On the countermeasures to the higher genus torsion point attacks on SIDH

Tako Boris Fouotsa, LASEC-EPFL

IRMAR, Rennes, December 2nd, 2022
Outline

Generalities and SIDH

Torsion point attacks

Countermeasures

Analysis of the countermeasures

Summary
Generalities and SIDH
Key agreement

Two parties: Alice (red) and Bob (blue)

Aim: share the same key (bit string, integer, ...)

Obstacle: they are far away from each other, internet is not safe.

Solution: Diffie-Hellman key agreement.
Both parties agree on group $G = \langle g \rangle$ of prime order $p$.

$$g^a \rightarrow A = g^a$$

$$b \downarrow \quad \text{and} \quad \downarrow b$$

$$B = g^b \rightarrow A^b = B^a = g^{ab}$$
Key agreement

Two parties: Alice (red) and Bob (blue)
Aim: share the same key (bit string, integer, ...)
Obstacle: they are far away from each other, internet is not safe.

Solution: Diffie-Hellman key agreement.
Both parties agree on group $G = \langle g \rangle$ of prime order $p$.

$$g^A = g^a, \quad B = g^b$$

$A^b = B^a = g^{ab}$
Key agreement

Two parties: Alice (red) and Bob (blue)
Aim: share the same key (bit string, integer, ...)
Obstacle: they are far away from each other, internet is not safe.
Solution: Diffie-Hellman key agreement.
Both parties agree on group $G = \langle g \rangle$ of prime order $p$.

\[
g^a \quad \rightarrow \quad A = g^a
\]
\[
B = g^b \quad \rightarrow \quad A^b = B^a = g^{ab}
\]
Key agreement

Two parties: Alice (red) and Bob (blue)

Aim: share the same key (bit string, integer, ...)

Obstacle: they are far away from each other, internet is not safe.

Solution: Diffie-Hellman key agreement.

Both parties agree on group $G = \langle g \rangle$ of prime order $p$.

\[ g^a \quad A = g^a \]

\[ b \quad B = g^b \]

\[ A^b = B^a = g^{ab} \]
Two parties: Alice (red) and Bob (blue)

Aim: share the same key (bit string, integer, ...)

Obstacle: they are far away from each other, internet is not safe.

Solution: Diffie-Hellman key agreement.
Both parties agree on group \( G = \langle g \rangle \) of prime order \( p \).

\[
g^A = g^a \\
B = g^b \\
A^b = B^a = g^{ab}
\]
Two parties: Alice (red) and Bob (blue)
Aim: share the same key (bit string, integer, ...)
Obstacle: they are far away from each other, internet is not safe.
Solution: Diffie-Hellman key agreement.
Both parties agree on group $G = \langle g \rangle$ of prime order $p$.

\[
g \rightarrow A = g^a
\]

\[
b \rightarrow B = g^b
\]

\[
A^b = B^a = g^{ab}
\]
Key agreement

Break the protocol: recover the shared key by spying on the internet (or channel).

CDH: Given \( g, p, A = g^a \) and \( B = g^b \), find \( g^{ab} \).

DL: Given \( g, p \) and \( A = g^a \), find \( a \).

Hard to break using classical computer

Easy to break with quantum computer
Key agreement

Break the protocol: recover the shared key by spying on the internet (or channel).

**CDH:** Given \( g, p, A = g^a \) and \( B = g^b \), find \( g^{ab} \).

**DL:** Given \( g, p \) and \( A = g^a \), find \( a \).

Hard to break using classical computer

Easy to break with quantum computer
Key agreement

Break the protocol: recover the shared key by spying on the internet (or channel).

**CDH:** Given $g, p, A = g^a$ and $B = g^b$, find $g^{ab}$.

**DL:** Given $g, p$ and $A = g^a$, find $a$.

Hard to break using classical computer

Easy to break with quantum computer
Post-quantum Cryptography

**Post-Quantum**: hard for both classical and quantum computers.

**Lattices, Codes, Isogenies, Multivariate equations, Hash Functions, ...**

**Isogeny-based Cryptography:**

- Very compact keys
- Offers a good replacement for Diffie-Hellman (NIKE)

But:

- Relatively slow
- Young field
Post-quantum Cryptography

**Post-Quantum**: hard for both classical and quantum computers.

**Lattices, Codes, Isogenies, Multivariate equations, Hash Functions, ...**

Isogeny-based Cryptography:

- Very compact keys
- Offers a good replacement for Diffie-Hellman (NIKE)

But:

- Relatively slow
- Young field
Post-quantum Cryptography

Post-Quantum: hard for both classical and quantum computers.

Lattices, Codes, Isogenies, Multivariate equations, Hash Functions, ...

Isogeny-based Cryptography:

- Very compact keys
- Offers a good replacement for Diffie-Hellman (NIKE)

But:

- Relatively slow
- Young field
Elliptic curves: $E : y^2 = x^3 + Ax + B$, are abelian groups.

Isogenies: rational maps between elliptic curves, that are group morphims. Degree := size of the kernel (separable isogenies)

DH with isogenies:

$$E_0 \xrightarrow{\phi_A} E_A = \text{Im} (\phi_A)$$

$$E_B = \text{Im} (\phi_B) \xrightarrow{\phi_A} E_{AB}$$
Elliptic curves: $E : y^2 = x^3 + Ax + B$, are abelian groups.

