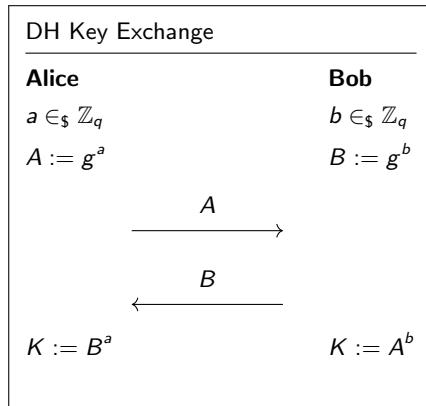


MIKE: Module Isogeny Key Exchange

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

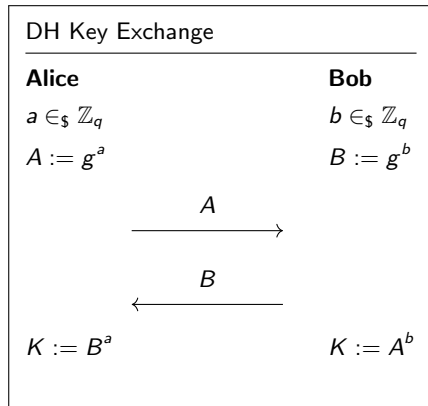
Mathematics of PQC; Raitenhaslach: September 7, 2026

A short history of Diffie-Hellman



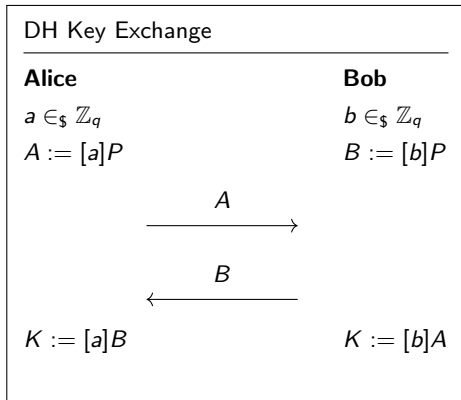
A short history of Diffie-Hellman

DH over:	e.g.	Classical sec.
Field	$\mathbb{Z}_p^\times$	$L_p(1/3)$



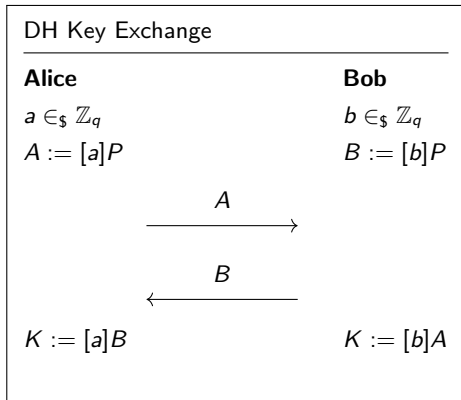
A short history of Diffie-Hellman

DH over:	e.g.	Classical sec.
Field	$\mathbb{Z}_p^\times$	$L_p(1/3)$
Gen group	ECC	$O(p^{1/2})$



A short history of Diffie-Hellman

DH over:	e.g.	Classical sec.	Quantum sec.
Field	$\mathbb{Z}_p^\times$	$L_p(1/3)$	$O(\log(p)^2)$
Gen group	ECC	$O(p^{1/2})$	$O(\log(p)^2)$



A short history of Diffie-Hellman

DH over:	e.g.	Classical sec.	Quantum sec.
Field	$\mathbb{Z}_p^\times$	$L_p(1/3)$	$O(\log(p)^2)$
Gen group	ECC	$O(p^{1/2})$	$O(\log(p)^2)$
Group action	CSIDH	$O(p^{1/4})$	

DH Key Exchange

Alice

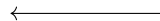
$a \in_{\$} G$

$A := a \star E$

A



B



$K := a \star B$

Bob

$b \in_{\$} G$

$B := b \star E$

$K := b \star A$

A short history of Diffie-Hellman

DH over:	e.g.	Classical sec.	Quantum sec.
Field	$\mathbb{Z}_p^\times$	$L_p(1/3)$	$O(\log(p)^2)$
Gen group	ECC	$O(p^{1/2})$	$O(\log(p)^2)$
Group action	CSIDH	$O(p^{1/4})$	$L_p(1/2)$

Less structure $\implies$ More security

DH Key Exchange

Alice

$a \in_{\$} G$

$A := a \star E$

Bob

$b \in_{\$} G$

$B := b \star E$

A



B



$K := a \star B$

$K := b \star A$

A short history of Diffie-Hellman

DH over:	e.g.	Classical sec.	Quantum sec.
Field	$\mathbb{Z}_p^\times$	$L_p(1/3)$	$O(\log(p)^2)$
Gen group	ECC	$O(p^{1/2})$	$O(\log(p)^2)$
Group action	CSIDH	$O(p^{1/4})$	$L_p(1/2)$
Monoid action	MIKE	$O(p^{1/3})$	$O(p^{2/9})$

