

MIKE (Module Isogeny Key Exchange): a fast and compact post-quantum NIKE

2026/10/06 — **Canari Seminar**

Damien Robert, on behalf of the MIKE team



Canari

The MIKE team

Andrea Basso, Pierrick Dartois, Max Duparc, Jonathan Komada Eriksen, Sabrina Kunzweiler, Michael Meyer, Giacomo Pope, Krijn Reijnders, Damien Robert, Ryan Rueger, and Sina Schaeffler.

[A group picture]

8 out of 11 members of the MIKE team hard at work at the Leuven Isogeny Days 7

Table of Contents

1 A brief history of isogeny based NIKEs

2 MIKE: mathematical tools

3 The module action

4 Implementing MIKE

5 MIKE: the future

Diffie-Hellman key exchange

[Diffie-Hellman 1976]: New Directions in Cryptography

$$\begin{array}{ccc} g_0 & \rightsquigarrow & g_A = g_0^{x_A} \\ \downarrow & & \downarrow \\ g_B = g_0^{x_B} & \rightsquigarrow & g_{AB} = g_0^{x_A x_B} \end{array}$$

- ☺ First example of a **public key** protocol
- ☺ **NIKE**: Non Interactive Key Exchange
- ☺ Can be turned into **public key encryption** (El Gamal)
- Diffie-Hellman: $G = (\mathbb{F}_{q'}^*, \times)$
- Koblitz-Miller (1985): $G = (E/\mathbb{F}_{q'}, +)$.
- ☹ Killed by Shor's (1994) **quantum** polynomial algorithm

Post-Quantum NIKE (Non Interactive Key-Exchange) via isogenies

- [Couveignes 1998]: key exchange based on the quadratic ideal action on elliptic curves

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

- Submitted to CRYPTO ...but rejected
- Only surviving trace until 2006: a talk at the cryptographic seminar of École Normale Supérieure.
- Rediscovered by [Rostovtsev–Stolbunov 2006], so Jean-Marc posts “Hard homogeneous spaces” to eprint
- Now by far his most cited paper!
- Improved by [De Feo, Kieffer, Smith 2018] (large search for nice ordinary elliptic curves)
- [Castricky, Lange, Martindale, Renes, Panny 2018]: CSIDH, via supersingular elliptic curves over $\mathbb{F}_p$.
- ☹ Susceptible to Kuperberg’s quantum subexponential algorithm
- ☹ Hard to make constant time^{*}
 - Lattice based NIKE Swoosh: huge keys (220 KB), not actively secure (requires ZK-proofs)

⇒ Paucity of post-quantum NIKes

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

Some equivalences of categories

Theorem (Complex multiplication)

Let $E_0/\mathbb{F}_q$ be an elliptic curve whose endomorphism ring $R = \text{End}_{\mathbb{F}_q}(E_0)$ is an *imaginary quadratic order*^a. Then there is an *equivalence of category* $I \mapsto I \cdot E_0$ between invertible ideals in $I \in \text{Cl}(R)$ and elliptic curves $E/\mathbb{F}_q$ horizontally isogeneous^b to $E/\mathbb{F}_q$.

^aThis is the case for $E_0/\mathbb{F}_q$ ordinary, or $E_0/\mathbb{F}_p$ supersingular

^bThis means that $\text{End}_{\mathbb{F}_q}(E) = R$.

Theorem (Deuring's correspondance)

Let $E_0/\mathbb{F}_{p^2}$ be a maximal supersingular elliptic curve, and let $O_0 = \text{End}_{\mathbb{F}_{p^2}}(E)$, a *maximal quaternionic order* in $B_{p,\infty}$. Then there is an *equivalence of category* $I \mapsto I \cdot E_0$ between left ideals in O_0 and maximal supersingular elliptic curves $E/\mathbb{F}_{p^2}$.

🌀 In the first case, $E = I \cdot E_0$ has same endomorphism ring as E_0 , but not in the second case.

Some equivalences of categories

- ☺ In the quaternionic case there is **no commutative class group action**, hence no Kuperberg's quantum subexponential attack
- ☹ In the quaternionic case there is **no commutative class group action**:

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

- If I_A, I_B have coprime norms, the isogeny diagram above is a **pushforward**. We can build pushforwards in the supersingular isogeny graph too!

$$\begin{array}{ccc} E_0 & \xrightarrow{2^a} & E_A \\ \downarrow 3^b & & \downarrow 3^b \\ E_B = & \xrightarrow{2^a} & E_{AB} \end{array}$$

SIDH

- $p = 2^a 3^b - 1$. $E(\mathbb{F}_{p^2}) = (\mathbb{Z}/(p+1)\mathbb{Z})^2$ if $E/\mathbb{F}_{p^2}$ is maximal supersingular.
- $E_0 : y^2 = x^3 + x$ (supersingular when $a \geq 2$) or $E_0 : y^2 = x^3 + 6x^2 + x$.
- $E_0[2^a] = \langle P_A, Q_A \rangle$, $E_0[3^b] = \langle P_B, Q_B \rangle$.