Isogenies: rational maps between elliptic curves, that are group morphims. Degree := size of the kernel (separable isogenies)

DH with isogenies:

\[
\begin{align*}
E_0 &\xrightarrow{\phi_A} E_A = \text{Im}(\phi_A) \\
E_B = \text{Im}(\phi_B) &\xrightarrow{\phi_B} E_B = \text{Im}(\phi_B) \\
E_A &\xrightarrow{\phi_B} E_{AB} \xrightarrow{\phi_A} E_{AB} \\
\end{align*}
\]
Diffie-Hellman with isogenies

Elliptic curves: $E : y^2 = x^3 + Ax + B$, are abelian groups.

Isogenies: rational maps between elliptic curves, that are group morphisms. Degree := size of the kernel (separable isogenies)

DH with isogenies:

$$
\begin{align*}
E_0 &\xrightarrow{\phi_A} E_A = \text{Im}(\phi_A) \\
E_B = \text{Im}(\phi_B) &\xrightarrow{\phi_B} E_{AB} \\
E_A &\xleftarrow{\phi_B} E_{AB} \\
\end{align*}
$$
Elliptic curves: \( E : y^2 = x^3 + Ax + B \), are abelian groups.

Isogenies: rational maps between elliptic curves, that are group morphisms. Degree := size of the kernel (separable isogenies)

DH with isogenies:

\[
\begin{align*}
E_0 & \xrightarrow{\phi_A} E_A = \text{Im}(\phi_A) \\
E_B = \text{Im}(\phi_B) & \xrightarrow{\phi_B} E_{AB} \\
\end{align*}
\]
Elliptic curves: $E : y^2 = x^3 + Ax + B$, are abelian groups.

Isogenies: rational maps between elliptic curves, that are group morphisms. Degree := size of the kernel (separable isogenies)

DH with isogenies:
Diffie-Hellman with isogenies

$E_0 \xrightarrow{\phi_A} E_A = \text{Im}(\phi_A)$

$E_B = \text{Im}(\phi_B) \xrightarrow{\phi_A'} E_{AB}$

Commutativity !!: use ordinary isogenies $\rightarrow$ CRS$^1$.

1. Inefficient
2. Quantum sub-exponential time (group actions)

$^1$Couveignes-Rostotsev-Stulbunov 1996/2006
Diffie-Hellman with isogenies

\[ E_0 \xrightarrow{\phi_A} E_A = \text{Im}(\phi_A) \]

\[ E_B = \text{Im}(\phi_B) \xrightarrow{\phi_A'} E_{AB} \]

Efficient and no quantum attack !!: use supersingular isogenies.

1. Do not commute !!
Efficient and no quantum attack !!: use supersingular isogenies.

1. Do not commute !!

Jao-De Feo 2011: Reveal torsion point images $\rightarrow$ SIDH
Diffie-Hellman with isogenies

\[ E_0, P_A, Q_A, P_B, Q_B \xrightarrow{\phi_A} E_A, \phi_A(P_B), \phi_A(Q_B) \]

\[ E_B, \phi_B(P_A), \phi_B(Q_A) \xrightarrow{\phi'_B} E_{AB} \]

Efficient and no quantum attack !!: use supersingular isogenies.

1. Do not commute !!

Jao-De Feo 2011: Reveal torsion point images → SIDH

Ambient field: \( \mathbb{F}_{p^2}, p = 2^a 3^b - 1 \).

\[ \deg \phi_A = 2^a \quad \deg \phi_B = 3^b \]

\[ E_0[2^a] = \langle P_A, Q_A \rangle, \quad E_0[3^b] = \langle P_B, Q_B \rangle \]
**Diffie-Hellman with isogenies**

\[ E_0, P_A, Q_A, P_B, Q_B \xrightarrow{\phi_A} E_A, \phi_A(P_B), \phi_A(Q_B) \]

\[ E_B, \phi_B(P_A), \phi_B(Q_A) \xrightarrow{\phi_A'} E_{AB} \]

**SSI-CDH:** Given \( E_0, P_A, Q_A, P_B, Q_B, E_A, \phi_A(P_B), \phi_A(Q_B), E_B, \phi_B(P_A) \) and \( \phi_B(Q_A) \), compute \( E_{AB} \).

**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 \( \phi_B \).
SIDH’s life span

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

GPST 2016: adaptive attack on SIDH, only countered by the FO transform

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 SIDH

CD-MM-R 2022, final shot: SIDH/SIKE is broken in seconds...

All these attacks exploit torsion point information !!

Non exhaustive list: BdQL+ 2019, ...
SIDH’s life span

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

GPST 2016: adaptive attack on SIDH, only countered by the FO transform

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 SIDH

CD-MM-R 2022, final shot: SIDH/SIKE is broken in seconds...

All these attacks exploit torsion point information!!

Non exhaustive list: BdQL+ 2019, ...
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 SIDH

CD-MM-R 2022, final shot: SIDH/SIKE is broken in seconds...

All these attacks exploit torsion point information !!

Non exhaustive list: BdQL+ 2019, ...
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,
dQKL+ 2021: improvement on Petit TPA, but SIDH still safe.
FP 2022: new adaptive attack on SIDH using TPA, no impact on SIDH
CD-MM-R 2022, final shot: SIDH/SIKE is broken in seconds...

