A polynomial time attack on instances of M-SIDH and FESTA[1]

Peigen Li

Beijing Institute of Mathematical Sciences and Applications

lpg22@bimsa.cn

December 12,2025

[1]The authors are Wouter Castryck and Frederik Vercauteren-Asiacrypto2023

Overview

1. SIDH
2. Modified SIDH
   - M-SIDH
   - FESTA
3. Attacks
   - Attack on M-SIDH
   - Attack on FESTA
   - Fail attack on CSIDH

key exchange protocols

- Diffie-Hellman key exchange based on elliptic curves(1985', Koblitz, Miller);

Hard problem

Given $P, Q(= [k]P) \in E[m]$, it's hard to find such k.

DHKE

Alice		**Bob**
$a \leftarrow \mathbb{Z}$		
	$\xrightarrow{P_1 = [a]P}$	
		$b \leftarrow \mathbb{Z}$
	$\xleftarrow{P_2 = [b]P}$	
$sk \leftarrow [a]P_2$		$sk \leftarrow [b]P_1$

Discrete log problem is broken by Shor's algorithm! This is the motivation of post-quantum cryptography.

key exchange protocols

- Diffie-Hellman key exchange
- Supersingular isogeny key exchange (SIDH/SIKE, 2011, De Feo, Jao, and Plut)

Hard problem

Given (supersingular) elliptic curves E and E' over a finite field, find a *(chain of low-degree) isogenies*

$$\varphi_n \circ \cdots \circ \varphi_1 \ : \ E \to E'.$$

key exchange protocols

- Diffie-Hellman key exchange
- Supersingular isogeny key exchange (SIDH/SIKE, 2011, De Feo, Jao, and Plut)

Hard problem

Given (supersingular) elliptic curves E and E' over a finite field, find a *(chain of low-degree) isogenies*

$$\varphi_n \circ \cdots \circ \varphi_1 \ : \ E \to E'.$$

The time complexity is $O(\sqrt{p})$ in the classical computer. In quantum computer, it's $O(p^{1/4})$.

Setup

- Suppersingular elliptic curve E over $\mathbb{F}_{p^2}$.
- Two distinct prime to p and coprime positive integers A and B.
- $E[A] = \langle P_A, Q_A \rangle$ and $E[B] = \langle P_B, Q_B \rangle$.

Setup

- Suppersingular elliptic curve E over $\mathbb{F}_{p^2}$.
- Two distinct prime to p and coprime positive integers A and B.
- $E[A] = \langle P_A, Q_A \rangle$ and $E[B] = \langle P_B, Q_B \rangle$.

For SIDH, set

$$p = f2^n3^m - 1, \quad A = 2^n \approx B = 3^m$$

For different scheme, the form of p may be different due to implementation and security consideration.

$$S_A = \ker \alpha = \langle P_A + aQ_A \rangle \subset E[A]$$

$$S_B = \ker \beta = \langle P_B + bQ_B \rangle \subset E[B]$$

$$\ker \alpha' = \langle \beta(S_A) \rangle$$

$$\ker \beta' = \langle \alpha(S_B) \rangle$$

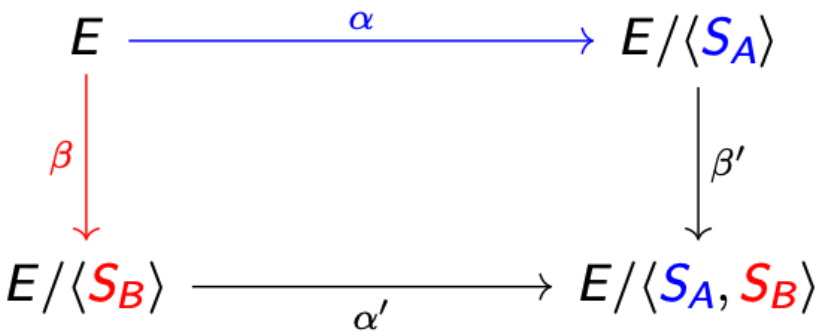


Figure: SIDH

SIDH

$$S_A = \ker \alpha = \langle P_A + aQ_A \rangle \subset E[A]$$

$$S_B = \ker \beta = \langle P_B + bQ_B \rangle \subset E[B]$$

$$\ker \alpha' = \langle \beta(S_A) \rangle$$

$$\ker \beta' = \langle \alpha(S_B) \rangle$$

$$\begin{array}{ccc} E & \xrightarrow{\alpha} & E/\langle S_A \rangle \\ \downarrow{\scriptstyle \beta} & & \downarrow{\scriptstyle \beta'} \\ E/\langle S_B \rangle & \xrightarrow[\alpha']{} & E/\langle S_A, S_B \rangle \end{array}$$

SIDH

Alice **Bob**

$a \leftarrow \mathbb{Z}/A\mathbb{Z}$

$$\xrightarrow{E_A = E/\langle P_A + aQ_A \rangle} \\ \xrightarrow{\alpha(P_B), \alpha(Q_B)}$$

$b \leftarrow \mathbb{Z}/B\mathbb{Z}$

$$\xleftarrow{E_B = E/\langle P_B + bQ_B \rangle} \\ \xleftarrow{\beta(P_A), \beta(Q_A)}$$

$sk \leftarrow E_B/\langle S_A \rangle$ $sk \leftarrow E_A/\langle S_B \rangle$

Why SIDH works?

Due to the fact that

$$E_B/\langle S_A\rangle \cong E/\langle S_A, S_B\rangle \cong E_A/\langle S_B\rangle$$

Why SIDH works?

Due to the fact that

$$E_B/\langle S_A\rangle \cong E/\langle S_A, S_B\rangle \cong E_A/\langle S_B\rangle$$

Thus the shared secret keys j-invariants are equal.

$$j((E_B/\langle S_A\rangle)) = j(E_A/\langle S_B\rangle)$$

SIDH

Indeed,

$$\langle S_A, S_B \rangle \subset \ker(E \to E_B \to E_B/\langle S_A \rangle)$$

is trivial.

$S_A = \ker \alpha = \langle P_A + aQ_A \rangle \subset E[A]$

$S_B = \ker \beta = \langle P_B + bQ_B \rangle \subset E[B]$

$\ker \alpha' = \langle \beta(S_A) \rangle$

$\ker \beta' = \langle \alpha(S_B) \rangle$

$$\begin{array}{ccc} E & \xrightarrow{\alpha} & E/\langle S_A \rangle \\ \downarrow{\scriptstyle \beta} & & \downarrow{\scriptstyle \beta'} \\ E/\langle S_B \rangle & \xrightarrow[\alpha']{} & E/\langle S_A, S_B \rangle \end{array}$$

SIDH

Indeed,

$$\langle S_A, S_B \rangle \subset \ker(E \to E_B \to E_B/\langle S_A \rangle)$$

is trivial.Conversely, suppose that $S \in \ker(E \to E_B/\langle S_A \rangle)$, we have

$$\beta(S) \in \ker(E_B \to E_B/\langle S_A \rangle) = \langle \beta(S_A) \rangle$$

SIDH

Indeed,

$$\langle S_A, S_B \rangle \subset \ker(E \to E_B \to E_B/\langle S_A \rangle)$$

is trivial.Conversely, suppose that $S \in \ker(E \to E_B/\langle S_A \rangle)$, we have

$$\beta(S) \in \ker(E_B \to E_B/\langle S_A \rangle) = \langle \beta(S_A) \rangle$$

So there exists some k such that

$$\beta(S) = k\beta(S_A) = \beta(kS_A)$$

SIDH

Indeed,

$$\langle S_A, S_B \rangle \subset \ker(E \to E_B \to E_B/\langle S_A \rangle)$$

is trivial.Conversely, suppose that $S \in \ker(E \to E_B/\langle S_A \rangle)$, we have

$$\beta(S) \in \ker(E_B \to E_B/\langle S_A \rangle) = \langle \beta(S_A) \rangle$$

So there exists some k such that

$$\beta(S) = k\beta(S_A) = \beta(kS_A)$$

Hence $S - kS_A \in \ker \beta = \langle S_B \rangle$, i.e., there is some l such that

$$S - kS_A = lS_B$$

Thus $S \in \langle S_A, S_B \rangle$.

SIDH

Indeed,

$$\langle S_A, S_B \rangle \subset \ker(E \to E_B \to E_B/\langle S_A \rangle)$$

is trivial.Conversely, suppose that $S \in \ker(E \to E_B/\langle S_A \rangle)$, we have

$$\beta(S) \in \ker(E_B \to E_B/\langle S_A \rangle) = \langle \beta(S_A) \rangle$$

So there exists some k such that

$$\beta(S) = k\beta(S_A) = \beta(kS_A)$$

Hence $S - kS_A \in \ker \beta = \langle S_B \rangle$, i.e., there is some l such that

$$S - kS_A = lS_B$$

Thus $S \in \langle S_A, S_B \rangle$.Hence the equality holds.

Why SIDH is (not) secure?

For SIDH, the authors think that

$$E, E[N] = \langle P, Q \rangle, \begin{pmatrix} \alpha(P) \\ \alpha(Q) \end{pmatrix}, E_\alpha (= \mathrm{im}\alpha) \overset{\textit{Hard!}}{\rightsquigarrow} \alpha \tag{1.1}$$

Why SIDH is (not) secure?

For SIDH, the authors think that

$$E, E[N] = \langle P, Q \rangle, \begin{pmatrix} \alpha(P) \\ \alpha(Q) \end{pmatrix}, E_\alpha (= \mathrm{im}\alpha) \overset{\textit{Hard}!}{\rightsquigarrow} \alpha \tag{1.1}$$

But the original hard problem is

$$E, E_\alpha \overset{\textit{Hard}!}{\rightsquigarrow} \alpha$$

Why SIDH is (not) secure?

For SIDH, the authors think that

$$E, E[N] = \langle P, Q \rangle, \begin{pmatrix} \alpha(P) \\ \alpha(Q) \end{pmatrix}, E_\alpha (= \mathrm{im}\alpha) \overset{\textit{Hard!}}{\rightsquigarrow} \alpha \tag{1.1}$$

But the original hard problem is

$$E, E_\alpha \overset{\textit{Hard!}}{\rightsquigarrow} \alpha$$

In 2022, Castryck and Decru,etc ... proposed an efficient attack on SIDH such that (1.1) becomes easy! We will discuss their attack later.