SIDH

- $p = 2^a 3^b - 1$. $E(\mathbb{F}_{p^2}) = (\mathbb{Z}/(p+1)\mathbb{Z})^2$ if $E/\mathbb{F}_{p^2}$ is maximal supersingular.
- $E_0 : y^2 = x^3 + x$ (supersingular when $a \geq 2$) or $E_0 : y^2 = x^3 + 6x^2 + x$.
- $E_0[2^a] = \langle P_A, Q_A \rangle$, $E_0[3^b] = \langle P_B, Q_B \rangle$.
- Alice's **secret** isogeny: ϕ_A of kernel $\langle P_A + x_A Q_A \rangle$.
- Bob's **secret** isogeny: ϕ_B of kernel $\langle P_B + x_B Q_B \rangle$.
- Key exchange:

$$\begin{array}{ccc} E_0 & \xrightarrow{\phi_A} & E_A \\ \downarrow \phi_B & & \downarrow \phi'_B \\ E_B & \xrightarrow{\phi'_A} & E_{AB} \end{array}$$

- E_{AB} is the **shared secret**.
- $\phi'_A \circ \phi_B = \phi'_B \circ \phi_A : E_0 \rightarrow E_{AB}$ has kernel $\text{Ker } \phi_A + \text{Ker } \phi_B$.

- $p = 2^a 3^b - 1$. $E(\mathbb{F}_{p^2}) = (\mathbb{Z}/(p+1)\mathbb{Z})^2$ if $E/\mathbb{F}_{p^2}$ is maximal supersingular.
- $E_0 : y^2 = x^3 + x$ (supersingular when $a \geq 2$) or $E_0 : y^2 = x^3 + 6x^2 + x$.
- $E_0[2^a] = \langle P_A, Q_A \rangle, E_0[3^b] = \langle P_B, Q_B \rangle$.
- Alice's **secret** isogeny: ϕ_A of kernel $\langle P_A + x_A Q_A \rangle$.
- Bob's **secret** isogeny: ϕ_B of kernel $\langle P_B + x_B Q_B \rangle$.
- Key exchange:

$$\begin{array}{ccc}
 E_0 & \xrightarrow{\phi_A} & E_A \\
 \downarrow \phi_B & & \downarrow \phi'_B \\
 E_B & \xrightarrow{\phi'_A} & E_{AB}
 \end{array}$$

- E_{AB} is the **shared secret**.
- $\phi'_A \circ \phi_B = \phi'_B \circ \phi_A : E_0 \rightarrow E_{AB}$ has kernel $\text{Ker } \phi_A + \text{Ker } \phi_B$.
- ϕ'_A has kernel $\phi_B(P_A + x_A Q_A)$, ϕ'_B has kernel $\phi_A(P_B + x_B Q_B)$.
- Alice publishes: $P'_B = \phi_A(P_B), Q'_B = \phi_A(Q_B)$.
Bob publishes: $P'_A = \phi_B(P_A), Q'_A = \phi_B(Q_A)$. ("Torsion points".)
- $\text{Ker } \phi'_A = \langle P'_A + x_A Q'_A \rangle, \text{Ker } \phi'_B = \langle P'_B + x_B Q'_B \rangle$.

SIDH attacks

$$\begin{array}{ccc} E_0 & \xrightarrow{\phi_A} & E_A, \phi_A(P_B), \phi_A(Q_B) \\ \downarrow \phi_B & & \downarrow \phi'_B \\ E_B, \phi_B(P_A), \phi_B(P_B) & \xrightarrow{\phi'_A} & E_{AB} \end{array}$$

- Quickly, the torsion point informations $P'_B = \phi_A(P_B), Q'_B = \phi_A(Q_B)$ proved to be a weakness.
- [Galbraith, Petit, Shani, Bo Ti 2016]: adaptative attacks
Reason: hard to validate public keys
SIDH $\mapsto$ SIKE
- [Petit 2017]: attacks on overstretched parameters
Using lollipop endomorphisms
- [Castricky–Decru; Maino–Martindale–Panny–Pope–Wesolowski; R. 2022]: SIDH attacks
Use the torsion points to interpolate the secret isogeny ϕ_A in polynomial time in $\log \deg \phi_A$
Uses higher dimensional isogenies.

