Module Isogeny Key Exchange : MIKE for high-schoolers

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

2026, May 12

Down to earth prerequisites everybody should know

- Let $\mathscr{M}$ be a category.

Down to earth prerequisites everybody should know

- Let $\mathscr{M}$ be a category.
- We say $\mathscr{M}$ is a **symmetric monoidal category** if there exists a **tensor product functor** $\otimes : \mathscr{M} \times \mathscr{M} \to \mathscr{M}$ which is associative, symmetric and with a **unit** $1 \in \mathscr{M}$.

Down to earth prerequisites everybody should know

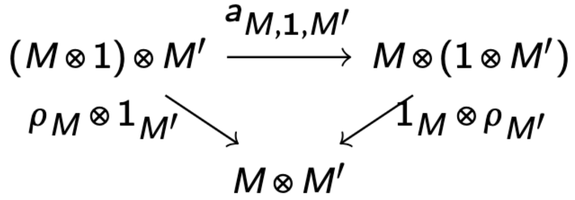
- Let $\mathscr{M}$ be a category.
- We say $\mathscr{M}$ is a **symmetric monoidal category** if there exists a **tensor product functor** $\otimes : \mathscr{M} \times \mathscr{M} \to \mathscr{M}$ which is associative, symmetric and with a **unit** $1 \in \mathscr{M}$.
- The tensor product functor should satisfy natural properties:

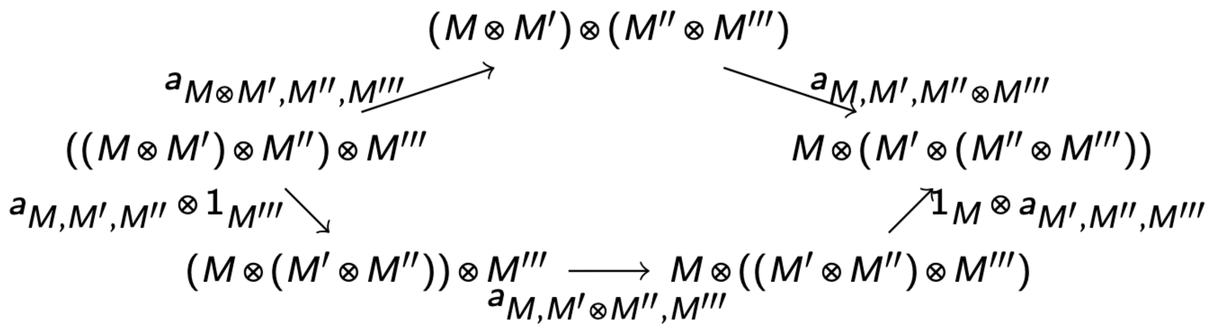
$$\begin{array}{ccc} (M \otimes 1) \otimes M' & \xrightarrow{a_{M,1,M'}} & M \otimes (1 \otimes M') \\ & {\scriptstyle \rho_M \otimes 1_{M'}} \searrow \quad \swarrow {\scriptstyle 1_M \otimes \rho_{M'}} & \\ & M \otimes M' & \end{array}$$

where $M, M', M'', M''' \in \mathscr{M}$ and the arrows are obvious isomorphisms.

Down to earth prerequisites everybody should know

- Let $\mathscr{M}$ be a category.
- We say $\mathscr{M}$ is a **symmetric monoidal category** if there exists a **tensor product functor** $\otimes : \mathscr{M} \times \mathscr{M} \to \mathscr{M}$ which is associative, symmetric and with a **unit** $1 \in \mathscr{M}$.
- The tensor product functor should satisfy natural properties:





where $M, M', M'', M''' \in \mathscr{M}$ and the arrows are obvious isomorphisms.