All these attacks exploit torsion point information!!

Non exhaustive list: BdQL+ 2019, ...
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,
dQKL+ 2021: improvement on Petit TPA, but SIDH still safe.
FP 2022: new adaptive attack on SIDH using TPA, no impact on SIDH

CD-MM-R 2022, final shot: SIDH/SIKE is broken in seconds...

All these attacks exploit torsion point information!!

Non exhaustive list: BdQL+ 2019, ...
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,
dQKL+ 2021: improvement on Petit TPA, but SIDH still safe.
FP 2022: new adaptive attack on SIDH using TPA,
CD-MM-R 2022, final shot: SIDH/SIKE is broken in seconds...

All these attacks exploit torsion point information !!

Non exhaustive list: BdQL+ 2019, ...
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,
dQKL+ 2021: improvement on Petit TPA, but SIDH still safe.
FP 2022: new adaptive attack on SIDH using TPA,
CD-MM-R 2022, final shot: SIDH/SIKE is broken in seconds...

All these attacks exploit torsion point information !!

Non exhaustive list: BdQL+ 2019, ...
CD-MM-R attacks require:

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

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 if fixed, but the torsion point images are scaled by a secret scalar.

Current analysis: field characteristic \( \log_2 p \approx 6000 \), as oppose to \( \log_2 p \approx 434 \) in SIDH, for 128 bits of security.
Torsion point attacks
More facts about isogenies

\[ E/F_q: \text{n-torsion group } (p \nmid n) \]
\[ E[n] = \langle P, Q \rangle \sim \mathbb{Z}/n\mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z} \]

Supersingular curves:

- \( \text{End}(E) \sim \mathcal{O}_{\text{max}} \subset B_{p,\infty} \)
- defined over \( \mathbb{F}_{p^2} \) and \( E(\mathbb{F}_{p^2}) \sim \mathbb{Z}/(p \pm 1)\mathbb{Z} \oplus \mathbb{Z}/(p \pm 1)\mathbb{Z} \)

Dual d-isogeny: \( \varphi: E \rightarrow E' \iff \exists!* \hat{\varphi}: E' \rightarrow E \), such that \( \hat{\varphi} \circ \varphi = [d]_E \) and \( \varphi \circ \hat{\varphi} = [d]_{E'} \).

We have

\[ \ker \hat{\varphi} = \varphi(E[d]) \quad \text{and} \quad \ker \varphi = \hat{\varphi}(E'[d]). \]

Pairings and isogenies: \( \phi: E \rightarrow E', E[N] = \langle P, Q \rangle \), then
\[ e_N(\phi(P), \phi(Q)) = e_N(P, Q)^{\text{deg } \phi} \]
More facts about isogenies

$E/\mathbb{F}_q$: n-torsion group ($p \nmid n$)

$$E[n] = \langle P, Q \rangle \simeq \mathbb{Z}/n\mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z}$$

Supersingular curves:

- $\text{End}(E) \simeq \mathcal{O}_{\text{max}} \subset \mathcal{B}_{p,\infty}$
- defined over $\mathbb{F}_{p^2}$ and $E(\mathbb{F}_{p^2}) \simeq \mathbb{Z}/(p \pm 1)\mathbb{Z} \oplus \mathbb{Z}/(p \pm 1)\mathbb{Z}$

Dual $d$-isogeny: $\varphi : E \to E' \iff \exists!* \hat{\varphi} : E' \to E$, such that $\hat{\varphi} \circ \varphi = [d]_E$ and $\varphi \circ \hat{\varphi} = [d]_{E'}$.

We have

$$\ker \hat{\varphi} = \varphi(E[d]) \quad \text{and} \quad \ker \varphi = \hat{\varphi}(E'[d]).$$

Pairings and isogenies: $\phi : E \to E'$, $E[N] = \langle P, Q \rangle$, then

$$e_N(\phi(P), \phi(Q)) = e_N(P, Q)^{\deg \phi}$$
More facts about isogenies

\(E/F_q\): \(n\)-torsion group \((p \nmid n)\)

\[E[n] = \langle P, Q \rangle \simeq \mathbb{Z}/n\mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z}\]

Supersingular curves:

- \(\text{End}(E) \simeq \mathcal{O}_{\text{max}} \subset \mathcal{B}_p,\infty\)
- defined over \(\mathbb{F}_{p^2}\) and \(E(\mathbb{F}_{p^2}) \simeq \mathbb{Z}/(p \pm 1)\mathbb{Z} \oplus \mathbb{Z}/(p \pm 1)\mathbb{Z}\)

Dual \(d\)-isogeny: \(\varphi: E \to E' \iff \exists!^* \hat{\varphi}: E' \to E\), such that \(\hat{\varphi} \circ \varphi = [d]_E\) and \(\varphi \circ \hat{\varphi} = [d]_{E'}\).