Less structure $\implies$ More security

DH Key Exchange

Alice

$a \in_{\$} G$

$A := a \star E$

A



B



$K := a \star B$

Bob

$b \in_{\$} G$

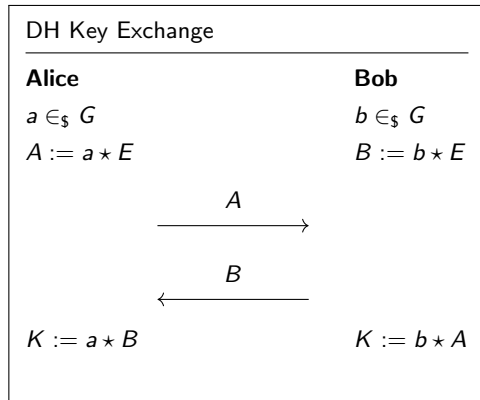
$B := b \star E$

$K := b \star A$

A short history of Diffie-Hellman

DH over:	e.g.	Classical sec.	Quantum sec.
Field	$\mathbb{Z}_p^\times$	$L_p(1/3)$	$O(\log(p)^2)$
Gen group	ECC	$O(p^{1/2})$	$O(\log(p)^2)$
Group action	CSIDH	$O(p^{1/4})$	$L_p(1/2)$
Monoid action	MIKE	$O(p^{1/3})$	$O(p^{2/9})$

Less structure $\implies$ More security



MIKE is a NIKÉ based on a symmetric graded monoid action.

Why you should care

$\log_2(p)$	sk	pk	KeyGen	KeyAgreement
251*	32 B	64 B	0.294 ms	2.167 ms (asm)
251*	32 B	64 B	0.335 ms	3.018 ms
383	48 B	92 B	1.095 ms	8.720 ms
505	64 B	128 B	2.525 ms	21.017 ms

Table: MIKE benchmarks¹

¹Timing measured on rust implementation on ARM M4 Pro chip, 4.5GHz.

*correspondence between prime and security in flux following [Wes26].

Why you should care

$\log_2(p)$	sk	pk	KeyGen	KeyAgreement
251*	32 B	64 B	0.294 ms	2.167 ms (asm)
251*	32 B	64 B	0.335 ms	3.018 ms
383	48 B	92 B	1.095 ms	8.720 ms
505	64 B	128 B	2.525 ms	21.017 ms

Table: MIKE benchmarks¹

- Compact

- Fast

¹Timing measured on rust implementation on ARM M4 Pro chip, 4.5GHz.

*correspondence between prime and security in flux following [Wes26].

Why you should care

$\log_2(p)$	sk	pk	KeyGen	KeyAgreement
251*	32 B	64 B	0.294 ms	2.167 ms (asm)
251*	32 B	64 B	0.335 ms	3.018 ms
383	48 B	92 B	1.095 ms	8.720 ms
505	64 B	128 B	2.525 ms	21.017 ms

Table: MIKE benchmarks¹

- Compact
- Secure
- Fast
- Cryptographically practical

¹Timing measured on rust implementation on ARM M4 Pro chip, 4.5GHz.

*correspondence between prime and security in flux following [Wes26].

Graded Monoid Action

- $(M, \otimes)$ a monoid.
- $\text{rk} : (M, \otimes) \rightarrow (\mathbb{N}_{>0}, \cdot)$

Graded Monoid Action

- $(M, \otimes)$ a monoid.
- $\text{rk} : (M, \otimes) \rightarrow (\mathbb{N}_{>0}, \cdot)$
- X a set.
- $\text{dim} : X \rightarrow \mathbb{N}_{>0}$

Graded Monoid Action

- $(M, \otimes)$ a monoid.
- $\text{rk} : (M, \otimes) \rightarrow (\mathbb{N}_{>0}, \cdot)$
- X a set.
- $\dim : X \rightarrow \mathbb{N}_{>0}$

Symmetric graded monoid action

$$\star : M \times X \longrightarrow X$$

such that:

Graded Monoid Action

- $(M, \otimes)$ a monoid.
- $\text{rk} : (M, \otimes) \rightarrow (\mathbb{N}_{>0}, \cdot)$
- X a set.
- $\dim : X \rightarrow \mathbb{N}_{>0}$

Symmetric graded monoid action

$$\star : M \times X \longrightarrow X$$

such that:

1. Neutral: $1 \star x = x$
2. Associativity: $m_1 \star (m_2 \star x) = (m_1 \otimes m_2) \star x$

Graded Monoid Action

- $(M, \otimes)$ a monoid.
- $\text{rk} : (M, \otimes) \rightarrow (\mathbb{N}_{>0}, \cdot)$
- X a set.
- $\dim : X \rightarrow \mathbb{N}_{>0}$

