# Masking SIDH: where do we stand?

Tako Boris Fouotsa, Tomoki Moriya and Christophe Petit

Isogeny days 2022

September 22, KU Leuven

# Research goal

The higher genus torsion point attacks by CD-MM-R 2022 require:

1. the torsion points information;
2. the degree of the secret isogeny.

In this work (ongoing), we investigate whether masking the torsion points information or the degree of the secret isogeny in SIDH prevents the CD-MM-R attack. More precisely,

- we suggest two countermeasure candidates: Masked-degree SIDH (MD-SIDH) and Masked torsion points SIDH (M-SIDH);
- we propose a security analysis of both schemes and mention further analysis which is being done.

# Table of contents

CD-MM-R attack

Masked-degree SIDH

Masked torsion points SIDH

Analysis of Masked-degree

Analysis of M-SIDH

Conclusion

# CD-MM-R attack

# CD-MM-R attack (1/2)

**CD-MM-R 2022: SIDH is broken in polynomial time.**

# CD-MM-R attack (1/2)

**CD-MM-R 2022**: **SIDH is broken in polynomial time.**

**Important algorithm (CD attack):**

Input: $\kappa\colon E_0 \to E_1$ of degree $3^b$

Output: $\exists \phi'_B$ s.t. $\phi_B = \phi'_B \circ \kappa \Rightarrow$ TRUE

1. Set $c = 2^{e_A - a} - 3^{e_B - b}$
2. Compute $\gamma\colon E_1 \to C$ of degree $c$
3. Compute $P_c = \gamma(\kappa(2^a P_A))$ and $Q_c = \gamma(\kappa(2^a Q_A))$
4. Compute $D := (C \times E_B)/\langle (P_c, 2^a \phi_B(P_A)), (Q_c, 2^a \phi_B(Q_A)) \rangle$
5. $D$: product $\Rightarrow$ output TRUE

# CD-MM-R attack (2/2)

**Important information for attacking SIDH:**

- Degree of the secret isogenies
- Image points of $P, Q$

# CD-MM-R attack (2/2)

**Important information for attacking SIDH:**

- Degree of the secret isogenies
- Image points of $P, Q$

$\longrightarrow$ Hide the degree of secret isogenies (Masked-degree SIDH)

# CD-MM-R attack (2/2)

**Important information for attacking SIDH:**

- Degree of the secret isogenies
- Image points of $P, Q$

$\longrightarrow$ Hide the degree of secret isogenies (Masked-degree SIDH)

$\longrightarrow$ Hide image points (Masked torsion points SIDH)

# Masked-degree SIDH

# Main idea for Masked-degree SIDH

- Set $p = \ell_1^{a_1} \cdots \ell_t^{a_t} q_1^{b_1} \cdots q_t^{b_t} f - 1$
  $\ell_1, \ldots, \ell_t, q_1 \ldots, q_t$ are distinct small primes
  $A := \prod_{i=1}^t \ell_i^{a_i}$ and $B := \prod_{i=1}^t q_i^{b_i}$

  Alice computes $\prod_{i=1}^t \ell_i^{a_i'}$-isogenies ($a_i' \in \{0, \ldots, a_i\}$)

$$\#\{\text{degree for Alice}\} = \prod_{i=1}^t (a_i + 1)$$

- The Weil pairing leaks $\prod_{i=1}^t \ell_i^{a_i'} \pmod{B}$

$$e_B(\phi_A(P_B), \phi_A(Q_B)) = e_B(P_B, Q_B)^{\deg \phi_A}$$

$\longrightarrow$ Randomize the image points by $\alpha \in (\mathbb{Z}/B\mathbb{Z})^\times$.

