Lie algebras and the security of cryptosystems based on classical varieties in disguise

joint with Wouter Castryck, Péter Kutas, Jun Bo Lau, Alexander Lemmens, Mickael Montessinos

CRYPTOGRAPHY SEMINAR @ RENNES

Nov 7th, 2025

* Thanks to Wouter Castryck for inspiring parts of these slides.

Summary

- A series of recent papers propose post-quantum cryptosystems based on
  - Veronese threefolds (key exchange, [2023, Tullio, Gyawali])
  - Veronese surfaces (key exchange, [2025, Alzati, Tullio, Gyawali, Tortora])
  - secants of Grassmannians (signature, [2023, Tullio, Gyawali])

  in disguise, i.e., they are given up to a secret projective transformation T.

- All these schemes can be broken in classical polynomial time by the Lie algebra method.

- In this talk, we focus on the key exchange protocol from Veronese threefolds as an example.

Background

Projective varieties

- Let k be a field, the projective space $\mathbf{P}_k^n = (k^{n+1}\backslash\{0\})/\sim$ where
$$[x_0 : x_1 : \cdots : x_n] \sim [\lambda x_0 : \lambda x_1 : \cdots : \lambda x_n] \text{ for any } \lambda \in k^*.$$

- A projective variety $\mathrm{X} \subset \mathbf{P}_k^n$ is the common zero set of homogeneous polynomials $F_1, \cdots, F_r \in k[x_0, x_1, \cdots, x_n]$.

- $\mathrm{X} = \mathrm{V}(\mathrm{F}_1, \mathrm{F}_2, \cdots, F_r) = \{[\mathrm{x}_0 : \mathrm{x}_1 : \cdots : x_n] \in \mathbf{P}_k^n \mid \mathrm{F}_i(x_0, x_1, \cdots, x_n) = 0, \forall\, i\}$.

  The defining ideal of X is
$$I(X) = \{\mathrm{F} \in k[x_0, x_1, \cdots, x_n]_{hom} \mid F(p) = 0, \forall\, p \in X\}.$$

Projective equivalence

Two varieties $X, X' \subset \mathbf{P}^n$ are projectively equivalent if

$$X' = T\,(X) \subseteq \mathbf{P}^n \quad \text{for} \quad T \in PGL_{n+1}(k).$$

The projective equivalence problem is to find T given equations for X, X'.

- let $I(X) = (F_1, \cdots, F_r)$, $I(X') = (F_1', \ldots, F_r')$,
- find $S \in GL_r(k), T \in PGL_n(k)$ such that

$$\begin{pmatrix} F_1' \\ \vdots \\ F_r' \end{pmatrix} = S \circ \begin{pmatrix} F_1 \circ T^{-1} \\ \vdots \\ F_r \circ T^{-1} \end{pmatrix}$$

system of non-linear equations in many variables

The group $\boldsymbol{PG}(X)$ of projective auto-equivalences is the group of automorphisms of $\mathbf{P}^n$ that sends X to itself. I.e.,

$$\boldsymbol{PG}(X) = \{T \in PGL_{n+1}(k) |\, T(X) = T\}.$$

Veronese varieties

The d-fold Veronese embedding of $\mathbf{P}^r$ is

$$v_d : \mathbf{P}^r \hookrightarrow \mathbf{P}^n, [x_0 : x_1 : \cdots : x_r] \mapsto [x_0^d : x_0^{d-1}x_1 : \cdots : x_r^d]$$

$n = \binom{d+r}{r} - 1$

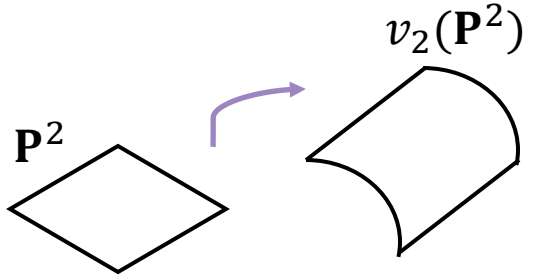
all degree-d monomials expressions in the x_i

The image $v_d(\mathbf{P}^r)$ is called a standard Veronese variety.

