System

Consider $\mathbb{F}_q = \{0, a_1, \dots, a_{q-1}\}$, then from [Saeed17]

$$\text{Mon}(n) = \left\{ (Q_{11}, \dots, Q_{nn}) \in \mathbb{K}^{n^2} \mid \begin{array}{l} Q_{i'j} Q_{ij} = 0 \quad \forall 1 \leq i' < i \leq n, 1 \leq j \leq n \\ \Pi_l(\Sigma_j (Q_{ij} - a_l)) = 0 \quad \forall 1 \leq i \leq n \end{array} \right\},$$

Let $V_1, V_2 \in \text{Gr}(k, n)$ such that $V_2 = Q \star_{\text{Mon}} V_1$ for a certain $Q \in \text{Mon}(n)$, we write the system

$$\mathcal{F}_{V_1, V_2}(Z_{11}, \dots, Z_{nn}) = \left\{ \begin{array}{l} p_{J_1}(Z \star_{\text{LCE}} V_1) = p_{J_1}(V_2) \\ \vdots \\ p_{J_{\binom{n}{k}}}(Z \star_{\text{LCE}} V_1) = p_{J_{\binom{n}{k}}}(V_2) \\ Z_{i'j} Z_{ij} = 0 \quad \forall 1 \leq i' < i \leq n, 1 \leq j \leq n \\ \Pi_l(\Sigma_j (Z_{ij} - a_l)) = 0 \quad \forall 1 \leq i \leq n \end{array} \right.$$

