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

Mickaël Montessinos[1]

joint work with Wouter Castryck[2] Mingjie Chen[2] Péter Kutas[13] Jun Bo Lau[2] Alexander Lemmens[2]

[1]Eötvös Loránd University, Hungary

[2]KU Leuven, Belgium

[3]University of Birmingham, United Kingdom

Thursday 14th May, 2026

Eurocrypt 2026

Hips don't Lie

Fix a projective variety $X_0 \subset \mathbb{P}^N_{\mathbb{F}_q}$. X is *projectively equivalent* to X_0, denoted by $X \sim X_0$, if there exists $T \in \mathrm{GL}_{N+1}(\mathbb{F}_q)$ such that $X = TX_0$.

The projective equivalence problem

Given $X \sim X_0$, compute some T such that $X = TX_0$.

Example

The curve $C \subset \mathbb{P}^2_{\mathbb{F}_5}$ with equation $xz = y^2 + yz + z^2$ is projectively equivalent to the conic $C_0 : y^2 = xz$ via

$$T = \begin{pmatrix} 1 & 3 & 3 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}.$$

Indeed, setting $u = x + 3y + 3z$, $v = y + z$ and $w = z$, we get:

$$y^2 = xz \iff uw = v^2 + vw + w^2.$$

True Lies

`Vero2`: A post-quantum protocol from the intersection of conics (Alzati, Di Tullio, Gyawali and Tortora, 2025). X_0 is a Veronese surface.

`Vero3`: A key exchange protocol from the intersection of quadric surfaces (Di Tullio, Gyawali, 2023). X_0 is a Veronese threefold.

`Grass`: A post-quantum signature scheme from the secant variety of the Grassmanian (Di Tullio, Gyawali, 2023). X_0 is a secant Grassmanian.

Theorem (Castryck, Chen, Kutas, Lau, Lemmens, M.)

- The security of the above protocols reduces heuristically to a projective equivalence problem with respect to the variety X_0.
- The projective equivalence problem to a Veronese variety over a finite field may be solved in polynomial time in the degree and size of the base field. (Known over $\mathbb{Q}$ from de Graaf, Harrison, Pílníková, Schicho (2006))

Little Lies

Several NIST candidate signature schemes rely on similar equivalence problems:

- MEDS relies on the Matrix Code Equivalence Problem.
- LESS relies on the Code Equivalence Problem.
- ATEQ relies on the Alternating Trilinear Form Equivalence Problem.

Obstacle

In all three cases, the relevant Lie algebras are trivial, preventing a naive application of the Lie algebra method.

Love the way you Lie

Set $n, d \in \mathbb{N}$ and $N = \binom{n+d}{n} - 1$. The *Veronese embedding of dimension n and degree d*[1] is the map

$$\begin{array}{rccc} \nu_d^{(n)}: & \mathbb{P}^n & \longrightarrow & \mathbb{P}^N \\ & (x_0 : x_1 : \cdots : x_n) & \longmapsto & (x_0^d : x_0^{d-1}x_1 : \ \ldots : x_n^d). \end{array}$$

Example

The map $\nu_2^{(1)}$ sends a point $(u : v) \in \mathbb{P}^1$ to $(u^2 : uv : v^2)$. It is a parametrisation of the conic $C_0 \subset \mathbb{P}^2$ with equation $y^2 - xz$.

In what follows, we fix:

- $X_0 = \nu_d^{(3)}(\mathbb{P}^3_{\mathbb{F}_q})$ is the Veronese threefold of degree d.
- $S \subset X_0$ is the image by $\nu_d^{(3)}$ of the Segre surface.