Symmetric graded monoid action

$$\star : M \times X \longrightarrow X$$

such that:

1. Neutral: $1 \star x = x$
2. Associativity: $m_1 \star (m_2 \star x) = (m_1 \otimes m_2) \star x$
3. Symmetric: $(m_1 \otimes m_2) \star x = (m_2 \otimes m_1) \star x$
4. Graded: $\dim(m \star x) = \text{rk}(m) \cdot \dim(x)$

Graded Monoid Action

- $(M, \otimes)$ a monoid.
- $\text{rk} : (M, \otimes) \rightarrow (\mathbb{N}_{>0}, \cdot)$
- X a set.
- $\dim : X \rightarrow \mathbb{N}_{>0}$

Symmetric graded monoid action

$$\star : M \times X \longrightarrow X$$

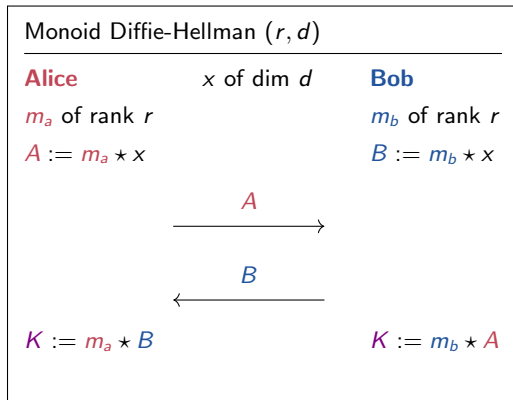
such that:

1. Neutral: $1 \star x = x$
2. Associativity: $m_1 \star (m_2 \star x) = (m_1 \otimes m_2) \star x$
3. Symmetric: $(m_1 \otimes m_2) \star x = (m_2 \otimes m_1) \star x$
4. Graded: $\dim(m \star x) = \text{rk}(m) \cdot \dim(x)$

► Graded monoid action cannot be group action !

Graded Monoid Diffie-Hellman

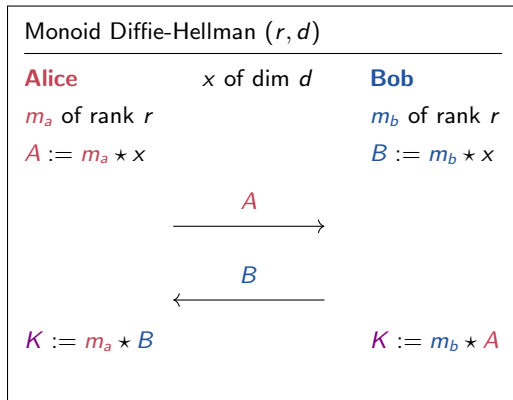
Diffie-Hellman just needs Monoid !



Graded Monoid Diffie-Hellman

Diffie-Hellman just needs Monoid !

We “just” need a cryptographic monoid action.



Elliptic curves

Work with *supersingular elliptic curves* over $\mathbb{F}_{p^2}$:

- Variety of dim 1
- Abelian group structure
- *Supersingular* if $|E(\mathbb{F}_{p^2})| = (p+1)^2$

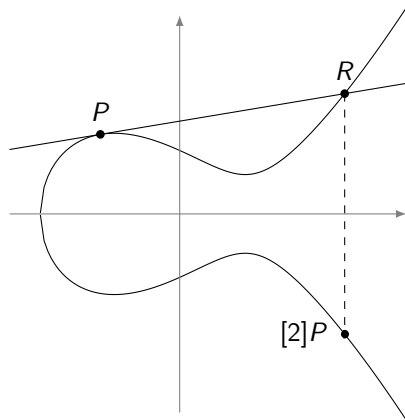


Figure: Elliptic curve

Abelian Varieties

Work with *maximal Abelian varieties* over $\mathbb{F}_{p^2}$:

- Variety of dim g
- Abelian group structure
- *maximal* if $|A(\mathbb{F}_{p^2})| = (p+1)^{2g}$

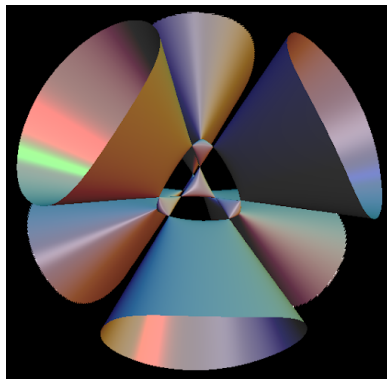


Figure: Abelian variety of dimension 2

Abelian Varieties

Work with *maximal Abelian varieties* over $\mathbb{F}_{p^2}$:

- Variety of dim g
- Abelian group structure
- *maximal* if $|A(\mathbb{F}_{p^2})| = (p+1)^{2g}$
- We still have isogenies

$$\phi : A \longrightarrow B \cong A / \ker(\phi)$$

- ▶ Fully characterised by their kernel.