with degree

$$\max\{k, q - 1, 2\}.$$

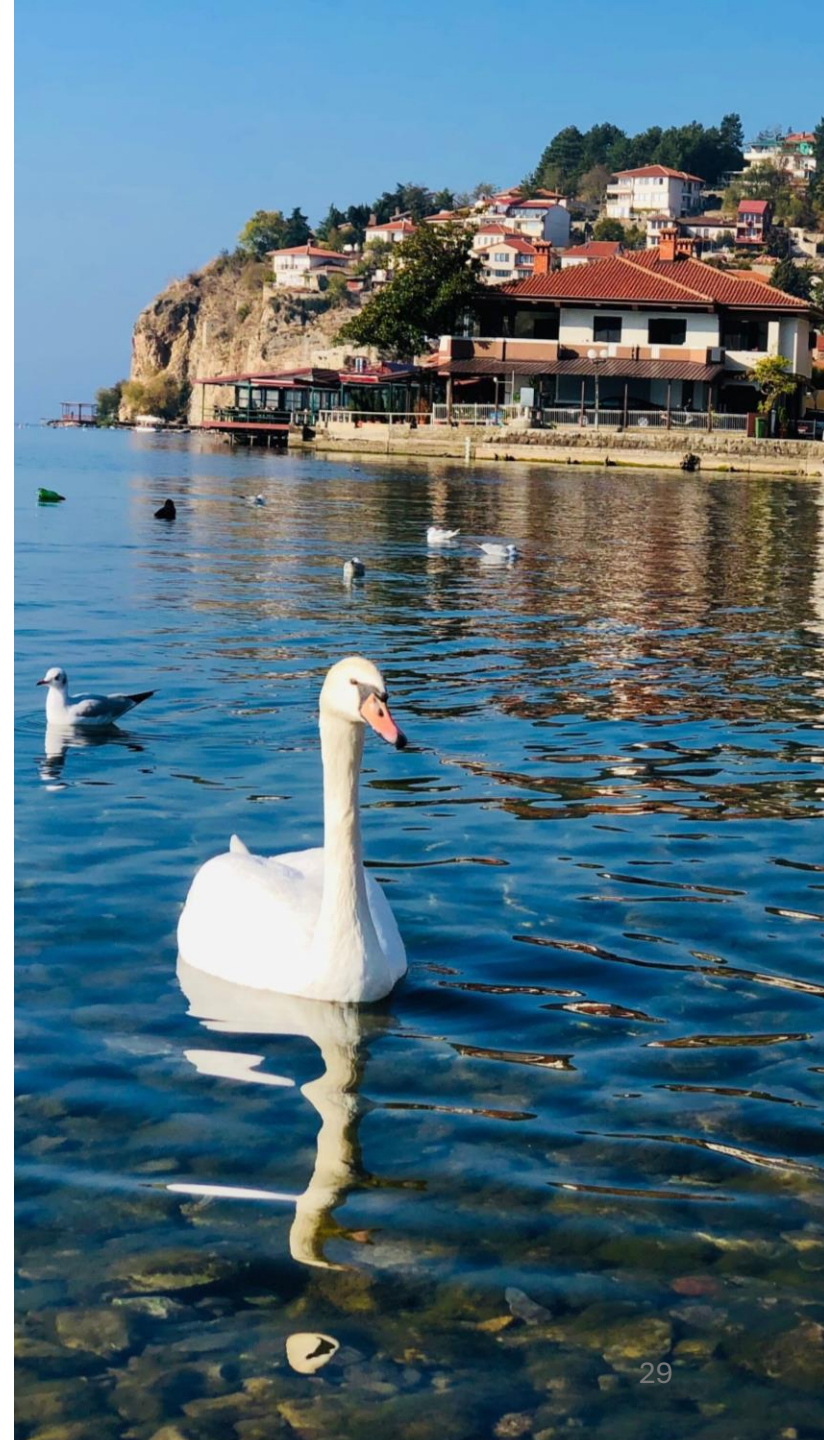
Comparison

★LCE

- Variables: $n^2 + k^2 + 1$
- Equations: $kn + \binom{n}{2}n + 1$
- Degree: $\max\{n + 1, q - 1, 2\}$

★Mon

- Variables: n^2
- Equations: $kn + \binom{n}{2}n$
- Degree: $\max\{k, q - 1, 2\}$



Our Example on LCE: a Second Step

Recall the quotient Linear Code Equivalence action

$$G = \text{Mon}(n), \quad X = \text{Gr}(k, n) \\ \star_{\text{Mon}} : \text{Mon}(n) \times \text{Gr}(k, n) \rightarrow \text{Gr}(k, n), (Q, M) \mapsto \text{RREF}(MQ).$$

It is known that

$$\text{Mon}(n) = \text{Diag}(n) \rtimes \mathcal{S}_n$$

and we can apply again our technique.

Our Example on LCE: a Second Step

Recall the quotient Linear Code Equivalence action

$$G = \text{Mon}(n), \quad X = \text{Gr}(k, n) \\ \star_{\text{Mon}} : \text{Mon}(n) \times \text{Gr}(k, n) \rightarrow \text{Gr}(k, n), (Q, M) \mapsto \text{RREF}(MQ).$$

It is known that

$$\text{Mon}(n) = \text{Diag}(n) \rtimes \mathcal{S}_n$$

and we can apply again our technique.

We define the relation on $\text{Gr}(k, n)$

$$V_1 \sim V_2 \Leftrightarrow \exists D \in \text{Diag}(n) : V_2 = D \star_{\text{Mon}} V_1,$$

and we get the quotient action [DMS26,DKQ+25]

$$G_2 = \mathcal{S}_n, \quad X_2 = \text{Gr}(k, n) / \text{Diag}(n) \\ \star_{\mathcal{S}} : \mathcal{S}_n \times X_2 \rightarrow X_2 \quad (P, [V]_{\text{Diag}}) \mapsto [P \star_{\text{Mon}} V]_{\text{Diag}}.$$

Projective Variety

Observe that, since $\text{Gr}(k, n)$ is a projective variety, we have

$$\mathbb{K}[\text{Gr}(k, n)]^{\text{Diag}(n)} = \mathbb{K}$$

and our approach adds nothing.

Projective Variety

Observe that, since $\text{Gr}(k, n)$ is a projective variety, we have

$$\mathbb{K}[\text{Gr}(k, n)]^{\text{Diag}(n)} = \mathbb{K}$$

and our approach adds nothing.

Hence, we move the field of rational functions over $\text{Gr}(k, n)$, invariant for $\text{Diag}(n)$

$$\mathbb{K}(\text{Gr}(k, n))^{\text{Diag}(n)}.$$

Projective Variety

Observe that, since $\text{Gr}(k, n)$ is a projective variety, we have

$$\mathbb{K}[\text{Gr}(k, n)]^{\text{Diag}(n)} = \mathbb{K}$$

and our approach adds nothing.

Hence, we move the field of rational functions over $\text{Gr}(k, n)$, invariant for $\text{Diag}(n)$

$$\mathbb{K}(\text{Gr}(k, n))^{\text{Diag}(n)}.$$

It can be shown that $\mathbb{K}(\text{Gr}(k, n))^{\text{Diag}(n)}$ is a finitely generated extension field over $\mathbb{K}$.

Moreover, there are monomials $b_1, \dots, b_t \in \mathbb{K}(\text{Gr}(k, n))$ such that

$$\mathbb{K}(\text{Gr}(k, n))^{\text{Diag}(n)} = \mathbb{K}[b_1, \dots, b_t].$$

The Last System (for now)

From [Saeed17] we have

$$\mathcal{S}_n = \left\{ (P_{11}, \dots, P_{nn}) \in \mathbb{K}^{n^2} \left| \begin{array}{l} P_{ij}P_{i'j} = 0, \quad \forall 1 \leq i, i', j \leq n, i \neq i' \\ \sum_j P_{ij} = 1, \quad \forall 1 \leq i \leq n \\ \sum_j P_{ij} = 1, \quad \forall 1 \leq j \leq n \end{array} \right. \right\},$$

