M-SIDH and MD-SIDH: Countering SIDH Attacks by Masking Information

Isogeny-Based Cryptography

TB Fouotsa[a], **T Moriya**[b], C. Petit[b,c]

Eurocrypt 2023, Lyon, France

[a]EPFL, [b]University of Birmingham, [c]Université Libre de Bruxelles

Outline

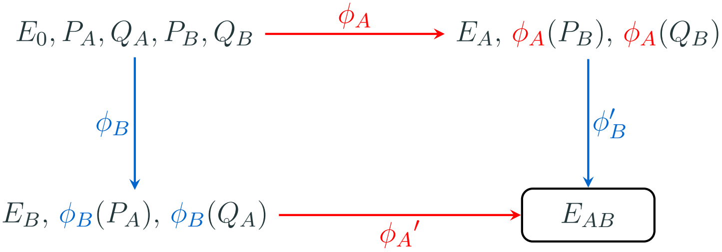
SIDH and the attacks

Countermeasures for SIDH attacks

Analysis of the countermeasures

Summary

SIDH and the attacks



Ambient field: $\mathbb{F}_{p^2}$, $p = 2^a 3^b - 1$. $\deg \phi_A = 2^a$ $\deg \phi_B = 3^b$

$E_0[2^a] = \langle P_A, Q_A \rangle$, $E_0[3^b] = \langle P_B, Q_B \rangle$

SSI-T: Given E_0, P_A, Q_A, P_B, Q_B, E_B, $\phi_B(P_A)$ and $\phi_B(Q_A)$, compute ϕ_B.

SIDH's life span

Life was nice till 2016: year where a demon possessed the TP!

GPST 2016: adaptive attack on SIDH,

Petit 2017: torsion point attack on imbalanced SIDH, no impact on SIDH

dQKL+ 2021: improvement on Petit TPA, but SIDH still safe.

FP 2022: new adaptive attack on SIDH using TPA, no impact on SIKE

SIDH attacks, final shot: SIDH/SIKE is broken in seconds...

All these attacks exploit torsion point information !!

Non exhaustive list: BdQL+ 2019, ...

The framework of the attacks

SSI-T Problem: Given E_0, $E[A] = \langle P, Q \rangle$, E, $\phi(P)$, $\phi(Q)$, compute ϕ.

Degree transformation: define a map Γ that can be used to transform ϕ to $\tau = \Gamma(\phi, input)$ such that:

1. Knowing $\tau = \Gamma(\phi, input)$, one can recover ϕ
2. τ can be evaluated on the A-torsion
3. τ can be recovered from its action on the A-torsion

The attack: Given a suitable description of Γ,

- Use 2. and 3. to recover τ
- Use 1. to derive ϕ from τ

SIDH attacks (2022)

Assume $\phi : E_0 \longrightarrow E_B$ has degree B and the TP have order A.
Set $a = A - B = a_1^2 + a_2^2 + a_3^2 + a_4^2$.

$$\tau = \Gamma(\phi, a) := \begin{bmatrix} \alpha_0 & \hat{\phi} Id_4 \\ -\phi Id_4 & \hat{\alpha}_B \end{bmatrix} \in \mathrm{End}(E_0^4 \times E_B^4)$$

where

- $\phi Id_4 : E_0^4 \longrightarrow E_B^4$ and $\hat{\phi} Id_4 : E_B^4 \longrightarrow E_0^4$
- $\alpha_0 \in \mathrm{End}(E_0^4)$ and $\alpha_B \in \mathrm{End}(E_B^4)$ having the same matrix representation

$$M = \begin{bmatrix} a_1 & -a_2 & -a_3 & -a_4 \\ a_2 & a_1 & a_4 & -a_3 \\ a_3 & -a_4 & a_1 & a_2 \\ a_4 & a_3 & -a_2 & a_1 \end{bmatrix}$$

SIDH attacks (2022)

Assume $\phi : E_0 \longrightarrow E_B$ has degree B and the TP have order A.
Set $a = A - B = a_1^2 + a_2^2 + a_3^2 + a_4^2$.

$$\tau = \Gamma(\phi, a) := \begin{bmatrix} \alpha_0 & \hat{\phi} Id_4 \\ -\phi Id_4 & \hat{\alpha}_B \end{bmatrix} \in \mathrm{End}(E_0^4 \times E_B^4)$$

