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

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.

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.

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.

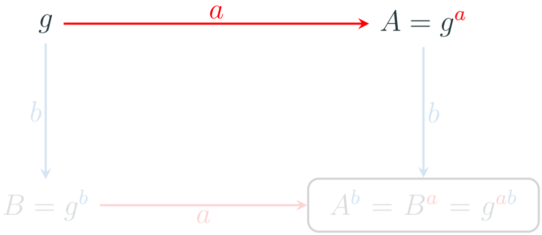
Key agreement

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.



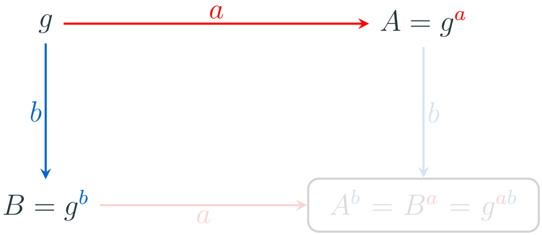
Key agreement

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.



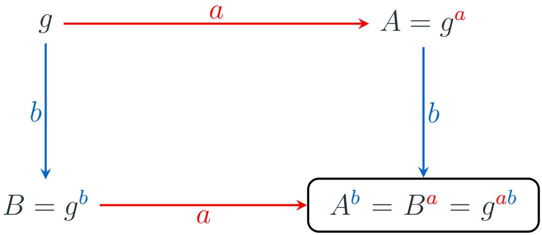
Key agreement

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

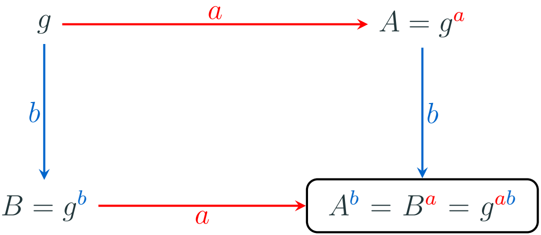
Aim: share the same key (bit string, integer, ...)

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.



Key agreement



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

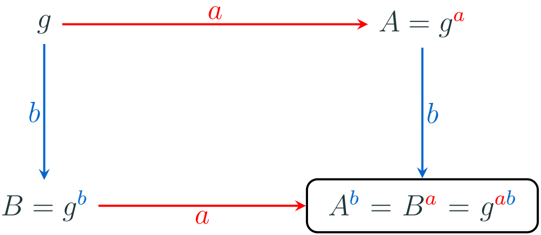
CDH: Given g, p, $A = g^a$ and $B = g^b$, find g^{ab}.

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 chanel).

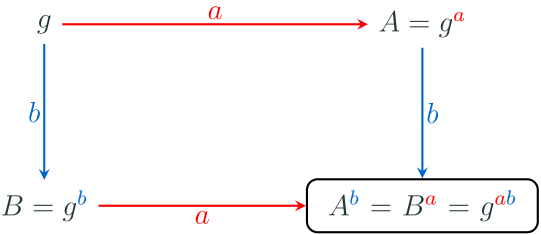
CDH: Given g, p, $A = g^a$ and $B = g^b$, find g^{ab}.

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 chanel).

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: 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: 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: 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

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 morphims. Degree := size of the kernel (separable isogenies)

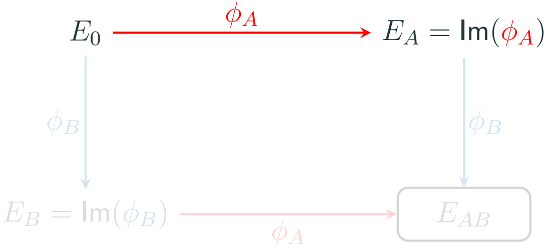
DH with isogenies:

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 morphims. Degree := size of the kernel (separable isogenies)

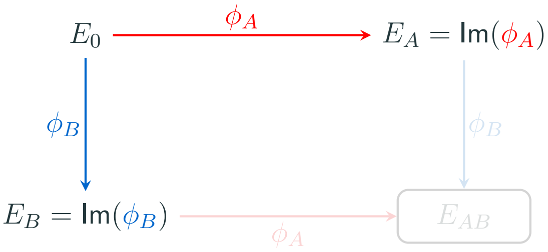
DH with isogenies:



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:

