

The history of MIKE (Module Isogeny Key Exchange)

2026/09/16 — **Leuven Isogeny Days 7**

Damien Robert, on behalf of the MIKE team



Inria

The MIKE team

- **Andrea Basso**
- Pierrick Dartois
- **Max Duparc**
- **Jonathan Komada Eriksen**
- **Sabrina Kunzweiler**
- Michael Meyer
- Giacomo Pope
- **Krijn Rijnders**
- **Damien Robert**
- **Ryan Rueger**
- **Sina Schaeffler**

We won 100% of our football matches!

Bold = currently here in Leuven!

Table of Contents

- 1 MIKE: an introduction
- 2 MIKE: the past
- 3 Intermezzo on the module action
- 4 MIKE: the present
- 5 MIKE: the future

Post-Quantum NIKÉ (Non Interactive Key-Exchange)

- 😊 Diffie-Hellman **key exchange** on a group: oldest example of public key cryptography
- ☹ Killed by Shor
- ☹ Paucity of **post-quantum NIKÉs**
- ☹ Swoosh: huge keys (220 KB), not actively secure (requires ZK-proofs)
- 😊 [Couveignes 1998; Rostovtsev–Stolbunov 2006; CSIDH 2018]:

$$\begin{array}{ccc} E_0 & \longrightarrow & E_A = I_A \star E_0 \\ \downarrow & & \downarrow \\ E_B = I_B \star E_0 & \longrightarrow & E_{AB} = (I_A \cdot I_B) \star E_0 \end{array}$$

- ☹ Susceptible to Kuperberg's **subexponential algorithm**, hard to make constant time^{*}

^{*} But see recent work of [Houben 2025]

How to build a NIKE?

- Take a **commutative gadget** $(G, \odot)$ acting on a **pointed stuff** (X, x_0)
- Alice picks $g_A \in G$ and send $x_A = g_A \star x_0$
- Bob picks $g_B \in G$ and send $x_B = g_B \star x_0$
- The **shared secret** is $(g_A \odot g_B) \star x_0 = g_A \star (g_B \star x_0) = g_B \star (g_A \star x_0)$.

$$\begin{array}{ccc} x_0 & \rightsquigarrow & x_A = g_A \star x_0 \\ \downarrow & & \downarrow \\ x_B = g_B \star x_0 & \rightsquigarrow & x_{AB} = (g_A \odot g_B) \star x_0 \end{array}$$

Example

- **Diffie-Hellman**: $(\mathbb{Z}, \times)$ acting on a commutative group X
- **CSIDH**: (Invertible ideals, $\cdot$) acting on elliptic curves
- **MIKE**: ((Hermitian) Projective modules, $\otimes$) acting on (principally polarised) abelian varieties

MIKE: Module Isogeny Key-Exchange

MIKE is a post-quantum NIKI which is fast, compact, constant time, actively secure and has a security proof

$$\begin{array}{ccc} E_0 & \rightsquigarrow & E_A = M_A \star E_0 \\ \downarrow \wr & & \downarrow \wr \\ E_B = M_B \star E_0 & \rightsquigarrow & E_{AB} = (M_A \otimes M_B) \star E_0 \end{array}$$

- Generalizes CSIDH by moving from **ideals** to **modules**.
- Involves **abelian varieties** of dimension 1, 2, and 4.

MIKE: Module Isogeny Key-Exchange

MIKE is a post-quantum NIKÉ which is fast, compact, constant time, actively secure and has a security proof

Post-Quantum: security relies on the CDH problem for rank 2 Hermitian modules
We have a security reduction to the supersingular endomorphism ring problem!

Compact:

- 64B for NIST level I
- 128B for NIST level V

Fast:

- Key generation $< 0.35\text{ms}$ (3ms for NIST level V)
- Key exchange $< 3\text{ms}$ (23ms for NIST level V)

Constant time: direct manipulation of kernels and isogenies, done in constant time

Actively secure: public key validation is easy (supersingularity test) and done on the fly in the key exchange

MIKE: Module Isogeny Key-Exchange

MIKE is a post-quantum NIKÉ which is fast, compact, constant time, actively secure and has a security proof

Post-Quantum: security relies on the CDH problem for rank 2 Hermitian modules
We have a security reduction to the supersingular endomorphism ring problem!

Compact:

- ~~64B for NIST level I~~ 80B for NIST level I
- ~~128B for NIST level V~~ 160B for NIST level V

Fast:

- ~~Key generation < 0.35ms~~ (3ms for NIST level V)
Key generation < 0.5ms (4.5ms for NIST level V)
- ~~Key exchange < 3ms~~ (23ms for NIST level V)
Key exchange 4.4ms (33ms for NIST level V)

Constant time: direct manipulation of kernels and isogenies, done in constant time

Actively secure: public key validation is easy (supersingularity test) and done on the fly in the key exchange

🐞 Slightly less awesome timings due to [Wesolowski 2026]. See Benjamin's talk on Thursday!

Computing the ideal action

- The **ideal action** is computed through **isogenies**
- To fix ideas: $E/\mathbb{F}_p$ a supersingular curve, $R = \text{End}_{\mathbb{F}_p}(E)$, $K = R \otimes_{\mathbb{Z}} \mathbb{Q} = \mathbb{Q}(\sqrt{-p})$.

$$R = \mathbb{Z}[\sqrt{-p}] \text{ or } \mathbb{Z}\left[\frac{1 + \sqrt{-p}}{2}\right].$$

- If $I = (N, \gamma) \subset R$, then $I \star E = E_I = E/E[I]$, where

$$E[I] = \{P \in E(\overline{\mathbb{F}}_q) \mid \alpha(P) = 0 \forall P \in I\} = E[N] \cap E[\gamma].$$

- The isogeny $\phi_I : E \rightarrow E_I$, of degree $N(I)$, depends on I
- But the **codomain** E_I only depend on the **class of I in $\text{Cl}(R)$** ^{*}.
- **Reformulation:** M is a rank 1 torsion free (projective) R -module
- Each different **embedding** $i : M \hookrightarrow R$ gives a different invertible ideal I , hence a different isogeny $\phi_I : E \rightarrow E_I$
- But they are all in the same equivalence class in $\text{Cl}(R)$, so $E_I = E_M$ only depends on M