Fact: τ has degree $B + a = A$

1. Knowing $\tau = \Gamma(\phi, input)$, one can recover ϕ
2. τ can be evaluated on the A-torsion
3. τ can be recovered from its action on the A-torsion

SIDH attacks (2022)

Assume $\phi : E_0 \longrightarrow E_B$ has degree B and the TP have order A.
Set $a = A - B = a_1^2 + a_2^2 + a_3^2 + a_4^2$.

$$\tau = \Gamma(\phi, a) := \begin{bmatrix} \alpha_0 & \hat{\phi} Id_4 \\ -\phi Id_4 & \hat{\alpha}_B \end{bmatrix} \in \mathrm{End}(E_0^4 \times E_B^4)$$

Fact: τ has degree $B + a = A$

1. Knowing $\tau = \Gamma(\phi, input)$, one can recover ϕ ✓
2. τ can be evaluated on the A-torsion
3. τ can be recovered from its action on the A-torsion

SIDH attacks (2022)

Assume $\phi : E_0 \longrightarrow E_B$ has degree B and the TP have order A.
Set $a = A - B = a_1^2 + a_2^2 + a_3^2 + a_4^2$.

$$\tau = \Gamma(\phi, a) := \begin{bmatrix} \alpha_0 & \hat{\phi} Id_4 \\ -\phi Id_4 & \hat{\alpha}_B \end{bmatrix} \in \mathrm{End}(E_0^4 \times E_B^4)$$

Fact: τ has degree $B + a = A$

1. Knowing $\tau = \Gamma(\phi, input)$, one can recover ϕ ✓
2. τ can be evaluated on the A-torsion ✓
3. τ can be recovered from its action on the A-torsion

SIDH attacks (2022)

Assume $\phi : E_0 \longrightarrow E_B$ has degree B and the TP have order A.
Set $a = A - B = a_1^2 + a_2^2 + a_3^2 + a_4^2$.

$$\tau = \Gamma(\phi, a) := \begin{bmatrix} \alpha_0 & \hat{\phi} Id_4 \\ -\phi Id_4 & \hat{\alpha}_B \end{bmatrix} \in \mathrm{End}(E_0^4 \times E_B^4)$$

Fact: τ has degree $B + a = A$

1. Knowing $\tau = \Gamma(\phi, input)$, one can recover ϕ ✓
2. τ can be evaluated on the A-torsion ✓
3. τ can be recovered from its action on the A-torsion ✓

SIDH attacks (2022)

Assume $\phi : E_0 \longrightarrow E_B$ has degree B and the TP have order A.
Set $a = A - B = a_1^2 + a_2^2 + a_3^2 + a_4^2$.

$$\tau = \Gamma(\phi, a) := \begin{bmatrix} \alpha_0 & \hat{\phi} Id_4 \\ -\phi Id_4 & \hat{\alpha}_B \end{bmatrix} \in \mathrm{End}(E_0^4 \times E_B^4)$$

Fact: τ has degree $B + a = A$

1. Knowing $\tau = \Gamma(\phi, input)$, one can recover ϕ ✓
2. τ can be evaluated on the A-torsion ✓
3. τ can be recovered from its action on the A-torsion ✓

Runs in polynomial time when $A^2 > B$

Countermeasures for SIDH attacks

Countermeasures

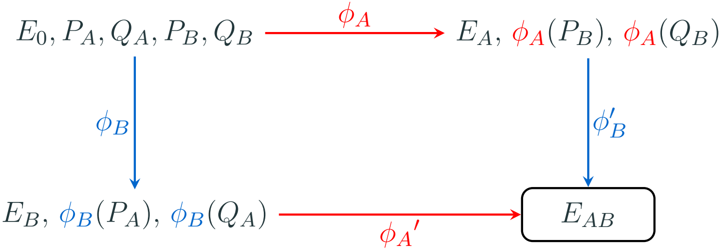
SIDH attacks require:

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

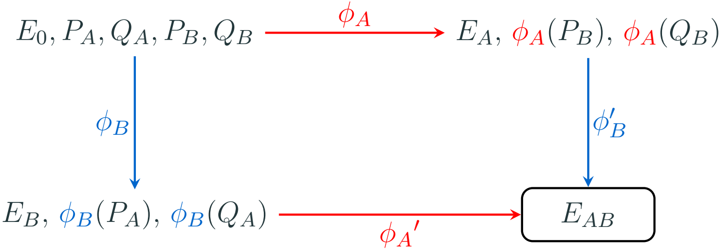
Two countermeasures:

- Masked-degree SIDH (MD-SIDH): the degree of the secret isogeny is secret;
- Masked torsion points SIDH (M-SIDH): the degree of the secret isogeny is fixed, but the torsion point images are scaled by a secret scalar.