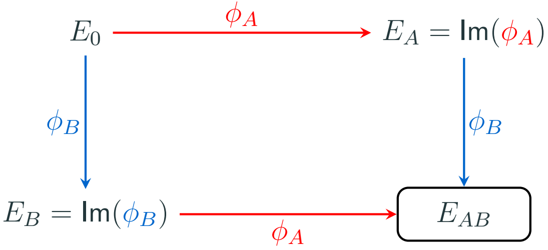


Diffie-Hellman with isogenies

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

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

DH with isogenies:

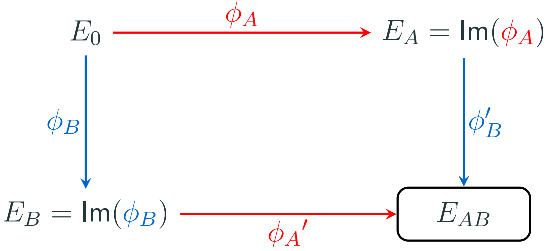


Diffie-Hellman with isogenies

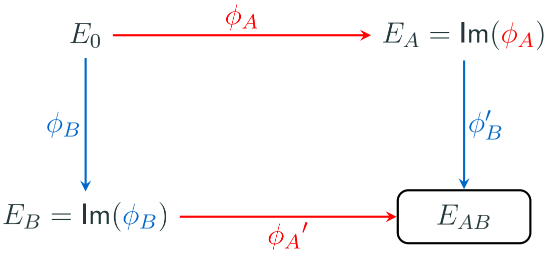
Elliptic curves: $E : y^2 = x^3 + Ax + B$, are abelian groups.

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

DH with isogenies:



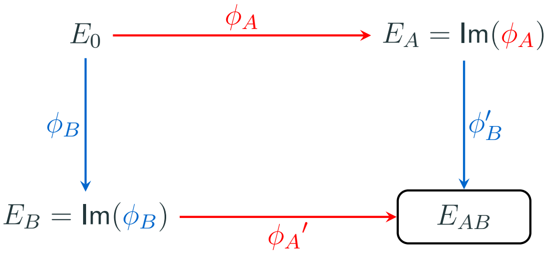
Diffie-Hellman with isogenies



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

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

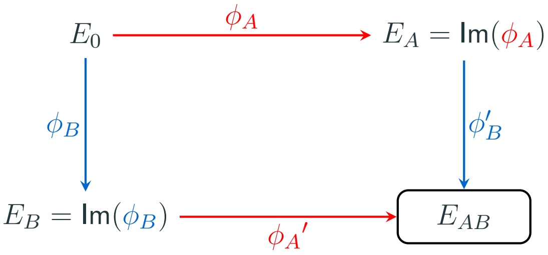
[1] Couveignes-Rostotsev-Stulbunov 1996/2006



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

1. Do not commute !!

Diffie-Hellman with isogenies

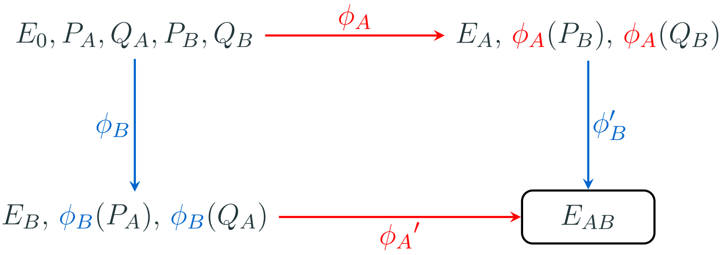


Efficient and no quantum attack !!: use supersingular isogenies.

1. ~~Do not commute !!~~

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

Diffie-Hellman with isogenies



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

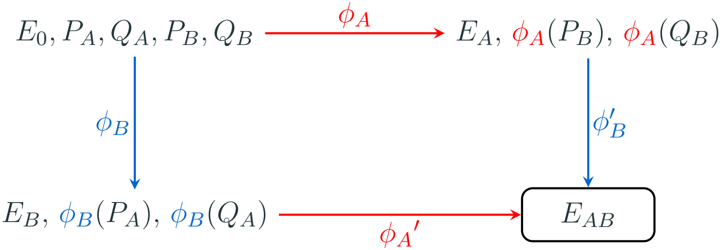
1. ~~Do not commute !!~~

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

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

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

Diffie-Hellman with isogenies



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 ϕ_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, ...