We have

\[\ker \hat{\varphi} = \varphi(E[d]) \quad \text{and} \quad \ker \varphi = \hat{\varphi}(E'[d]).\]

Pairings and isogenies: \(\phi: E \to E', E[N] = \langle P, Q \rangle\), then

\[e_N(\phi(P), \phi(Q)) = e_N(P, Q)^{\deg \phi}\]
More facts about isogenies

\[ E/\mathbb{F}_q: \ n\text{-torsion group } (p \nmid n) \]
\[ E[n] = \langle P, Q \rangle \cong \mathbb{Z}/n\mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z} \]

Supersingular curves:

- \( \text{End}(E) \cong \mathcal{O}_{\text{max}} \subset \mathcal{B}_{p,\infty} \)
- defined over \( \mathbb{F}_{p^2} \) and \( E(\mathbb{F}_{p^2}) \cong \mathbb{Z}/(p \pm 1)\mathbb{Z} \oplus \mathbb{Z}/(p \pm 1)\mathbb{Z} \)

Dual d-isogeny: \( \varphi : E \rightarrow E' \iff \exists!* \hat{\varphi} : E' \rightarrow E \), such that \( \hat{\varphi} \circ \varphi = [d]_E \) and \( \varphi \circ \hat{\varphi} = [d]_{E'} \).

We have

\[ \ker \hat{\varphi} = \varphi(E[d]) \quad \text{and} \quad \ker \varphi = \hat{\varphi}(E'[d]). \]

Pairings and isogenies: \( \phi : E \rightarrow E', \ E[N] = \langle P, Q \rangle, \) then

\[ e_N(\phi(P), \phi(Q)) = e_N(P, Q)^{\deg \phi} \]
The framework

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

**Degree transformation:** define a map $\Gamma$ that can be used to transform $\phi$ to $\tau = \Gamma(\phi, \text{input})$ such that:

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

**The attack:** Given a suitable description of $\Gamma$,

- Use 2. and 3. to recover $\tau$
- Use 1. to derive $\phi$ from $\tau
Assumes that $\text{End}(E_0)$ is known. \textit{input} = $[\theta \in \text{End}(E_0), d \in \mathbb{Z}]$.

\[ \tau = \Gamma(\phi, \theta, d) := [d] + \phi \circ \theta \circ \hat{\phi} \]

s.t. $\deg \tau = B^2e$ with $e$ small.

1. Knowing $\tau = \Gamma(\phi, \text{input})$, one can recover $\phi$
2. $\tau$ can be evaluated on the $B$-torsion
3. $\tau$ can be recovered from its action on the $B$-torsion
Assumes that $\text{End}(E_0)$ is known. \textit{input} = $[\theta \in \text{End}(E_0), d \in \mathbb{Z}]$.

\[ \tau = \Gamma(\phi, \theta, d) := [d] + \phi \circ \theta \circ \hat{\phi} \]

s.t. \deg \tau = B^2 e \text{ with } e \text{ small.}

1. Knowing $\tau = \Gamma(\phi, \text{input})$, one can recover $\phi$
2. $\tau$ can be evaluated on the $B$-torsion
3. $\tau$ can be recovered from its action on the $B$-torsion
Assumes that $\text{End}(E_0)$ is known. \textit{input} $= [\theta \in \text{End}(E_0), d \in \mathbb{Z}]$. 

$$\tau = \Gamma(\phi, \theta, d) := [d] + \phi \circ \theta \circ \hat{\phi}$$

s.t. $\text{deg} \tau = B^2e$ with $e$ small.

1. Knowing $\tau = \Gamma(\phi, \text{input})$, one can recover $\phi$
2. $\tau$ can be evaluated on the $B$-torsion
3. $\tau$ can be recovered from its action on the $B$-torsion
Assumes that $\text{End}(E_0)$ is known. \textit{input} = $[\theta \in \text{End}(E_0), \, d \in \mathbb{Z}]$.

$$\tau = \Gamma(\phi, \theta, d) := [d] + \phi \circ \theta \circ \hat{\phi}$$

s.t. $\deg \tau = B^2 e$ with $e$ small.

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

$$\ker \hat{\phi} = \ast \ker(\tau - [d]) \cap E[A]$$
Assumes that $\text{End}(E_0)$ is known. \textit{input} = $[\theta \in \text{End}(E_0), d \in \mathbb{Z}]$.

$$\tau = \Gamma(\phi, \theta, d) := [d] + \phi \circ \theta \circ \hat{\phi}$$

s.t. $\text{deg} \tau = B^2e$ with $e$ small.

1. Knowing $\tau = \Gamma(\phi, \text{input})$, one can recover $\phi$.
2. $\tau$ can be evaluated on the $B$-torsion.
3. $\tau$ can be recovered from its action on the $B$-torsion.
Assumes that $\text{End}(E_0)$ is known. $\text{input} = [\theta \in \text{End}(E_0), d \in \mathbb{Z}]$.

$$\tau = \Gamma(\phi, \theta, d) := [d] + \phi \circ \theta \circ \hat{\phi}$$

s.t. $\deg \tau = B^2e$ with $e$ small.

1. Knowing $\tau = \Gamma(\phi, \text{input})$, one can recover $\phi$.

2. $\tau$ can be evaluated on the $B$-torsion.

3. $\tau$ can be recovered from its action on the $B$-torsion.
Assumes that $\text{End}(E_0)$ is known. \textit{input} = $[\theta \in \text{End}(E_0), d \in \mathbb{Z}]$.

$$\tau = \Gamma(\phi, \theta, d) := [d] + \phi \circ \theta \circ \hat{\phi}$$

s.t. $\deg \tau = B^2 e$ with $e$ small.