MD-SIDH


E_0, P_A, Q_A, P_B, Q_B
ϕ_A
$E_A,\ \phi_A(P_B),\ \phi_A(Q_B)$
ϕ_B
ϕ'_B
$E_B,\ \phi_B(P_A),\ \phi_B(Q_A)$
$\phi_A{}'$
E_{AB}

MD-SIDH

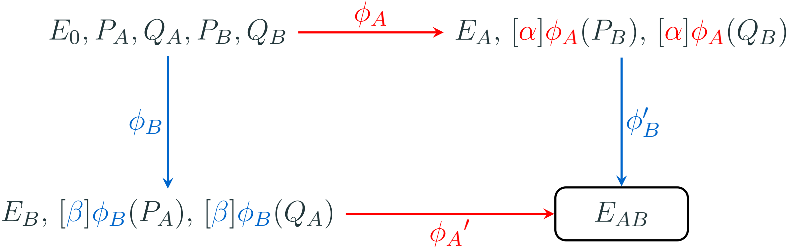


Ambient field: $\mathbb{F}_{p^2},\ p = \ell_1^{a_1} \cdots \ell_t^{a_t} q_1^{b_1} \cdots q_t^{b_t} f - 1$

$A := \prod_{i=1}^{t} \ell_i^{a_i} \qquad B := \prod_{i=1}^{t} q_i^{b_i}, \quad A \approx B.$

$\deg \phi_A = A', \quad A' | A, \qquad \deg \phi_B = B', \quad B' | B.$

MD-SIDH



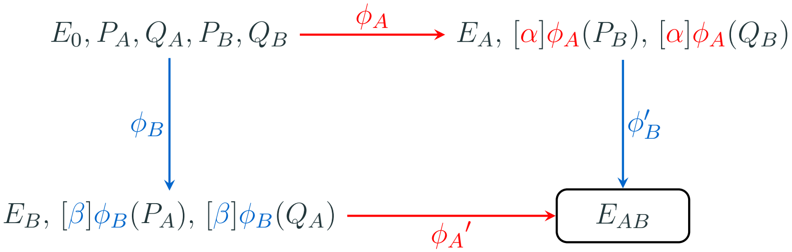
Ambient field: $\mathbb{F}_{p^2}$, $p = \ell_1^{a_1} \cdots \ell_t^{a_t} q_1^{b_1} \cdots q_t^{b_t} f - 1$

$A := \prod_{i=1}^{t} \ell_i^{a_i} \qquad B := \prod_{i=1}^{t} q_i^{b_i}, \quad A \approx B.$

$\deg \phi_A = A', \quad A' | A, \qquad \deg \phi_B = B', \quad B' | B.$

Hide the degree from pairings: $\alpha \in (\mathbb{Z}/B\mathbb{Z})^\times \quad \beta \in (\mathbb{Z}/A\mathbb{Z})^\times$

MD-SIDH



Ambient field: $\mathbb{F}_{p^2}$, $p = \ell_1^{a_1} \cdots \ell_t^{a_t} q_1^{b_1} \cdots q_t^{b_t} f - 1$

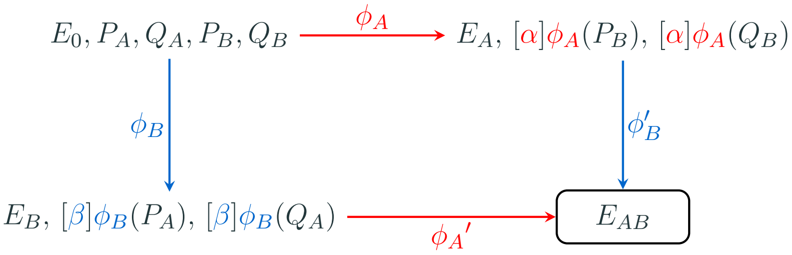
$A := \prod_{i=1}^t \ell_i^{a_i} \qquad B := \prod_{i=1}^t q_i^{b_i}, \quad A \approx B.$

$\deg \phi_A = A'$, $\quad A'|A$, $\qquad \deg \phi_B = B'$, $\quad B'|B$.