Modified SIDH

To fix the problem of SIDH, some modified versions of SIDH were proposed, such as

- M-SIDH (Eurocrypto-2023, Tako Boris Fouotsa, Tomoki Moriya, and Christophe Petit)

Modified SIDH

To fix the problem of SIDH, some modified versions of SIDH were proposed, such as

- M-SIDH (Eurocrypto-2023, Tako Boris Fouotsa, Tomoki Moriya, and Christophe Petit)
- FESTA (Asiacrypto-2023, Andrea Basso, Luciano Maino, and Giacomo Pope)

M-SIDH

Alice		**Bob**
$a \leftarrow \mathbb{Z}/A\mathbb{Z}$		
$\lambda \leftarrow (\mathbb{Z}/B\mathbb{Z})^\times$	$\xrightarrow{E_A = E/\langle P_A + aQ_A\rangle \quad \lambda\alpha(P_B), \lambda\alpha(Q_B)}$	
		$b \leftarrow \mathbb{Z}/B\mathbb{Z}$
		$\mu \leftarrow (\mathbb{Z}/A\mathbb{Z})^\times$
	$\xleftarrow{E_B = E/\langle P_B + bQ_B\rangle \quad \mu\beta(P_A), \mu\beta(Q_A)}$	
$sk \leftarrow E_B/\langle \mu\beta(P_A + aQ_A)\rangle$		$sk \leftarrow E_A/\langle \lambda\alpha(P_B + bQ_B)\rangle$

Why M-SIDH works?

Alice		Bob
$a \leftarrow \mathbb{Z}/A\mathbb{Z}$		
$\lambda \leftarrow (\mathbb{Z}/B\mathbb{Z})^\times$	$\xrightarrow{E_A = E/\langle P_A + aQ_A\rangle,\ \lambda\alpha(P_B), \lambda\alpha(Q_B)}$	
		$b \leftarrow \mathbb{Z}/B\mathbb{Z}$
		$\mu \leftarrow (\mathbb{Z}/A\mathbb{Z})^\times$
	$\xleftarrow{E_B = E/\langle P_B + bQ_B\rangle,\ \mu\beta(P_A), \mu\beta(Q_A)}$	
$sk \leftarrow E_B/\langle \mu\beta(P_A + aQ_A)\rangle$		$sk \leftarrow E_A/\langle \lambda\alpha(P_B + bQ_B)\rangle$

Why M-SIDH works?

Due to the fact that

$$\lambda \in (\mathbb{Z}/B\mathbb{Z})^\times \implies \langle \lambda\alpha(P_B + bQ_B)\rangle = \langle \alpha(P_B + bQ_B)\rangle \in E_A[B]$$

and

$$\mu \in (\mathbb{Z}/A\mathbb{Z})^\times \implies \langle \mu\beta(P_A + aQ_A)\rangle = \langle \beta(P_A + aQ_A)\rangle \in E_B[A]$$

Hence the shared secret keys are equal.

What does M-SIDH do?

Alice	Bob
$a \leftarrow \mathbb{Z}/A\mathbb{Z}$	
$\lambda \leftarrow (\mathbb{Z}/B\mathbb{Z})^\times$	
$E_A = E/\langle P_A + aQ_A \rangle$, $\lambda\alpha(P_B), \lambda\alpha(Q_B)$ $\longrightarrow$	
	$b \leftarrow \mathbb{Z}/B\mathbb{Z}$
	$\mu \leftarrow (\mathbb{Z}/A\mathbb{Z})^\times$
$E_B = E/\langle P_B + bQ_B \rangle$, $\mu\beta(P_A), \mu\beta(Q_A)$ $\longleftarrow$	
$sk \leftarrow E_B/\langle \mu\beta(P_A + aQ_A) \rangle$	$sk \leftarrow E_A/\langle \lambda\alpha(P_B + bQ_B) \rangle$

What does M-SIDH do?

M-SIDH masks the images of basis points of $E[B]$ (resp. $E[A]$) under isogeny α (resp. β) by multiplying random units in $(\mathbb{Z}/B\mathbb{Z})^\times$ (resp. $(\mathbb{Z}/A\mathbb{Z})^\times$). That is, replaces the images

$$(\alpha(P), \alpha(Q))$$

by

$$(\lambda\alpha(P), \lambda\alpha(Q)) = (\alpha(P), \alpha(Q)) \cdot \begin{pmatrix} \lambda & 0 \\ 0 & \lambda \end{pmatrix}$$

for random $\lambda \in (\mathbb{Z}/B\mathbb{Z})^\times$.

Why M-SIDH is "secure"?

For SIDH,

$$E, E[N] = \langle P, Q \rangle, \begin{pmatrix} \alpha(P) \\ \alpha(Q) \end{pmatrix}, E_\alpha \overset{\text{Easy!}}{\rightsquigarrow} \alpha$$

Why M-SIDH is "secure"?

For SIDH,

$$E, E[N] = \langle P, Q \rangle, \begin{pmatrix} \alpha(P) \\ \alpha(Q) \end{pmatrix}, E_\alpha \overset{\text{Easy!}}{\rightsquigarrow} \alpha$$

However, the authors of M-SIDH think that

$$E, E[N] = \langle P, Q \rangle, \begin{pmatrix} \lambda\alpha(P) \\ \lambda\alpha(Q) \end{pmatrix}, E_\alpha \overset{\text{Hard!}}{\rightsquigarrow} \alpha$$

Reduction of M-SIDH

Lemma

Let $\varphi : E \to E_1$ be an isogeny of unknown degree d. Let B be a smooth integer coprime to $\deg(\varphi)$ *such that $E[B] \subset E(\mathbb{F}_{p^2})$. Set $E[B] = \langle P, Q \rangle$. Then given*

$$P, Q, \varphi(P), \varphi(Q), \tag{2.1}$$

we can compute $\deg(\varphi) \mod B$ *in polynomial time.*

Reduction of M-SIDH

Lemma

Let $\varphi : E \to E_1$ be an isogeny of unknown degree d. Let B be a smooth integer coprime to $\deg(\varphi)$ such that $E[B] \subset E(\mathbb{F}_{p^2})$. Set $E[B] = \langle P, Q \rangle$. Then given

$$P, Q, \varphi(P), \varphi(Q), \tag{2.1}$$

we can compute $\deg(\varphi) \mod B$ in polynomial time.

Proof.

$$e_B(\varphi(P), \varphi(Q)) = e_B(P, Q)^{\deg(\varphi)} \in \mu_B \subset \mathbb{F}_{p^2}^*.$$

Applying Pohlig-Hellman algorithm on the discrete log problem, the complexity is

$$O(\sum_{q|B} \log q \cdot \sqrt{q})$$

For M-SIDH, we know that

$$P_B, Q_B, \lambda\alpha(P_B), \lambda\alpha(Q_B), \deg(\alpha). \tag{2.2}$$

For M-SIDH, we know that

$$P_B, Q_B, \lambda\alpha(P_B), \lambda\alpha(Q_B), \deg(\alpha). \tag{2.2}$$

By the lemma above, we can compute

$$\deg(\lambda\alpha) = \lambda^2 \deg(\alpha) \mod B \tag{2.3}$$

in polynomial time.

For M-SIDH, we know that

$$P_B, Q_B, \lambda\alpha(P_B), \lambda\alpha(Q_B), \deg(\alpha). \tag{2.2}$$

By the lemma above, we can compute

$$\deg(\lambda\alpha) = \lambda^2 \deg(\alpha) \mod B \tag{2.3}$$

in polynomial time.Thus we can find some λ_0 such that $\lambda_0^2 \equiv \lambda^2 \mod B$. Replacing λ with $\lambda\lambda_0^{-1}$, we may assume that

$$\lambda^2 \equiv 1 \mod B.$$

Same for μ.

Trivial attack on M-SIDH

Chinese Remainder theorem

Suppose that $B = B_1 B_2 \cdots B_k$ where B_i are pairwise coprime. Then there is an isomorphism

$$\mathbb{Z}/B\mathbb{Z} \cong \mathbb{Z}/B_1\mathbb{Z} \times \mathbb{Z}/B_2\mathbb{Z} \times \cdots \times \mathbb{Z}/B_k\mathbb{Z}$$

Hence

$$\lambda^2 \equiv 1 \mod B \iff \lambda^2 \equiv 1 \mod B_i, \forall 1 \leq i \leq k.$$

Trivial attack on M-SIDH

Chinese Remainder theorem

Suppose that $B = B_1 B_2 \cdots B_k$ where B_i are pairwise coprime. Then there is an isomorphism

$$\mathbb{Z}/B\mathbb{Z} \cong \mathbb{Z}/B_1\mathbb{Z} \times \mathbb{Z}/B_2\mathbb{Z} \times \cdots \times \mathbb{Z}/B_k\mathbb{Z}$$

Hence

$$\lambda^2 \equiv 1 \mod B \iff \lambda^2 \equiv 1 \mod B_i, \forall 1 \leq i \leq k.$$

There is a trivial attack on M-SIDH as follows:

Trivial attack

Exhaustively search all possible pairs λ such that $\lambda^2 \equiv 1 \mod B$. After finding the correct λ, we can recover the original SIDH instance. The number of such λ is 2^k, where k is the number of distinct prime factors of B.

Let p be an odd prime. Note that

$$\#\{\lambda \in \mathbb{Z}/p^e\mathbb{Z} : \lambda^2 \equiv 1 \mod p^e\} = 2$$

Let p be an odd prime. Note that

$$\#\{\lambda \in \mathbb{Z}/p^e\mathbb{Z} : \lambda^2 \equiv 1 \mod p^e\} = 2$$

Indeed, we have

$$\lambda^2 \equiv 1 \mod p^e \iff p^e | \lambda^2 - 1 = (\lambda - 1)(\lambda + 1). \qquad (2.4)$$

Let p be an odd prime. Note that

$$\#\{\lambda \in \mathbb{Z}/p^e\mathbb{Z} : \lambda^2 \equiv 1 \mod p^e\} = 2$$

Indeed, we have

$$\lambda^2 \equiv 1 \mod p^e \iff p^e | \lambda^2 - 1 = (\lambda - 1)(\lambda + 1). \tag{2.4}$$

On the other hand, we have

$$\gcd(\lambda - 1, \lambda + 1) = 1, 2 \Rightarrow p^e | \lambda - 1 \text{ or } p^e | \lambda + 1.$$

Prevent trivial attack

We may choose A, B such that they have $2k$ distinct prime factors. For example, we can choose

$$p = 4f \prod_{i=1}^{4k} \ell_i - 1$$

where ℓ_i are distinct small primes and f is a small integer. Let

$$A = \prod_{i=1}^{2k} \ell_{2i-1}, \quad B = \prod_{i=1}^{2k} \ell_{2i}.$$

Prevent trivial attack

We may choose A, B such that they have $2k$ distinct prime factors. For example, we can choose

$$p = 4f \prod_{i=1}^{4k} \ell_i - 1$$

where ℓ_i are distinct small primes and f is a small integer. Let

$$A = \prod_{i=1}^{2k} \ell_{2i-1}, \quad B = \prod_{i=1}^{2k} \ell_{2i}.$$

Due to the large number of small primes required, the total bit-size of p may be too large for practical applications. e.g. the suggest 128-bit parameter set has p of size 5911 bits.

FESTA, an efficient isogeny-based public-key encryption (PKE) protocol based on a constructive application of the SIDH attacks.