^{*}Here $\text{Cl}(R)$ is the Picard group $\text{Pic}(R)$ of invertible ideals

Computing the module action

$A/\mathbb{F}_p$ a “standard”^{*} supersingular abelian variety, with the natural orientation by $R = \mathbb{Z}[\sqrt{-p}]$ or its maximal order

Definition

Let M be a torsion free rank g projective R -module. Fix an embedding $i : M \hookrightarrow R^g$, generators $(m_1, \dots, m_n)$ of M and write

$$i(M) = \begin{pmatrix} m_{11} & m_{12} & \dots & m_{1n} \\ m_{21} & m_{22} & \dots & m_{2n} \\ \dots & & & \\ m_{g1} & m_{g2} & \dots & m_{gn} \end{pmatrix} R^n.$$

Then $M \star A = A^g / A^g[M]$, where

$$\begin{aligned} A^g[M] &= \{P \in A^g(\overline{\mathbb{F}}_q) \mid i(m)(P) = 0 \ \forall m \in M.\} \\ &= \{P \in A^g(\overline{\mathbb{F}}_q) \mid \sum_{i=1}^g m_{i1}P_i = 0, \sum_{i=1}^g m_{i2}P_i = 0, \dots, \sum_{i=1}^g m_{in}P_i = 0\} \end{aligned}$$

Magic properties (I)

- $M \star A$ only depends on M , not on the choice of i
- $M_2 \star (M_1 \star A) = (M_1 \otimes_R M_2) \star_A = M_1 \star (M_2 \star A).$

Computing the module action

$A/\mathbb{F}_p$ a “standard”^{*} supersingular abelian variety, with the natural orientation by $R = \mathbb{Z}[\sqrt{-p}]$ or its maximal order

Definition

Then $M \star A = A^\mathcal{G}/A^\mathcal{G}[M]$, where

$$\begin{aligned} A^\mathcal{G}[M] &= \{P \in A^\mathcal{G}(\overline{\mathbb{F}}_q) \mid i(m)(P) = 0 \ \forall m \in M.\} \\ &= \{P \in A^\mathcal{G}(\overline{\mathbb{F}}_q) \mid \sum_{i=1}^g m_{i1}P_i = 0, \sum_{i=1}^g m_{i2}P_i = 0, \dots, \sum_{i=1}^g m_{in}P_i = 0\} \end{aligned}$$

- In practice, we work with principally polarised abelian varieties (A, λ_A) .
- Need $A^\mathcal{G}[M] \subset A[N]$ to be maximal isotropic for the Weil pairing $e_{N\lambda}$.
- This is equivalent to $i(M)^\# = \frac{1}{N}i(M)$ where

$$i(M)^\# = \{v \in K^\mathcal{G} \mid \sum_{i=1}^g v_i \overline{m_i} \in R \ \forall m \in i(M)\}$$

- This can be reformulated in terms of unimodular Hermitian modules.

^{*}i.e. in the isogeny class of $E^\mathcal{G}$, $E/\mathbb{F}_p$ supersingular

Supersingular ideal action vs rank 2 module action

- $E_0/\mathbb{F}_p$ supersingular, $R = \text{End}_{\mathbb{F}_p}(E_0)$ a quadratic imaginary order, $O_0 = \text{End}_{\overline{\mathbb{F}_p}}(E_0)$ a quaternionic order in $B_{p,\infty}$
- **Deuring**: Supersingular isogenies $\phi : E_0 \rightarrow E_I$ over $\mathbb{F}_{p^2}$ are given by quaternionic ideals

$$\phi : E_0 \rightarrow E_I = E_0/E_0[I]$$

where $I \subset O_0$ is a left O_0 -ideal. E_I is an elliptic curve over $\mathbb{F}_{p^2}$.

- I is also a rank 2 R -module M_I , so we can build

$$A_I = M_I \star E_0$$

an abelian surface over $\mathbb{F}_p$

Magic properties (II)

- If $R = \mathbb{Z}[\sqrt{-p}]$, $A_I = WE_I$ is the **Weil restriction** of E_I .
This is the descent of $E_I \times E_I^\sigma$ to $\mathbb{F}_p$ where σ , the Frobenius, acts by $\sigma(P, Q) = (\sigma(Q), \sigma(P))$
- If $R = \mathbb{Z}[\frac{1+\sqrt{-p}}{2}]$, $A_I = W'E_I$ is the **Scholten restriction** of E_I .

$$W'E_I = WE_I / \{(T, \sigma(T)) \mid \forall T \in E[2]\}.$$

MIKE's key exchange: the dimension 4 commutative diagram

Key generation:

- Alice fixes a rank 2 module M_A and computes $X_A = M_A \star E_0$ via a dimension 2 $\mathbb{F}_p$ -isogeny $E_0^2 \rightarrow X_A$;
- Bob fixes a rank 2 module M_B and computes $X_B = M_B \star E_0$ via a dimension 2 $\mathbb{F}_p$ -isogeny $E_0^2 \rightarrow X_B$;

$$\begin{array}{ccc} E_0^2 & \longrightarrow & X_A = M_A \star E_0 \\ \downarrow & & \\ X_B = M_B \star E_0 & & \end{array}$$

Key exchange:

$$\begin{array}{ccc} E_0^4 & \longrightarrow & X_A^2 = (M_A \star E_0)^2 \\ \downarrow & & \downarrow \\ X_B^2 = (M_B \star E_0)^2 & \longrightarrow & X_{AB} = (M_A \otimes_R M_B) \star E_0 \end{array}$$

MIKE's key exchange: the dimension 4 commutative diagram

Key generation:

- Alice fixes a quaternionic ideal I_A and computes $E_A = I_A \star E_0$ via a dimension 1 $\mathbb{F}_{p^2}$ -isogeny $E_0 \rightarrow E_A$
- Bob fixes a quaternionic ideal I_B and computes $E_B = I_B \star E_0$ via a dimension 1 $\mathbb{F}_p$ -isogeny $E_0 \rightarrow E_B$

$$\begin{array}{ccc} E_0 & \longrightarrow & E_A = I_A \star E_0 \\ \downarrow & & \\ E_B = I_B \star E_0 & & \end{array}$$