Hide the degree from pairings: $\alpha \in (\mathbb{Z}/B\mathbb{Z})^\times \quad \beta \in (\mathbb{Z}/A\mathbb{Z})^\times$

There are about $\prod_{i=1}^t (a_i + 1)$ possibilities of degrees!

M-SIDH



Ambient field: $\mathbb{F}_{p^2}$, $p = \ell_1 \cdots \ell_t q_1 \cdots q_t f - 1$

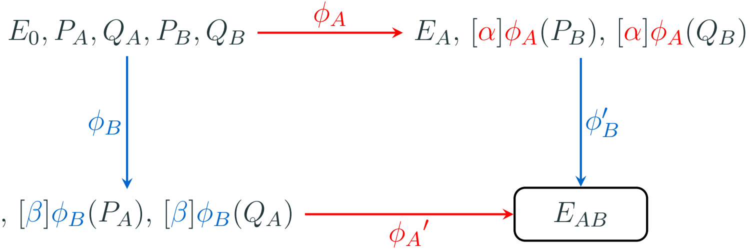
$A := \prod_{i=1}^{t} \ell_i \qquad B := \prod_{i=1}^{t} q_i, \quad A \approx B.$

$\deg \phi_A = A, \qquad \deg \phi_B = B.$

$E_0[A] = \langle P_A, Q_A \rangle, \quad E_0[B] = \langle P_B, Q_B \rangle$

Hide the exact TP images: $\alpha \in \mu(A) \quad \beta \in \mu(A)$

M-SIDH



Ambient field: $\mathbb{F}_{p^2}$, $p = \ell_1 \cdots \ell_t q_1 \cdots q_t f - 1$

$A := \prod_{i=1}^{t} \ell_i \qquad B := \prod_{i=1}^{t} q_i, \quad A \approx B.$

$\deg \phi_A = A, \qquad \deg \phi_B = B.$

$E_0[A] = \langle P_A, Q_A \rangle, \quad E_0[B] = \langle P_B, Q_B \rangle$

Hide the exact TP images: $\alpha \in \mu(A) \quad \beta \in \mu(A)$

$\alpha^2 \equiv 1 \pmod{A}$ has about 2^t solutions by CRT!

Does this work?

In the SIDH attacks, we had

$$\tau = \Gamma(\phi, a) := \begin{bmatrix} \alpha_0 & \hat{\phi} Id_4 \\ -\phi Id_4 & \hat{\alpha}_B \end{bmatrix}$$

of degree $A = B + a$.

For M-SIDH, it becomes

$$\tau = \Gamma(\phi, a) := \begin{bmatrix} \alpha_0 & [\alpha]\hat{\phi} Id_4 \\ -[\alpha]\phi Id_4 & \hat{\alpha}_B \end{bmatrix}$$

whose degree is
$a + \alpha^2 B = A - B + \alpha^2 B = A + B(\alpha^2 - 1) \approx BA^2$.

The attack would require $\sqrt{BA^2} \approx \sqrt{B}A$ TP information.

Analysis of the countermeasures

Case of M-SIDH (General case)

SIDH attacks : works when $A^2 > B$.

Goal: Find (P'_A, Q'_A) and $(\phi_B(P'_A), \phi_B(Q'_A))$ s.t. $\mathrm{ord}(P'_A)^2 > B$.

In M-SIDH, $B \approx A = (\sqrt{A})^2$.

Hence we can use less torsion $A' = \prod_{i=t'}^{t} \ell_i > \sqrt{A}$.

$P'_A = [\prod_{i=1}^{t'-1} \ell_i]P_A$, $Q'_A = [\prod_{i=1}^{t'-1} \ell_i]Q_A$.

Guessing the exact torsion point: $O(2^{t-t'})$

Consequence: A and B must have at least 2λ distinct prime factors each.

Case of M-SIDH (General case)

SIDH attacks : works when $A^2 > B$.

Goal: Find (P'_A, Q'_A) and $(\phi_B(P'_A), \phi_B(Q'_A))$ s.t. $\mathrm{ord}(P'_A)^2 > B$.

In M-SIDH, $B \approx A = (\sqrt{A})^2$.

Hence we can use less torsion $A' = \prod_{i=t'}^{t} \ell_i > \sqrt{A}$.