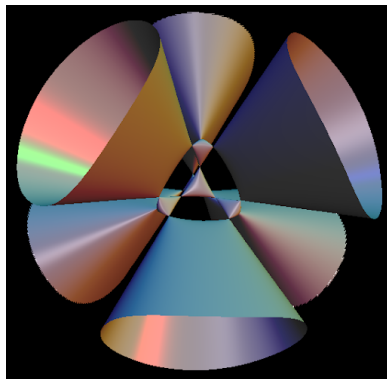


Figure: Abelian variety of dimension 2

Abelian Varieties

Work with *maximal Abelian varieties* over $\mathbb{F}_{p^2}$:

- Variety of dim g
- Abelian group structure
- *maximal* if $|A(\mathbb{F}_{p^2})| = (p+1)^{2g}$

- We still have isogenies

$$\phi : A \longrightarrow B \cong A / \ker(\phi)$$

- ▶ Fully characterised by their kernel.

- $\text{End}(A)$ are orders of $\mathbb{Q}$ -algebras.

$\simeq$ Lattices with multiplicative structure inherited from integer ring R .

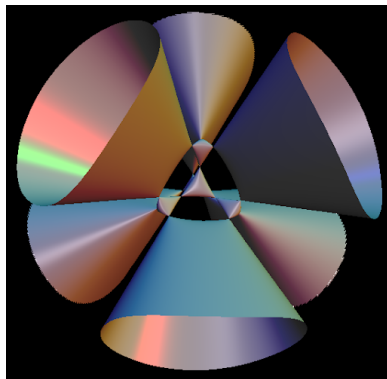


Figure: Abelian variety of dimension 2

Orientation

- Let $R = \mathbb{Z}[\sqrt{-p}]$:

$$A \text{ defined over } \mathbb{F}_p \iff \iota_A : R \hookrightarrow \text{End}(A)^a$$

^aprimitive embedding

Orientation

- Let $R = \mathbb{Z}[\sqrt{-p}]$:

$$A \text{ defined over } \mathbb{F}_p \iff \iota_A : R \hookrightarrow \text{End}(A)^a$$

$$\phi : A \rightarrow B \text{ defined over } \mathbb{F}_p \iff \forall \alpha \in R, \iota_B(\alpha) \circ \phi = \phi \circ \iota_A(\alpha)$$

^aprimitive embedding

Orientation

- Let $R = \mathbb{Z}[\sqrt{-p}]$:

$$\text{Category } \mathcal{AV}_R \left\{ \begin{array}{ll} A \text{ defined over } \mathbb{F}_p & \Longleftrightarrow \iota_A : R \hookrightarrow \text{End}(A)^a \\ \phi : A \rightarrow B \text{ defined over } \mathbb{F}_p & \Longleftrightarrow \forall \alpha \in R, \iota_B(\alpha) \circ \phi = \phi \circ \iota_A(\alpha) \end{array} \right.$$

^aprimitive embedding

Orientation

- Let $R = \mathbb{Z}[\sqrt{-p}]$:

$$\text{Category } \mathcal{AV}_R \left\{ \begin{array}{ll} A \text{ defined over } \mathbb{F}_p & \Longleftrightarrow \iota_A : R \hookrightarrow \text{End}(A)^a \\ \phi : A \rightarrow B \text{ defined over } \mathbb{F}_p & \Longleftrightarrow \forall \alpha \in R, \iota_B(\alpha) \circ \phi = \phi \circ \iota_A(\alpha) \end{array} \right.$$

- Let L be a R -Lattice:

^aprimitive embedding

Orientation

- Let $R = \mathbb{Z}[\sqrt{-p}]$:

$$\text{Category } \mathcal{AV}_R \left\{ \begin{array}{ll} A \text{ defined over } \mathbb{F}_p & \iff \iota_A : R \hookrightarrow \text{End}(A)^a \\ \phi : A \rightarrow B \text{ defined over } \mathbb{F}_p & \iff \forall \alpha \in R, \iota_B(\alpha) \circ \phi = \phi \circ \iota_A(\alpha) \end{array} \right.$$

- Let L be a R -Lattice:

$$R^n \xrightarrow{M} R^m \longrightarrow L \longrightarrow 0$$

with $M \in \text{Mat}_{m,n}(R)$ and $\text{rk}(\mathcal{L}) = m - n$.

^aprimitive embedding

As R is a Dedekind ring.

As R is a Dedekind ring.

Lattices $\iff$ finitely presented torsion free Modules

As R is a Dedekind ring.

Lattices $\iff$ finitely presented torsion free Modules

Thesis

f.p.t.f.-Module based crypto $\gg$ Lattice based crypto !