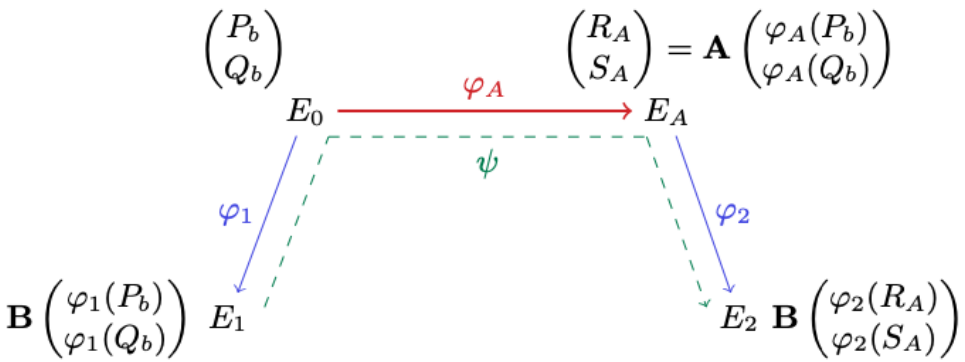


Figure: FESTA

FESTA constructs a trapdoor function $f_{(E_A,R_A,S_A)}(K_1, K_2, B)$.

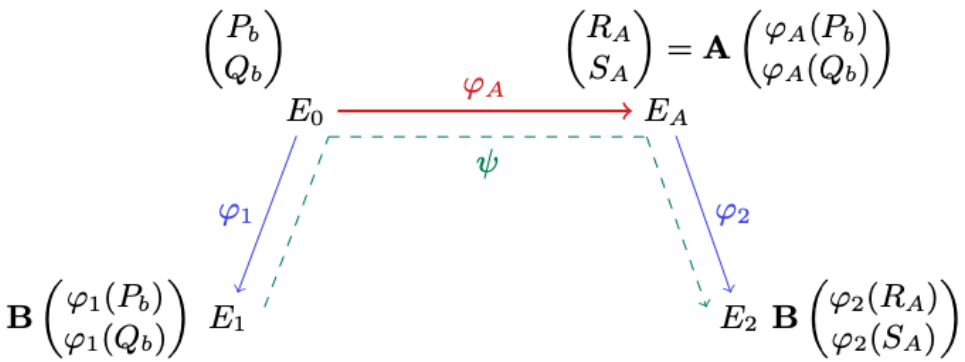


Figure: FESTA

FESTA constructs a trapdoor function $f_{(E_A,R_A,S_A)}(K_1, K_2, B)$. Given A, we can recover $\ker \varphi_1 = K_1$ and $\ker \varphi_2 = K_2$.

Why does FESTA work?

Why does FESTA work?

Set

$$\begin{pmatrix} R_1 \\ S_1 \end{pmatrix} = B \begin{pmatrix} \varphi_1(P_b) \\ \varphi_1(Q_b) \end{pmatrix}, \quad \begin{pmatrix} R_2 \\ S_2 \end{pmatrix} = B \begin{pmatrix} \varphi_2(R_A) \\ \varphi_2(S_A) \end{pmatrix}$$

Why does FESTA work?

Set

$$\begin{pmatrix} R_1 \\ S_1 \end{pmatrix} = B \begin{pmatrix} \varphi_1(P_b) \\ \varphi_1(Q_b) \end{pmatrix}, \quad \begin{pmatrix} R_2 \\ S_2 \end{pmatrix} = B \begin{pmatrix} \varphi_2(R_A) \\ \varphi_2(S_A) \end{pmatrix}$$

Then we have

$$d_1 \begin{pmatrix} R_2 \\ S_2 \end{pmatrix} = B \cdot A \cdot B^{-1} \begin{pmatrix} \psi(R_1) \\ \psi(S_1) \end{pmatrix} = A \begin{pmatrix} \psi(R_1) \\ \psi(S_1) \end{pmatrix}$$

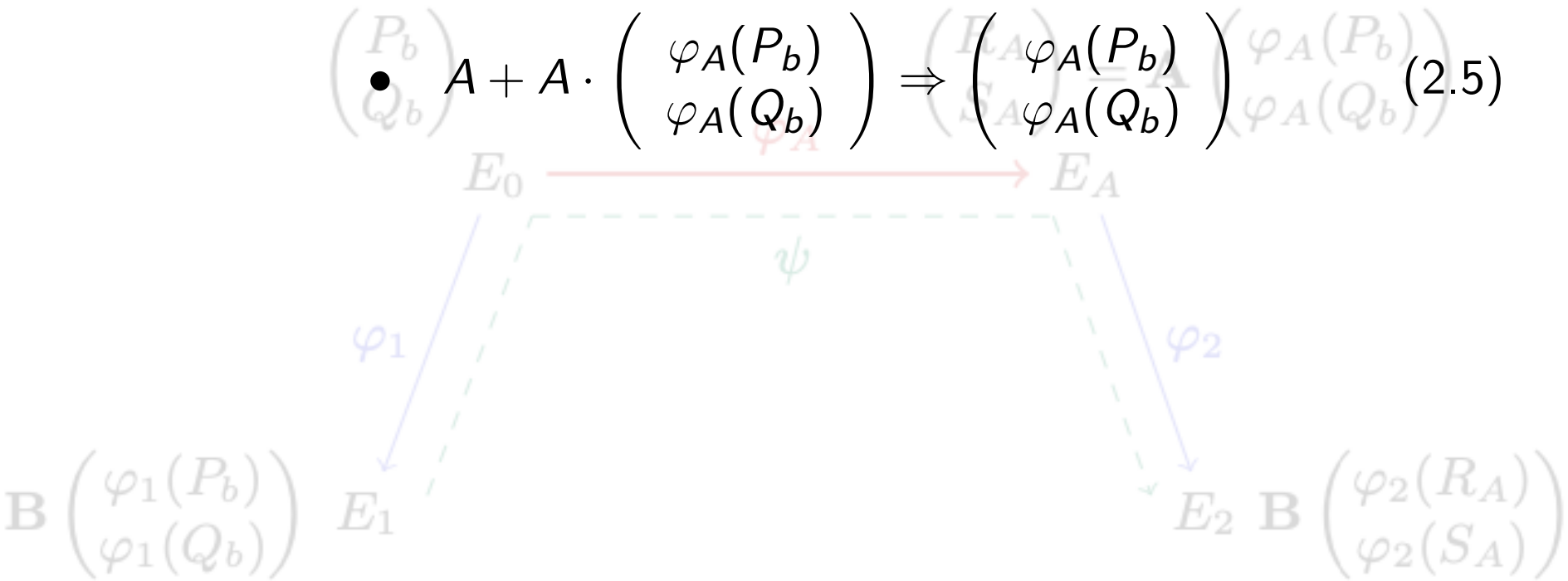
where we assume that $AB = BA$ and $\psi = \varphi_2 \circ \varphi_A \circ \hat{\varphi}_1$. Then $\ker(\psi)[d_1] = \ker \hat{\varphi}_1$ due to the fact $d_1, d_2, \deg \varphi_A$ are coprime.

FESTA

$\begin{pmatrix} P_b \\ Q_b \end{pmatrix}$
$\begin{pmatrix} R_A \\ S_A \end{pmatrix} = \mathbf{A} \begin{pmatrix} \varphi_A(P_b) \\ \varphi_A(Q_b) \end{pmatrix}$
φ_A
E_0
E_A
ψ
φ_1
φ_2
$\mathbf{B} \begin{pmatrix} \varphi_1(P_b) \\ \varphi_1(Q_b) \end{pmatrix}$
E_1
E_2
$\mathbf{B} \begin{pmatrix} \varphi_2(R_A) \\ \varphi_2(S_A) \end{pmatrix}$

Thus, we have

- $$A + A \cdot \begin{pmatrix} \varphi_A(P_b) \\ \varphi_A(Q_b) \end{pmatrix} \Rightarrow \begin{pmatrix} \varphi_A(P_b) \\ \varphi_A(Q_b) \end{pmatrix} \tag{2.5}$$



Thus, we have

- $$A + A \cdot \begin{pmatrix} \varphi_A(P_b) \\ \varphi_A(Q_b) \end{pmatrix} \Rightarrow \begin{pmatrix} \varphi_A(P_b) \\ \varphi_A(Q_b) \end{pmatrix} \tag{2.5}$$
- $$\begin{pmatrix} P_b \\ Q_b \end{pmatrix} + \begin{pmatrix} \varphi_A(P_b) \\ \varphi_A(Q_b) \end{pmatrix} \xRightarrow{sidh-attack} \varphi_A \tag{2.6}$$

Thus, we have

- $$A + A \cdot \begin{pmatrix} \varphi_A(P_b) \\ \varphi_A(Q_b) \end{pmatrix} \Rightarrow \begin{pmatrix} \varphi_A(P_b) \\ \varphi_A(Q_b) \end{pmatrix} \tag{2.5}$$
- $$\begin{pmatrix} P_b \\ Q_b \end{pmatrix} + \begin{pmatrix} \varphi_A(P_b) \\ \varphi_A(Q_b) \end{pmatrix} \xRightarrow{sidh-attack} \varphi_A \tag{2.6}$$
- $$A + d_1 \cdot A^{-1} \cdot \begin{pmatrix} R_2 \\ S_2 \end{pmatrix} \Rightarrow \begin{pmatrix} \psi(R_1) \\ \psi(S_1) \end{pmatrix} \tag{2.7}$$

Thus, we have

- $$A + A \cdot \begin{pmatrix} \varphi_A(P_b) \\ \varphi_A(Q_b) \end{pmatrix} \Rightarrow \begin{pmatrix} \varphi_A(P_b) \\ \varphi_A(Q_b) \end{pmatrix} \tag{2.5}$$
- $$\begin{pmatrix} P_b \\ Q_b \end{pmatrix} + \begin{pmatrix} \varphi_A(P_b) \\ \varphi_A(Q_b) \end{pmatrix} \xRightarrow{sidh-attack} \varphi_A \tag{2.6}$$
- $$A + d_1 \cdot A^{-1} \cdot \begin{pmatrix} R_2 \\ S_2 \end{pmatrix} \Rightarrow \begin{pmatrix} \psi(R_1) \\ \psi(S_1) \end{pmatrix} \tag{2.7}$$
- $$\begin{pmatrix} R_1 \\ S_1 \end{pmatrix} + \begin{pmatrix} \psi(R_1) \\ \psi(S_1) \end{pmatrix} \xRightarrow{sidh-attack} \psi \tag{2.8}$$

Thus, we have

- $$A + A \cdot \begin{pmatrix} \varphi_A(P_b) \\ \varphi_A(Q_b) \end{pmatrix} \Rightarrow \begin{pmatrix} \varphi_A(P_b) \\ \varphi_A(Q_b) \end{pmatrix} \tag{2.5}$$
- $$\begin{pmatrix} P_b \\ Q_b \end{pmatrix} + \begin{pmatrix} \varphi_A(P_b) \\ \varphi_A(Q_b) \end{pmatrix} \xRightarrow{sidh-attack} \varphi_A \tag{2.6}$$
- $$A + d_1 \cdot A^{-1} \cdot \begin{pmatrix} R_2 \\ S_2 \end{pmatrix} \Rightarrow \begin{pmatrix} \psi(R_1) \\ \psi(S_1) \end{pmatrix} \tag{2.7}$$
- $$\begin{pmatrix} R_1 \\ S_1 \end{pmatrix} + \begin{pmatrix} \psi(R_1) \\ \psi(S_1) \end{pmatrix} \xRightarrow{sidh-attack} \psi \tag{2.8}$$

At last, $\ker(\psi)[d_1] = \hat{\varphi}_1$.