Example:

$$\begin{matrix} z_0 & z_1 & z_2 & z_3 & z_4 & z_5 \\ \| & \| & \| & \| & \| & \| \end{matrix}$$

- $\mathbf{P}^2 \hookrightarrow \mathbf{P}^5 : [x : y : z] \mapsto [x^2 : xy : xz : y^2 : yz : z^2]$
- defining ideal: $(z_0z_3 - z_1^2,\ z_0z_4 - z_1z_2,\ z_1z_4 - z_2z_3, z_1z_5 - z_2z_4,\ z_2^2 - z_0z_5,\ z_4^2 - z_3z_5)$



Projective auto-equivalences for Veronese varieties

Any $A \in PGL_{r+1}(F_q)$ lifts uniquely to $M \in \boldsymbol{PG}(v_d(\mathbf{P}^r), k) \subset PGL_{n+1}(k)$

- it is a change of coordinates $\begin{pmatrix} x_0 \\ x_1 \\ \vdots \\ x_r \end{pmatrix} \mapsto A \begin{pmatrix} x_0 \\ x_1 \\ \vdots \\ x_r \end{pmatrix}$
- this induces a change of coordinates of $span_k\{x_0^d, x_0^{d-1}x_1, \cdots, x_r^d\}$
- leading to a change of coordinates of $\mathbf{P}^n$

  (i.e., $M \in \boldsymbol{PG}(v_d(\mathbf{P}^r), k) \subset PGL_{n+1}(k)$)

$\Longrightarrow \quad \boldsymbol{PG}(v_d(\mathbf{P}^r), k) \cong PGL_{r+1}(k)$

Lie algebra

A Lie algebra over k is a vector space $\mathfrak{g}$ with a bilinear operator $[\cdot,\cdot] : \mathfrak{g} \times \mathfrak{g} \to \mathfrak{g}$ such that

$$[x, x] = 0,$$

$$[x, [y, z]] + [z, [x, y]] + [y, [z, x]] = 0. \text{ (Jacobi identity)}$$

Examples:

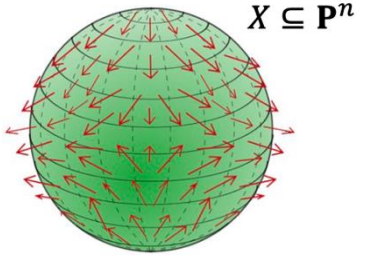
- $\mathfrak{gl}_n = \mathrm{M_n(k)}$, together with the bilinear operator $[\mathrm{A}, B] = AB - BA$.
- $\mathfrak{sl}_n$ = trace-zero matrices in $\mathrm{M_n(k)}$, with the same bilinear operator

Lie algebra of varieties

Consider a variety $X \subset \mathbf{P}^n$ over k, its Lie algebra $\mathfrak{g}(X,k)$ is a subalgebra of $\mathfrak{gl}_{n+1}(k)$:

- can think of a matrix $A \in \mathfrak{gl}_{n+1}(k)$ as a vector field in $\mathbf{P}^n$

  $\mathfrak{g}(X,k)$ consists of those A for which this vector field is tangent to X



- in terms of equations:

  - write $A = (a_{i,j})$ and $I(X) = (F_1, F_2, \cdots, F_r)$
  - $F_i\big((I + \epsilon A)\boldsymbol{x}\big) = F_i(\boldsymbol{x}) + \epsilon \, \Sigma_{k,l=1}^{n} \frac{\partial F_i}{\partial x_k} a_{k,l} x_l + O(\epsilon^2)$

infinitesimal transformation

should be in $I(X)$

Lie algebra of Veronese varieties

Recall that we saw the defining ideal of $v_2(\mathbf{P}^2)$ is

$$(z_0z_3 - z_1^2,\ z_0z_4 - z_1z_2,\ z_1z_4 - z_2z_3, z_1z_5 - z_2z_4,\ z_2^2 - z_0z_5,\ z_4^2 - z_3z_5).$$

One can calculate that $\mathfrak{g}_{v_2(\mathbf{P}^2)}$ is the span of

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 & 0 & 0 \\ 0 & 0 & 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 0 & 0 & -1 \end{pmatrix}, \begin{pmatrix} 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1/2 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1/2 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1/2 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1/2 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix},$$

$$\begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 2 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 2 & 0 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 2 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 2 \end{pmatrix}$$