# Masked-degree SIDH (public key generation)

$E_0$: a supersingular elliptic curve $/\mathbb{F}_{p^2}$
$P_A, Q_A$: generators of $E_0[A]$
$P_B, Q_B$: generators of $E_0[B]$

**Public key (Alice):**

1. Take

$$(a'_1, \ldots, a'_t) \in \{0, 1, \ldots, a_1\}^t, \quad \alpha \in (\mathbb{Z}/B\mathbb{Z})^\times, \quad k_A \in \mathbb{Z}/A\mathbb{Z}.$$

   Set $A' = \prod_{i=1}^{t} \ell_i^{a'_i}$.
2. Let $R_A = [\frac{A}{A'}](P_A + k_A Q_A)$
3. Compute $\mathrm{pk}_A = (E_A := E_0/\langle R_A \rangle, [\alpha]\phi_A(P_B), [\alpha]\phi_A(Q_B))$. Set $\mathrm{sk}_A = (A', k_A)$

# MD-SIDH: key exchange and key recovery problem

Bob proceeds similarly to generate his secret/public key pair, and the key exchange continues like in a normal SIDH.

**Problem**

*$A = \ell_1^{a_1} \cdots \ell_t^{a_t}$ and let $B = q_1^{b_1} \cdots q_t^{b_t}$, $p = ABf - 1$, $A \approx B$. Set $E_0[B] = \langle P, Q \rangle$. Let $A' = \ell_1^{a'_1} \cdots \ell_t^{a'_t}$ be a uniformly random divisor of $A$ and let $\alpha$ be a uniformly random element of $\mathbb{Z}/B\mathbb{Z}^\times$. Let $\phi : E_0 \to E$ be a uniformly random isogeny of degree $A'$.*
*Given $E_0, P, Q, E_A, P' = [\alpha]\phi(P), Q' = [\alpha]\phi(Q)$, compute $\phi$.*

# Masked torsion points SIDH

# Main idea for Masked torsion points SIDH

- Set $p = ABf - 1$, $A = \ell_1 \cdots \ell_t$ and $B = q_1 \cdots q_t$ are smooth square free coprimes integers

  Alice computes $A$-isogeny $\phi_A$ (fixed degree)

- Alice samples $\alpha \in (\mathbb{Z}/B\mathbb{Z})^\times$ computes $[\alpha]\phi_A(P_B), [\alpha]\phi_A(Q_B)$

  The Weil pairing leaks $\alpha^2 \pmod{B}$

  $\longrightarrow$ Number of solutions of $x^2 \equiv \alpha^2$ in $\mathbb{Z}/B\mathbb{Z}$ is $2^t$

Set $t = \lambda$.

# Masked torsion points SIDH (public key generation)

$E_0$: a supersingular elliptic curve $/\mathbb{F}_{p^2}$
$P_A, Q_A$: generators of $E_0[A]$
$P_B, Q_B$: generators of $E_0[B]$

**Public key (Alice):**

1. Take
$$\alpha \in (\mathbb{Z}/B\mathbb{Z})^\times, \quad k_A \in \mathbb{Z}/A\mathbb{Z}.$$
2. Let $R_A = P_A + k_A Q_A$
3. Compute $\mathrm{pk}_A = (E_A := E_0/\langle R_A \rangle, [\alpha]\phi_A(P_B), [\alpha]\phi_A(Q_B))$, set $\mathrm{sk}_A = k_A$.

# M-SIDH: key exchange and key recovery problem

Bob proceeds similarly to generate his secret/public key pair, and the key exchange continues like in a normal SIDH.

**Problem**

*$A = \ell_1 \cdots \ell_t$ and let $B = q_1 \cdots q_t$, $p = ABf - 1$, $A \approx B$. Set $E_0[B] = \langle P, Q \rangle$. Let $\alpha$ be a uniformly random element of $\mathbb{Z}/B\mathbb{Z}^\times$. Let $\phi : E_0 \to E$ be a uniformly random isogeny of degree $A$. Given $E_0, P, Q, E_A, P' = [\alpha]\phi(P), Q' = [\alpha]\phi(Q)$, compute $\phi$.*

# Analysis of Masked-degree

# Overview

Recall: $A = \ell_1^{a_1} \cdots \ell_t^{a_t}$, $\quad B = q_1^{b_1} \cdots q_t^{b_t}$, $\quad E_0[B] = \langle P, Q \rangle$,
$A' = \ell_1^{a'_1} \cdots \ell_t^{a'_t}$, $\quad \alpha \in \mathbb{Z}/B\mathbb{Z}^\times \quad \phi : E_0 \to E$ of degree $A'$.
We are given $E_0, P, Q, E_A, P' = [\alpha]\phi(P), Q' = [\alpha]\phi(Q)$ and we want to compute $\phi$.