Key exchange:

$$\begin{array}{ccc} E_0^4 & \longrightarrow & X_A^2 = (W'E_A)^2 \\ \downarrow & & \downarrow \\ X_B^2 = (W'E_B)^2 & \longrightarrow & X_{AB} = (M_A \otimes_R M_B) \star E_0 \end{array}$$

- ☺ One N -isogeny in dimension one over $\mathbb{F}_{p^2}$ rather than in dimension two over $\mathbb{F}_p$
- ☺ Send one j -invariant over $\mathbb{F}_{p^2}$ rather than three Igusa invariants over $\mathbb{F}_p$ ($2 \log p$ vs $3 \log p$)
- ☺ X_{AB} lands in a special locus on which we have an extra automorphism $[i]$ that helps speed up the dimension four isogeny computations.

MIKE in practice

Parameters

- $E_0 : y^2 = x^3 - x/\mathbb{F}_p^*, p = c2^f - 1$
- Basis (P, Q) of $E_0[2^e]$, where $e + 2 \leq f^*$: $P \in E_0[2^e](\mathbb{F}_p)$ of exact order 2^e , $Q = [i]P$.
- $O_0 = R \oplus Ri$ with $R = \mathbb{Z}[\frac{1+\pi_p}{2}]$ the maximal order

Key generation

- Alice's secret key: x_A
- Alice's public key: $E_A = E_0 / \langle P + x_A Q \rangle$

Shared secret

- Construct $W'E_B$
- Build $K_A = \{P \in (W'E_B)^2[2^e] \mid \alpha P_1 + \beta P_2 = 0, -\bar{\beta}P_1 + \bar{\alpha}P_2 = 0\}$
- Compute $X_{AB} = (W'E_B)^2/K$
- Take modular invariants of X_{AB}

Lemma

- $I_A = (2^e, \gamma = \alpha + \beta i) \subset O_0$ where $\gamma = (\frac{1+\pi_p}{2} - 1)(1 - x_A i)$
- $M_A \subset R^2 = \begin{pmatrix} 2^e & 0 & \alpha & \beta \\ 0 & 2^e & -\bar{\beta} & \bar{\alpha} \end{pmatrix} R^4$.

* This curve has $j = 1728$, like $y^2 = x^3 + x$. The advantage of the former is that it is oriented by the maximal order and so has rational level 2 theta structure

* Technical condition for nice gluings formulas

MIKE in practice

In practice, we compute the isogeny directly from $WE_B = E_B \times E_B^\sigma$ rather than the 2-isogeneous $W'E_B = WE_B$:

Theorem

Let (P, Q) be a basis of $E_B[2^{e+2}]$, $\chi_A = x_A^{-1} \pmod{2^{e+2}}$ then

$$S_1 = (-[\chi_A]Q, [\chi_A]\sigma(Q), -[\chi_A]Q, [\chi_A]\sigma(Q)), \quad S_3 = (P, \sigma(P), -P, -\sigma(P))$$

$$S_2 = ([\chi_A]P, -[\chi_A]\sigma(P), [\chi_A]P, -[\chi_A]\sigma(P)), \quad S_4 = (Q, \sigma(Q), -Q, -\sigma(Q))$$

$$T_1 = ([x_A(1-x_A)/2]P, [x_A(1-x_A)/2]\sigma(P), [x_A(1+x_A)/2]P, x_A(1+x_A)/2\sigma(P)),$$

$$T_2 = ([x_A(1-x_A)/2]Q, [x_A(1-x_A)/2]\sigma(Q), [x_A(1+x_A)/2]Q, x_A(1+x_A)/2\sigma(Q)),$$

$$T_3 = ([x_A(1+x_A)/2]Q, -[x_A(1+x_A)/2]\sigma(Q), [x_A(1-x_A)/2]Q, -[x_A(1-x_A)/2]\sigma(Q)),$$

$$T_4 = (-[x_A(1+x_A)/2]P, [x_A(1+x_A)/2]\sigma(P), -[x_A(1-x_A)/2]P, +[x_A(1-x_A)/2]\sigma(P)),$$

is a symplectic basis of $(WE_B)^2[2^{e+2}]$ such that the quotient by $[4]\langle T_1, \dots, T_4 \rangle$ gives X_{AB} .

☺ No quaternions / modules in the code

☺ Constant time implementation!

Table of Contents

- 1 MIKE: an introduction
- 2 **MIKE: the past**
- 3 Intermezzo on the module action
- 4 MIKE: the present
- 5 MIKE: the future

Serre's $\mathcal{H}om$ and $\otimes$ functors (I)

- **Kronecker–Weber**: $\Lambda_E \mapsto \mathfrak{a}^{-1}\Lambda_E$ induces an ideal action $\mathfrak{a} \star E$ by invertible ideals $\mathfrak{a} \in \text{Cl}(R)$ on elliptic curves $E/\mathbb{C}$ having complex multiplication by R . (R quadratic imaginary order.)
- **Deuring**: extends the action to elliptic curves $E/\mathbb{F}_q$ by lifting and reduction:

$$\mathfrak{a} \star E = E/E[\mathfrak{a}].$$

- [Serre 1965–1966] for his course to Collège de France introduces the construction

$$\mathcal{H}om_R(\mathfrak{a}, E)$$

to define $\mathfrak{a} \star E$ intrinsically

- Mentioned in [Waterhouse 1969], and used in [Giraud 1968]^{*} to revisit the Shimura class group action on CM abelian varieties.

^{*}Giraud credits Serre and Tate for this construction.

Serre's $\mathcal{H}om$ and $\otimes$ functors (I)

- [Serre 1985] for his course “Rational Points on Curves over Finite Fields”: introduces

$$\mathcal{H}om_R(M, E) \text{ and } M \otimes_R E$$

for M an arbitrary finitely presented module and E an R -oriented object in an abelian category.

