MIKE: Fast and compact post-quantum NIKE

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

Swiss Crypto Day, Zurich
September 4, 2026

Diffie-Hellman Key Exchange

- Group $(\mathbb{Z}/p\mathbb{Z})^\times, \times$
- Generator g

	Alice	**Bob**
secret	$a \in [0, n-1]$	$b \in [0, n-1]$
public	$A = g^a$	$B = g^b$
shared	$B^a = g^{ba} = g^{ab} = A^b$	

Elliptic Curve Diffie-Hellman Key Exchange

- Group $E(\mathbb{F}_p), +$
- Generator P

	Alice	**Bob**
secret	$a \in [0, n-1]$	$b \in [0, n-1]$
public	$A = [a]P$	$B = [b]P$
shared	$[a]B = [ba]P = [ab]P = [b]A$	

Group-action Diffie-Hellman Key Exchange

- Commutative group G, set X with $(G, X) \to X$ such that $s(s'Q) = (ss')Q$
- Element P of X

	Alice	**Bob**
secret	$a \in G$	$b \in G$
public	$A = aP$	$B = bP$
shared	$aB = a(bP) = b(aP) = bA$	

Removing structure to gain security

	Structure	**Attack complexity**
DH	$(\mathbb{Z}/p\mathbb{Z})^\times$	subexponential classical
ECDH	Other group	polynomial quantum
CSIDH & friends	Group action	subexponential quantum

Removing structure to gain security

	Structure	**Attack complexity**
DH	$(\mathbb{Z}/p\mathbb{Z})^\times$	subexponential classical
ECDH	Other group	polynomial quantum
CSIDH & friends	Group action	subexponential quantum
MIKE	Monoid action	exponential quantum

Monoid and monoid action

Monoid: “Group without inverses”

Monoid action of M on set S:
Application $M \times S \to S$ such that $(m_1 m_2)s = (m_1(m_2, s))$

Monoid and monoid action

Monoid: "Group without inverses"

Monoid action of M on set S:
Application $M \times S \to S$ such that $(m_1 m_2)s = (m_1(m_2, s))$

Action of a commutative monoid is sufficient for a Diffie-Hellman-like NIKE!

	Alice	**Bob**
secret	$a \in M$	$b \in M$
public	$A = aP$	$B = bP$
shared	$aB = a(bP) = b(aP) = bA$	

If monoid action isn't a group action, subexponential quantum attack does not apply!

Non-group monoid: example

Idea of Damien Robert[1]:

Hermitian modules over $\mathbb{Z}[\sqrt{-p}]$ acting on principally polarized abelian varieties

[1] "The module action for isogeny based cryptography", Damien Robert, 2024, ia.cr/2024/1556

Non-group monoid: example

Idea of Damien Robert[1]:

≈ Lattices (with tensor product) acting on ≈ products of elliptic curves

[1] "The module action for isogeny based cryptography", Damien Robert, 2024, ia.cr/2024/1556

Non-group monoid: example

Idea of Damien Robert[1]:

$\approx$ Lattices (with tensor product) acting on $\approx$ products of elliptic curves

Consequences:

- $\dim(MA) = \text{rank}(M)\dim(A)$

[1] "The module action for isogeny based cryptography", Damien Robert, 2024, `ia.cr/2024/1556`

Non-group monoid: example

Idea of Damien Robert[1]:

≈ Lattices (with tensor product) acting on ≈ products of elliptic curves

Consequences:

- $\dim(MA) = \mathrm{rank}(M)\dim(A)$
- Action computation requires an (HD) isogeny

[1] "The module action for isogeny based cryptography", Damien Robert, 2024, ia.cr/2024/1556

Non-group monoid: example

Idea of Damien Robert[1]:

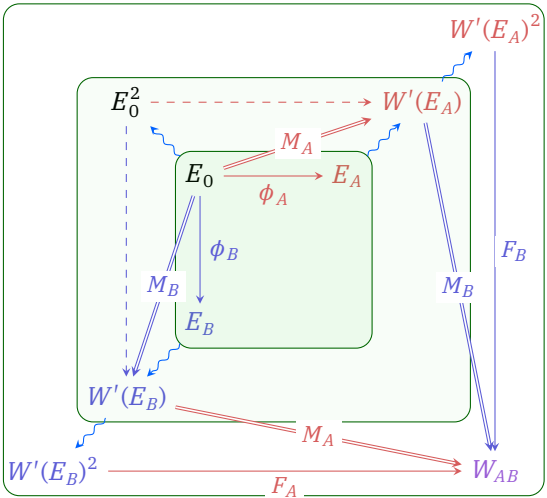
≈ Lattices (with tensor product) acting on ≈ products of elliptic curves

Consequences:

- $\dim(MA) = \mathrm{rank}(M)\dim(A)$
- Action computation requires an (HD) isogeny
- Security based on endomorphism ring problem (in QROM and AIM+) and gap-CDH

[1] "The module action for isogeny based cryptography", Damien Robert, 2024, `ia.cr/2024/1556`

Computation of the NIKE



Performance

prime size	sk	pk	KeyGen	KeyAgrement
251	32 B	64 B	0.34 ms	3.0 ms
383	48 B	92 B	1.1 ms	8.7 ms
505	64 B	128 B	2.5 ms	21 ms

Table: MIKE benchmarks[2]

Parameters will change (and increase) due to a recent attack improvement[3]

[2] Timing measured on rust implementation on ARM M4 Pro chip, 4.5GHz.

[3] "The supersingular isogeny problem in time and memory $p^{1/3+o(1)}$", Benjamin Wesolowski, 2026, `ia.cr/2026/1486`

Coming to an eprint near you soon!