1. Knowing $\tau = \Gamma(\phi, \text{input})$, one can recover $\phi$

2. $\tau$ can be evaluated on the $B$-torsion

3. $\tau$ can be recovered from its action on the $B$-torsion

Requires: $B > pA$; while in SIDH $A \approx B \approx \sqrt{p}$. 
Assume $\phi : E_0 \to E_B$ has degree $B$ and the TP have order $A$. Set $a = A - B = a_1^2 + a_2^2 + a_3^2 + a_4^2$.

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

where

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

$$M = \begin{bmatrix} a_1 & -a_2 & -a_3 & -a_4 \\ a_2 & a_1 & a_4 & -a_3 \\ a_3 & -a_4 & a_1 & a_2 \\ a_4 & a_3 & -a_2 & a_1 \end{bmatrix}$$
Assume $\phi : E_0 \to E_B$ has degree $B$ and the TP have order $A$. Set $a = A - B = a_1^2 + a_2^2 + a_3^2 + a_4^2$.

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

Fact: $\tau$ has degree $B + a = A$

1. Knowing $\tau = \Gamma(\phi, \text{input})$, one can recover $\phi$
2. $\tau$ can be evaluated on the $A$-torsion
3. $\tau$ can be recovered from its action on the $A$-torsion
Assume $\phi : E_0 \longrightarrow E_B$ has degree $B$ and the TP have order $A$. Set $a = A - B = a_1^2 + a_2^2 + a_3^2 + a_4^2$.

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

Fact: $\tau$ has degree $B + a = A$

1. Knowing $\tau = \Gamma(\phi, \text{input})$, one can recover $\phi$

2. $\tau$ can be evaluated on the $A$-torsion

3. $\tau$ can be recovered from its action on the $A$-torsion
Assume $\phi : E_0 \longrightarrow E_B$ has degree $B$ and the TP have order $A$.
Set $a = A - B = a_1^2 + a_2^2 + a_3^2 + a_4^2$.

$$
\tau = \Gamma(\phi, a) := \begin{bmatrix}
\alpha_0 & \hat{\phi}I_{d_4} \\
-\phi I_{d_4} & \hat{\alpha}_B
\end{bmatrix} \in \text{End}(E_0^4 \times E_B^4)
$$

Fact: $\tau$ has degree $B + a = A$

1. Knowing $\tau = \Gamma(\phi, \text{input})$, one can recover $\phi$
2. $\tau$ can be evaluated on the $A$-torsion
3. $\tau$ can be recovered from its action on the $A$-torsion
Assume $\phi : E_0 \longrightarrow E_B$ has degree $B$ and the TP have order $A$. Set $a = A - B = a_1^2 + a_2^2 + a_3^2 + a_4^2$.

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

Fact: $\tau$ has degree $B + a = A$

1. Knowing $\tau = \Gamma(\phi, \text{input})$, one can recover $\phi$
2. $\tau$ can be evaluated on the $A$-torsion
3. $\tau$ can be recovered from its action on the $A$-torsion
Assume $\phi : E_0 \rightarrow E_B$ has degree $B$ and the TP have order $A$. Set $a = A - B = a_1^2 + a_2^2 + a_3^2 + a_4^2$.

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

Fact: $\tau$ has degree $B + a = A$

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

Runs in polynomial time when $A^2 > B$ !!
Breaks SIDH/SIKE/SETA/...
Countermeasures
Masked degree SIDH

\[ E_0, P_A, Q_A, P_B, Q_B \xrightarrow{\phi_A} E_A, \phi_A(P_B), \phi_A(Q_B) \]

\[ E_B, \phi_B(P_A), \phi_B(Q_A) \xrightarrow{\phi_A'} E_{AB} \]
Masked degree SIDH

\[ \begin{align*}
E_0, P_A, Q_A, P_B, Q_B & \xrightarrow{\phi_A} E_A, \phi_A(P_B), \phi_A(Q_B) \\
E_B, \phi_B(P_A), \phi_B(Q_A) & \xrightarrow{\phi_A'} E_{AB}
\end{align*} \]

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

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

\[ \deg \phi_A = A', \quad A' | A, \quad \deg \phi_B = B', \quad B' | B. \]

\[ E_0[A] = \langle P_A, Q_A \rangle, \quad E_0[B] = \langle P_B, Q_B \rangle \]
Masked degree SIDH

\[ E_0, P_A, Q_A, P_B, Q_B \xrightarrow{\phi_A} E_A, [\alpha]\phi_A(P_B), [\alpha]\phi_A(Q_B) \]

\[ E_B, [\beta]\phi_B(P_A), [\beta]\phi_B(Q_A) \xrightarrow{\phi_A'} E_{AB} \]

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

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

\( \deg \phi_A = A', \quad A'|A, \quad \deg \phi_B = B', \quad B'|B. \)

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

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

\[
\begin{array}{c}
E_0, P_A, Q_A, P_B, Q_B \\
\phi_A \\
E_A, [\alpha] \phi_A(P_B), [\alpha] \phi_A(Q_B) \\
\phi_B \\
E_B, [\beta] \phi_B(P_A), [\beta] \phi_B(Q_A) \\
\phi_A' \\
E_{AB}
\end{array}
\]

Ambient field: \( \mathbb{F}_{p^2}, p = \ell_1 \cdots \ell_\lambda q_1 \cdots q_\lambda f - 1 \)

\[
A := \prod_{i=1}^\lambda \ell_i \quad B := \prod_{i=1}^\lambda q_i, \quad A \approx B.
\]

\[
\deg \phi_A = A, \quad \deg \phi_B = B.
\]

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

Hide the exact TP images: \( \alpha \in \mu_2(\mathbb{Z}/B\mathbb{Z}) \quad \beta \in \mu_2(\mathbb{Z}/A\mathbb{Z}) \)
Analysis of the countermeasures
CD-MM-R attack : works when $A^2 > B$.