- Applies this for $E/\mathbb{F}_q$ and $R = \text{End}_{\mathbb{F}_q}(E)$.
- **Fully faithfulness:** $\text{Hom}(M_1 \otimes_R E, M_2 \otimes_R E) = \text{Hom}_R(M_1, M_2)$ when M_1, M_2 are projective;
- **Polarisations:** If M projective, $(M \otimes_R A)^\vee = M^\vee \otimes_R A^\vee$, so $(M \otimes_R E)^\vee = M^\vee \otimes_R E$, and polarisations on $M \otimes_R E$ correspond to positive definite Hermitian forms of discriminant 1
Example: polarisations on E^2 in terms of 2×2 Hermitian matrices.
- **Essential surjectivity:** When $E/\mathbb{F}_q$ is an ordinary elliptic curve and $R = \text{End}_{\mathbb{F}_q}(E)$ is a maximal order, shows that if A is R -oriented and isogeneous to E^g , then $A = P \otimes_R E$ for some projective module P of rank g
- [Serre 2001], $E_0/\mathbb{F}_q$ is ordinary, and $R = \text{End}(E_0)$ is maximal:
 $M \mapsto M \otimes_R E_0$ is an **equivalence of categories**, with inverse $A \mapsto \text{Hom}_R(E_0, A)$, between torsion free R -modules of finite rank and R -oriented abelian varieties isogeneous to E_0^g .
Also gives more details on how to view polarisations as Hermitian forms.

Serre's $\mathcal{H}om$ and $\otimes$ functors (II)

- [Jordan, Keeton, Poonen, Rains, Shepherd-Barron, Tate 2016]: Show that $M \mapsto \mathcal{H}om_R(M, E_0)$ and $A \mapsto \mathcal{H}om_R(A, E_0)$ is an equivalence of category for any $E_0/\mathbb{F}_q$ (ordinary or supersingular) with $R = \text{End}_{\mathbb{F}_q}(E_0)$, between torsion free R -modules of finite rank, and $Z(R)$ -oriented abelian varieties isogeneous to E_0^g .
- [Kirschmer, Narbonne, Ritzenthaler, R. 2021]:* first algorithmic implementation of the $\mathcal{H}om_R(M, E_0)$ functor! Use it to explore dim 3 and 4 isogeny graphs of E_0^g, E_0 ordinary. Also prove that polarisations come from Hermitian forms in the non maximal case*.
- [Page, R. 2023]: extension to the case where R is a primitive orientation by a quadratic imaginary order on an elliptic curve $E_0/\mathbb{F}_q$ $\diamond$.

For more general equivalences of categories between abelian varieties and (non commutative) “linear algebra” data (often via lifting to characteristic zero), see also: [Deligne, Howe, Centeleghe-Stix, Marseglia]...

*Project started in 2011 with Christophe, via 3×3 Hermitian matrices to build polarisations on E^3 ! It is thanks to Christophe that I learnt of Serre’s construction.

* But in retrospect, Serre’s argument from 2001 is much better...

$\diamond \infty$! Beware that when p is inert in R the functor is not essentially surjective anymore, we would need Dieudonné modules to represent infinitesimal data.

Cryptographic applications (I)

- 2022: Abelian varieties enter the picture following the break of SIDH [Castricky-Decru; Maino-Martindale-Panny-Pope-Wesolowski; R. 2023]
- But Kani's lemma is only used as a tool to compute isogenies between elliptic curves

Cryptographic applications (I)

- 2022: Abelian varieties enter the picture following the break of SIDH [Castricky-Decru; Maino-Martindale-Panny-Pope-Wesolowski; R. 2023]
- But Kani's lemma is only used as a tool to compute isogenies between elliptic curves
- [Nakagawa, Onuki 2023]: QFESTA

Cryptographic applications (I)

- 2022: Abelian varieties enter the picture following the break of SIDH [Castricky-Decru; Maino-Martindale-Panny-Pope-Wesolowski; R. 2023]
- But Kani's lemma is only used as a tool to compute isogenies between elliptic curves
- [Nakagawa, Onuki 2023]: QFESTA

Antonio Sanso: Hi Damien! Do you think we could use QFESTA to compute the ordinary class group action?

Cryptographic applications (I)

- 2022: Abelian varieties enter the picture following the break of SIDH [Castricky-Decru; Maino-Martindale-Panny-Pope-Wesolowski; R. 2023]
- But Kani's lemma is only used as a tool to compute isogenies between elliptic curves
- [Nakagawa, Onuki 2023]: QFESTA

Antonio Sanso: Hi Damien! Do you think we could use QFESTA to compute the ordinary class group action?

- We try to adapt QFESTA, but without success 😞

Cryptographic applications (I)

- **Idea:** go beyond Kani, and use the full power of the equivalence of categories?

Cryptographic applications (I)

- **Idea:** go beyond Kani, and use the full power of the equivalence of categories?

Damien: Hi Aure!! I have a norm equation that looks a lot like the KLPT norm equation. Do you know how to solve it?

Cryptographic applications (I)

- **Idea:** go beyond Kani, and use the full power of the equivalence of categories?

Damien: Hi Aurel! I have a norm equation that looks a lot like the KLPT norm equation. Do you know how to solve it?

Aurel: But of course Damien! Thanks to an exceptional isomorphism $B^\times \simeq GU'(nrd)$, the algebraic version of the classical isomorphism identifying $SU_2(\mathbb{C})$ with the group of Hamiltonian quaternions of norm 1, this is exactly KLPT!

Cryptographic applications (I)

- **Idea:** go beyond Kani, and use the full power of the equivalence of categories?

Damien: Hi Aurel! I have a norm equation that looks a lot like the KLPT norm equation. Do you know how to solve it?

Aurel: But of course Damien! Thanks to an exceptional isomorphism $B^\times \simeq GU'(nrd)$, the algebraic version of the classical isomorphism identifying $SU_2(\mathbb{C})$ with the group of Hamiltonian quaternions of norm 1, this is exactly KLPT!

Aurel: Oh by the way, here is a GP script that solves the norm equation!

Cryptographic applications (I)

- **Idea:** go beyond Kani, and use the **full power of the equivalence of categories?**

Damien: Hi Aurel! I have a norm equation that looks a lot like the KLPT norm equation. Do you know how to solve it?