Down to earth prerequisites everybody should know

- Let $\mathscr{M}$ be a category.
- We say $\mathscr{M}$ is a **symmetric monoidal category** if there exists a **tensor product functor** $\otimes : \mathscr{M} \times \mathscr{M} \to \mathscr{M}$ which is associative, symmetric and with a **unit** $1 \in \mathscr{M}$.
- The tensor product functor should satisfy natural properties:

$$\begin{array}{ccc} (M \otimes 1) \otimes M' & \xrightarrow{a_{M,1,M'}} & M \otimes (1 \otimes M') \\ & {\scriptstyle \rho_M \otimes 1_{M'}} \searrow \quad \swarrow {\scriptstyle 1_M \otimes \rho_{M'}} & \\ & M \otimes M' & \end{array}$$

$$\begin{array}{ccccc} (M \otimes M') \otimes M'' & \xrightarrow{a_{M,M',M''}} & M \otimes (M' \otimes M'') & \xrightarrow{B_{M,M' \otimes M''}} & (M' \otimes M'') \otimes M \\ \downarrow {\scriptstyle B_{M,M'} \otimes 1_{M''}} & & & & {\scriptstyle a_{M',M'',M}} \downarrow \\ (M' \otimes M) \otimes M'' & \xrightarrow[a_{M',M,M''}]{} & M' \otimes (M \otimes M'') & \xrightarrow[1_{M'} \otimes B_{M,M''}]{} & M' \otimes (M'' \otimes M) \end{array}$$

$$\begin{array}{ccccc} & & (M \otimes M') \otimes (M'' \otimes M''') & & \\ & {\scriptstyle a_{M \otimes M',M'',M'''}} \nearrow & & \searrow {\scriptstyle a_{M,M',M'' \otimes M'''}} & \\ ((M \otimes M') \otimes M'') \otimes M''' & & & & M \otimes (M' \otimes (M'' \otimes M''')) \\ {\scriptstyle a_{M,M',M''} \otimes 1_{M'''}} \searrow & & & & \nearrow {\scriptstyle 1_M \otimes a_{M',M'',M'''}} \\ & (M \otimes (M' \otimes M'')) \otimes M''' & \xrightarrow[a_{M,M' \otimes M'',M'''}]{} & M \otimes ((M' \otimes M'') \otimes M''') & \end{array}$$

where $M, M', M'', M''' \in \mathscr{M}$ and the arrows are obvious isomorphisms.


3


2


1

Everybody says isogenies are slow

Lattice people tryin’ to get in my head

Everybody says isogenies are slow

Lattice people tryin’ to get in my head

Abstract mathematics are my own heart talkin'

Everybody says isogenies are slow

Lattice people tryin’ to get in my head

Abstract mathematics are my own heart talkin'

I need to count core cycles instead

Everybody says isogenies are slow

Lattice people tryin’ to get in my head

Abstract mathematics are my own heart talkin'

I need to count core cycles instead

(Did you ever) hear of abelian categories ?

(Did you ever) hear of abelian categories ?

(Did you ever) hear of a monoidal action ?

(Did you ever) hear of abelian categories ?

(Did you ever) hear of a monoidal action ?

(Did you ever) instantiate a contravariant functor ?

(Did you ever) hear of abelian categories ?

(Did you ever) hear of a monoidal action ?

(Did you ever) instantiate a contravariant functor ?

Did you ever need a NIKE, well you can count on MIKE

(Did you ever) hear of abelian categories ?

(Did you ever) hear of a monoidal action ?

(Did you ever) instantiate a contravariant functor ?

Did you ever need a NIKE, well you can count on MIKE

Let’s look again for: a simple NIKE (Simple NIKE)

Let’s look again for: a simple NIKE (Simple NIKE)

Post-quantum, small and fast, that all is MIKE (all is MIKE)

Let’s look again for: a simple NIKE (Simple NIKE)

Post-quantum, small and fast, that all is MIKE (all is MIKE)

Secure and constant-time? It’s all we like (MIKE as we like)

Let’s look again for: a simple NIKE (Simple NIKE)

Post-quantum, small and fast, that all is MIKE (all is MIKE)

Secure and constant-time? It’s all we like (MIKE as we like)

Bet on it, bet on it, bet on it, bet on it (Bet on MIKE)

Let’s look again for: a simple NIKE (Simple NIKE)

Post-quantum, small and fast, that all is MIKE (all is MIKE)

Secure and constant-time? It’s all we like (MIKE as we like)

Bet on it, bet on it, bet on it, bet on it (Bet on MIKE)

We wanna make it right, MIKE is the way

We wanna make it right, MIKE is the way

Only 64 bytes, believe what we say,

We wanna make it right, MIKE is the way

Only 64 bytes, believe what we say,

Just 5 milliseconds, for sure that is ok ?