In general: $\mathfrak{g}(v_d(\mathbf{P}^r)) \cong \mathfrak{gl}_{r+1}$

Key exchange from Veronese threefolds

Intuition

- S_P is the image of the standard Segre embedding $s_{1,1}$

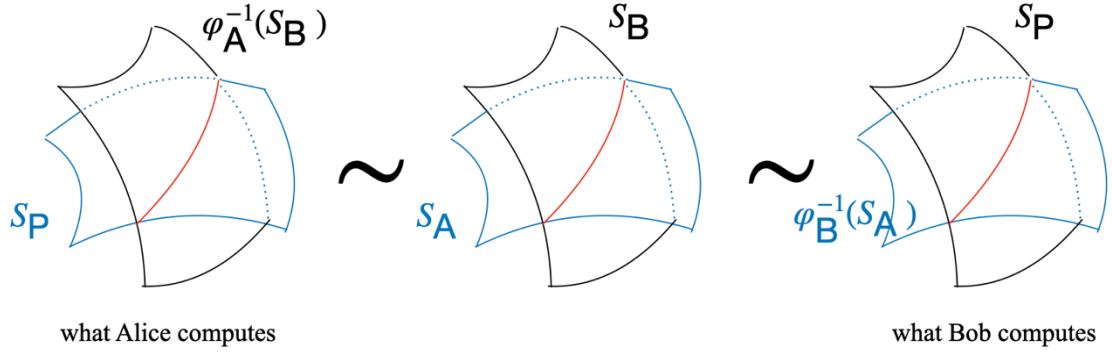
$$\mathbf{P}^1 \times \mathbf{P}^1 \hookrightarrow \mathbf{P}^3 : ([x_0 : x_1], [y_0 : y_1]) \mapsto [x_0y_0 : x_1y_1 : x_0y_1 : x_1y_0],$$

  defined by the equation $xy - zw = 0$ in $\mathbf{P}^3$.

- Alice chooses a secret automorphism φ_A of $\mathbf{P}^3$, let $S_A = \varphi_A(S_P)$.

  Bob chooses a secret automorphism φ_B of $\mathbf{P}^3$, let $S_B = \varphi_B(S_P)$.

- The intersection $S_A \cap S_B$ is an elliptic curve and its $j-$invariant is the shared secret.



Set up

- secretly embed $\mathbf{P}^3$ as a disguised Veronese threefold $V_T \coloneqq T \circ v_d(\mathbf{P}^3) \hookrightarrow \mathbf{P}^n$ by choosing $T \in PGL_{n+1}(F_q)$
- each of the n components of $(v_d \circ s_{1,1})([x_0 : x_1], [y_0 : y_1])$ is a degree $2d$ monomial expression in x_0, x_1, y_0, y_1 that is of degree d in x_0, x_1 and degree d in y_0, y_1

$$(v_d \circ s_{1,1})([x_0 : x_1], [y_0 : y_1]) = \Sigma_{d,1,1} \begin{pmatrix} x_0^d y_0^d \\ \vdots \\ x_1^d y_1^d \end{pmatrix} \text{ with } \Sigma_{d,1,1} \in \{0,1\}^{n \times (d+1)^2}$$

- reveal how S_P sits in $\mathbf{P}^n$ via $v_T \coloneqq T \circ v_d$ by giving the matrix $\Sigma_P \coloneqq T \cdot \Sigma_{d,1,1}$
- generate bunch of matrices $M_1, M_2, \cdots, M_k \in \boldsymbol{PG}(V_T, F_q)$.

public parameter $pp = (\Sigma_P, M_1, M_2, \cdots, M_k)$

Key generation

- Alice samples secret $A = M_1^{e_1} \cdot M_2^{e_2} \cdot \cdots \cdot M_k^{e_k}$

  let Φ_A denote the corresponding automorphism ($\Phi_A : \mathbf{P}^n \to \mathbf{P}^n$, fixes V_T)

- by construction, there exists some φ_A, automorphism of $\mathbf{P}^3$ such that

$$\Phi_A \circ v_T = v_T \circ \varphi_A$$

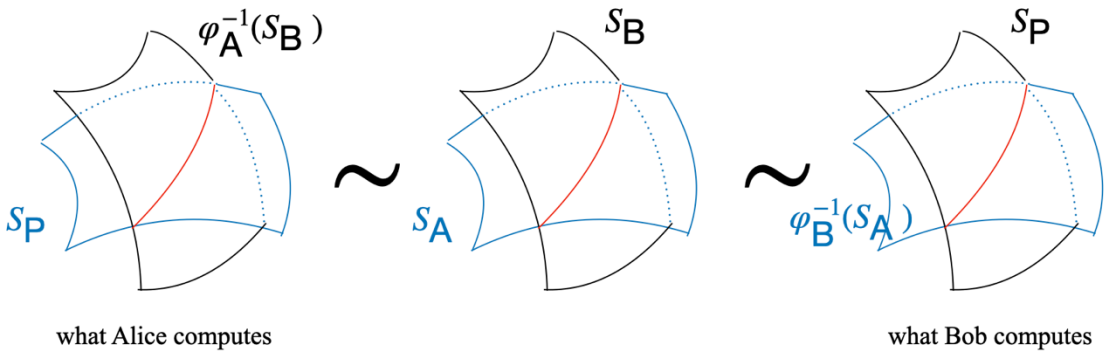
- $\Sigma_A := A \cdot \Sigma_P$ encodes the embedding $\Phi_A \circ v_T \circ s_{1,1} = v_T \circ \varphi_A \circ s_{1,1}$.
- compute H_A, a hyperplane containing $v_T(\varphi_A(S_P))$