Aurel: But of course Damien! Thanks to an exceptional isomorphism $B^\times \simeq GU'(nrd)$, the algebraic version of the classical isomorphism identifying $SU_2(\mathbb{C})$ with the group of Hamiltonian quaternions of norm 1, this is exactly KLPT!

Aurel: Oh by the way, here is a GP script that solves the norm equation!

Damien: Thanks Aurel!

Cryptographic applications (I)

- **Idea:** go beyond Kani, and use the **full power of the equivalence of categories?**

Damien: Hi Aurel! I have a norm equation that looks a lot like the KLPT norm equation. Do you know how to solve it?

Aurel: But of course Damien! Thanks to an exceptional isomorphism $B^\times \simeq GU'(nrd)$, the algebraic version of the classical isomorphism identifying $SU_2(\mathbb{C})$ with the group of Hamiltonian quaternions of norm 1, this is exactly KLPT!

Aurel: Oh by the way, here is a GP script that solves the norm equation!

Damien: Thanks Aurel!

- “Clapotis: Evaluating the isogeny class group action in polynomial time” [Page, R. 2023 2024 2025 2026?]
- ☹ Unraveling the construction: this is again Kani’s lemma! $\Rightarrow$ Clapoti [Page, R. 2023]

Cryptographic applications (II)

Main question: is there any application of the equivalence of category, beyond Kani's lemma?

Cryptographic applications (II)

Main question: is there any application of the equivalence of category, beyond Kani's lemma?

[R. April 2024] Talk: "Isogeny++: From ideals to modules".

- **ModuleSQISign:** Short signatures for oriented isogenies?
- **ModuleSIDH:** combining torsion noise and oriented commutative group action for a key exchange?

🕸 ModuleSIDH broken by [Eriksen, Invernizzi, Vercauteren 2026]

Cryptographic applications (III)

The equivalence of category does not tell the full picture, because we can pick a base elliptic curve E_0 , and each base point gives a new equivalence. A bit like the **ideal action**, but with **modules** rather than ideals. Gee, I wonder how we could call this phenomena?

Cryptographic applications (III)

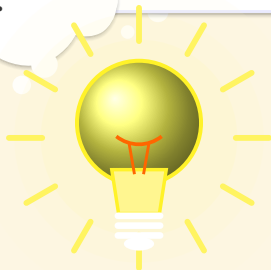
Five months later...

The equivalence of category does not tell the full picture, because we can pick a base elliptic curve E_0 , and each base point gives a new equivalence. A bit like the **ideal action**, but with **modules** instead of **ideals**. Gee, I wonder how we could call this phenom-

Cryptographic applications (III)

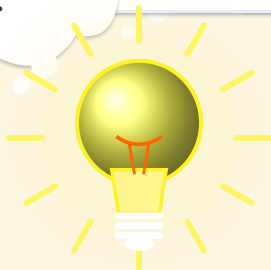
The equivalence of category does not tell the full picture, because we can pick a base elliptic curve E_0 , and each base point gives a new equivalence. A bit like the **ideal action**, but with **modules** instead of **ideals**. Gee, I wonder how we could call this phenom-

Five months later...



The equivalence of category does not tell the full picture, because we can pick a base elliptic curve E_0 , and each base point gives a new equivalence. A bit like the **ideal action**, but with **modules** instead of ideals. Geez, I wonder how we could call this phenom-

Five months later...



A module action!

Cryptographic applications (III)

- In September 2024, while preparing my slides for LID 5, I realized the correct notion was that of a (contravariant) **module action**!
- $\otimes$ -MIKE^{*} is born ≈ 5 seconds later.
- **Key idea**: if R is **commutative**, then $A = \mathcal{H}om_R(M, E)$ is still oriented by R , so we can **iterate the construction**!

More generally, even for non commutative rings, if M is a (R, S_1) -bimodule, and A is (R, S_2) -bioriented, then $\mathcal{H}om_R(M, A)$ has a natural (S_1, S_2) -biorientation.

The above example is then a special case: when R is commutative, a R -module is naturally a (R, R) -bimodule.

^{*} Called $\otimes$ -SIDH at the time. Luca suggested to use MIKE instead. Terminology: $\otimes$ -MIKE is any NIKE from the general module action, while MIKE is our specific instantiation.

The module action and $\otimes$ -MIKE

- [R. October 2024] Talk: “From ideals to modules for isogeny based cryptography” at LID 5 introduces the module action and $\otimes$ -MIKE
- [R. November 2024] Preprint: “The module action for isogeny based cryptography”

The module action and $\otimes$ -MIKE

- [R. October 2024] Talk: “From ideals to modules for isogeny based cryptography” at LID 5 introduces the module action and $\otimes$ -MIKE
- [R. November 2024] Preprint: “The module action for isogeny based cryptography”

Potential problem:

Recall MIKE’s commutative diagram:

$$\begin{array}{ccc} E_0^4 & \longrightarrow & W'E_A^2 \\ \downarrow & & \downarrow \\ W'E_B^2 & \longrightarrow & \text{Mike}(E_A, E_B) \end{array}$$

- If $E_0 \rightarrow E_A$ and $E_0 \rightarrow E_B$ are both 2^e -isogenies with disjoint kernels, won’t $\text{Mike}(E_A, E_B)$ be trivial?
- Should we use 2^a and 3^b as in SIDH?
- ☹ But then we would need to use SIDH primes and use larger primes

The module action and $\otimes$ -MIKE

March 2025:

Jonathan: But if this was interpretation was true, then surely this could be used to attack the general isogeny problem somehow?!

The module action and $\otimes$ -MIKE

March 2025:

Jonathan: But if this was interpretation was true, then surely this could be used to attack the general isogeny problem somehow?!

Damien: Urgh, it's probably me that screwed up somewhere again, I'll need to think about this...Hopefully this means that we will be able to use 2^e isogenies for both Alice and Bob in the end :)

The module action and $\otimes$ -MIKE

March 2025:

Jonathan: But if this was interpretation was true, then surely this could be used to attack the general isogeny problem somehow?!