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

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

Guessing the exact torsion point: $O(2^{\lambda-t})$

**Consequence:** $A$ and $B$ must have at least $2\lambda$ distinct prime factors each.
Given a small $\theta \in \text{End}(E_0)$, eliminate the scalar $\beta$ in M-SIDH:

\[
\begin{align*}
\theta & \quad E_0 \quad [\beta] \circ \phi_B \\
[\beta] \circ \phi_B \quad & \quad E \\
\hat{\phi}_B \quad & \quad \tau
\end{align*}
\]

With respect to the $A$ torsion, we have:

\[
([\beta] \circ \phi_B) \circ \theta \circ ([\beta] \circ \phi_B) = [\beta^2] \circ \phi_B \circ \theta \circ \hat{\phi}_B \equiv \phi_B \circ \theta \circ \hat{\phi}_B =: \tau.
\]

\[
\deg \tau = B^2 \deg \theta.
\]

CD-MM-R on $\tau$ requires:

\[
\sqrt{\deg \tau} = B \sqrt{\deg \theta} \approx B \quad \text{(for small $\theta$)}.
\]

**Consequence:** No small endomorphisms in $E_0$, if possible, no known endomorphism at all.
Given a small $\theta \in \text{End}(E_0)$, eliminate the scalar $\beta$ in M-SIDH:

$$E_0 \xrightarrow{[\beta] \phi_B} E$$

With respect to the $A$ torsion, we have:

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

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

CD-MM-R on $\tau$ requires: $\sqrt{\deg \tau} = B \sqrt{\deg \theta} \approx B$ (for small $\theta$).

Consequence: No small endomorphisms in $E_0$, if possible, no known endomorphism at all.
Given a small $\theta \in \text{End}(E_0)$, eliminate the scalar $\beta$ in M-SIDH:

Given a small $\theta \in \text{End}(E_0)$, eliminate the scalar $\beta$ in M-SIDH:

With respect to the $A$ torsion, we have:

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

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

CD-MM-R on $\tau$ requires: $\sqrt{\deg \tau} = B \sqrt{\deg \theta} \approx B$ (for small $\theta$).

Consequence: No small endomorphisms in $E_0$, if possible, no known endomorphism at all.
Given a small $\theta \in \text{End}(E_0)$, eliminate the scalar $\beta$ in M-SIDH:

\[
\theta \quad \xrightarrow{\phi_B \beta} \quad [\beta] \phi_B \quad \xrightarrow{\theta \hat{\phi}_B} \quad E_0 \quad \xrightarrow{\phi_B \beta} \quad [\beta] \hat{\phi}_B \quad \xrightarrow{\theta} \quad E
\]

With respect to the $A$ torsion, we have:

\[
([\beta] \phi_B) \circ \theta \circ ([\beta] \phi_B) = [\beta^2] \circ \phi_B \circ \theta \circ \hat{\phi}_B \equiv \phi_B \circ \theta \circ \hat{\phi}_B =: \tau.
\]

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

CD-MM-R on $\tau$ requires: $\sqrt{\deg \tau} = B \sqrt{\deg \theta} \approx B$ (for small $\theta$).

**Consequence:** No small endomorphisms in $E_0$, if possible, no known endomorphism at all.
Case of MD-SIDH: recovering the square free part

Recall: $\deg \phi_B = B'|B$, TP are scaled by $\beta \in \mathbb{Z}/B\mathbb{Z}$.

Pairings are used to recover $\beta^2 B' \mod A$. Define:

$$\chi_i : (\mathbb{Z}/\ell_i^{a_i}\mathbb{Z})^\times \rightarrow \mathbb{Z}/2\mathbb{Z}$$

$$x \mapsto \begin{cases} 
1 & \text{if } x \text{ is a quad. residue modulo } \ell_i^{b_i}; \\
0 & \text{if not.}
\end{cases}$$

$$\Phi : D(q_1 \cdots q_t) \rightarrow (\mathbb{Z}/2\mathbb{Z})^t$$

$$N \mapsto (\chi_1(N), \ldots, \chi_t(N))$$

Claims:

- We can evaluate $\Phi$ on the square free part of $B'$
- $\Phi$ is almost injective.

Consequence: We can recover the square free part $B'_1$ of $B'$.  

16/21
Case of MD-SIDH: recovering the square free part

Recall: \( \deg \phi_B = B'|B \), TP are scaled by \( \beta \in \mathbb{Z}/B\mathbb{Z} \).