$P'_A = [\prod_{i=1}^{t'-1} \ell_i] P_A$, $Q'_A = [\prod_{i=1}^{t'-1} \ell_i] Q_A$.

Guessing the exact torsion point: $O(2^{t-t'})$

Consequence: A and B must have at least 2λ distinct prime factors each.

Case of M-SIDH (General case)

SIDH attacks : works when $A^2 > B$.

Goal: Find (P'_A, Q'_A) and $(\phi_B(P'_A), \phi_B(Q'_A))$ s.t. $\text{ord}(P'_A)^2 > B$.

In M-SIDH, $B \approx A = (\sqrt{A})^2$.

Hence we can use less torsion $A' = \prod_{i=t'}^{t} \ell_i > \sqrt{A}$.

$P'_A = [\prod_{i=1}^{t'-1} \ell_i]P_A$, $Q'_A = [\prod_{i=1}^{t'-1} \ell_i]Q_A$.

Guessing the exact torsion point: $O(2^{t-t'})$

Consequence: A and B must have at least 2λ distinct prime factors each.

Case of M-SIDH (General case)

SIDH attacks : works when $A^2 > B$.

Goal: Find (P'_A, Q'_A) and $(\phi_B(P'_A), \phi_B(Q'_A))$ s.t. $\mathrm{ord}(P'_A)^2 > B$.

In M-SIDH, $B \approx A = (\sqrt{A})^2$.

Hence we can use less torsion $A' = \prod_{i=t'}^{t} \ell_i > \sqrt{A}$.

$P'_A = [\prod_{i=1}^{t'-1} \ell_i]P_A$, $Q'_A = [\prod_{i=1}^{t'-1} \ell_i]Q_A$.

Guessing the exact torsion point: $O(2^{t-t'})$

Consequence: A and B must have at least 2λ distinct prime factors each.

Case of M-SIDH (E_0 has a special endomorphism)

Setting : E_0 has a small degree endomorphism θ.

Key : We can compute $\phi_B \circ \theta \circ \hat{\phi_B}([\beta]\phi_B(P_A))$.

With respect to the A torsion, we have:

$$([\beta]\phi_B) \circ \theta \circ (\widehat{[\beta]\phi_B}) = [\beta^2] \circ \phi_B \circ \theta \circ \widehat{\phi_B} \equiv \phi_B \circ \theta \circ \widehat{\phi_B} =: \tau.$$

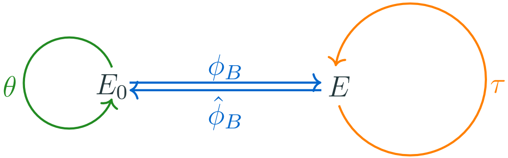
$\deg \tau = B^2 \deg \theta$.

SIDH attacks on τ requires : $\sqrt{\deg \tau} = B\sqrt{\deg \theta} \approx B$ torsions.

Consequence: No small endomorphisms in E_0, if possible, no known endomorphism at all.

Case of M-SIDH (E_0 has a special endomorphism)

Setting : E_0 has a small degree endomorphism θ.



Key : We can compute $\phi_B \circ \theta \circ \hat{\phi_B}([\beta]\phi_B(P_A))$.

With respect to the A torsion, we have:

$$([\beta]\phi_B) \circ \theta \circ (\widehat{[\beta]\phi_B}) = [\beta^2] \circ \phi_B \circ \theta \circ \widehat{\phi_B} \equiv \phi_B \circ \theta \circ \widehat{\phi_B} =: \tau.$$

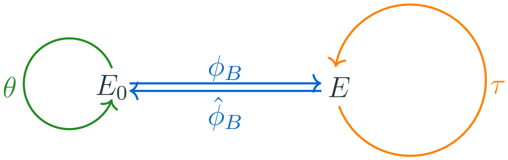
$\deg \tau = B^2 \deg \theta$.

SIDH attacks on τ requires : $\sqrt{\deg \tau} = B\sqrt{\deg \theta} \approx B$ torsions.

Consequence: No small endomorphisms in E_0, if possible, no known endomorphism at all.

Case of M-SIDH (E_0 has a special endomorphism)

Setting : E_0 has a small degree endomorphism θ.