Damien: Urgh, it's probably me that screwed up somewhere again, I'll need to think about this...Hopefully this means that we will be able to use 2^e isogenies for both Alice and Bob in the end :)

Poll:

- 1 Who think this led to an attack on the general isogeny problem?
- 2 Who think this was me screwing up somewhere again?

The module action and $\otimes$ -MIKE

March 2025:

Jonathan: But if this was interpretation was true, then surely this could be used to attack the general isogeny problem somehow?!

Damien: Urgh, it's probably me that screwed up somewhere again, I'll need to think about this...Hopefully this means that we will be able to use 2^e isogenies for both Alice and Bob in the end :)

Poll:

- 1 Who think this led to an attack on the general isogeny problem?
- 2 Who think this was me screwing up somewhere again?

The MIKE diagram is not a pushforward diagram in general

Table of Contents

- 1 MIKE: an introduction
- 2 MIKE: the past
- 3 Intermezzo on the module action
- 4 MIKE: the present
- 5 MIKE: the future

The practical construction

A an abelian variety oriented by R .

M a torsion free rank g R -module.

Definition

Take any embedding $i : M \hookrightarrow R^g$. Then $M \star A$ is the abelian variety $A^g / A^g[i(M)]$.

😊 Concrete and algorithmic definition

☹ Non functorial:

- ▶ Why does it not depend on the choice of i ?
- ▶ What is $M_B \star (M_A \star A)$?

The abelian category construction [Serre]

- $M \cdot A := \mathcal{H}om_R(M, A)$
- Assume this $\mathcal{H}om$ behaves like a standard Hom
- Then if we have a presentation $R^m \rightarrow R^g \rightarrow M \rightarrow 0$ of M , the long exact sequence should give:

$$0 \rightarrow \mathcal{H}om_R(M, A) \rightarrow \mathcal{H}om_R(R^g, A) \rightarrow \mathcal{H}om_R(R^m, A) \rightarrow \mathcal{E}xt_R^1(M, A) \rightarrow \dots$$

- “Clearly” $\mathcal{H}om_R(R, A) = A^m$ so $\mathcal{H}om_R(R^m, A) = A^m$
- Let’s use this as a definiton!

Definition

Take a presentation $G : R^m \rightarrow R^g \rightarrow M \rightarrow 0$. Then $\mathcal{H}om_R(M, A)$ is the kernel of $G^T : A^g \rightarrow A^m$.

- 😊 Concrete definition
- 😊 Works for any R -oriented object in an abelian category
For us: abelian category of commutative proper group schemes over k
- 😊 Similar definition for $M \otimes_R A$
(and even $\mathcal{E}xt_R^i(M, A)$, $\text{Tor}_R^i(m, A)$)
- 😞 Unicity?

The categorical construction [Serre]

Definition

In a category $\mathfrak{C}$ enriched in R -modules (i.e. $\text{Hom}_{\mathfrak{C}}(A, B)$ is an R -module for $A, B \in \mathfrak{C}$), the **power object** $\text{Hom}_{\mathfrak{C}}(M, A)$ for $A \in \mathfrak{C}$, if it exists, is the unique element in $\mathfrak{C}$ such that

$$\text{Hom}_{\mathfrak{C}}(B, \text{Hom}_R(M, A)) = \text{Hom}_R(M, \text{Hom}_{\mathfrak{C}}(B, A)) \quad \forall B \in \mathfrak{C}$$

😊 Unicity immediate

😊 Functorial

😊 Easy to prove:

$$\text{Hom}_R(M_1, \text{Hom}_R(M_2, A)) = \text{Hom}_R(M_1 \otimes_R M_2, A)$$

😊 Extend to copower objects $M \otimes_R x$

The functor of points construction [Serre]

Definition

$\mathcal{H}om_R(M, A)$ is the commutative proper group scheme whose functor of points is given by $k' \mapsto \operatorname{Hom}_R(M, A(k'))$ for all k -algebras k' .

- 😊 Unicity
- 😊 Gives the R -module structure of $(M \cdot A)(k')$ in terms of the one of $A(k')$
- 😊 Similar definition for $M \otimes_R A$

The ~~use fancy words~~ topos construction

Definition

$\mathcal{H}om_R(M, A)$ is the **internal hom** in the big fppf topos over k of the constant fppf sheaf associated to M and of the fppf sheaf associated to A

- ☺ Most natural definition.
- ☺ Same construction for $M \otimes_R A$.
- ☺ All standard properties of $\mathcal{H}om_R, \otimes_R$ follow from the usual ones by reasoning in the **internal logic of the topos**

Equivalence of the constructions

Theorem

Let A be an R -oriented abelian variety. For any f.p. R -module M , the following constructions of $\mathcal{H}om_R(M, A)$ coincide:

- *abelian category construction*
- *categorical construction*
- *functor of points construction*
- *topos theoretic construction*

If M is “nice enough” (e.g. M is projective), these also coincide with the *practical* construction $M \star A$.

Theorem

Let R be a quadratic imaginary order^a, E_0 primitively oriented by R , and $A = M_A \cdot E_0$. Then $M \star A$ is always equal to $(M \cdot A)^{\circ\circ}$, the *reduced subscheme of the connected component* of $M \cdot A$.

The following are equivalent:

- $M \star A = M \cdot A$;
- $M \cdot A$ is an *abelian variety*;
- M and M_A have *coprime relative conductors*
- $M \otimes_R M_A$ is *torsion free*
- $\mathrm{Tor}_1^R(M, M_A) = 0$
- M and M_A are *Tor independent*

This is always the case for M projective.

^aThis can be extended to R a CM order with maximal real multiplication (this condition guarantees that R is a Bass order).

Table of Contents

- 1 MIKE: an introduction
- 2 MIKE: the past
- 3 Intermezzo on the module action
- 4 MIKE: the present**
- 5 MIKE: the future

MIKE

- 19 September 2025: call for help to work on MIKE

- 19 September 2025: call for help to work on MIKE
- 26 September 2025: **key generation**


MIKE > Scholtens commutes with the action!!
 




SEP 26, 2025


Jonathan Komada Eriksen EDITED
 10:26 AM

Heyo!