# Overview

Recall: $A = \ell_1^{a_1} \cdots \ell_t^{a_t}, \quad B = q_1^{b_1} \cdots q_t^{b_t}, \quad E_0[B] = \langle P, Q \rangle,$
$A' = \ell_1^{a'_1} \cdots \ell_t^{a'_t}, \quad \alpha \in \mathbb{Z}/B\mathbb{Z}^\times \quad \phi : E_0 \to E$ of degree $A'$.
We are given $E_0, P, Q, E_A, P' = [\alpha]\phi(P), Q' = [\alpha]\phi(Q)$ and we want to compute $\phi$.

We show that :

- one can efficiently recover the square free part $A'_1$ of the secret degree $A'$.
- When the square free part of the secret degree is known, one can reduce an MD-SIDH instance to an M-SIDH instance.

# Recovering the square free part of the degree

$A' = \ell_1^{a'_1} \cdots \ell_t^{a'_t}$ is determined by $\underline{a}' = (a'_1, \cdots, a'_t)$. Define $a(\ell_1^{a'_1} \cdots \ell_t^{a'_t}) = (a'_1, \cdots, a'_t)$ and $A(\underline{a}') = \ell_1^{a'_1} \cdots \ell_t^{a'_t}$. Set

$$\begin{array}{rccl} \chi_i : & (\mathbb{Z}/q_i^{b_i}\mathbb{Z})^\times & \longrightarrow & \mathbb{Z}/2\mathbb{Z} \\ & x & \longmapsto & \begin{cases} 1 & \text{if x is a quad. residue modulo } q_i^{b_i}; \\ 0 & \text{if not.} \end{cases} \end{array}$$

# Recovering the square free part of the degree

$A' = \ell_1^{a'_1} \cdots \ell_t^{a'_t}$ is determined by $\underline{a}' = (a'_1, \cdots, a'_t)$. Define $a(\ell_1^{a'_1} \cdots \ell_t^{a'_t}) = (a'_1, \cdots, a'_t)$ and $A(\underline{a}') = \ell_1^{a'_1} \cdots \ell_t^{a'_t}$. Set

$$\begin{array}{rccl} \chi_i : & (\mathbb{Z}/q_i^{b_i}\mathbb{Z})^\times & \longrightarrow & \mathbb{Z}/2\mathbb{Z} \\ & x & \longmapsto & \begin{cases} 1 & \text{if x is a quad. residue modulo } q_i^{b_i}; \\ 0 & \text{if not.} \end{cases} \end{array}$$

$$\begin{array}{rccc} \Phi : & (\mathbb{Z}/2\mathbb{Z})^t & \longrightarrow & (\mathbb{Z}/2\mathbb{Z})^t \\ & \underline{a}' & \longmapsto & (\chi_1(A(\underline{a}')), \ldots, \chi_t(A(\underline{a}'))) \end{array}$$

We can evaluate $\Phi$ on $a(A') \mod 2$: in fact, the Weil pairing leaks $\alpha^2 A' \mod B$ and $a(\alpha^2 A') = a(A') \mod 2$.