Key : <u>We can compute $\phi_B \circ \theta \circ \hat{\phi_B}([\beta]\phi_B(P_A))$.</u>

With respect to the A torsion, we have:

$$([\beta]\phi_B) \circ \theta \circ (\widehat{[\beta]\phi_B}) = [\beta^2] \circ \phi_B \circ \theta \circ \widehat{\phi_B} \equiv \phi_B \circ \theta \circ \widehat{\phi_B} =: \tau.$$

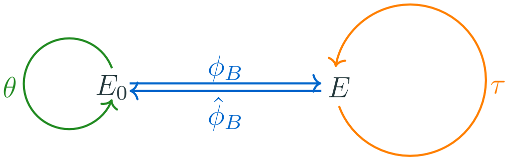
$\deg \tau = B^2 \deg \theta$.

SIDH attacks on τ requires : $\sqrt{\deg \tau} = B\sqrt{\deg \theta} \approx B$ torsions.

Consequence: No small endomorphisms in E_0, if possible, no known endomorphism at all.

Case of M-SIDH (E_0 has a special endomorphism)

Setting : E_0 has a small degree endomorphism θ.



Key : We can compute $\phi_B \circ \theta \circ \hat{\phi}_B([\beta]\phi_B(P_A))$.

With respect to the A torsion, we have:

$$([\beta]\phi_B) \circ \theta \circ (\widehat{[\beta]\phi_B}) = [\beta^2] \circ \phi_B \circ \theta \circ \widehat{\phi_B} \equiv \phi_B \circ \theta \circ \widehat{\phi_B} =: \tau.$$

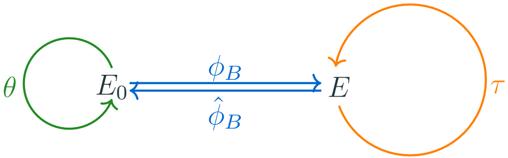
$\deg \tau = B^2 \deg \theta$.

SIDH attacks on τ requires : $\sqrt{\deg \tau} = B\sqrt{\deg \theta} \approx B$ torsions.

Consequence: No small endomorphisms in E_0, if possible, no known endomorphism at all.

Case of M-SIDH (E_0 has a special endomorphism)

Setting : E_0 has a small degree endomorphism θ.



Key : We can compute $\phi_B \circ \theta \circ \hat{\phi}_B([\beta]\phi_B(P_A))$.

With respect to the A torsion, we have:

$$([\beta]\phi_B) \circ \theta \circ (\widehat{[\beta]\phi_B}) = [\beta^2] \circ \phi_B \circ \theta \circ \widehat{\phi_B} \equiv \phi_B \circ \theta \circ \widehat{\phi_B} =: \tau.$$

$\deg \tau = B^2 \deg \theta$.

SIDH attacks on τ requires : $\sqrt{\deg \tau} = B\sqrt{\deg \theta} \approx B$ torsions.

Consequence: No small endomorphisms in E_0, if possible, no known endomorphism at all.

Case of MD-SIDH (1/2)

Sec. of MD-SIDH reduces to of M-SIDH under SIDH attacks.

Key : SIDH attacks also work on non-cyclic isogenies.

Recall: $\deg \phi_B = B' | B$, TP are scaled by $\beta \in \mathbb{Z}/B\mathbb{Z}$.
Denote the square free part of B' by B'_1.

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

$$\begin{array}{rccc} \Phi : & (\mathbb{Z}/2\mathbb{Z})^t & \longrightarrow & (\mathbb{Z}/2\mathbb{Z})^t \\ & (b_1, \ldots, b_t) & \longmapsto & (\chi_1(N_1), \ldots, \chi_t(N_t)) \end{array}$$

where $N_i := q_1^{b_1} \cdots q_t^{b_t} \pmod{\ell_i^{a_i}}$.

Claims:

- The image of $\Phi \leftrightarrow$ Information of B'_1 leaked by Weil pairing
- Φ is almost injective.

Consequence: We can recover B'_1 by using Weil pairing.

Case of MD-SIDH (1/2)

Sec. of MD-SIDH reduces to of M-SIDH under SIDH attacks.

Key : SIDH attacks also work on non-cyclic isogenies.

Recall: $\deg \phi_B = B' | B$, TP are scaled by $\beta \in \mathbb{Z}/B\mathbb{Z}$.
Denote the square free part of B' by B'_1.

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

$$\begin{array}{rccc} \Phi : & (\mathbb{Z}/2\mathbb{Z})^t & \longrightarrow & (\mathbb{Z}/2\mathbb{Z})^t \\ & (b_1, \ldots, b_t) & \longmapsto & (\chi_1(N_1), \ldots, \chi_t(N_t)) \end{array}$$

where $N_i := q_1^{b_1} \cdots q_t^{b_t} \pmod{\ell_i^{a_i}}$.