Just uploaded some code which, using the Scholten stuff @Krijn worked on, which numerically verifies Damien's result, that Scholten's construction really commutes with the action!! 🎉

I.e., given a quaternion ideal $I = (2^e, \gamma)$ of $\text{End}(E_0)$, where $E_0 : y^2 = x^3 - x$ (the minus is important!), we can compute $E_I = I \cdot E_0$ in the usual ideal-to-isogeny way, and then take scholtens construction $H_1 = W'_{\mathbb{F}_{p^2}/\mathbb{F}}(E_I)$, or we can compute the rank-2 module action $H_2 = M_I \cdot E_0$. The code verifies (when it runs, its a bit buggy still) that $H_1 \simeq H_2$. Check out `testing_rank2_action.py` in the repo if you wanna see for yourself :)

Deriving the kernel is surprisingly easy, it really seems to just be given by what was written in the Building Blocks channel.


 You, Krijn, Giacomo Pope

<https://www.youtube.com/watch?v=0CugLD9HF94>
10:37 AM



Is this the MIKE-version of the experimental physicists showing Peter Higgs the first experimental evidence of the Higgs boson?

February 2026: **first successful key exchange!***

FEB 3	
 Max Duparc EDITED I have implemented the rest of the dim 4 chain. We now compute the dim 4 isogeny up to the end. (its pushed on the repo). Up to mistake on my side. We are ready to test dim 4 invariants.	9:47 AM
 Damien @Max Duparc I implemented a first draft of moduli invariants. I cannot test at work because the Sage version is too old, I'll test when I get back home.	10:54 AM
 Max Duparc	
Damien	2:36 PM
Well at least the modular invariants are the same...	
Damien	2:38 PM
And they change at each invocation	
So good news, it seems we have a working key exchange, congrats everyone!!	2:40 PM

Strange phenomena: 6 out of our 136 level $(2, 2)$ even theta constants are null...

Strange phenomena: 6 out of our 136 level $(2, 2)$ even theta constants are null...

Damien: Hi Sabrina! Have you ever heard of fourfolds with exactly 6 vanishing even theta constants?

Strange phenomena: 6 out of our 136 level $(2, 2)$ even theta constants are null...

Damien: Hi Sabrina! Have you ever heard of fourfolds with exactly 6 vanishing even theta constants?

Sabrina: But of course Damien! Everyone knows these are fourfolds of Weil type!

Strange phenomena: 6 out of our 136 level $(2,2)$ even theta constants are null...

Damien: Hi Sabrina! Have you ever heard of fourfolds with exactly 6 vanishing even theta constants?

Sabrina: But of course Damien! Everyone knows these are fourfolds of Weil type!

Sabrina: Oh by the way, if you need modular invariants you could look at the level $(2,2)$ theta constants invariant by $[i]$!

Strange phenomena: 6 out of our 136 level $(2,2)$ even theta constants are null...

Damien: Hi Sabrina! Have you ever heard of fourfolds with exactly 6 vanishing even theta constants?

Sabrina: But of course Damien! Everyone knows these are fourfolds of Weil type!

Sabrina: Oh by the way, if you need modular invariants you could look at the level $(2,2)$ theta constants invariant by $[i]$!

Damien: Thanks Sabrina!

The paper

- Paper almost finalized
- Only 27 pages!
 - + 100 pages of appendices ...
- Two sets of parameters: one more conservative, one more aggressive
- Sage and Rust implementation
- Ongoing C implementation
- A bit scared of incoming AI slop

A word on the implementation

- MIKE is easy and nice to implement!
- Only 3000 lines of Rust code!
- One exception...

A word on the implementation

- MIKE is easy and nice to implement!
- Only 3000 lines of Rust code!
- One exception...



A word on the implementation

Max Duparc

I went quickly on some proofs to make it more compact, but I can give more details if you want.

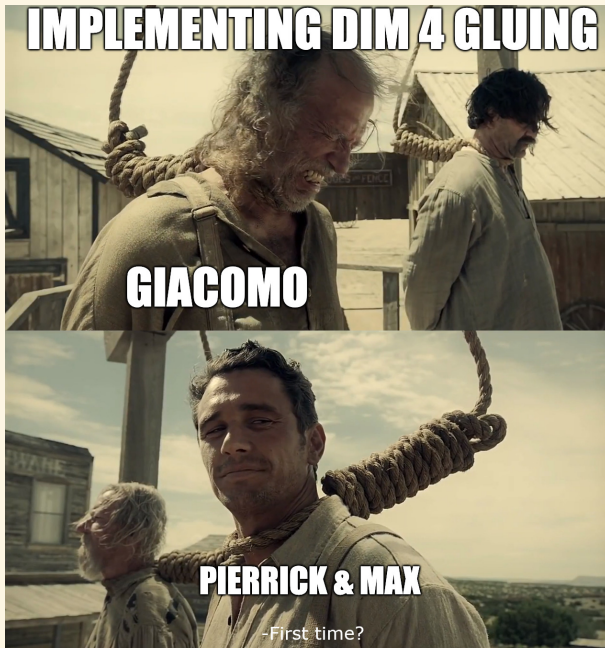
Damien EDITED

Writes a 20 page appendix on gluings

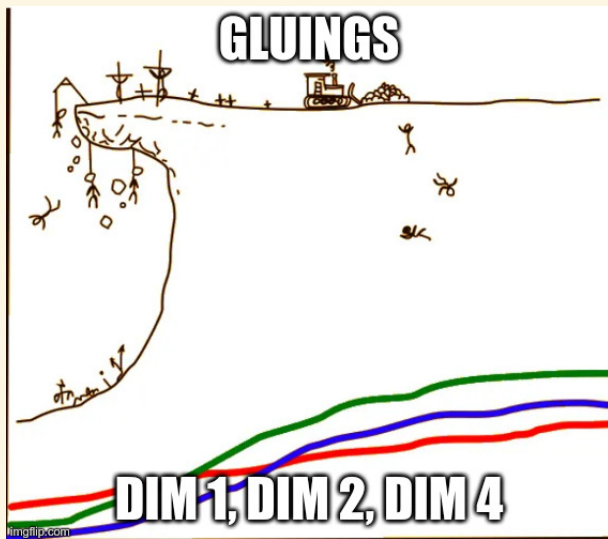
"Oh by the way, my proofs are a bit compact, should I give more details?" 🦊

Max Duparc EDITED

It is true that this could also be interpreted as a threat.