MIKE = SIDH done right

- Torsion points = bad, so we **remove torsion points**
- Isogeny of coprime degrees force larger prime parameters $p = c2^a3^b - 1$, so **we allow Alice and Bob to both use 2^e -isogenies.**

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 , $Q = [i]P$.

Key generation

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

$$\begin{array}{ccc} E_0 & \xrightarrow{2^e} & E_A \\ \downarrow 2^e & & \downarrow \text{wavy} \\ E_B = & \rightsquigarrow & ??? \end{array}$$

But how to build a shared secret out of this?

* 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

◇ Or rather it's j -invariant $j(E_A)$

MIKE's shared secret

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 $(WE_B)^2[2^{e+2}]$.

Definition

X_{AB} is the quotient of $(WE_B)^2$ by $[4]\langle T_1, \dots, T_4 \rangle$, this is a principally polarised abelian variety.

Magic property (I)

$$X_{AB} \simeq X_{BA} \text{ (as ppavs)}$$

Proof.

Trivial



MIKE: Module Isogeny Key-Exchange

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

$$\begin{array}{ccc} E_0 & \rightsquigarrow & X_A = M_A \star E_0 \\ \downarrow & & \downarrow \\ X_B = M_B \star E_0 & \rightsquigarrow & X_{AB} = (M_A \otimes M_B) \star E_0 \end{array}$$

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

*Not SIDH, despite the similar key generation!

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 isogeny path problem!

Compact:

- 80B for NIST level I (160B for NIST level V)

Fast^{*}:

- Key generation 0.65ms (4.21ms for NIST level V)
- Key exchange 4.9ms (28.6ms 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

^{*}Benchmarked on AMD Ryzen 7 PRO 7840U @ 3.3GHz with turboboost and multithreading disabled.

Table of Contents

1 A brief history of isogeny based NIKEs

2 **MIKE: mathematical tools**

3 The module action

4 Implementing MIKE

5 MIKE: the future

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

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

More equivalences of categories

Theorem ([Jordan, Keeton, Poonen, Rains, Shepherd-Barron, Tate 2016])

Let $E_0/\mathbb{F}_q$ be an elliptic curve such that $R = \text{End}_{\mathbb{F}_q}(E_0)$ is an *imaginary quadratic order*. Then there is a *contravariant equivalence of category* $M \mapsto M \cdot E_0$ between *torsion free modules* M of finite rank g over R and R -oriented^a abelian varieties $A/\mathbb{F}_q$ isogeneous to E_0^g . The inverse is given by $A \mapsto \text{Hom}_R(A, E_0)$.

^aThis mean we have an embedding $R \hookrightarrow \text{End}_{\mathbb{F}_q}(A)$.

- There is also a version when $\text{End}_{\mathbb{F}_q}(E_0)$ is a *maximal quaternionic order*, generalizing Deuring's correspondance.
- And a version for *R-oriented elliptic curves* (but we only have a fully faithful action in general, not an essentially surjective one) [Page-R. 20??].

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.

Table of Contents

1 A brief history of isogeny based NIKEs

2 MIKE: mathematical tools

3 The module action

4 Implementing MIKE

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 definition!

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 A brief history of isogeny based NIKEs

2 MIKE: mathematical tools

3 The module action

4 **Implementing MIKE**

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.  Max Duparc	10:54 AM
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

The paper

- Paper finalized
- Only 30 pages!
+ 100 pages of appendices ...
- Two sets of parameters: one more conservative, one more aggressive
- Python/Sage high level implementation
- C and Rust low level implementation

<https://mike.isogeni.es/>

A word on the implementation

- MIKE is **easy and nice** to implement!
- Only 3000 lines of Rust code, and 1000 lines of Python
- One exception...

A word on the implementation

- MIKE is **easy** and **nice** to implement!
- Only 3000 lines of Rust code, and 1000 lines of Python
- 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