As R is a Dedekind ring.

Lattices $\iff$ finitely presented torsion free Modules

Thesis

f.p.t.f.-Module based crypto $\gg$ Lattice based crypto !

- In MIKE, Lattices are called Modules²!

²Because what else could it be!

Lattice Module action

Let L a R -lattice of rank r and A a R -oriented abelian variety

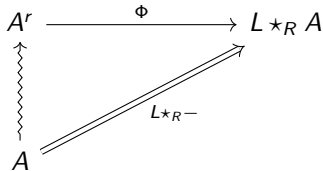
Lattice Module action

Let L a R -lattice of rank r and A a R -oriented abelian variety

Module action

The **module action** $L \star_R A$ is:

$$\Phi_L : A^r \longrightarrow L \star_R A$$



Lattice Module action

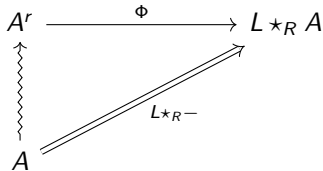
Let L a R -lattice of rank r and A a R -oriented abelian variety

Module action

The **module action** $L \star_R A$ is:

$$\Phi_L : A^r \longrightarrow L \star_R A$$

$$\ker(\Phi_L) = A^r[M] = \ker(\iota_A(M)^\top \cdot (P_i)_{1 \leq i \leq m})$$



A Cryptographic Module Action

Theorem [Rob24]

$$\star_R : (R\text{-Lattices}, \otimes^b) \times \mathcal{AV}_R \rightarrow \mathcal{AV}_R$$

is a graded symmetrical monoid action.

${}^b\otimes$ is the R -tensor product

A Cryptographic Module Action

Theorem [Rob24]

$$\star_R : (R\text{-Lattices}, \otimes^b) \times \mathcal{AV}_R \rightarrow \mathcal{AV}_R$$

is a graded symmetrical monoid action.

$^b\otimes$ is the R -tensor product

Theorem

Let E_0 s.t. $R \cong \text{End}(E_0)$.

$$\begin{array}{ccc} R\text{-Lattices} & \xrightarrow{-\star_R E_0} & \mathcal{AV}_R \\ L & \longrightarrow & L \star_R E_0 \end{array}$$

is an symmetric anti-equivalence of category.

A Cryptographic Module Action

Theorem [Rob24]

$$\star_R : (R\text{-Lattices}, \otimes^b) \times \mathcal{AV}_R \rightarrow \mathcal{AV}_R$$

is a graded symmetrical monoid action.

${}^b\otimes$ is the R -tensor product

Theorem

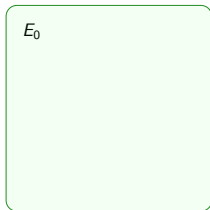
Let E_0 s.t. $R \cong \text{End}(E_0)$.

$$\begin{array}{ccc} R\text{-Lattices} & \xrightarrow{-\star_R E_0} & \mathcal{AV}_R \\ L & \longrightarrow & L \star_R E_0 \end{array}$$

is an symmetric anti-equivalence of category.

This is MIKE's cryptographic graded monoid action (almost) !

MIKE (idea)



MIKE (Idea)

Alice

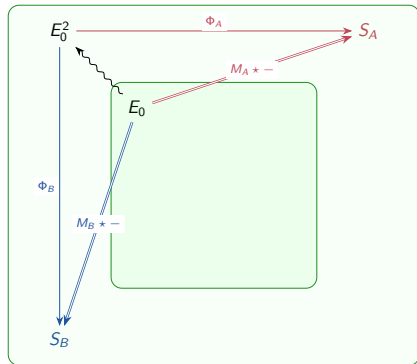
E_0 of dim 1

Bob

M_A of rank 2

M_B of rank 2

MIKE (idea)



MIKE (Idea)

Alice

E_0 of dim 1

Bob

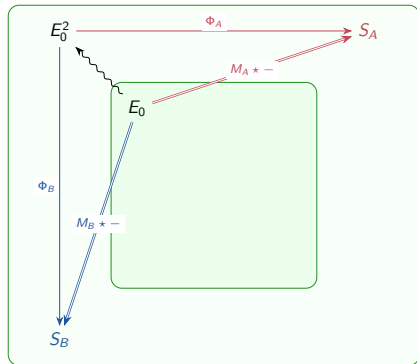
M_A of rank 2

M_B of rank 2

$S_A := M_A \star_R E_0$

$S_B := M_B \star_R E_0$

MIKE (idea)



MIKE (Idea)