Countermeasures

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

$E/\mathbb{F}_q$: 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:

- $\mathrm{End}(E) \simeq \mathcal{O}_{\max} \subset \mathcal{B}_{p,\infty}$
- 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: $\phi : E \longrightarrow E'$, $E[N] = \langle P, Q \rangle$, then

$$e_N(\phi(P), \phi(Q)) = e_N(P, Q)^{\deg \phi}$$

More facts about isogenies

$E/\mathbb{F}_q$: n-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:

- $\mathrm{End}(E) \simeq \mathcal{O}_{\mathrm{max}} \subset \mathcal{B}_{p,\infty}$
- 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: $\phi : E \longrightarrow E'$, $E[N] = \langle P, Q \rangle$, then

$$e_N(\phi(P), \phi(Q)) = e_N(P, Q)^{\deg \phi}$$

More facts about isogenies

$E/\mathbb{F}_q$: n-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:

- $\mathrm{End}(E) \simeq \mathcal{O}_{\max} \subset \mathcal{B}_{p,\infty}$
- 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: $\phi : E \longrightarrow E'$, $E[N] = \langle P, Q \rangle$, then

$$e_N(\phi(P), \phi(Q)) = e_N(P, Q)^{\deg \phi}$$

More facts about isogenies

$E/\mathbb{F}_q$: n-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:

- $\mathrm{End}(E) \simeq \mathcal{O}_{\max} \subset \mathcal{B}_{p,\infty}$
- 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: $\phi : E \longrightarrow E'$, $E[N] = \langle P, Q \rangle$, 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 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 B-torsion
3. τ can be recovered from its action on the B-torsion

The attack: Given a suitable description of Γ,

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

Assumes that End(E_0) is known. $input = [\theta \in End(E_0),\, d \in \mathbb{Z}]$.

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

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

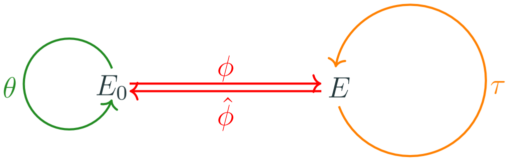
1. Knowing $\tau = \Gamma(\phi, input)$, one can recover ϕ
2. τ can be evaluated on the B-torsion
3. τ can be recovered from its action on the B-torsion

Petit2017 and dQKL+2021

Assumes that End(E_0) is known. $input = [\theta \in End(E_0),\, d \in \mathbb{Z}]$.

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

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



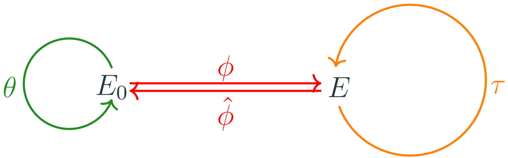
1. Knowing $\tau = \Gamma(\phi, input)$, one can recover ϕ
2. τ can be evaluated on the B-torsion
3. τ can be recovered from its action on the B-torsion

Petit2017 and dQKL+2021

Assumes that End(E_0) is known. $input = [\theta \in End(E_0),\, d \in \mathbb{Z}]$.

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

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



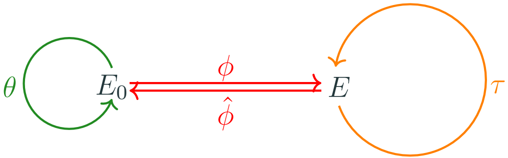
1. Knowing $\tau = \Gamma(\phi, input)$, one can recover ϕ
2. τ can be evaluated on the B-torsion
3. τ can be recovered from its action on the B-torsion

Petit2017 and dQKL+2021

Assumes that End(E_0) is known. $input = [\theta \in End(E_0),\, d \in \mathbb{Z}]$.

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

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



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

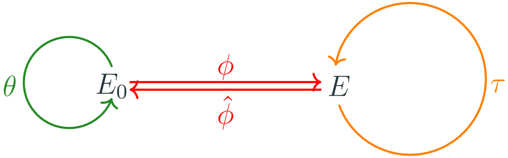
$\ker \hat{\phi} =^* \ker(\tau - [d]) \cap E[A]$

Petit2017 and dQKL+2021

Assumes that End(E_0) is known. $input = [\theta \in End(E_0),\, d \in \mathbb{Z}]$.

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

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



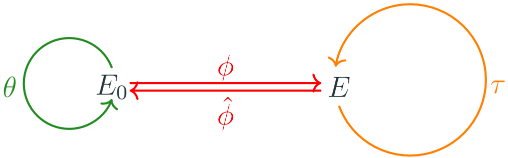
1. Knowing $\tau = \Gamma(\phi, input)$, one can recover ϕ ✓
2. τ can be evaluated on the B-torsion ✓
3. τ can be recovered from its action on the B-torsion

Petit2017 and dQKL+2021

Assumes that End(E_0) is known. $input = [\theta \in End(E_0),\, d \in \mathbb{Z}]$.