A word on the implementation



Modular invariants in MIKE

- Modular invariants in dimension 4 look intractable (a generic ppav is not a Jacobian)
- Luckily the fourfolds in MIKE land in a special locus of the moduli space, where we have a special automorphism $[i]$
- We have a complete set of absolute invariants for this special locus (abelian fourfolds of Weil type)!

Tools used:

- $[i]$ -theta characteristics
- Level $(1 + i, 1 + i)$ -theta coordinates
- Symmetric, alternate and Hermitian biextensions
- Alternate Weil-Cartier pairings
- Bimodules and exceptional quadratic twist isomorphisms
- The spinor and the Plücker map
- Lots of linear algebra
- Lots of explicit computations
- ...

Modular invariants in MIKE



Looking forward to understand how MIKE's invariants actually work thanks to Sabrina's talk!

On the security proof

😊 We have a security proof!

On the security proof

😊 We have a security proof!

- MIKE's DLog (i.e. secret key recovery) is hard if the **supersingular isogeny problem is hard**;

On the security proof

😊 We have a security proof!

- MIKE's DLog (i.e. secret key recovery) is hard if the supersingular isogeny problem is hard;
- MIKE is an actively secure NIKE in the QROM if gapCDH is hard (i.e. quantum CDH is hard even given access to a quantum DDH oracle)
- MIKE is a passively secure NIKE if CDH is hard
- MIKE gives an IND-CCA secure KEM if CDH is hard

On the security proof

😊 We have a security proof!

- MIKE's DLog (i.e. secret key recovery) is hard if the **supersingular isogeny problem** is hard;
- MIKE is an actively secure NIKE in the QROM if **gapCDH** is hard (i.e. quantum CDH is hard even given access to a quantum DDH oracle)
- MIKE is a passively secure NIKE if **CDH is hard**
- MIKE gives an IND-CCA secure KEM if **CDH is hard**
- Under the **Higher Dimensional Algebraic Isogeny Model (AIM+)**, MIKE's **CDH is hard** if the **EndRing** problem is hard
- See Andrea's talk at LID 6 for the Algebraic Isogeny Model (this is a more powerful model than the Algebraic Group Action Model)

On the security proof

😊 We have a security proof!

- MIKE's DLog (i.e. secret key recovery) is hard if the **supersingular isogeny problem** is hard;
- MIKE is an actively secure NIKE in the QROM if **gapCDH** is hard (i.e. quantum CDH is hard even given access to a quantum DDH oracle)
- MIKE is a passively secure NIKE if **CDH is hard**
- MIKE gives an IND-CCA secure KEM if **CDH is hard**
- Under the **Higher Dimensional Algebraic Isogeny Model (AIM+)**, MIKE's **CDH is hard** if the **EndRing** problem is hard
- See Andrea's talk at LID 6 for the Algebraic Isogeny Model (this is a more powerful model than the Algebraic Group Action Model)
- 🧙 For our aggressive parameters, we need an extra **indistinguishable** assumption

Table of Contents

- 1 MIKE: an introduction
- 2 MIKE: the past
- 3 Intermezzo on the module action
- 4 MIKE: the present
- 5 MIKE: the future

Near term plans

Faster dimension four isogeny formulas for MIKE:

- We use the automorphism $[i]$ to speed up our dimension 4 isogeny computations, e.g. only keeping track of 2 generators of the kernel rather than 4
- Exploit it further?
- Work on the full Kummer $A/\langle i \rangle$? 10 “even” coordinates or 6 “odd” coordinates instead of 16 coordinates
- Working doubling formulas
- Isogeny formulas exist but currently not practical
- Use level 1 + i -theta functions?
- Only 4 “coordinates” with values in $\mathbb{G}_m^{\otimes_{\mathbb{Z}} \mathbb{Z}[i]}$
- Compute the 2^e -isogeny as a $(1 + i)^{2^e}$ -isogeny

Cryptographic applications of the module action:

- Signatures?
- Others?

Symmetric monoidal actions

- Like in CSIDH, the action is computed through suitable isogenies
- Key fact: a module morphism $\psi : M_2 \rightarrow M_1$ acts on an abelian variety A to give

$$\phi : M_1 \cdot A \rightarrow M_2 \cdot A$$

- $M \hookrightarrow R^g$ gives an explicit isogeny $A^g \rightarrow M \cdot A$
- We can also act by modules on morphisms of abelian varieties, and even by morphisms on morphisms.
- **Abstraction:** action by a symmetric monoidal category
- Other natural cryptographic examples?
- Cryptographic applications?

Derived actions

- The $\otimes_R$ construction gives a **covariant action**: $M \mapsto M \otimes_R A$
- **Badly behaved** with torsion: $R/nR \otimes_R A = 0$
- The $\mathcal{H}om_R$ action gives the correct kernels: if $\psi : M_2 \hookrightarrow M_1$ is an isogeny, then $\phi : M_1 \cdot A \rightarrow M_2 \cdot A$ has for kernel $(M_2/M_1) \cdot A$:

$$\begin{aligned} 0 \rightarrow M_2 \rightarrow M_1 \rightarrow M_1/M_2 \rightarrow 0 \\ 0 \rightarrow M_1/M_2 \cdot A \rightarrow M_2 \cdot A \rightarrow M_1 \cdot A \rightarrow \mathcal{E}xt_R^1(M_1/M_2, A) \rightarrow \dots \end{aligned}$$

- But the $\mathcal{H}om_R$ action can still be **badly behaved**, especially on **finite group schemes**
- The “correct” actions lives in the **derived category** (seen as an ∞ -category), using the **internal Hom** and **tensor product** in the ambient ∞ -topos

$$\mathcal{R}\mathcal{H}om_R(M, A), \quad M \otimes_R^L A$$

- Implementing $\otimes^L$ -MIKE is left as an exercise^{*}
- Could potentially be useful to incorporate **torsion in the key exchange**

^{*}Fun fact: since for MIKE we act by projective modules, our action coincide with the derived action