Alice

E_0 of dim 1

Bob

M_A of rank 2

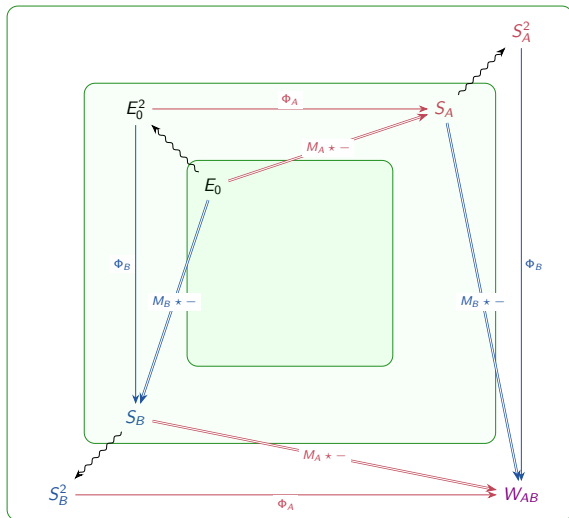
M_B of rank 2

$S_A := M_A \star_R E_0$

$S_B := M_B \star_R E_0$



MIKE (idea)



MIKE (Idea)

Alice

E_0 of dim 1

Bob

M_A of rank 2

M_B of rank 2

$S_A := M_A \star_R E_0$

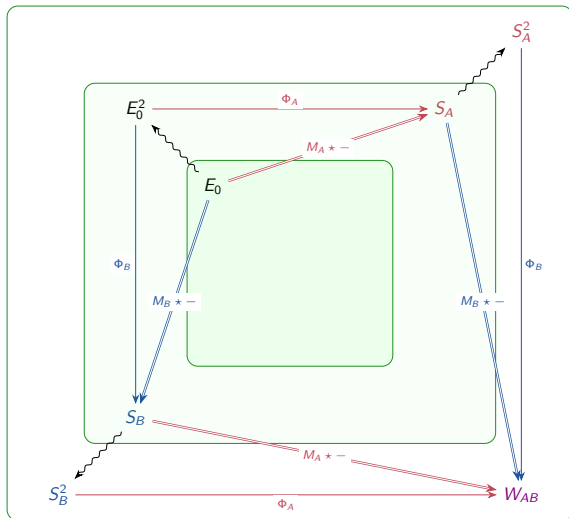
$S_B := M_B \star_R E_0$



$M_A \star_R S_B$

$M_B \star_R S_A$

MIKE (idea)



MIKE (Idea)

Alice

E_0 of dim 1

Bob

M_A of rank 2

M_B of rank 2

$S_A := M_A \star_R E_0$

$S_B := M_B \star_R E_0$

$S_A \rightarrow$

$\leftarrow S_B$

$$M_A \star_R S_B \cong (M_A \otimes M_B) \star_R E_0 \cong M_B \star_R S_A$$

MIKE's secret trick

MIKE's secret trick

$\phi_I : E_0 \rightarrow E_I$ isogeny over $\mathbb{F}_{p^2}$

MIKE's secret trick

$\phi_I : E_0 \rightarrow E_I$ isogeny over $\mathbb{F}_{p^2}$ $\overset{\text{Deuring}}{\longleftrightarrow}$ / left- $\mathcal{O}_0$ integral ideal

MIKE's secret trick

$\phi_I : E_0 \rightarrow E_I$ isogeny over $\mathbb{F}_{p^2}$ $\overset{\text{Deuring}}{\longleftrightarrow}$ I left- $\mathcal{O}_0$ integral ideal $\overset{\text{by def.}}{\longleftrightarrow}$ M_I rank 2 $\mathbb{Z}[\sqrt{-p}]$ -lattice

MIKE's secret trick

$\phi_I : E_0 \rightarrow E_I$ isogeny over $\mathbb{F}_{p^2}$ $\overset{\text{Deuring}}{\longleftrightarrow}$ I left- $\mathcal{O}_0$ integral ideal $\overset{\text{by def.}}{\longleftrightarrow}$ M_I rank 2 $\mathbb{Z}[\sqrt{-p}]$ -lattice

Theorem:

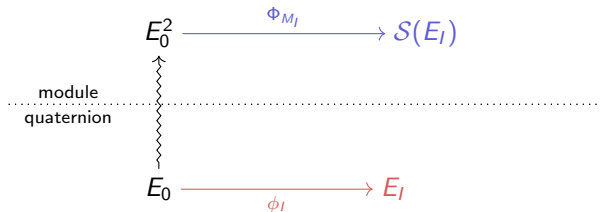
$$M_I \star_{\mathbb{Z}[\sqrt{-p}]} E_0 \cong S(E_I)$$

MIKE's secret trick

$\phi_I : E_0 \rightarrow E_I$ isogeny over $\mathbb{F}_{p^2}$ $\overset{\text{Deuring}}{\longleftrightarrow}$ I left- $\mathcal{O}_0$ integral ideal $\overset{\text{by def.}}{\longleftrightarrow}$ M_I rank 2 $\mathbb{Z}[\sqrt{-p}]$ -lattice