# Recovering the square free part of the degree

$A' = \ell_1^{a'_1} \cdots \ell_t^{a'_t}$ is determined by $\underline{a}' = (a'_1, \cdots, a'_t)$. Define $a(\ell_1^{a'_1} \cdots \ell_t^{a'_t}) = (a'_1, \cdots, a'_t)$ and $A(\underline{a}') = \ell_1^{a'_1} \cdots \ell_t^{a'_t}$. Set

$$\begin{array}{rccl} \chi_i : & (\mathbb{Z}/q_i^{b_i}\mathbb{Z})^\times & \longrightarrow & \mathbb{Z}/2\mathbb{Z} \\ & x & \longmapsto & \begin{cases} 1 & \text{if x is a quad. residue modulo } q_i^{b_i}; \\ 0 & \text{if not.} \end{cases} \end{array}$$

$$\begin{array}{rccc} \Phi : & (\mathbb{Z}/2\mathbb{Z})^t & \longrightarrow & (\mathbb{Z}/2\mathbb{Z})^t \\ & \underline{a}' & \longmapsto & (\chi_1(A(\underline{a}')), \ldots, \chi_t(A(\underline{a}'))) \end{array}$$

We can evaluate $\Phi$ on $a(A') \mod 2$: in fact, the Weil pairing leaks $\alpha^2 A' \mod B$ and $a(\alpha^2 A') = a(A') \mod 2$.

$\longrightarrow$ After evaluating $\Phi$ on $a(A') \mod 2$, we only have $\#\ker(\Phi)$ candidates for the square free part $A'_1$ of $A'$.

## On the size of $\ker\Phi$

**Kovalenko, Levitskaya, Savchuk (1986)**: *$T$ random $t \times t$-matrix $T$ over $\mathbb{Z}/2\mathbb{Z}$; then* $\Pr\left[\,\mathrm{rank}(T) \geq t-3\right] \to$ 99.4% *as* $t \to \infty$

## On the size of $\ker \Phi$

**Kovalenko, Levitskaya, Savchuk (1986)**: *$T$ random $t \times t$-matrix $T$ over $\mathbb{Z}/2\mathbb{Z}$; then* $\Pr[\operatorname{rank}(T) \geq t-3] \to 99.4\%$ *as $t \to \infty$* In

practice $t$ is small $\lambda/2 \leq t \leq \lambda$; and we are the ones choosing the primes $q_i$, so the matrix of $\Phi$ is not truly random. But, we still expect its rank to be at least $t-3$ for practical parameters: choosing the $\ell_i$'s and the $q_i$'s in a biased way would make these primes be very large and the size of $p$ becomes impractical.

# On the size of $\ker \Phi$

**Kovalenko, Levitskaya, Savchuk (1986)**: *$T$ random $t \times t$-matrix $T$ over $\mathbb{Z}/2\mathbb{Z}$; then* $\Pr[\operatorname{rank}(T) \geq t-3] \to 99.4\%$ *as $t \to \infty$* In

practice $t$ is small $\lambda/2 \leq t \leq \lambda$; and we are the ones choosing the primes $q_i$, so the matrix of $\Phi$ is not truly random. But, we still expect its rank to be at least $t-3$ for practical parameters: choosing the $\ell_i$'s and the $q_i$'s in a biased way would make these primes be very large and the size of $p$ becomes impractical. $\longrightarrow$

Heuristically, we expect to have $\ker \Phi \leq 2^3 = 8$ with high probability. This is the case for the parameters suggested by Moriya 2022.

## Reducing MD-SIDH to M-SIDH

Assume that we know $A_1'$. Set $A_0 = \max\{n \mid n|A, n^2 A_1' \leq A\}$. Then $\exists \alpha_0$, divisor of $A$, $N_A := A_0^2 A_1' = \alpha_0^2 A' \leq A$.

# Reducing MD-SIDH to M-SIDH

Assume that we know $A_1'$. Set $A_0 = \max\{n \mid n|A, n^2 A_1' \leq A\}$. Then $\exists \alpha_0$, divisor of $A$, $N_A := A_0^2 A_1' = \alpha_0^2 A' \leq A$.