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

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



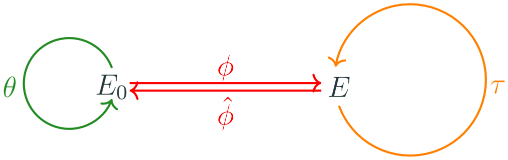
1. Knowing $\tau = \Gamma(\phi, input)$, one can recover ϕ ✓
2. τ can be evaluated on the B-torsion ✓
3. τ can be recovered from its action on the B-torsion ✓

Petit2017 and dQKL+2021

Assumes that End(E_0) is known. $input = [\theta \in End(E_0),\, d \in \mathbb{Z}]$.

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

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



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

Requires: $B > pA$; while in SIDH $A \approx B \approx \sqrt{p}$.

Assume $\phi : E_0 \longrightarrow E_B$ 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

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

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

CD-MM-R 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

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

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 ✓

CD-MM-R 2022

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

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

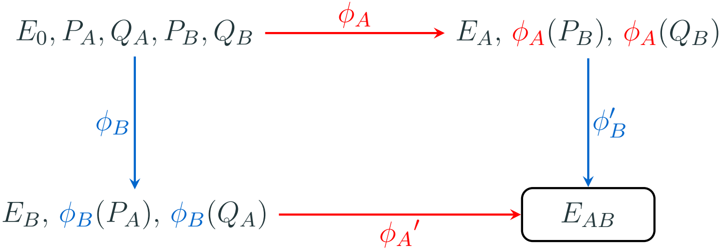
Fact: τ has degree $B + a = A$

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 ✓

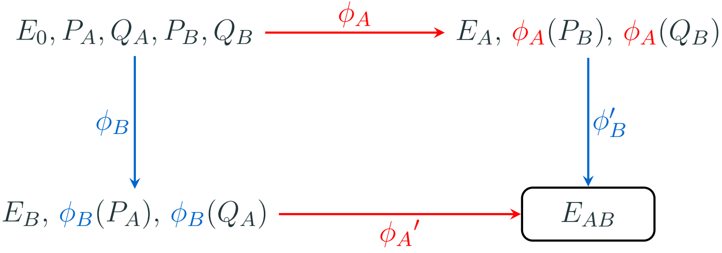
Runs in polynomial time when $A^2 > B$!!
Breaks SIDH/SIKE/SETA/...

Countermeasures

Masked degree SIDH



Masked degree SIDH



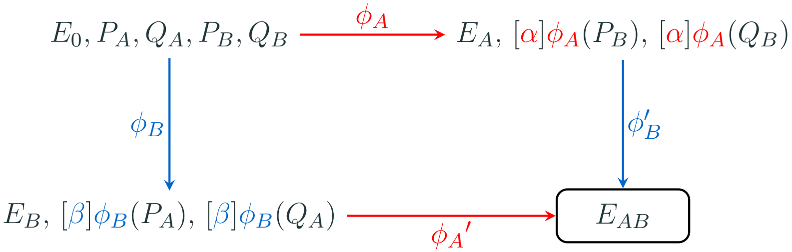
Ambient field: $\mathbb{F}_{p^2}$, $p = \ell_1^{a_1} \cdots \ell_t^{a_t} q_1^{b_1} \cdots q_t^{b_t} f - 1$

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

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

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

Masked degree SIDH



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

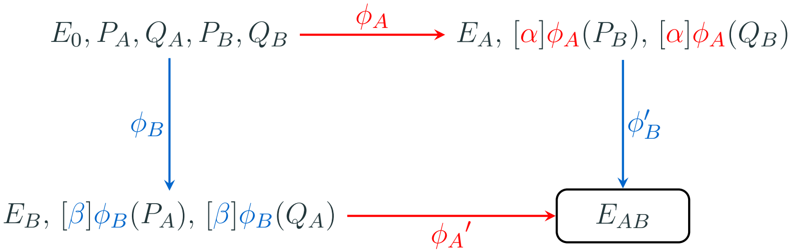
$A := \prod_{i=1}^{t} \ell_i^{a_i} \qquad B := \prod_{i=1}^{t} q_i^{b_i}, \quad A \approx B.$

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

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

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



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

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

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

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

Hide the exact TP images: $\alpha \in \mu_2(\mathbb{Z}/B\mathbb{Z}) \quad \beta \in \mu_2(\mathbb{Z}/A\mathbb{Z})$

Analysis of the countermeasures

Case of M-SIDH: using less torsion

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 2λ distinct prime factors each.