Theorem:

$$M_I \star_{\mathbb{Z}[\sqrt{-p}]} E_0 \cong S(E_I)$$

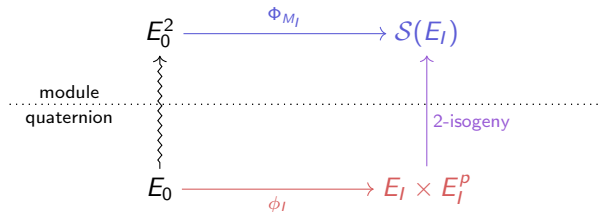


MIKE's secret trick

$\phi_I : E_0 \rightarrow E_I$ isogeny over $\mathbb{F}_{p^2}$ $\overset{\text{Deuring}}{\longleftrightarrow}$ I left- $\mathcal{O}_0$ integral ideal $\overset{\text{by def.}}{\longleftrightarrow}$ M_I rank 2 $\mathbb{Z}[\sqrt{-p}]$ -lattice

Theorem:

$$M_I \star_{\mathbb{Z}[\sqrt{-p}]} E_0 \cong S(E_I)$$



Consequences

1. MIKE's dim 2 isogenies over $\mathbb{F}_p$ are dim 1 isogenies over $\mathbb{F}_{p^2}$!
 - ▶ *Public keys compression* ($3p \rightarrow 2p$).
 - ▶ *Key security* $\iff$ *Isogeny problem*.

Consequences

1. MIKE's dim 2 isogenies over $\mathbb{F}_p$ are dim 1 isogenies over $\mathbb{F}_{p^2}$!
 - ▶ *Public keys compression* ($3p \rightarrow 2p$).
 - ▶ *Key security* $\iff$ *Isogeny problem*.
2. No need for lattices in implementation!
 - ▶ *Constant time implementation!*

Consequences

1. MIKE's dim 2 isogenies over $\mathbb{F}_p$ are dim 1 isogenies over $\mathbb{F}_{p^2}$!
 - ▶ *Public keys compression* ($3p \rightarrow 2p$).
 - ▶ *Key security* $\iff$ *Isogeny problem*.
2. No need for lattices in implementation!
 - ▶ *Constant time implementation!*
3. Shared keys are Weil type fourfolds.
 - ▶ *Can efficiently compute invariants*.

Consequences

1. MIKE's dim 2 isogenies over $\mathbb{F}_p$ are dim 1 isogenies over $\mathbb{F}_{p^2}$!
 - ▶ *Public keys compression* ($3p \rightarrow 2p$).
 - ▶ *Key security* $\iff$ *Isogeny problem*.
2. No need for lattices in implementation!
 - ▶ *Constant time implementation!*
3. Shared keys are Weil type fourfolds.
 - ▶ *Can efficiently compute invariants*.
4. Better rabbits interpolation.
 - ▶ *2x faster than generic dim 4 chain*.



Consequences

1. MIKE's dim 2 isogenies over $\mathbb{F}_p$ are dim 1 isogenies over $\mathbb{F}_{p^2}$!
 - ▶ *Public keys compression* ($3p \rightarrow 2p$).
 - ▶ *Key security* $\iff$ *Isogeny problem*.
2. No need for lattices in implementation!
 - ▶ *Constant time implementation!*
3. Shared keys are Weil type fourfolds.
 - ▶ *Can efficiently compute invariants*.
4. Better rabbits interpolation.
 - ▶ *2x faster than generic dim 4 chain*.
5. Good security.
 - ▶ *reduces to End-ring problem assuming a q -DDH oracle in AIM+.*

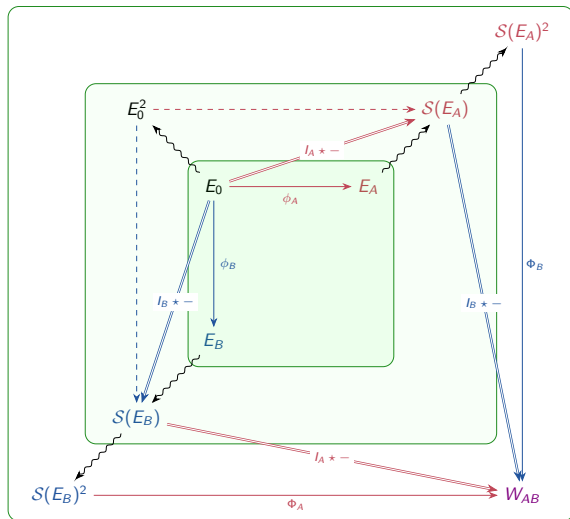


Consequences

1. MIKE's dim 2 isogenies over $\mathbb{F}_p$ are dim 1 isogenies over $\mathbb{F}_{p^2}$!
 - ▶ *Public keys compression* ($3p \rightarrow 2p$).
 - ▶ *Key security* $\iff$ *Isogeny problem*.
2. No need for lattices in implementation!
 - ▶ *Constant time implementation!*
3. Shared keys are Weil type fourfolds.
 - ▶ *Can efficiently compute invariants*.
4. Better rabbits interpolation.
 - ▶ *2x faster than generic dim 4 chain*.
5. Good security.
 - ▶ *reduces to End-ring problem assuming a q -DDH oracle in AIM+.*