We wanna make it right, MIKE is the way

Only 64 bytes, believe what we say,

Just 5 milliseconds, for sure that is ok ?

Bet on it, bet on it, bet on it, bet on it

We wanna make it right, MIKE is the way

Only 64 bytes, believe what we say,

Just 5 milliseconds, for sure that is ok ?

Bet on it, bet on it, bet on it, bet on it

How will we know if it's a path worth takin' ?

How will we know if it's a path worth takin’ ?

That it won't be too easy to break ?

How will we know if it's a path worth takin’ ?

That it won't be too easy to break ?

Since SIKE was lost, there is no more fakin'

How will we know if it's a path worth takin’ ?

That it won't be too easy to break ?

Since SIKE was lost, there is no more fakin'

We don't wanna make the same mistakes

How will we know if it's a path worth takin’ ?

That it won't be too easy to break ?

Since SIKE was lost, there is no more fakin'

We don't wanna make the same mistakes

(Did you ever) Have your dreams all broken with SIKE?

(Did you ever) Have your dreams all broken with SIKE?

(Did you ever) Blame the maths, and fear their next strike?

(Did you ever) Have your dreams all broken with SIKE?

(Did you ever) Blame the maths, and fear their next strike?

(We will never) count on torsion points again

(Did you ever) Have your dreams all broken with SIKE?

(Did you ever) Blame the maths, and fear their next strike?

(We will never) count on torsion points again

We won’t play this game again, our tools are different

(Did you ever) Have your dreams all broken with SIKE?

(Did you ever) Blame the maths, and fear their next strike?

(We will never) count on torsion points again

We won’t play this game again, our tools are different

Let’s look again for: a simple NIKE (Simple NIKE)

Let’s look again for: a simple NIKE (Simple NIKE)

Post-quantum, small and fast, that all is MIKE (all is MIKE)

Let’s look again for: a simple NIKE (Simple NIKE)

Post-quantum, small and fast, that all is MIKE (all is MIKE)

And actively secure? It’s all we like (MIKE as we like)

Let’s look again for: a simple NIKE (Simple NIKE)

Post-quantum, small and fast, that all is MIKE (all is MIKE)

And actively secure? It’s all we like (MIKE as we like)

Bet on it, bet on it, bet on it, bet on it (Bet on MIKE)

Let’s look again for: a simple NIKE (Simple NIKE)

Post-quantum, small and fast, that all is MIKE (all is MIKE)

And actively secure? It’s all we like (MIKE as we like)

Bet on it, bet on it, bet on it, bet on it (Bet on MIKE)

We wanna make it right, MIKE is the way

We wanna make it right, MIKE is the way

Only 64 bytes, believe what we say,

We wanna make it right, MIKE is the way

Only 64 bytes, believe what we say,

Just 5 milliseconds, for sure that is ok ?

We wanna make it right, MIKE is the way

Only 64 bytes, believe what we say,

Just 5 milliseconds, for sure that is ok ?

Bet on it, bet on it, bet on it, bet on it

We wanna make it right, MIKE is the way

Only 64 bytes, believe what we say,

Just 5 milliseconds, for sure that is ok ?

Bet on it, bet on it, bet on it, bet on it

Instantiating a symmetric monoidal action

- Let $\mathscr{M}$ be a symmetric monoidal category and $\mathscr{C}$ be another category.
- A **symmetric monoidal action** is a functor $\mathscr{M} \times \mathscr{C} \to \mathscr{C}$ which respects the obvious coherence conditions.
- It can also be seen as a strong monoidal functor $\mathscr{M} \to \mathrm{End}(\mathscr{C})$.
- We can instantiate a symmetric monoidal action with the **power construction**. If $M \in \mathscr{M}$ and $C \in \mathscr{C}$, the **power object** $\mathscr{HOM}_{\mathscr{M}}(M, C) \in \mathscr{C}$ (if it exists) is the unique object satisfying the universal property:

$$\mathrm{Hom}_{\mathscr{C}}(C', \mathscr{HOM}_{\mathscr{M}}(M, C)) = \mathrm{Hom}_{\mathscr{C}}(M, \mathrm{Hom}_{\mathscr{C}}(C', C)),$$

  for all $C' \in \mathscr{C}$.
- **Trivial example:** for any commutative ring R, the action of finitely presented R-modules on R-oriented commutative proper group schemes. The construction is left as an exercise.