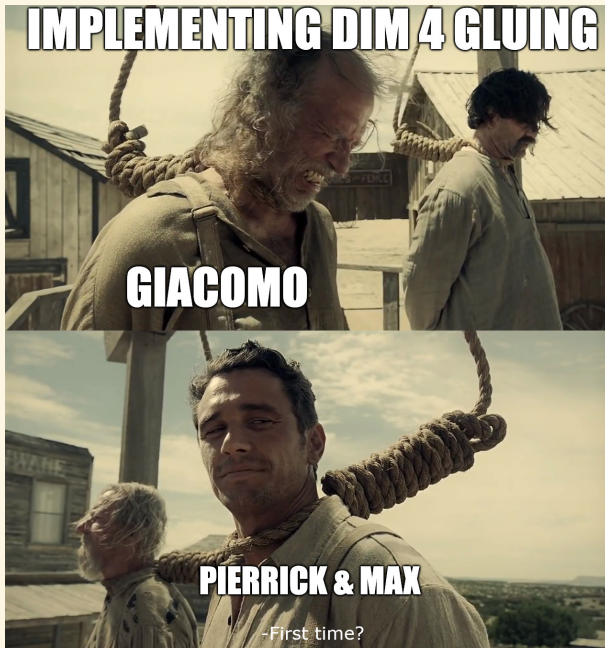
Writes a 20 page appendix on gluings

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

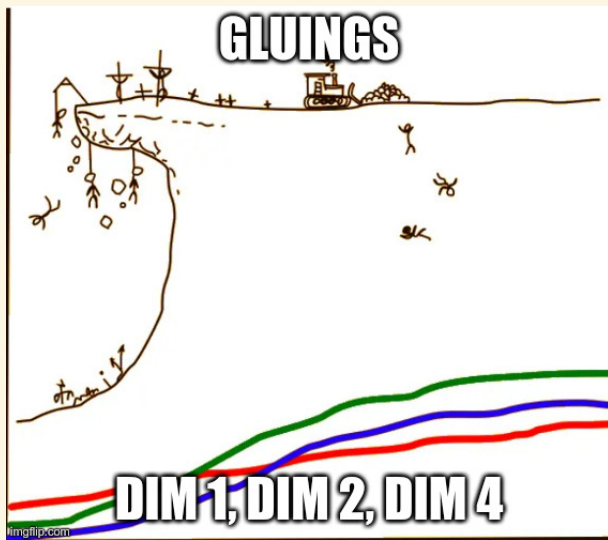
Max Duparc EDITED

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

A word on the implementation



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
- ...

^{*}Fun fact: these play a key role in the Hodge conjecture for abelian fourfolds!

Theorem

Let

$$(a_{00} : a_{01} : a_{02} : a_{03} : a_{04} : 0 : a_{06} : 0 : a_{08} : a_{09} : 0 : 0 : a_{12} : 0 : 0 : a_{15})$$

be theta constants of level $(1 + i, 1 + i)$ of a MIKE shared keys X_{AB} . Let

$$J_k = \sum_{i=0}^{15} a_i^{2k}.$$

Then $(J_1 : J_2 : J_3 : J_4 : J_5) \in \mathbb{P}(1 : 2 : 3 : 4 : 5)$ are a *complete set of absolute $\mathbb{F}_p$ -invariants*^a.

^aMore precisely they are invariants of level $\Gamma(1, 1 + i)$, and there is only one $\mathbb{F}_p$ -rational such structure.

[An AI generated picture]

Artistic rendition of Sabrina discovering the MIKE invariants

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

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

🧠 For our aggressive parameters, we need an extra indistinguishable assumption

Outline of the security proof

- In the AIM+ model, an adversary has to “explain” a new abelian variety by an isogeny (or more generally a surjective morphism) from a known abelian variety or by a product.
- Suppose access to a MIKE CDH oracle, we want to use it, given E_A , to compute the endomorphism ring* $\text{End}(E_A)$
- We use the key generation to get E_B , and pass $(E_0, \{E_A, E_B\})$ to the oracle to get $\text{MIKE}(E_A, E_B)$, along with an explanation $\gamma : \prod_{i=1}^4 E_i \rightarrow \text{MIKE}(E_A, E_B)$, where $E_i \in \{E_0, E_A, E_B\}$.
- The shared secret step gives us a known isogeny $\text{MIKE}(E_A, E_B) \rightarrow E_A^4$.
- Composing, we get a non trivial isogeny $E_i \rightarrow E_A$, and $E_i \neq E_A$ with probability $\geq 1/2$.
- Since we know $\text{End}(E_0)$ and $\text{End}(E_B)$ we can recover $\text{End}(E_A)$

*By well known reductions, this is sufficient to solve the isogeny problem.

Parameters

- [Aubry, Oyono, Vincent 2026]: Minimal degree of an isogeny between a supersingular elliptic curve and its conjugate.
- [Wesolowski 2026]: The supersingular isogeny problem in time and memory $p^{1/3+o(1)}$
- Previously the best attack was $p^{1/2} \log^{O(1)} p$ but with $O(1)$ memory
- Time-Memory tradeoff
- Increased parameter size
- Aggressive and Conservative parameter sets
- The aggressive set uses isogenies of length $e \approx 2\lambda$ while $\log_2(p) \gg 2\lambda$

Table of Contents

1 A brief history of isogeny based NIKEs

2 MIKE: mathematical tools

3 The module action

4 Implementing MIKE

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 $A^g \twoheadrightarrow M \cdot A$
- 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

Conclusion