Pairings are used to recover \( \beta^2 B' \mod A \). Define:

\[
\chi_i: \left( \mathbb{Z}/\ell_i^{a_i}\mathbb{Z} \right)^\times \rightarrow \mathbb{Z}/2\mathbb{Z} \quad x \mapsto \begin{cases} 1 & \text{if } x \text{ is a quad. residue modulo } \ell_i^{b_i}; \\ 0 & \text{if not.} \end{cases}
\]

\[
\Phi: D(q_1 \cdots q_t) \rightarrow (\mathbb{Z}/2\mathbb{Z})^t \quad N \mapsto (\chi_1(N), \ldots, \chi_t(N))
\]

Claims:

- We can evaluate \( \Phi \) on the square free part of \( B' \)
- \( \Phi \) is almost injective.

Consequence: We can recover the square free part \( B'_1 \) of \( B' \).
Case of MD-SIDH: recovering the square free part

Recall: $\deg \phi_B = B'|B$, TP are scaled by $\beta \in \mathbb{Z}/B\mathbb{Z}$.

Pairings are used to recover $\beta^2 B' \mod A$. Define:

$$\chi_i: (\mathbb{Z}/\ell_i^{a_i}\mathbb{Z})^\times \rightarrow \mathbb{Z}/2\mathbb{Z}$$

$$x \mapsto \begin{cases} 1 & \text{if } x \text{ is a quad. residue modulo } \ell_i^{b_i}; \\ 0 & \text{if not.} \end{cases}$$

$$\Phi: D(q_1 \cdots q_t) \rightarrow (\mathbb{Z}/2\mathbb{Z})^t$$

$$N \mapsto (\chi_1(N), \ldots, \chi_t(N))$$

Claims:

- We can evaluate $\Phi$ on the square free part of $B'$
- $\Phi$ is almost injective.

Consequence: We can recover the square free part $B'_1$ of $B'$. 
Case of MD-SIDH: recovering the square free part

Recall: \( \deg \phi_B = B' | B \), TP are scaled by \( \beta \in \mathbb{Z}/B\mathbb{Z} \).

Pairings are used to recover \( \beta^2 B' \mod A \). Define:

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

\[
\Phi : D(q_1 \cdots q_t) \longrightarrow (\mathbb{Z}/2\mathbb{Z})^t \\
N \longmapsto (\chi_1(N), \ldots, \chi_t(N))
\]

Claims:

- We can evaluate \( \Phi \) on the square free part of \( B' \)
- \( \Phi \) is almost injective.

Consequence: We can recover the square free part \( B'_1 \) of \( B' \).
Case of MD-SIDH: reduction to M-SIDH

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

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

Set $\beta_1' = \beta_0^2B' \cdot (\beta^2B')^{-1} \mod A = (\beta_0 \cdot \beta^{-1})^2 \mod A$.

Sampling $\beta_1'$ in $\sqrt{\beta_1^2} \mod A$, then $\beta_1' = \mu \beta_1$ where $\mu \in \mu_2(\mathbb{Z}/AZ)$.

\[ [\beta_1']P' = [\mu \cdot \beta_1]P' = [\mu]\phi_0(P) \]
\[ [\beta_1']Q' = [\mu \cdot \beta_1]P' = [\mu]\phi_0(Q) \]

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

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.

$$
\begin{align*}
P' &= [\beta] \phi(P) = ((\beta \beta_0^{-1}) \cdot \beta_0) \phi(P) = [\beta \beta_0^{-1}] \phi_0(P) \\
Q' &= [\beta] \phi(Q) = ((\beta \beta_0^{-1}) \cdot \beta_0) \phi(Q) = [\beta \beta_0^{-1}] \phi_0(Q)
\end{align*}
$$

Compute: $\beta_1^2 = \beta_0^2 B' \cdot (\beta^2 B')^{-1} \mod A = (\beta_0 \cdot \beta^{-1})^2 \mod A$.

Sampling $\beta'_1$ in $\sqrt{\beta_1^2} \mod A$, then $\beta'_1 = \mu \beta_1$ where $\mu \in \mu_2(\mathbb{Z}/A\mathbb{Z})$.

$$
\begin{align*}
[\beta'_1] P' &= [\mu \cdot \beta_1] P' = [\mu] \phi_0(P) \\
[\beta'_1] Q' &= [\mu \cdot \beta_1] P' = [\mu] \phi_0(Q)
\end{align*}
$$

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

Assume that we know $B_1'$. Set $B_0 = \max\{n \mid n \mid B, n^2 B_1' \leq B\}$. 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.

$$
\begin{align*}
P' &= [\beta] \phi(P) = [(\beta \beta_0^{-1}) \cdot \beta_0] \phi(P) = [\beta \beta_0^{-1}] \phi_0(P) \\
Q' &= [\beta] \phi(Q) = [(\beta \beta_0^{-1}) \cdot \beta_0] \phi(Q) = [\beta \beta_0^{-1}] \phi_0(Q)
\end{align*}
$$

Compute: $\beta_1^2 = \beta_0^2 B' \cdot (\beta^2 B')^{-1} \mod A = (\beta_0 \cdot \beta^{-1})^2 \mod A$.