Set $\phi_0 = [\alpha_0] \circ \phi$, then $\deg(\phi_0) = N_A$ is known.

$$P' = [\alpha]\phi(P) = [(\alpha\alpha_0^{-1}) \cdot \alpha_0]\phi(P) = [\alpha\alpha_0^{-1}]\phi_0(P)$$
$$Q' = [\alpha]\phi(Q) = [(\alpha\alpha_0^{-1}) \cdot \alpha_0]\phi(Q) = [\alpha\alpha_0^{-1}]\phi_0(Q)$$

# Reducing MD-SIDH to M-SIDH

Assume that we know $A_1'$. Set $A_0 = \max\{n \mid n|A, n^2 A_1' \le A\}$. Then $\exists \alpha_0$, divisor of $A$, $N_A := A_0^2 A_1' = \alpha_0^2 A' \le A$.

Set $\phi_0 = [\alpha_0] \circ \phi$, then $\deg(\phi_0) = N_A$ is known.

$$\begin{aligned} P' &= [\alpha]\phi(P) = [(\alpha\alpha_0^{-1}) \cdot \alpha_0]\phi(P) = [\alpha\alpha_0^{-1}]\phi_0(P) \\ Q' &= [\alpha]\phi(Q) = [(\alpha\alpha_0^{-1}) \cdot \alpha_0]\phi(Q) = [\alpha\alpha_0^{-1}]\phi_0(Q) \end{aligned}$$

Compute $\alpha_1^2 = \alpha_0^2 A' \cdot (\alpha^2 A')^{-1} \mod B = (\alpha_0 \cdot \alpha^{-1})^2 \mod B$. Sampling a random square root $\alpha_1'$ of $\alpha_1^2 \mod B$, then $\alpha_1' = \mu\alpha_1$ where $\mu$ is some square root of unity. We compute

$$\begin{aligned} [\alpha_1']P' &= [\mu \cdot \alpha_1]P' = [\mu]\phi_0(P) \\ [\alpha_1']Q' &= [\mu \cdot \alpha_1]P' = [\mu]\phi_0(Q) \end{aligned}$$

# Consequence on MD-SIDH

- Recovering $\mu$ enables the CD-MM-R attack: one can try all the $2^t$ possible values of $\mu$.
- The parameters suggested by Moriya 2022 ($t = \lambda/2$) are not secure.
- In general, one needs $t = \lambda$; and any attack on M-SIDH is likely to apply to MD-SIDH as well.

# Analysis of M-SIDH

# Overview

Recall: $A = \ell_1 \cdots \ell_t, \quad B = q_1 \cdots q_t, \quad A \approx B, \quad E_0[B] = \langle P, Q \rangle,$
$\alpha \in \mathbb{Z}/B\mathbb{Z}^\times, \quad \phi : E_0 \to E$ of degree $A$. We are given
$E_0, P, Q, E_A, P' = [\alpha]\phi(P), Q' = [\alpha]\phi(Q)$ and we want to compute $\phi$.

*We show that if $E_0$ is $M$-small with $M$ of polynomial size in $\log p$, then the CD-MM-R can be used to recover the secret isogeny.*

# Lollipoping M-SIDH (1/2)

**Main input:** the latest version of Damien's attack only requires $B^2 > A$ i,e, with $B$ torsion point information, one can attack isogenies of degree up to $A \approx B^2$.

[1] which can be efficiently evaluated.

# Lollipoping M-SIDH (1/2)

**Main input:** the latest version of Damien's attack only requires $B^2 > A$ i,e, with $B$ torsion point information, one can attack isogenies of degree up to $A \approx B^2$.

**Main idea:** Attack $\phi_A \circ \theta \circ \widehat{\phi}_A$ instead of $\phi_A$, with $\theta$ being a non-trivial small endomorphism[1] of $E_0$.

Eliminating the scalar $\alpha$ in M-SIDH: one can always assume $\alpha^2 = 1 \mod B$ (Weil pairing ...)

$$([\alpha]\phi) \circ \theta \circ (\widehat{[\alpha]\phi}) = [\alpha^2] \circ \phi \circ \theta \circ \widehat{\phi} = \phi \circ \theta \circ \widehat{\phi} =: \tau.$$

[1] which can be efficiently evaluated.