[1] the dimension may be omitted from the notation when clear from context

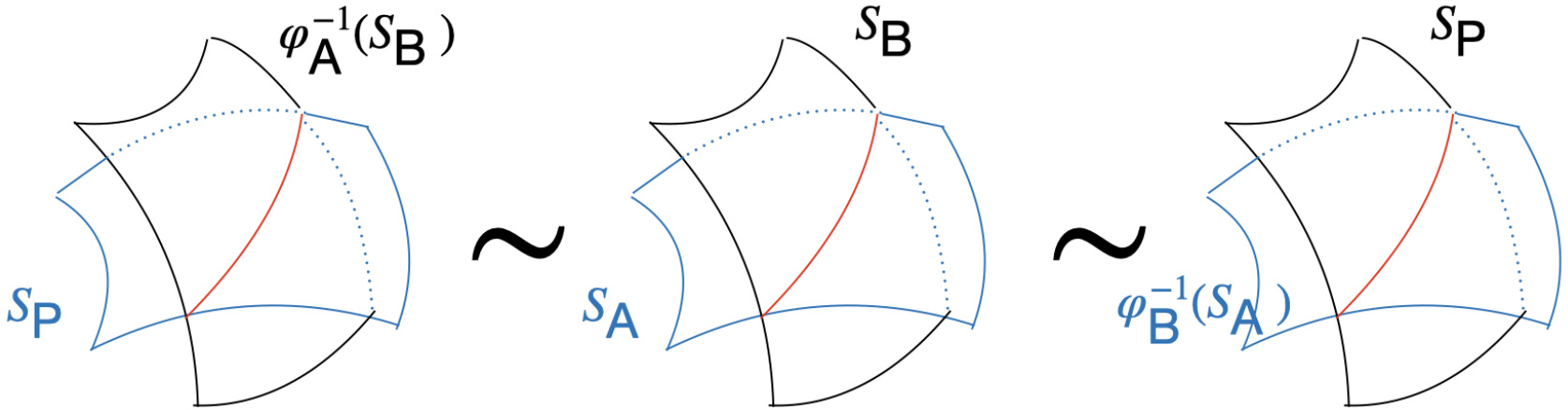
A beautiful Lie

Setup: Let $X = TX_0$ be X_0 in disguise, let $S_P = TS$.

Private keys: Let $\varphi_A, \varphi_B \in \mathrm{Aut}(X)$

Public keys: Let H_A, H_B be random hyperplanes containing respectively $S_A = \varphi_A(S_P)$ and $S_B = \varphi_B(S_P)$.

Key exchange: $S \cap \varphi_A^{-1}(H_B)$ and $S \cap \varphi_B^{-1}(H_A)$ are isomorphic curves, with one component a copy of $E = \varphi_A(S) \cap \varphi_B(S)$. E is an elliptic curve, its j-invariant is the shared key.



If you Lie down with me

Recovering equations for X

- In the actual protocol, equations for X are not published. Instead, the setup includes a map $\mathbb{P}^1 \times \mathbb{P}^1 \to S_P$ and some automorphisms of X.
- Points of X are recovered by sampling points in S_P and applying random automorphisms of X.
- A system of quartic equations can then be interpolated.

Shared key recovery reduces to the projective equivalence problem

- Assume knowledge of a projective equivalence $T : X \to X_0$
- Compute $H'_A = TH_A \cap X_0$ and $H'_B = TH_B \cap X_0$
- Recover surfaces $S'_A = (\nu_d^{(3)})^{-1}(H'_A)$ and $S'_B = (\nu_d^{(3)})^{-1}(H'_B)$
- Extract equations for $E = S'_A \cap S'_B$ by factorisation, find the j-invariant.