What does FESTA do?

For SIDH $\rightsquigarrow$ M-SIDH,

$$\begin{pmatrix} \alpha(P) \\ \alpha(Q) \end{pmatrix} \overset{\textit{Replace}}{\rightsquigarrow} \begin{pmatrix} \lambda & 0 \\ 0 & \lambda \end{pmatrix} \begin{pmatrix} \alpha(P) \\ \alpha(Q) \end{pmatrix}$$

What does FESTA do?

For SIDH $\rightsquigarrow$ M-SIDH,

$$\begin{pmatrix} \alpha(P) \\ \alpha(Q) \end{pmatrix} \overset{\textit{Replace}}{\rightsquigarrow} \begin{pmatrix} \lambda & 0 \\ 0 & \lambda \end{pmatrix} \begin{pmatrix} \alpha(P) \\ \alpha(Q) \end{pmatrix}$$

For SIDH $\rightsquigarrow$ FESTA,

$$\begin{pmatrix} \alpha(P) \\ \alpha(Q) \end{pmatrix} \overset{\textit{Replace}}{\rightsquigarrow} \begin{pmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{pmatrix} \begin{pmatrix} \alpha(P) \\ \alpha(Q) \end{pmatrix}$$

where $E[B] = \langle P, Q \rangle$ and $\lambda, \lambda_1, \lambda_2 \in (\mathbb{Z}/B\mathbb{Z})^\times$.

For the same reason as M-SIDH, we may assume that $\lambda_1\lambda_2 = 1$ since we can use Weil pairing calculate

$$\lambda_1\lambda_2 \deg \alpha \mod B. \tag{2.9}$$

For the same reason as M-SIDH, we may assume that $\lambda_1\lambda_2 = 1$ since we can use Weil pairing calculate

$$\lambda_1\lambda_2 \deg \alpha \mod B. \tag{2.9}$$

Thus we can take some $\lambda_0 \equiv \lambda_1\lambda_2 \mod B$ and replace λ_1 by $\lambda_0^{-1}\lambda_1$. So we may assume that $\lambda_1\lambda_2 = 1$.

For the same reason as M-SIDH, we may assume that $\lambda_1\lambda_2 = 1$ since we can use Weil pairing calculate

$$\lambda_1\lambda_2 \deg \alpha \mod B. \tag{2.9}$$

Thus we can take some $\lambda_0 \equiv \lambda_1\lambda_2 \mod B$ and replace λ_1 by $\lambda_0^{-1}\lambda_1$. So we may assume that $\lambda_1\lambda_2 = 1$.

However for FESTA, the condition $\lambda_1\lambda_2 \equiv 1 \mod B$ does not leak any information about λ_1, unlike in M-SIDH where the relation $\lambda^2 \equiv 1 \mod B$ always holds. Hence we may assume that $B = 2^e$.

Why FESTA is "secure"?

The authors of FESTA think that

$$E, E[N] = \langle P, Q \rangle, \begin{pmatrix} \lambda & 0 \\ 0 & \lambda^{-1} \end{pmatrix} \cdot \begin{pmatrix} \alpha(P) \\ \alpha(Q) \end{pmatrix}, E_\alpha \overset{\text{Hard!}}{\rightsquigarrow} \alpha$$

CSIDH "reduce" to FESTA

The isogenies used in CSIDH are $\mathbb{F}_p$-rational, the isogeny $\varphi : E_0 \to E$ satisfies that

$$\varphi \circ \pi_0 = \pi \circ \varphi \tag{2.10}$$

where π_0 and π are the Frobenius endomorphisms of E_0 and E respectively.

Note the characteristic polynomial of π_0 is $x^2 + p$. If $(\frac{-p}{\ell}) = 1$, there exists some $P \in E_0[\ell]$ such that

$$\pi_0(P) = \mu_1 P. \tag{2.11}$$

Note the characteristic polynomial of π_0 is $x^2 + p$. If $(\frac{-p}{\ell}) = 1$, there exists some $P \in E_0[\ell]$ such that

$$\pi_0(P) = \mu_1 P. \tag{2.11}$$

Applying φ to both sides of the above equations, we have

$$\pi \circ \varphi(P) = \varphi \circ \pi_0(P) = \mu_1 \varphi(P). \tag{2.12}$$

Note the characteristic polynomial of π_0 is $x^2 + p$. If $(\frac{-p}{\ell}) = 1$, there exists some $P \in E_0[\ell]$ such that

$$\pi_0(P) = \mu_1 P. \tag{2.11}$$

Applying φ to both sides of the above equations, we have

$$\pi \circ \varphi(P) = \varphi \circ \pi_0(P) = \mu_1 \varphi(P). \tag{2.12}$$

Therefore if $S \in E[\ell]$ is an eigenvector of π with eigenvalue μ_1, we know that there exists some λ such that

$$S = \lambda \varphi(P). \tag{2.13}$$

Note the characteristic polynomial of π_0 is $x^2 + p$. If $(\frac{-p}{\ell}) = 1$, there exists some $P \in E_0[\ell]$ such that

$$\pi_0(P) = \mu_1 P. \tag{2.11}$$

Applying φ to both sides of the above equations, we have

$$\pi \circ \varphi(P) = \varphi \circ \pi_0(P) = \mu_1 \varphi(P). \tag{2.12}$$

Therefore if $S \in E[\ell]$ is an eigenvector of π with eigenvalue μ_1, we know that there exists some λ such that

$$S = \lambda \varphi(P). \tag{2.13}$$

At such, the CSIDH case looks very similar to FESTA case. Unlike FESTA, the information P, Q exists automatically in CSIDH.

Kani's lemma

Theorem

Let N_1, N_2 and D be pairwise coprime positive integers such that $D = N_1 + N_2$. Let E_0, E_1, E_2 and E_3 be elliptic curves connected by the following commutative diagram of isogenies:

$$\begin{array}{ccc} E_0 & \xrightarrow{\psi_2} & E_2 \\ {\scriptstyle \psi_1}\downarrow & \overset{f}{\nearrow} & \downarrow{\scriptstyle \psi_1'} \\ E_1 & \xrightarrow[\psi_2']{} & E_3 \end{array}$$

where $\deg(\psi_i) = \deg(\psi_i') = N_i$ *for* $i = 1, 2$. *Then the isogeny*

$$\Psi = \begin{pmatrix} \hat{\psi}_1 & -\hat{\psi}_2 \\ \psi_2' & \psi_1' \end{pmatrix} : E_1 \times E_2 \to E_0 \times E_3.$$

is a (D, D)-isogeny with kernel $\{([N_2]P, f(P));\ P \in E_1[D]\}$

Main theorem

Theorem

Let $\varphi : E_0 \to E$ be a secret isogeny. Assume we are given

1. *elliptic curves E_0 and E;*
2. *integer $d = \deg(\varphi)$ and N which both smooth, coprime to each other and satisfy $N^2 > d$;*
3. *generators $P, Q \in E_0[N]$ and their images $\varphi(P), \varphi(Q) \in E[N]$.*

Then φ can be computed in polynomial time.

Main theorem

Theorem

Let $\varphi : E_0 \to E$ be a secret isogeny. Assume we are given

1. *elliptic curves E_0 and E;*
2. *integer $d = \deg(\varphi)$ and N which both smooth, coprime to each other and satisfy $N^2 > d$;*
3. *generators $P, Q \in E_0[N]$ and their images $\varphi(P), \varphi(Q) \in E[N]$.*

Then φ can be computed in polynomial time.

Problem in SIDH becomes easy

Suppose that $\varphi : E_0 \to E$ with degree 3^{e_B}. Given the $E_0[2^{e_A}] = \langle P, Q \rangle$ and the images $\varphi(P), \varphi(Q)$. It's easy to find such φ.

Main problem

For M-SIDH,

$$E_0, E_0[N] = \langle P, Q \rangle, \begin{pmatrix} \lambda & 0 \\ 0 & \lambda \end{pmatrix} \cdot \begin{pmatrix} \varphi(P) \\ \varphi(Q) \end{pmatrix} = \begin{pmatrix} S \\ T \end{pmatrix}, E \overset{\text{Hard?}}{\rightsquigarrow} \varphi$$

Main problem

For M-SIDH,

$$E_0, E_0[N] = \langle P, Q \rangle, \begin{pmatrix} \lambda & 0 \\ 0 & \lambda \end{pmatrix} \cdot \begin{pmatrix} \varphi(P) \\ \varphi(Q) \end{pmatrix} = \begin{pmatrix} S \\ T \end{pmatrix}, E \overset{\text{Hard?}}{\rightsquigarrow} \varphi$$

For FESTA,

$$E_0, E_0[N] = \langle P, Q \rangle, \begin{pmatrix} \lambda & 0 \\ 0 & \lambda^{-1} \end{pmatrix} \cdot \begin{pmatrix} \varphi(P) \\ \varphi(Q) \end{pmatrix} = \begin{pmatrix} S \\ T \end{pmatrix}, E \overset{\text{Hard?}}{\rightsquigarrow} \varphi$$

Naive lollipop attacks for M-SIDH

When $E_0 : y^2 = x^3 + x$, we have the endomorphism

$$\tau : E_0 \to E_0, \quad \tau(x, y) = (-x, iy).$$

Consider the following diagram

$$\tau \circlearrowright E_0 \xrightarrow{\varphi} E$$

Let

$$\psi := \varphi \circ \tau \circ \hat{\varphi} : E \to E.$$

Since we know the images of P, Q under $[\lambda]\varphi$, thus we focus on

$$[\lambda]\varphi \circ \tau \circ \widehat{[\lambda]\varphi} = [\lambda^2]\psi.$$

Since we already assume that $\lambda^2 \equiv 1 \mod N$, we can recover ψ using the Kani's lemma as in the SIDH case.

Since we know the images of P, Q under $[\lambda]\varphi$, thus we focus on

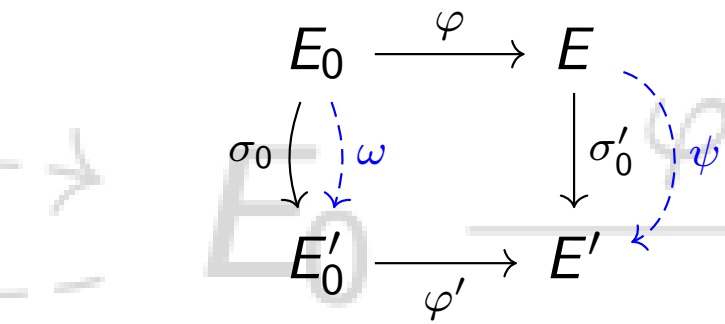
$$[\lambda]\varphi \circ \tau \circ \widehat{[\lambda]\varphi} = [\lambda^2]\psi.$$

Since we already assume that $\lambda^2 \equiv 1 \mod N$, we can recover ψ using the Kani's lemma as in the SIDH case. We need $N^2 \geq \deg(\psi) = d^2$ to ensure that this works.