  can be done by sampling a random non-zero vector in the left kernel of Σ_A

Alice's public key $\mathrm{pk_A} = H_A$, secret key $\mathrm{sk_A} = (e_1, e_2, \cdots, e_k)$.

Similarly, Bob's public key $\mathrm{pk_B} = H_B$, secret key $\mathrm{sk_B} = (e_1', e_2', \cdots, e_k')$.

Obtaining a shared secret



Take Alice as an example

- she computes the preimage of H_B in $\mathbf{P}^3$ via her secret key

  it is a surface containing $\varphi_A^{-1}(S_B)$
- she computes the intersection $S_P \cap surface\ (\supset \varphi_A^{-1}(S_B))$
- it is a curve of bidegree (d, d), and it contains a component of bidegree $(2,2)$
- such a component is likely unique when $d > 4$

concrete parameters for NIST I:

$q = 2^{128} + 51,$
$d = 14$

Attacking the scheme

Recovering any T' is enough

any $T' \in PGL_n(F_q)$ such that $V_T = T'(v_d(\mathbf{P}^3))$ (recall $V_T = T(v_d(\mathbf{P}^3))$)

$T'T^{-1} \in \boldsymbol{PG}(V_T)$

let $\phi \in PGL_3(F_q)$ that corresponds to $T'T^{-1}$, then an attacker can compute

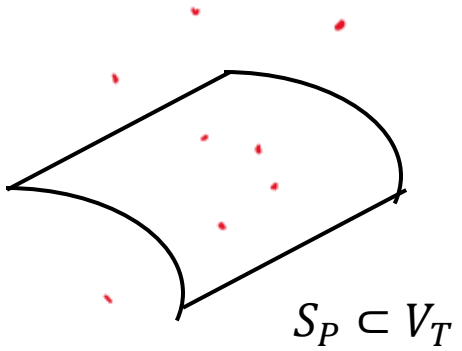
$$v_{T'}^{-1}(H_A) \cap v_{T'}^{-1}(H_B) \supset \phi^{-1}(S_A) \cap \phi^{-1}(S_B)$$

and obtain the shared secret as Alice (Bob) would.

Defining ideal of V_T

public data suffices to recover the ideal of $V_T \subset \mathbf{P}^n$

- It is known that the ideal of $v_d(\mathbf{P}^3)$ is generated by $O(d\text{^}6)$ quadratic binomials, hence $I(V_T)$ is generated by $O(d\text{^}6)$ quadratic polynomials.
- One can sample points on V_T using the knowledge of S_P and automorphisms $M_1, M_2, \cdots, M_k$
- Find generating polynomials using interpolation data.



The Lie algebra method

Overview

Let $X \subset \mathbf{P}^n, X' = T(X)$, then

$\mathfrak{g}(X,k) \to \mathfrak{g}(X',k)$: M $\mapsto TMT^{-1}$ is an isomorphism of Lie algebras.

Question: Can we recover T from an isomorphism of $\mathfrak{g}(X,k) \to \mathfrak{g}(X',k)$?

The Lie algebra method [de Graaf, Harrison, Pilnikova and Schicho, 2006, $\mathbb{Q}$]

high level description

1) compute the Lie algebras $\mathfrak{g}(X,k), \mathfrak{g}(X',k)$
2) find a Lie algebra isomorphism φ: $\mathfrak{g}(X,k) \to \mathfrak{g}(X',k)$
3) using linear algebra, find the matrices $T \in GL_{n+1}(k)$ such that

$$TMT^{-1} = \varphi(M) \text{ or, equivalently, } TM = \varphi(M)\,T$$

and identify a T that defines a projective transformation mapping X to X'.

(We work with finite field F_q in what follows.)