Claims:

- The image of $\Phi \leftrightarrow$ Information of B'_1 leaked by Weil pairing
- Φ is almost injective.

Consequence: We can recover B'_1 by using Weil pairing.

Case of MD-SIDH (1/2)

Sec. of MD-SIDH reduces to of M-SIDH under SIDH attacks.

Key : SIDH attacks also work on non-cyclic isogenies.

Recall: $\deg \phi_B = B' | B$, TP are scaled by $\beta \in \mathbb{Z}/B\mathbb{Z}$.
Denote the square free part of B' by B'_1.

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

$$\Phi : \quad (\mathbb{Z}/2\mathbb{Z})^t \longrightarrow (\mathbb{Z}/2\mathbb{Z})^t$$
$$(b_1, \ldots, b_t) \longmapsto (\chi_1(N_1), \ldots, \chi_t(N_t))$$

where $N_i := q_1^{b_1} \cdots q_t^{b_t} \pmod{\ell_i^{a_i}}$.

Claims:

- The image of $\Phi \leftrightarrow$ Information of B'_1 leaked by Weil pairing
- Φ is almost injective.

Consequence: We can recover B'_1 by using Weil pairing.

Case of MD-SIDH (1/2)

Sec. of MD-SIDH reduces to of M-SIDH under SIDH attacks.

Key : SIDH attacks also work on non-cyclic isogenies.

Recall: $\deg \phi_B = B' | B$, TP are scaled by $\beta \in \mathbb{Z}/B\mathbb{Z}$.
Denote the square free part of B' by B'_1.

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

$$\Phi : \begin{array}{ccc} (\mathbb{Z}/2\mathbb{Z})^t & \longrightarrow & (\mathbb{Z}/2\mathbb{Z})^t \\ (b_1, \ldots, b_t) & \longmapsto & (\chi_1(N_1), \ldots, \chi_t(N_t)) \end{array}$$

where $N_i := q_1^{b_1} \cdots q_t^{b_t} \pmod{\ell_i^{a_i}}$.

Claims:

- The image of $\Phi \leftrightarrow$ Information of B'_1 leaked by Weil pairing
- Φ is almost injective.

Consequence: We can recover B'_1 by using Weil pairing.

Case of MD-SIDH (1/2)

Sec. of MD-SIDH reduces to of M-SIDH under SIDH attacks.

Key : SIDH attacks also work on non-cyclic isogenies.

Recall: $\deg \phi_B = B' | B$, TP are scaled by $\beta \in \mathbb{Z}/B\mathbb{Z}$.
Denote the square free part of B' by B'_1.

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

$$\begin{array}{rccc} \Phi : & (\mathbb{Z}/2\mathbb{Z})^t & \longrightarrow & (\mathbb{Z}/2\mathbb{Z})^t \\ & (b_1, \ldots, b_t) & \longmapsto & (\chi_1(N_1), \ldots, \chi_t(N_t)) \end{array}$$

where $N_i := q_1^{b_1} \cdots q_t^{b_t} \pmod{\ell_i^{a_i}}$.

Claims:

- The image of $\Phi \leftrightarrow$ Information of B'_1 leaked by Weil pairing
- Φ is almost injective.

Consequence: We can recover B'_1 by using Weil pairing.

Case of MD-SIDH (2/2)

Assume that we know B_1'. Set $B_0 = \max\{n \mid n|B, n^2 B_1' \leq B\}$.
Then $\exists \beta_0$, divisor of B, $N_B := B_0^2 B_1' = \beta_0^2 B' \leq B$.

Set $\phi_0 = [\beta_0] \circ \phi_B$, then $\deg(\phi_0) = N_B$ is known.

$$[\beta]\phi_B(P) = [(\beta\beta_0^{-1}) \cdot \beta_0]\phi_B(P) = [\beta\beta_0^{-1}]\phi_0(P)$$
$$[\beta]\phi_B(Q) = [(\beta\beta_0^{-1}) \cdot \beta_0]\phi_B(Q) = [\beta\beta_0^{-1}]\phi_0(Q)$$

Set $\beta' = \beta\beta_0^{-1} \mod A$.