Then we can recover φ from ψ.

Strategy-Generalized Lollipop Attacks

Consider the following diagram



where $\sigma_0' = \varphi_* \sigma_0$ and $\varphi' = \sigma_{0*} \varphi$. We hope

$$\psi := \varphi' \circ \omega \circ \hat{\varphi} : E \to E' \overset{\text{Recover}}{\rightsquigarrow} \hat{\varphi} \tag{3.1}$$

Lemma

Assume the matrix M such that

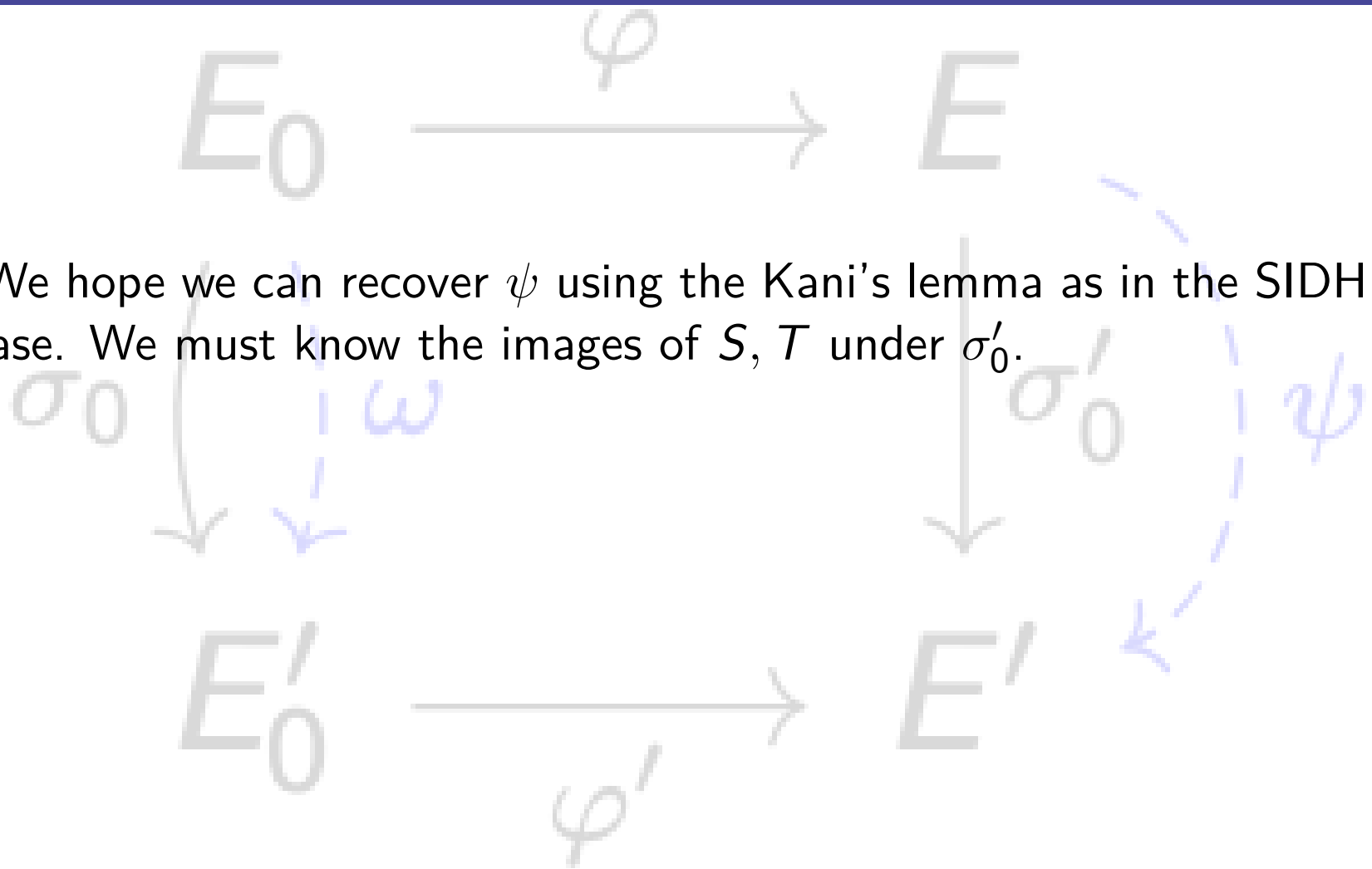
$$\hat{\sigma}_0 \circ \omega \begin{pmatrix} P \\ Q \end{pmatrix} = M \cdot \begin{pmatrix} P \\ Q \end{pmatrix} \tag{3.2}$$

commutes with A. Then we have

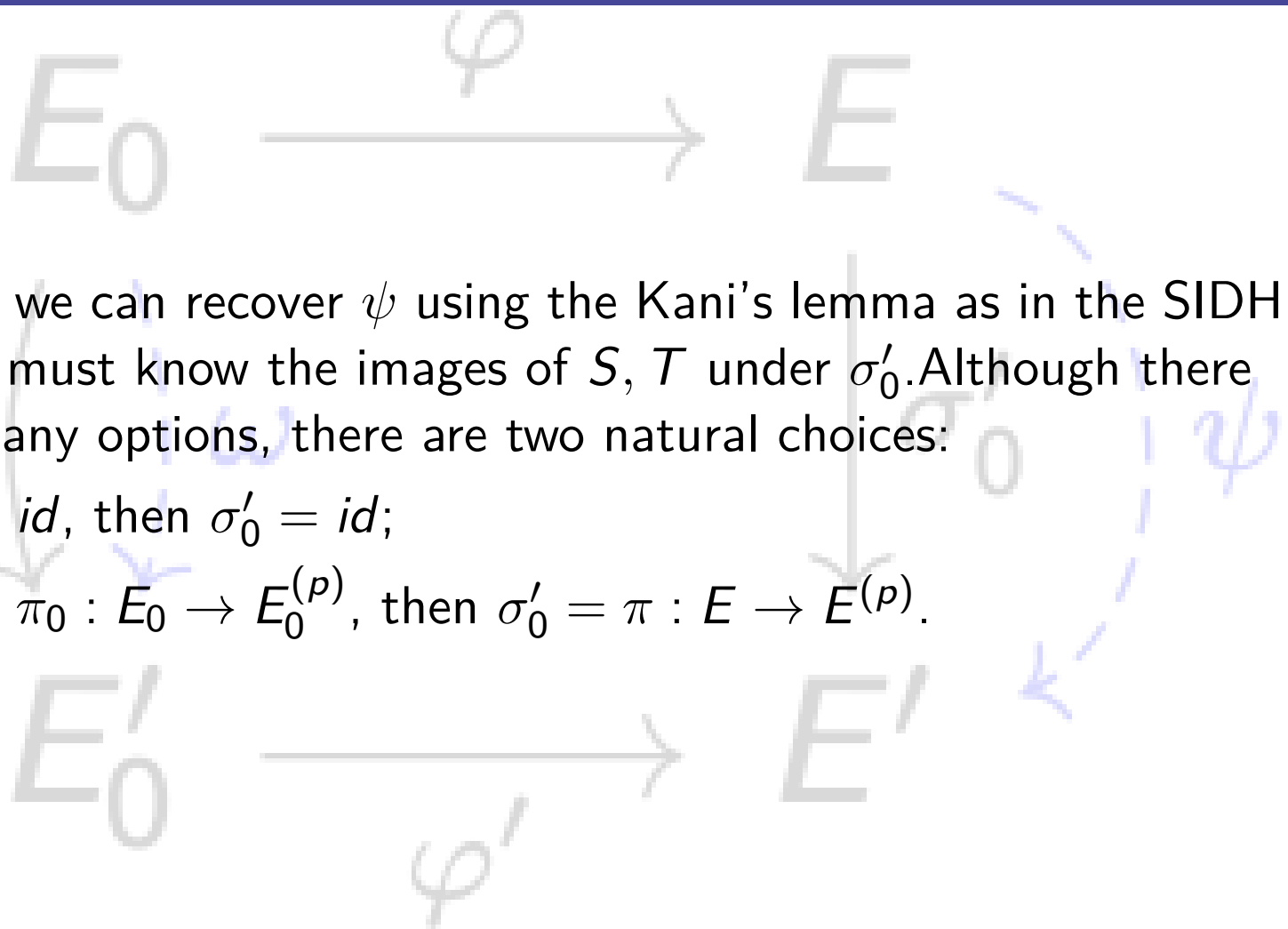
$$\deg(\sigma_0) \cdot \psi \begin{pmatrix} S \\ T \end{pmatrix} = \deg(\varphi) \cdot M \cdot \sigma_0' \begin{pmatrix} S \\ T \end{pmatrix} \tag{3.3}$$

Proof.