Lies my teacher told me

Definition

A *Lie algebra* over a field k is a vector space L with a bilinear product $[\cdot,\cdot]\colon L^2 \to L$ satisfying the *Jacobi* condition

$$[a,[b,c]]+[c,[b,a]]+[b,[c,a]]=0$$

Example

$\mathfrak{gl}_n(k)$ is the algebra of square matrices of degree n over k, with the Lie bracket product:

$$[A,B]=AB-BA$$

Definition

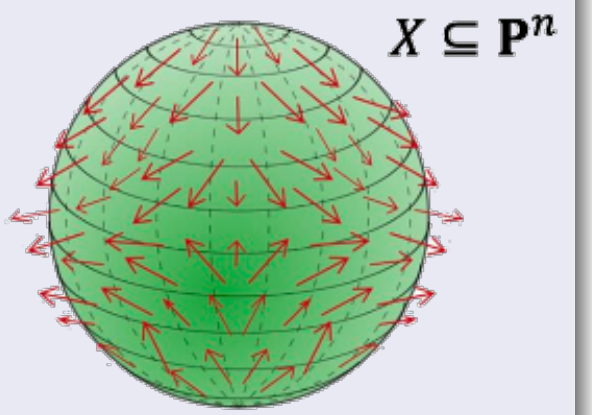
If L is a Lie algebra over k, a *representation* of L is a homomorphism $\rho\colon L \to \mathfrak{gl}_n(k)$.

House of Lies

Let $X \subset \mathbb{P}_k^N$ be a projective variety.

Definition

The Lie algebra $L(X, k)$ is the set of matrices $M \in \mathrm{GL}_{N+1}(k)$ such that $M.x \subset T_x(X)$ for all $X \in X$.



Intuitions

- $L(X, k)$ comes with a representation $L(X, k) \to \mathfrak{gl}_{N+1}(k)$.
- $L(X, k)$ is defined by linear equations.
- $L(X, k)$ is the Lie algebra of the algebraic group

$$\{T \in \mathrm{GL}_{N+1}(k) \mid TX = X\}.$$

Lie to me

Facts

- If $X \sim X_0 = \nu^{(3)}(\mathbb{P}^n_{\mathbb{F}_q}) \subset \mathbb{P}^N_{\mathbb{F}_q}$, then $L(X, \mathbb{F}_q) \simeq \mathfrak{gl}_4(\mathbb{F}_q)$.
- If $TL(X_0, k)T^{-1} = L(X, k)$, then $TX_0 = X$.

Algorithm

Input: Equations for X.

Output: $T \in \mathrm{GL}_{N+1}(\mathbb{F}_q)$ such that $TX_0 = X$.

1. Compute $L(X, \mathbb{F}_q)$ (linear algebra)
2. Compute an isomorphism $\varphi\colon L(X, \mathbb{F}_q) \to \mathfrak{gl}_4(\mathbb{F}_q)$
3. Post-compose φ with an appropriate automorphism of $\mathfrak{gl}_4(\mathbb{F}_q)$.
4. Find $T \in \mathrm{GL}_{N+1}(\mathbb{F}_q)$ such that $TL(X_0, \mathbb{F}_q)T^{-1}$ induces the map φ.
5. Compute such a T (linear algebra)

Would I Lie to you?

P.S.A

If a scheme relies on a disguised projective variety $X_0 \subset \mathbb{P}^N(\mathbb{F}_q)$, it may be vulnerable to a Lie algebra attack if the following is true:

- The group of automorphisms of $L(X_0, \mathbb{F}_q)$ is easily described.
- Isomorphisms to the Lie algebra $L(X_0, \mathbb{F}_q)$ can be computed efficiently.
- The group $\{T \in \mathrm{GL}_{N+1}(\mathbb{F}_q) \mid TL(X_0, \mathbb{F}_q)T^{-1}\}$ is trivial.
- The group $G(X_0, \mathbb{F}_q) = \{P \in \mathrm{GL}_n(\mathbb{F}_q) \mid TX = X\}$ acts transitively on X_0 and has a Borel subgroup which fixes a unique point in $\mathbb{P}^N(\mathbb{F}_q)$.

No Lie

More details in the eprint:
https://ia.cr/2026/351

Implementation in Magma:
https://gitlab.com/Mickanos/equivalence-to-veronese-varieties