Sampling $\beta_1'$ in $\sqrt{\beta_1^2} \mod A$, then $\beta_1' = \mu \beta_1$ where $\mu \in \mu_2(\mathbb{Z}/AZ)$.

$$
\begin{align*}
[\beta_1'] P' &= [\mu \cdot \beta_1] P' = [\mu] \phi_0(P) \\
[\beta_1'] Q' &= [\mu \cdot \beta_1] P' = [\mu] \phi_0(Q)
\end{align*}
$$

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

Assume that we know $B_1'$. Set $B_0 = \max\{n \mid n\mid B, n^2 B_1' \leq B\}$. 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.

$$
\begin{align*}
P' &= [\beta] \phi(P) = [(\beta \beta_0^{-1}) \cdot \beta_0] \phi(P) = [\beta \beta_0^{-1}] \phi_0(P) \\
Q' &= [\beta] \phi(Q) = [(\beta \beta_0^{-1}) \cdot \beta_0] \phi(Q) = [\beta \beta_0^{-1}] \phi_0(Q)
\end{align*}
$$

Compute: $\beta_1^2 = \beta_0^2 B' \cdot (\beta^2 B')^{-1} \mod A = (\beta_0 \cdot \beta^{-1})^2 \mod A$.

Sampling $\beta_1'$ in $\sqrt{\beta_1^2} \mod A$, then $\beta_1' = \mu \beta_1$ where $\mu \in \mu_2(\mathbb{Z}/A\mathbb{Z})$.

$$
\begin{align*}
[\beta_1'] P' &= [\mu \cdot \beta_1] P' = [\mu] \phi_0(P) \\
[\beta_1'] Q' &= [\mu \cdot \beta_1] P' = [\mu] \phi_0(Q)
\end{align*}
$$

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

- GPST and the F-Petit adaptive attacks on M-SIDH: straightforward.
- FP adaptive attack on MD-SIDH: uses the reduction of MD-SIDH to M-SIDH.
- GPST on MD-SIDH: not straightforward, but possible.

Parameter selection:

- $n|B$, $n > \sqrt{B} \rightarrow \lambda$ odd prime factors.
- $End(E_0)$ unknown

<table>
<thead>
<tr>
<th>AES</th>
<th>NIST</th>
<th>$p$ (in bits)</th>
<th>secret key</th>
<th>public key</th>
</tr>
</thead>
<tbody>
<tr>
<td>128</td>
<td>level 1</td>
<td>5911</td>
<td>$\approx 369$ bytes</td>
<td>4434 bytes</td>
</tr>
<tr>
<td>192</td>
<td>level 3</td>
<td>9382</td>
<td>$\approx 586$ bytes</td>
<td>7037 bytes</td>
</tr>
<tr>
<td>256</td>
<td>level 5</td>
<td>13000</td>
<td>$\approx 812$ bytes</td>
<td>9750 bytes</td>
</tr>
</tbody>
</table>
Two days ago on eprint: Applying Castryck-Decru Attack on the Masked Torsion Point Images SIDH variant

Successfully applies CD attack on M-SIDH with SIDH primes.

Claims that it will also be successfull with M-SIDH primes.

Success rate of CD attack on M-SIDH with SIDH primes:
Expected : $1/2$  
Observed : $1$.

Not an attack: it is due to the implementation of CD attack and some particularities of the $2^a$ torsion.
(See twitter: Peter Kutas//Benjamin Wesolowski//Luca De Feo//F.)
Two days ago on eprint: Applying Castryck-Decru Attack on the Masked Torsion Point Images SIDH variant

Successfully applies CD attack on M-SIDH with SIDH primes.

Claims that it will also be successful with M-SIDH primes.

Success rate of CD attack on M-SIDH with SIDH primes:
Expected: $\frac{1}{2}$  \hspace{1cm} Observed: 1.

Not an attack: it is due to the implementation of CD attack and some particularities of the $2^a$ torsion.

(See twitter: Peter Kutas//Benjamin Wesolowski//Luca De Feo//F.)
Two days ago on eprint: **Applying Castryck-Decru Attack on the Masked Torsion Point Images SIDH variant**

Successfully applies CD attack on M-SIDH with SIDH primes.

Claims that it will also be successful with M-SIDH primes.

Success rate of CD attack on M-SIDH with SIDH primes:

**Expected**: $1/2$  
**Observed**: $1$.  

Not an attack: it is due to the implementation of CD attack and some particularities of the $2^a$ torsion.  
(See twitter: Peter Kutas//Benjamin Wesolowski//Luca De Feo//F.)
Two days ago on eprint: Applying Castryck-Decru Attack on the Masked Torsion Point Images SIDH variant

Successfully applies CD attack on M-SIDH with SIDH primes.

Claims that it will also be successful with M-SIDH primes.

Success rate of CD attack on M-SIDH with SIDH primes:

Expected : $1/2$  
Observed : $1$.

Not an attack: it is due to the implementation of CD attack and some particularities of the $2^a$ torsion.

(See twitter: Peter Kutas//Benjamin Wesolowski//Luca De Feo//F.)
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 $\approx 6000$ bits!

Still vulnerable to adaptive attacks. Require FO to achieve IND-CCA security.

More details here and there! Upcoming eprint with the updates...
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 $\approx 6000$ bits!

Still vulnerable to adaptive attacks. Require FO to achieve IND-CCA security.

More details here and there! Upcoming eprint with the updates...
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 $\approx 6000$ bits!

Still vulnerable to adaptive attacks. Require FO to achieve IND-CCA security.

More details here and there! Upcoming eprint with the updates...
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 \( \approx 6000 \) bits!

Still vulnerable to adaptive attacks. Require FO to achieve IND-CCA security.

More details here and there! Upcoming eprint with the updates...
Happy to discuss your comments and questions !!!