Check directly. □

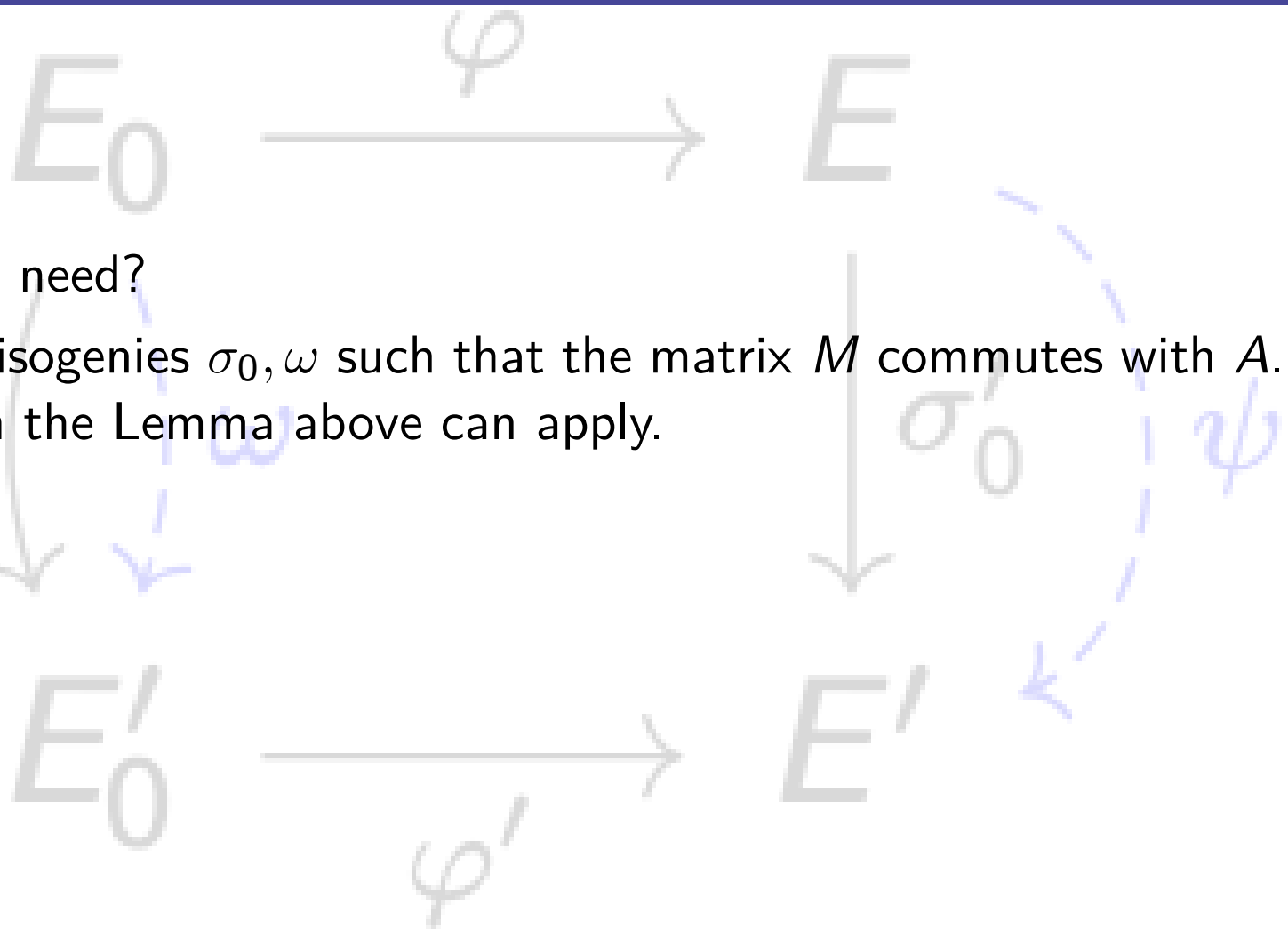


We hope we can recover ψ using the Kani's lemma as in the SIDH case. We must know the images of S, T under σ'_0.



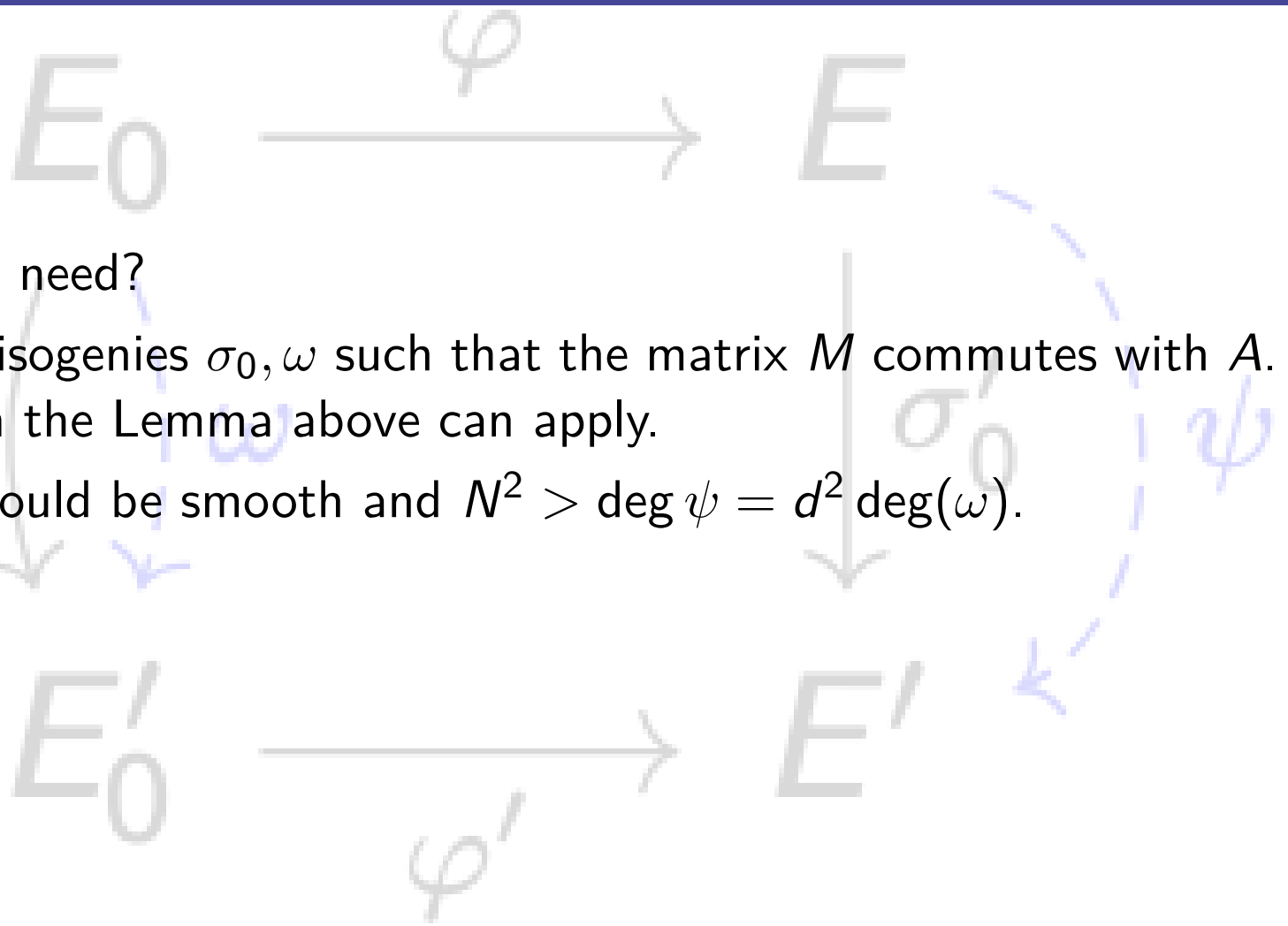
We hope we can recover ψ using the Kani's lemma as in the SIDH case. We must know the images of S, T under σ_0'.Although there are not many options, there are two natural choices:

- $\sigma_0 = id$, then $\sigma_0' = id$;
- $\sigma_0 = \pi_0 : E_0 \to E_0^{(p)}$, then $\sigma_0' = \pi : E \to E^{(p)}$.



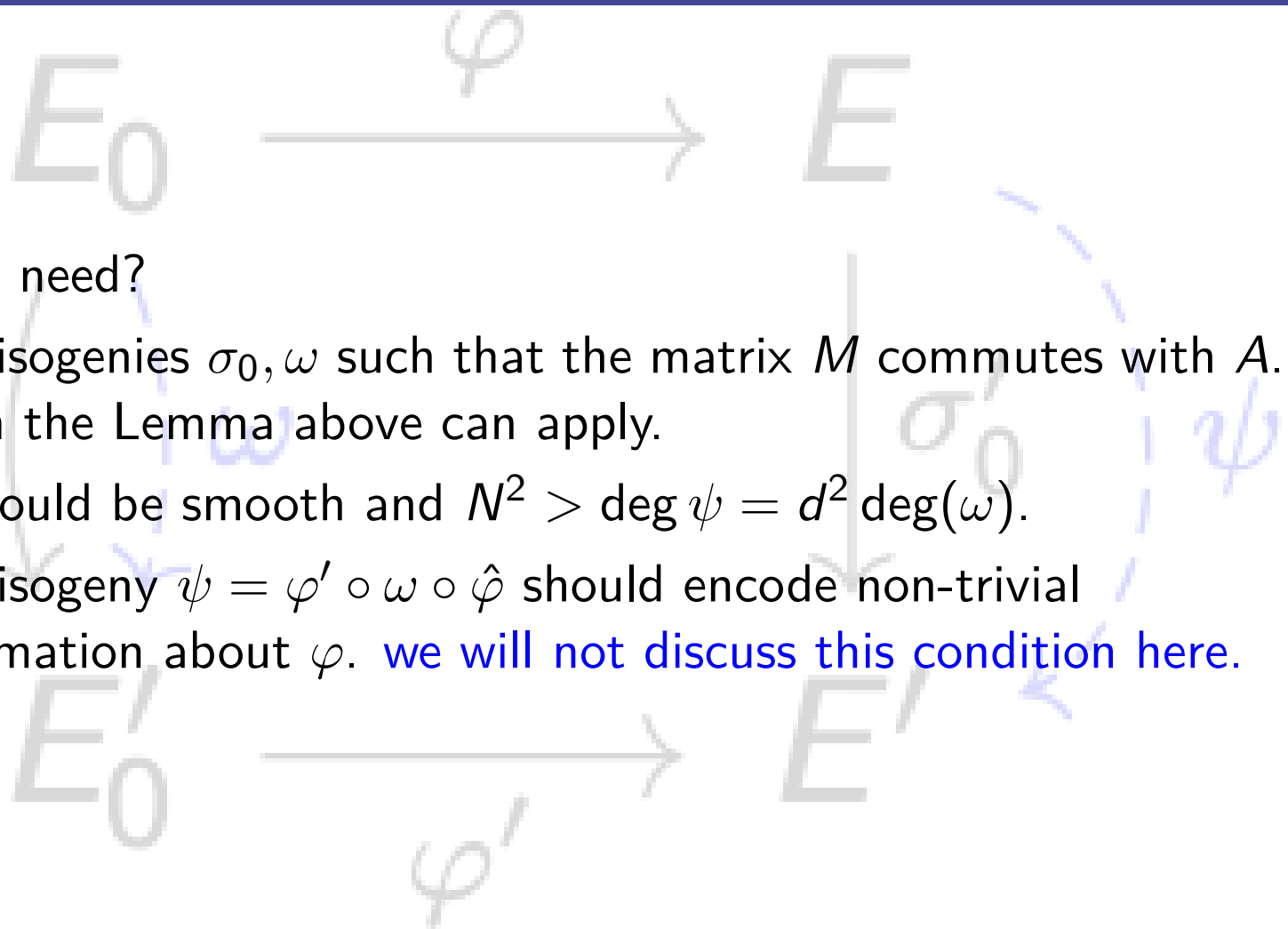
What we need?

- The isogenies σ_0, ω such that the matrix M commutes with A. Then the Lemma above can apply.



What we need?

- The isogenies σ_0, ω such that the matrix M commutes with A. Then the Lemma above can apply.
- N should be smooth and $N^2 > \deg \psi = d^2 \deg(\omega)$.



What we need?

- The isogenies σ_0, ω such that the matrix M commutes with A. Then the Lemma above can apply.
- N should be smooth and $N^2 > \deg \psi = d^2 \deg(\omega)$.
- The isogeny $\psi = \varphi' \circ \omega \circ \hat{\varphi}$ should encode non-trivial information about φ. we will not discuss this condition here.

For M-SIDH, A is a scalar matrix, thus any endomorphism ω satisfies the first condition.

$\sigma_0 = id$ in M-SIDH

Let ω be an endomorphism and set $\psi = \varphi \circ \omega \circ \hat{\varphi}$, then we have

$$\psi \begin{pmatrix} S \\ T \end{pmatrix} = \deg(\varphi) \cdot M \cdot \begin{pmatrix} S \\ T \end{pmatrix} \tag{3.4}$$

where M is the matrix of ω on $E_0[N]$ with respect to the basis P, Q.