*All above results are what makes MIKE!
No time to explain them!*





MIKE

Alice

$$s_A \in \mathbb{Z}_{2^f-2}$$

$$E_A := \phi_A(E_0)$$

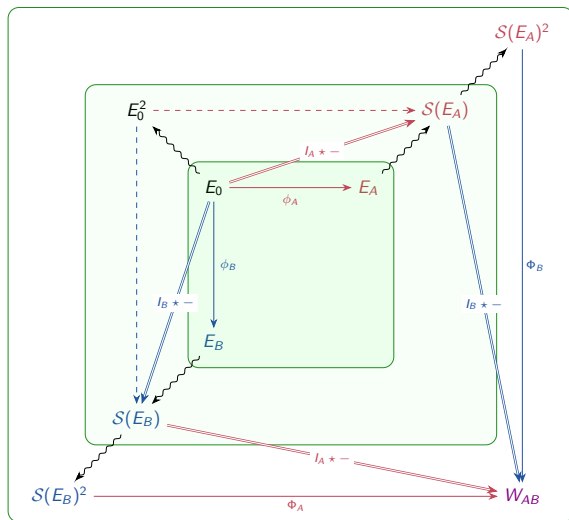
Bob

$$s_B \in \mathbb{Z}_{2^f-2}$$

$$E_B := \phi_B(E_0)$$



$$I_A \star_R S(E_B) \cong (I_A \otimes I_B) \star_R E_0 \cong I_B \star_R S(E_A)$$



MIKE

Alice

$$s_A \in \mathbb{Z}_{2^f-2}$$

$$E_A := \phi_A(E_0)$$

Bob

$$s_B \in \mathbb{Z}_{2^f-2}$$

$$E_B := \phi_B(E_0)$$



$$I_A \star_R S(E_B) \cong (I_A \otimes I_B) \star_R E_0 \cong I_B \star_R S(E_A)$$

**A monster of simplicity
coming to an eprint near you soon !**

References I



Damien Robert, *The module action for isogeny based cryptography*, Cryptology ePrint Archive, Report 2024/1556, 2024.



Benjamin Wesolowski, *The supersingular isogeny problem in time and memory $p^{1/3+o(1)}$* , Cryptology ePrint Archive, Paper 2026/1486, 2026.

Module action is an action

Module action (Theoretical PoV)

The **module action** $M \star_R A$ is the unique object in $\mathcal{AV}_R$ such that $\forall X \in \mathcal{AV}_R$

$$\text{Hom}_{\mathcal{AV}_R}(X, M \star_R A) = \text{Hom}_R(M, \text{Hom}_{\mathcal{AV}_R}(X, A))$$

- f.p.t.f R -modules are a multiplicative graded monoid using tensor product $\otimes$

$$M_2 \star_R (M_1 \star_R A) = (M_2 \otimes M_1) \star_R A$$

$$\begin{aligned} \text{Hom}_{\mathcal{AV}_R}(X, M_2 \star_R (M_1 \star_R A)) &= \text{Hom}_R(M_2, \text{Hom}_{\mathcal{AV}_R}(X, (M_1 \star_R A))) \\ &= \text{Hom}_R(M_2, \text{Hom}_R(M_1, \text{Hom}_{\mathcal{AV}_R}(X, A))) \\ &= \text{Hom}_R(M_2 \otimes M_1, \text{Hom}_{\mathcal{AV}_R}(X, A)) \\ &= \text{Hom}_{\mathcal{AV}_R}(X, (M_2 \otimes M_1) \star_R A) \end{aligned}$$

More detailed Module Action on PPAVs

<i>Modules</i>		<i>Varieties</i>
$\psi_M : M \xrightarrow{\cong} M^\vee$ $\parallel$ $H_M : M \times M \rightarrow R$	$\xlongequal{\quad}$	$\lambda_A : A \xrightarrow{\cong} A^\vee$ $\parallel$ $e_A : A \times A \rightarrow \overline{\mathbb{F}}_p$
$\xlongequal{\quad}$		

$$(M, H_M) \star_R \lambda_A : (M \star_R A)^\vee \xrightarrow{\text{Dual}} M^\vee \star_R A^\vee \xrightarrow{\psi_M} M \star_R A^\vee \xrightarrow{M \star_R \lambda_A} M \star_R A$$