The Last System (for now)

From [Saeed17] we have

$$\mathcal{S}_n = \left\{ (P_{11}, \dots, P_{nn}) \in \mathbb{K}^{n^2} \left| \begin{array}{l} P_{ij}P_{i'j} = 0, \quad \forall 1 \leq i, i', j \leq n, i \neq i' \\ \sum_j P_{ij} = 1, \quad \forall 1 \leq i \leq n \\ \sum_j P_{ij} = 1, \quad \forall 1 \leq j \leq n \end{array} \right. \right\},$$

Let $V_1, V_2 \in \text{Gr}(k, n)$ such that $[V_2]_{\text{Diag}} = [P \star V_1]_{\text{Diag}}$ for a certain $P \in \mathcal{S}_n$, we write the system

$$\mathcal{F}_{V_1, V_2}(Z_{11}, \dots, Z_{nn}) = \left\{ \begin{array}{l} b_1(p(Z \star_{\text{Mon}} V_1)) = b_1(p(V_2)) \\ \vdots \\ b_t(p(Z \star_{\text{Mon}} V_1)) = b_t(p(V_2)) \\ Z_{ij}Z_{i'j} = 0, \quad \forall 1 \leq i, i', j \leq n, i \neq i' \\ \sum_j Z_{ij} = 1, \quad \forall 1 \leq i \leq n \\ \sum_j Z_{ij} = 1, \quad \forall 1 \leq j \leq n \end{array} \right.$$

with degree $\max\{\deg(b_i)k, 2\}$.

Final Comparison

★LCE

- Variables: $n^2 + k^2 + 1$
- Equations: $kn + \binom{n}{2}n + 1$
- Degree: $\max\{n + 1, q - 1, 2\}$

★Mon

- Variables: n^2
- Equations: $kn + \binom{n}{2}n$
- Degree: $\max\{k, q - 1, 2\}$

★ $\mathcal{S}$

- Variables: n^2
- Equations: $kn + n^2 + 2n$
- Degree: $\max\{\deg(b_i)k, 2\}$

What is Under the Carpet

$\star_{\mathcal{S}}$

- Variables: n^2
- Equations: $kn + n^2 + 2n$
- Degree: $\max\{\deg(b_i)k, 2\}$

Recall that we are considering the Plücker coordinates: they are homogeneous polynomials in the entries of the generator matrix, with $k!$ monomials!

We are far from a practical algebraic cryptanalysis of $\star_{\text{Mon}}$ and $\star_{\mathcal{S}}$.

New Directions and Open Problems

- Use the Plücker coordinates as a distinguisher?

New Directions and Open Problems

- Use the Plücker coordinates as a distinguisher?
- A more suitable parametrization of X and G for the Linear Equivalence Problem.

New Directions and Open Problems

- Use the Plücker coordinates as a distinguisher?
- A more suitable parametrization of X and G for the Linear Equivalence Problem.
- What if we drop the ‘group’ from ‘group action’? In [CPS25] the LCE problem is modelled using a small subset of $\mathcal{S}_n$.

New Directions and Open Problems

- Use the Plücker coordinates as a distinguisher?
- A more suitable parametrization of X and G for the Linear Equivalence Problem.
- What if we drop the ‘group’ from ‘group action’? In [CPS25] the LCE problem is modelled using a small subset of $\mathcal{S}_n$.
- Explore other algebraic group actions and the application to MPC/TC/Vole in the Head.



Thank You

References

- [ADMP20] Alamati, De Feo, Montgomery, Patranabis. ‘Cryptographic group actions and applications.’ *Asiacrypt 2020*.
- [CPS25] Chou, Persichetti, Santini. ‘On linear equivalence, canonical forms, and digital signatures’. *Designs, Codes, and Cryptography* (2025).
- [DD24] D’Alconzo, Di Scala. ‘Representations of Group Actions and their Applications in Cryptography.’ *Finite Fields and Their Applications* (2024).
- [DMS26] D’Alconzo, Meneghetti, Signorini. ‘Group factorisation for smaller signatures from cryptographic group actions.’ *Designs, Codes, and Cryptography* (2026).
- [DKQ+25] Duong, Khuc, Qiao, Susilo, Zhang. ‘Blind Signatures from Cryptographic Group Actions.’ *ePrint* (2025).
- [Noether1916] Noether. ‘Der Endlichkeitsatz der Invarianten endlicher Gruppen’. (1916).
- [PV94] Popov, Vinberg. ‘Invariant Theory.’ *Algebraic Geometry IV: Linear Algebraic Groups Invariant Theory* (1994).
- [Saeed17] Saeed. ‘Algebraic approach for code equivalence.’ *PhD Thesis* (2017).