$\sigma_0 = id$ in M-SIDH

Let ω be an endomorphism and set $\psi = \varphi \circ \omega \circ \hat{\varphi}$, then we have

$$\psi \begin{pmatrix} S \\ T \end{pmatrix} = \deg(\varphi) \cdot M \cdot \begin{pmatrix} S \\ T \end{pmatrix} \tag{3.4}$$

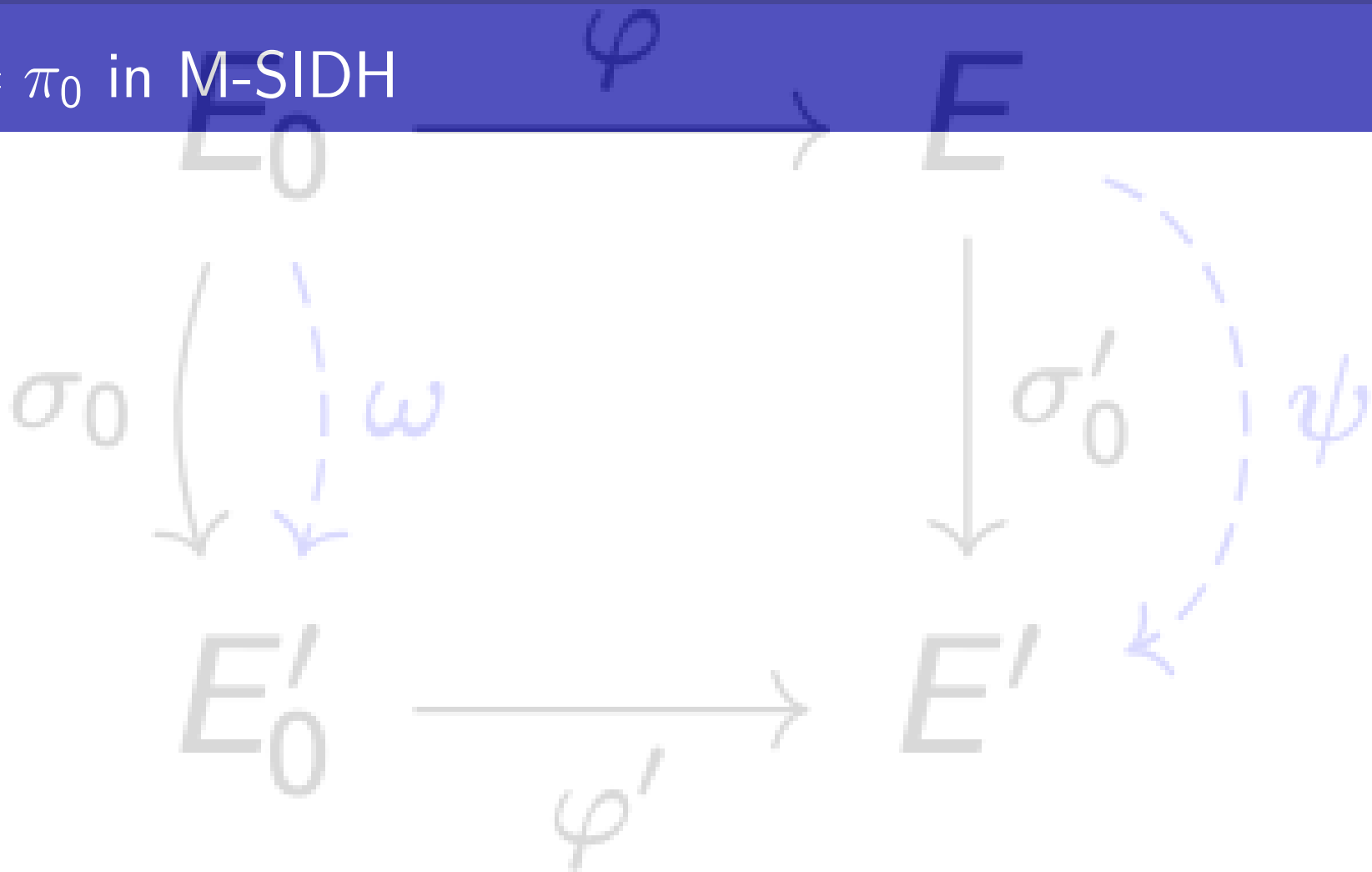
where M is the matrix of ω on $E_0[N]$ with respect to the basis P, Q.We hope that

$$N^2 > \deg(\psi) = d^2 \cdot \deg(\omega) \tag{3.5}$$

That is, $N > d\sqrt{\deg(\omega)}$.

Thus, as soon as E_0 comes equipped with a small non-scalar endomorphism ω then one should consider M-SIDH broken. The same conclusion applies for E.

$\sigma_0 = \pi_0$ in M-SIDH



$\sigma_0 = \pi_0$ in M-SIDH

If E_0 is the $\mathbb{F}_p$-rational, we can take $\omega = id$ and consider $\psi = \varphi^{(p)} \circ \hat{\varphi}$. Then we have

$$\psi \begin{pmatrix} S \\ T \end{pmatrix} = p^{-1} \cdot \deg(\varphi) \cdot M \cdot \pi \begin{pmatrix} S \\ T \end{pmatrix} \tag{3.6}$$

where M is the matrix of $\hat{\pi}_0$ on $E_0[N]$ with respect to the basis P, Q and $\pi : E \to E^{(p)}$.

$\sigma_0 = \pi_0$ in M-SIDH

If E_0 is the $\mathbb{F}_p$-rational, we can take $\omega = id$ and consider $\psi = \varphi^{(p)} \circ \hat{\varphi}$. Then we have

$$\psi \begin{pmatrix} S \\ T \end{pmatrix} = p^{-1} \cdot \deg(\varphi) \cdot M \cdot \pi \begin{pmatrix} S \\ T \end{pmatrix} \tag{3.6}$$

where M is the matrix of $\hat{\pi}_0$ on $E_0[N]$ with respect to the basis P, Q and $\pi : E \to E^{(p)}$.In such case, we need

$$N^2 > \deg(\psi) = d^2 \tag{3.7}$$

That is, $N > d$. This condition is always satisfied in practice.

As a conclusion, one should consider M-SIDH broken whenever E_0 or E is defined over $\mathbb{F}_p$.

As a conclusion, one should consider M-SIDH broken whenever E_0 or E is defined over $\mathbb{F}_p$.

More general, if E_0 is not $\mathbb{F}_p$-rational, but such that there exists a low degree isogeny $\omega : E_0 \to E_0^{(p)}$. Then we consider $\psi = \varphi^{(p)} \circ \omega \circ \hat{\varphi}$ as long as $N > d\sqrt{w}$. As such, if E_0 is close to its Frobenius conjugate, then M-SIDH is insecure.

Attack on FESTA

For the first condition

$$MA = AM. \tag{3.8}$$

When M is diagonal, this holds naturally. Thus we may hope that the torsion points P, Q are eigenvectors of $\hat{\sigma}_0 \circ \omega$.

Attack on FESTA

For the first condition

$$MA = AM. \tag{3.8}$$

When M is diagonal, this holds naturally. Thus we may hope that the torsion points P, Q are eigenvectors of $\hat{\sigma}_0 \circ \omega$.

If P, Q are eigenvectors of $\hat{\sigma}_0 \circ \omega$, FESTA will be broken as soon as $N^2 > \deg(\psi)$. We call such eigenspaces weak eigenspaces. Thus we calculate the proportion of weak eigenspaces for FESTA in the full basis.

For FESTA, the author used the curve

$$E_0 : y^2 = x^3 + 6x^2 + x \tag{3.9}$$

If we consider $G = \langle (0,0) \rangle$ and the 2-isogeny $\theta : E_0 \to E_1$ with kernel G, by Velu's formulas, we have

$$\theta : E_0 \to E_1 \cong y^2 = x^3 + x.$$

For FESTA, the author used the curve

$$E_0 : y^2 = x^3 + 6x^2 + x \tag{3.9}$$

If we consider $G = \langle (0,0) \rangle$ and the 2-isogeny $\theta : E_0 \to E_1$ with kernel G, by Velu's formulas, we have

$$\theta : E_0 \to E_1 \cong y^2 = x^3 + x.$$

Then we have

$$\hat{\theta} \circ \mathrm{End}(E_1) \circ \theta \subset \mathrm{End}(E_0).$$

For FESTA, the author used the curve

$$E_0 : y^2 = x^3 + 6x^2 + x \tag{3.9}$$

If we consider $G = \langle (0,0) \rangle$ and the 2-isogeny $\theta : E_0 \to E_1$ with kernel G, by Velu's formulas, we have

$$\theta : E_0 \to E_1 \cong y^2 = x^3 + x.$$

Then we have

$$\hat{\theta} \circ \mathrm{End}(E_1) \circ \theta \subset \mathrm{End}(E_0).$$

More precisely, we have

$$\mathrm{End}(E_0) = \mathbb{Z} + \mathbb{Z}\frac{\pi_0 - 1}{2} + \mathbb{Z}(i - i\pi_0) + \mathbb{Z}\frac{i + i\pi_0}{4}. \tag{3.10}$$

Since $\deg(\pi_0) = p$ and we hope ω has small degree, thus we restrict ourselves to

$$\omega = \alpha + 2\beta i \in \mathrm{End}(E_0). \tag{3.11}$$

$\sigma_0 = id$ in FESTA

If P is an eigenvector of ω, then we have

$$\omega(P) = \lambda P \tag{3.12}$$

for some $\lambda \in (\mathbb{Z}/N\mathbb{Z})^\times$.

$\sigma_0 = id$ in FESTA

If P is an eigenvector of ω, then we have

$$\omega(P) = \lambda P \tag{3.12}$$

for some $\lambda \in (\mathbb{Z}/N\mathbb{Z})^\times$.Since $\omega = \alpha + 2\beta i$, we have

$$2i(P) = \frac{\lambda - \alpha}{\beta} P, \tag{3.13}$$

where we assume that $(\beta, N) = 1$. Thus only the eigenspace of $2i$ are weak.