Case of M-SIDH: using lollipop endomorphisms

Given a small $\theta \in End(E_0)$, eliminate the scalar β in M-SIDH:

With respect to the A torsion, we have:

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

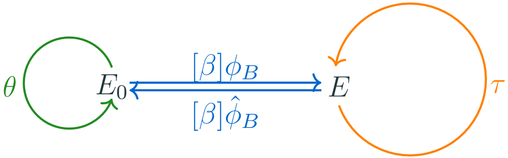
$\deg \tau = B^2 \deg \theta$.

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

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

Case of M-SIDH: using lollipop endomorphisms

Given a small $\theta \in End(E_0)$, eliminate the scalar β in M-SIDH:



With respect to the A torsion, we have:

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

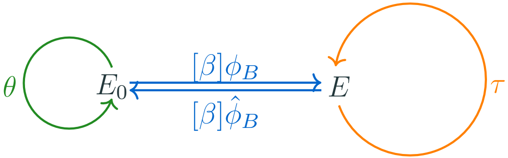
$\deg \tau = B^2 \deg \theta$.

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

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

Case of M-SIDH: using lollipop endomorphisms

Given a small $\theta \in End(E_0)$, eliminate the scalar β in M-SIDH:



With respect to the A torsion, we have:

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

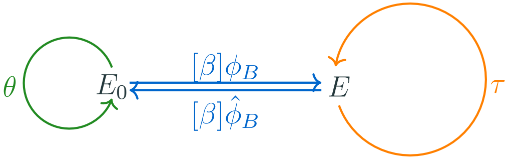
$\deg \tau = B^2 \deg \theta$.

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

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

Case of M-SIDH: using lollipop endomorphisms

Given a small $\theta \in End(E_0)$, eliminate the scalar β in M-SIDH:



With respect to the A torsion, we have:

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

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

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

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:

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

$$\begin{array}{rccc} \Phi : & D(q_1 \cdots q_t) & \longrightarrow & (\mathbb{Z}/2\mathbb{Z})^t \\ & N & \longmapsto & (\chi_1(N), \ldots, \chi_t(N)) \end{array}$$

Claims:

- We can evaluate Φ on the square free part of B'
- Φ 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:

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

$$\begin{array}{rccc} \Phi \colon & D(q_1 \cdots q_t) & \longrightarrow & (\mathbb{Z}/2\mathbb{Z})^t \\ & N & \longmapsto & (\chi_1(N), \ldots, \chi_t(N)) \end{array}$$

Claims:

- We can evaluate Φ on the square free part of B'
- Φ 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:

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

$$\Phi \colon \begin{array}{ccc} D(q_1 \cdots q_t) & \longrightarrow & (\mathbb{Z}/2\mathbb{Z})^t \\ N & \longmapsto & (\chi_1(N), \ldots, \chi_t(N)) \end{array}$$

Claims:

- We can evaluate Φ on the square free part of B'
- Φ 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:

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

$$\Phi \colon \begin{array}{rcl} D(q_1 \cdots q_t) & \longrightarrow & (\mathbb{Z}/2\mathbb{Z})^t \\ N & \longmapsto & (\chi_1(N), \ldots, \chi_t(N)) \end{array}$$

Claims:

- We can evaluate Φ on the square free part of B'
- Φ 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 $B_0 = \max\{n \mid n|B, n^2 B'_1 \leq B\}$.
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.

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

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

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

$$[\beta'_1]P' = [\mu \cdot \beta_1]P' = [\mu]\phi_0(P)$$
$$[\beta'_1]Q' = [\mu \cdot \beta_1]P' = [\mu]\phi_0(Q)$$

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.

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

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

Sampling β_1' in $\sqrt{\beta_1^2 \mod A}$, then $\beta_1' = \mu\beta_1$ where $\mu \in \mu_2(\mathbb{Z}/A\mathbb{Z})$.

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

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.

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

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

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

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

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.

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

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

Sampling β_1' in $\sqrt{\beta_1^2 \mod A}$, then $\beta_1' = \mu\beta_1$ where $\mu \in \mu_2(\mathbb{Z}/A\mathbb{Z})$.

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

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:

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

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

On the claims of eprint 2022/1667

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.)

On the claims of eprint 2022/1667

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.)

On the claims of eprint 2022/1667

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.)

On the claims of eprint 2022/1667

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.)

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 !

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 ≈ 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 ≈ 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 ≈ 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 !!!