# Lollipoping M-SIDH (1/2)

**Main input**: the latest version of Damien's attack only requires $B^2 > A$ i,e, with $B$ torsion point information, one can attack isogenies of degree up to $A \approx B^2$.

**Main idea**: Attack $\phi_A \circ \theta \circ \widehat{\phi}_A$ instead of $\phi_A$, with $\theta$ being a non-trivial small endomorphism[1] of $E_0$.

Eliminating the scalar $\alpha$ in M-SIDH: one can always assume $\alpha^2 = 1 \mod B$ (Weil pairing ...)

$$([\alpha]\phi) \circ \theta \circ (\widehat{[\alpha]\phi}) = [\alpha^2] \circ \phi \circ \theta \circ \widehat{\phi} = \phi \circ \theta \circ \widehat{\phi} =: \tau.$$

Magic: No secret scalar appears in $\tau$ and $\deg \tau = A^2 \deg \theta$.

[1] which can be efficiently evaluated.

# Lollipoping M-SIDH (2/2)

- If $A^2 \deg\theta < B^2$, then just run the CD-MM-R attack.

# Lollipoping M-SIDH (2/2)

- If $A^2 \deg\theta < B^2$, then just run the CD-MM-R attack.
- If $A^2 \deg\theta > B^2$, then one can
  - guess part ($\approx \sqrt{\deg\theta}$ ) of the secret isogeny from the end curve, $O(\sqrt{\deg\theta})$ guesses; or
  - guess supplementary ($\approx \sqrt{\deg\theta}$ ) torsion point information, $O(\sqrt{\deg\theta}^3)$ guesses.

  Run the CD-MM-R attack with each guess.

# Lollipoping M-SIDH (2/2)

- If $A^2 \deg \theta < B^2$, then just run the CD-MM-R attack.
- If $A^2 \deg \theta > B^2$, then one can
  - guess part ($\approx \sqrt{\deg \theta}$ ) of the secret isogeny from the end curve, $O(\sqrt{\deg \theta})$ guesses; or
  - guess supplementary ($\approx \sqrt{\deg \theta}$ ) torsion point information, $O(\sqrt{\deg \theta}^3)$ guesses.

  Run the CD-MM-R attack with each guess.
- In general, for an $M$-small curve with known endomorphism ring, one can recover the secret isogeny in time $O(\sqrt{M})$.
- With the MD-SIDH to M-SIDH reduction, this Lollipop attack extends to MD-SIDH as well.

# Conclusion

# Conclusion

- We presented two countermeasure ideas for the higher genus torsion point attacks: MD-SIDH and M-SIDH.

# Conclusion

- We presented two countermeasure ideas for the higher genus torsion point attacks: MD-SIDH and M-SIDH.
- We provided an advance analysis of both schemes.

# Conclusion

- We presented two countermeasure ideas for the higher genus torsion point attacks: MD-SIDH and M-SIDH.
- We provided an advance analysis of both schemes.
  - MD-SIDH was reduced to M-SIDH and suggested parameters (Moriya 2022) are not secure.
  - A Lollipop attack breaks both schemes when the starting curve has small non trivial endomorphisms that can be efficiently evaluated.

# Conclusion

- We presented two countermeasure ideas for the higher genus torsion point attacks: MD-SIDH and M-SIDH.
- We provided an advance analysis of both schemes.
  - MD-SIDH was reduced to M-SIDH and suggested parameters (Moriya 2022) are not secure.
  - A Lollipop attack breaks both schemes when the starting curve has small non trivial endomorphisms that can be efficiently evaluated.
- *As a consequence, any instantiation would require a starting curve with unknown endomorphism ring.*

Ongoing: can one run the lollipop attack when the starting curve has unknown endomorphism ring?

Thanks