$(P, Q, [\beta]\phi_B(P), [\beta]\phi_B(Q))$ with B_1' (MD-SIDH)

$||$

$(P, Q, [\beta']\phi_0(P), [\beta']\phi_0(Q))$ with $\deg \phi_0 = N_B$ (M-SIDH)

Consequence: We can transform an MD-SIDH instance into an M-SIDH instance, and apply previous attacks.

Case of MD-SIDH (2/2)

Assume that we know B_1'. Set $B_0 = \max\{n \mid n|B, n^2 B_1' \leq B\}$.
Then $\exists \beta_0$, divisor of B, $N_B := B_0^2 B_1' = \beta_0^2 B' \leq B$.

Set $\phi_0 = [\beta_0] \circ \phi_B$, then $\deg(\phi_0) = N_B$ is known.

$$[\beta]\phi_B(P) = [(\beta\beta_0^{-1}) \cdot \beta_0]\phi_B(P) = [\beta\beta_0^{-1}]\phi_0(P)$$
$$[\beta]\phi_B(Q) = [(\beta\beta_0^{-1}) \cdot \beta_0]\phi_B(Q) = [\beta\beta_0^{-1}]\phi_0(Q)$$

Set $\beta' = \beta\beta_0^{-1} \mod A$.

$(P, Q, [\beta]\phi_B(P), [\beta]\phi_B(Q))$ with B_1' (MD-SIDH)

||

$(P, Q, [\beta']\phi_0(P), [\beta']\phi_0(Q))$ with $\deg \phi_0 = N_B$ (M-SIDH)

Consequence: We can transform an MD-SIDH instance into an M-SIDH instance, and apply previous attacks.

Case of MD-SIDH (2/2)

Assume that we know B_1'. Set $B_0 = \max\{n \mid n|B, n^2 B_1' \leq B\}$.
Then $\exists \beta_0$, divisor of B, $N_B := B_0^2 B_1' = \beta_0^2 B' \leq B$.

Set $\phi_0 = [\beta_0] \circ \phi_B$, then $\deg(\phi_0) = N_B$ is known.

$$
\left|\begin{array}{l}
[\beta]\phi_B(P) = [(\beta\beta_0^{-1}) \cdot \beta_0]\phi_B(P) = [\beta\beta_0^{-1}]\phi_0(P) \\
[\beta]\phi_B(Q) = [(\beta\beta_0^{-1}) \cdot \beta_0]\phi_B(Q) = [\beta\beta_0^{-1}]\phi_0(Q)
\end{array}\right.
$$

Set $\beta' = \beta\beta_0^{-1} \mod A$.

$$
\begin{array}{c}
(P, Q, [\beta]\phi_B(P), [\beta]\phi_B(Q)) \text{ with } B_1' \text{ (MD-SIDH)} \\
|| \\
(P, Q, [\beta']\phi_0(P), [\beta']\phi_0(Q)) \text{ with } \deg\phi_0 = N_B \text{ (M-SIDH)}
\end{array}
$$

Consequence: We can transform an MD-SIDH instance into an M-SIDH instance, and apply previous attacks.

Parameters size

Parameter selection:

- $A = \prod_{i=1}^{t} \ell_i$ s.t. $t - t' \geq \lambda$ where $\prod_{i=t'}^{t} \ell_i > \sqrt{A}$ (t is at least 2λ)
- $\mathrm{End}(E_0)$ unknown

AES	NIST	p (in bits)	secret key	public key
128	level 1	5911	$\approx$ 369 bytes	4434 bytes
192	level 3	9382	$\approx$ 586 bytes	7037 bytes
256	level 5	13000	$\approx$ 812 bytes	9750 bytes

Summary

Summary

Torsion points were there to make SIDH work.

But today, they killed SIDH.

Two countermeasure ideas were suggested and analysed: M-SIDH and MD-SIDH.

Outcome of the analysis: field characteristic must be at least ≈ 6000 bits !

Summary

Torsion points were there to make SIDH work.

But today, they killed SIDH.

Two countermeasure ideas were suggested and analysed: M-SIDH and MD-SIDH.

Outcome of the analysis: field characteristic must be at least ≈ 6000 bits !

Summary

Torsion points were there to make SIDH work.

But today, they killed SIDH.

Two countermeasure ideas were suggested and analysed: M-SIDH and MD-SIDH.

Outcome of the analysis: field characteristic must be at least ≈ 6000 bits !

Thank you for listening! Any questions?