Computing the Lie algebra

Let $X \subset \mathbf{P}^N$ and $I(X) = (F_1, F_2, \cdots, F_r)$

(assume F_i are of the same degree (= m) for simplicity)

To compute $\mathfrak{g}(X, F_q)$:

- let $h = \binom{N+m}{m} = \dim F_q[x_0, \cdots, x_N]_m$
- compute a free family of linear forms $(f_1, \cdots, f_{h-r})$ on $F_q[x_0, \cdots, x_N]_m$

  s.t. $span_{F_q}(F_1, \cdots, F_r) = \cap_{i=1}^{d-m} \ker(f_i)$
- compute a basis of the solution space of the linear system

$$f_\alpha\left(\Sigma_{k,l=1}^{n} a_{k,l} \frac{\partial F_\beta}{\partial x_k} x_l\right) = 0,\ 1 \le \alpha \le \mathrm{h} - \mathrm{r}, 1 \le \beta \le r$$

The Lie algebra isomorphism

for veronese threefolds $N = 3 + 1$

Input: a Lie algebra $\mathfrak{g}$ isomorphic to $\mathfrak{gl}_N(F_q)$ $(N \geq 2)$

Output: an isomorphism $\varphi: \mathfrak{g} \to \mathfrak{gl}_N(F_q)$

Let $e_{i,j}$ $(i, j = \{1, \cdots, N\})$ be the standard F_q-basis of $\mathfrak{gl}_N(F_q)$

$$\mathfrak{gl}_N(F_q) = \mathrm{diag}_N(F_q) \oplus_{i \neq j} < e_{i,j} >$$

Can be characterized as "eigenspace" of the map

$$\phi_{i,j}: \lambda_1 e_{1,1} + \cdots + \lambda_N e_{N,N} \mapsto \lambda_i - \lambda_j$$

in the sense that

$$[h, e_{i,j}] = \phi_{i,j}(h) e_{i,j} \text{ for } h \in \mathrm{diag}_N(F_q).$$

The Lie algebra isomorphism

for veronese threefolds
$N = 3 + 1$

Input: a Lie algebra $\mathfrak{g}$ isomorphic to $\mathfrak{gl}_N(F_q)$ $(N \geq 2)$

Output: an isomorphism $\varphi: \mathfrak{g} \to \mathfrak{gl}_N(F_q)$

Let $e_{i,j}$ $(i,j = \{1, \cdots, N\})$ be the standard F_q-basis of $\mathfrak{gl}_N(F_q)$

$\mathfrak{gl}_N(F_q) = \mathbf{diag}_N(F_q) \oplus_{i \neq j} < e_{i,j} >$

generalization to $\mathfrak{g}$

- split Cartan subalgebra
- root system
- root space

Can be characterized as "eigenspace" of the map

$\phi_{i,j}: \lambda_1 e_{1,1} + \cdots + \lambda_N e_{N,N} \mapsto \lambda_i - \lambda_j$

in the sense that

$[h, e_{i,j}] = \phi_{i,j}(h) e_{i,j}$ for $h \in \mathrm{diag}_N(F_q)$.

The projective equivalence

Is an isomorphism φ of Lie algebras $\mathfrak{g}\left(v_d(\mathbf{P}^r), F_q\right), \mathfrak{g}\left(V_T, F_q\right) \subset \mathfrak{gl}_{n+1}(F_q)$ necessarily induced by an automorphism in $PGL_{n+1}(F_q)$?

NO

Facts about $\mathfrak{g}\left(v_d(\mathbf{P}^r), F_q\right)$:

- $\mathfrak{g}\left(v_d(\mathbf{P}^r), F_q\right) \cong \mathfrak{gl}_{r+1}\left(F_q\right)$
- $Aut^{inn}\left(\mathfrak{gl}_{r+1}\left(F_q\right)\right) = \{M \mapsto B^{-1}MB \mid B \in PGL_{r+1}(F_q)\}$
- $Aut\left(\mathfrak{gl}_{r+1}\left(F_q\right)\right) \,/\, Aut^{inn}\left(\mathfrak{gl}_{r+1}\left(F_q\right)\right)$ can be written down explicitly

Algorithm sketch

1) try to use linear algebra to find $T \in GL_{n+1}(k)$ such that $TMT^{-1} = \varphi(M)$ for a basis of $\mathfrak{g}\left(v_d(\mathbf{P}^r), F_q\right)$
2) if no solution, then correct φ with an outer automorphism

Conclusion

Conclusion

- Polynomial time attacks on three protocols based on disguised classical varieties.
- Attacks are based on the Lie algebra method, which itself could be an interesting cryptographic tool for other schemes.

Thank you!
Question?