ALL I GOTTA DO

- We can instantiate a symmetric monoidal action with the **power construction**. If $M \in \mathscr{M}$ and $C \in \mathscr{C}$, the **power object** $\mathscr{HOM}_{\mathscr{M}}(M, C) \in \mathscr{C}$ (if it exists) is the unique object satisfying the universal property:

$$\mathrm{Hom}_{\mathscr{C}}(C', \mathscr{HOM}_{\mathscr{M}}(M, C)) = \mathrm{Hom}_{\mathscr{C}}(M, \mathrm{Hom}_{\mathscr{C}}(C', C)),$$

  for all $C' \in \mathscr{C}$.

- **Trivial example:** for any commutative ring R, the action of finitely presented R-modules on R-oriented commutative proper group schemes. The construction is left as an exercise.

ALL I GOTTA DO

- We can instantiate a symmetric monoidal action with the **power construction**. If $M \in \mathscr{M}$ and $C \in \mathscr{C}$, the **power object** $\mathscr{HOM}_{\mathscr{M}}(M, C) \in \mathscr{C}$ (if it exists) is the unique object satisfying the

IS BELIEVE

- **Trivial example:** for any commutative ring R, the action of finitely presented R-modules on R-oriented commutative proper group schemes. The construction is left as an exercise.

We’re not gonna stop

Not gonna stop 'til we get our shot

We’re not gonna stop

Not gonna stop 'til we get our shot

Our simple NIKE, all as we like

We’re not gonna stop

Not gonna stop 'til we get our shot

Our simple NIKE, all as we like

Post-quantum, small and fast? That’s MIKE

We’re not gonna stop

Not gonna stop 'til we get our shot

Our simple NIKE, all as we like

Post-quantum, small and fast? That’s MIKE

Bet on it, bet on it, bet on it, bet on—, our NIKE

Bet on it, bet on it, bet on it, bet on it (Bet on MIKE)

We’re not gonna stop

Not gonna stop 'til we get our shot

Our simple NIKE, all as we like

Post-quantum, small and fast? That’s MIKE

Bet on it, bet on it, bet on it, bet on—, our NIKE

Bet on it, bet on it, bet on it, bet on it (Bet on MIKE)

We wanna make it right, MIKE is the way

We wanna make it right, MIKE is the way

Only 64 bytes, believe what we say,

We wanna make it right, MIKE is the way

Only 64 bytes, believe what we say,

Just 5 milliseconds, for sure that is ok ?

We wanna make it right, MIKE is the way

Only 64 bytes, believe what we say,

Just 5 milliseconds, for sure that is ok ?

Bet on it, bet on it, bet on it, bet on MIKE

We wanna make it right, MIKE is the way

Only 64 bytes, believe what we say,

Just 5 milliseconds, for sure that is ok ?

Bet on it, bet on it, bet on it, bet on MIKE

MIKE: a fast and compact post-quantum NIKE

Coming to an eprint near you later in 2026!

- Tiny public keys: 64B
  - A single $j \in \mathbb{F}_{p^2}$, no torsion points
- Constant time
- Actively secure
- Fast:
  - Key generation: < 1 ms
  - Full key exchange < 5 ms
- Based on: eprint:2024/1556

Authors:

Andrea Basso
Pierrick Alexis Dartois
Max Jackson Samuel Sydney William Leslie Ashley Artie Lenny Arnulf Guc
Jonathan Komada Eriksen
Sabrina Kunzweiler
Michael Gregor Meyer
Giacomo Pope
Krijn Cornelius Johannes Maria Reijnders
Damien Olivier Robert
Ryan Orlando Gawain Erhard Rueger
Sina Alexandra Schaeffler

Lyrics by:

Pierrick Dartois
Sina Schaeffler
Jonathan Komada Eriksen

Big thanks to Singers:

Jolijn Cottaar
Pierrick Dartois
Jonathan Komada Eriksen
Valerie Gilchrist
Riccardo Invernizzi
Anaëlle Le Dévéhat
Antonin Leroux