$\sigma_0 = \pi_0$ in FESTA

We have to analysis the eigenvectors of $\hat{\pi}_0 \circ \omega$. Since $\pi_0^2 = [-p]$, we have $\hat{\pi}_0 = -\pi_0$. Thus

$$\hat{\pi}_0 \circ \omega = -\pi_0 \circ \omega. \tag{3.14}$$

$\sigma_0 = \pi_0$ in FESTA

We have to analysis the eigenvectors of $\hat{\pi}_0 \circ \omega$. Since $\pi_0^2 = [-p]$, we have $\hat{\pi}_0 = -\pi_0$. Thus

$$\hat{\pi}_0 \circ \omega = -\pi_0 \circ \omega. \tag{3.14}$$

Since $p \equiv -1 \mod N$, we have

$$\pi_0^2 + p \equiv (\pi_0 + 1) \cdot (\pi_0 - 1) = 0 \mod N. \tag{3.15}$$

Let U, V be a basis of eigenvectors of π_0 on $E[N]$. Since $\pi_0 \circ 2i = -2i \circ \pi_0$, we assume that $V = 2i(U)$, we still have

$$\pi_0(V) = -V, \quad \pi_0(U) = U.$$

If $P = U + aV$ is an eigenvector of $\hat{\pi}_0 \circ \omega$, then we have

$$\pi_0 \circ (\alpha + \beta \cdot 2i)(U + aV) = \lambda(U + aV),$$

which implies that

$$4a^2\beta - 2a\alpha - \beta \equiv 0 \mod N. \tag{3.16}$$

If $P = U + aV$ is an eigenvector of $\hat{\pi}_0 \circ \omega$, then we have

$$\pi_0 \circ (\alpha + \beta \cdot 2i)(U + aV) = \lambda(U + aV),$$

which implies that

$$4a^2\beta - 2a\alpha - \beta \equiv 0 \mod N. \tag{3.16}$$

Combining with the condition

$$N^2 \geq \deg(\psi) = d^2 \cdot \deg(\omega) = d^2(\alpha^2 + 4\beta^2),$$

we can search for weak eigenspaces and get the proportion of weak eigenspaces for FESTA in the full basis, which is about

$$O(\min\{\frac{1}{d^2}, \frac{1}{B}\}).$$

Fail attack on CSIDH

For basis P, Q of $E_0[N]$, $S, T \in E[N]$ consisting of Frobenius eigenvectors, we have

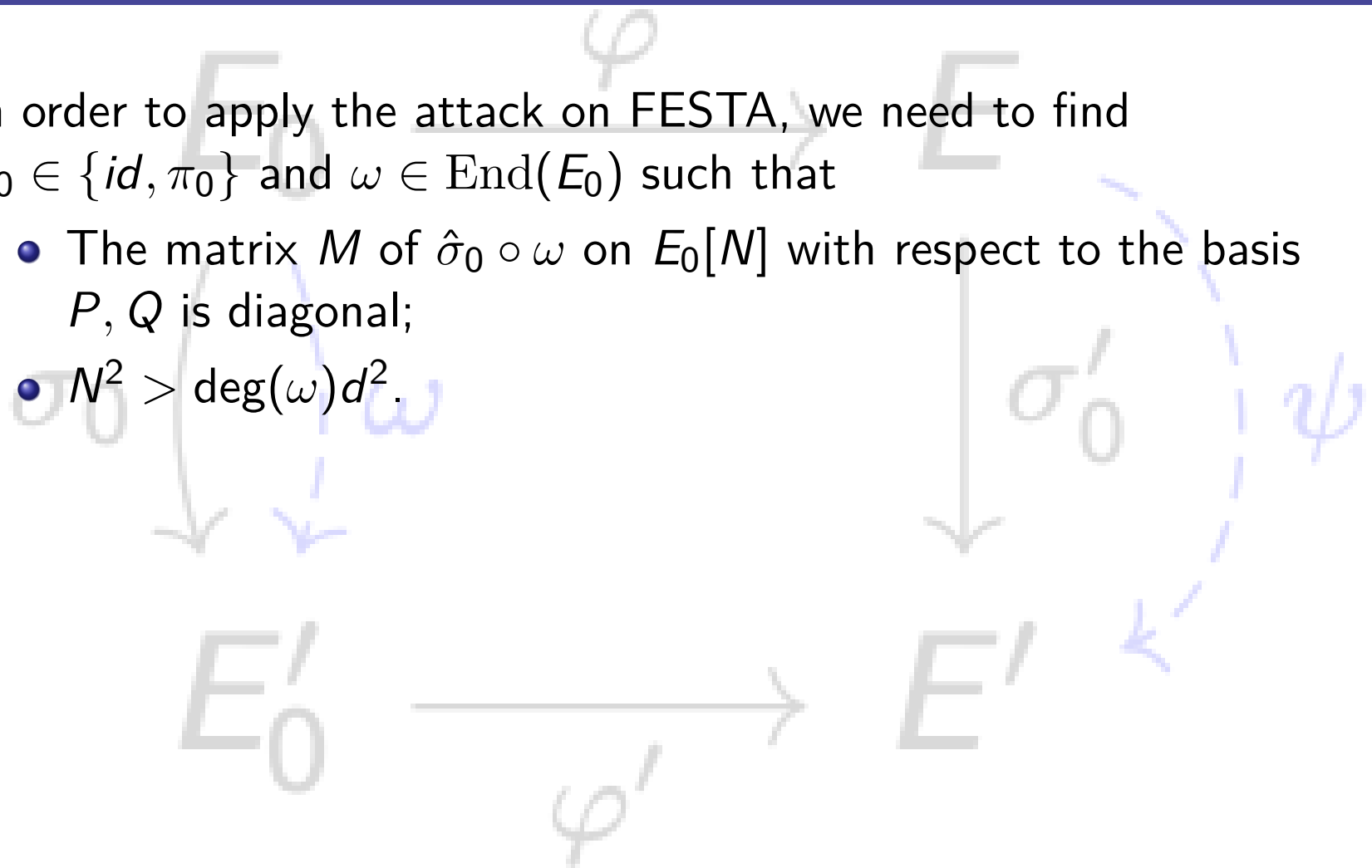
$$\begin{pmatrix} S \\ T \end{pmatrix} = \begin{pmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{pmatrix} \begin{pmatrix} \varphi(P) \\ \varphi(Q) \end{pmatrix}$$

where $\lambda_1, \lambda_2 \in (\mathbb{Z}/N\mathbb{Z})^\times$ and N can be taken arbitrarily large.

Fail attack on CSIDH

In order to apply the attack on FESTA, we need to find $\sigma_0 \in \{id, \pi_0\}$ and $\omega \in \mathrm{End}(E_0)$ such that

- The matrix M of $\hat{\sigma}_0 \circ \omega$ on $E_0[N]$ with respect to the basis P, Q is diagonal;
- $N^2 > \deg(\omega) d^2$.



In order to apply the attack on FESTA, we need to find $\sigma_0 \in \{id, \pi_0\}$ and $\omega \in \mathrm{End}(E_0)$ such that

- The matrix M of $\hat{\sigma}_0 \circ \omega$ on $E_0[N]$ with respect to the basis P, Q is diagonal;
- $N^2 > \deg(\omega) d^2$.

Unfortunately, these conditions imply that

$$\sigma_0 \circ \omega(\ker(\varphi)) = \ker(\varphi). \tag{3.17}$$

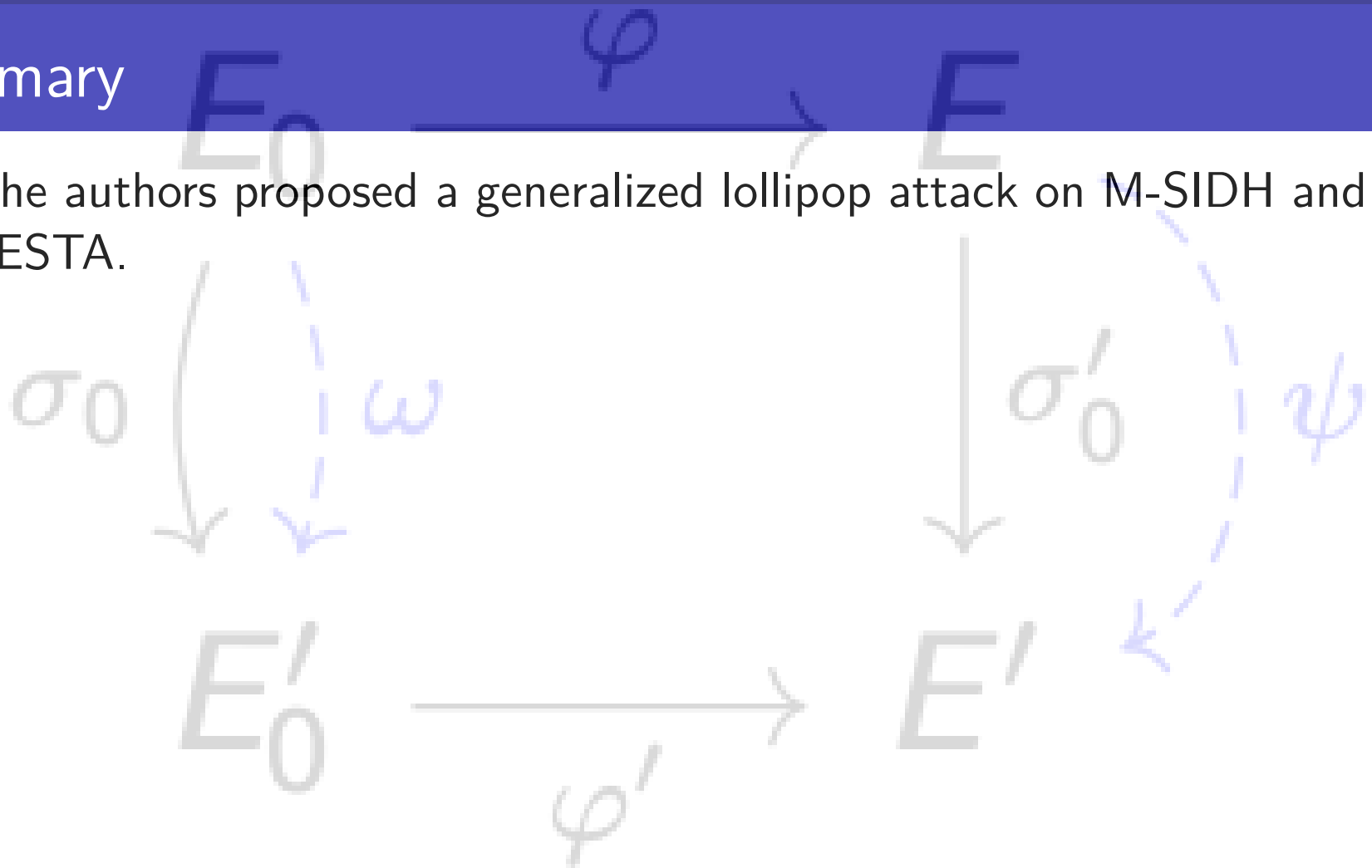
Thus

$$E[d] = \ker(\psi)[d]. \tag{3.18}$$

So we cannot get any new information of φ from ψ.

Summary

The authors proposed a generalized lollipop attack on M-SIDH and FESTA.



Summary

The authors proposed a generalized lollipop attack on M-SIDH and FESTA.

- For M-SIDH, it is broken whenever E_0 has a small endomorphism or is defined over $\mathbb{F}_p$. More general, if E_0 is close to its Frobenius conjugate or itself, then M-SIDH is insecure.

Summary

The authors proposed a generalized lollipop attack on M-SIDH and FESTA.

- For M-SIDH, it is broken whenever E_0 has a small endomorphism or is defined over $\mathbb{F}_p$. More general, if E_0 is close to its Frobenius conjugate or itself, then M-SIDH is insecure.
- For FESTA, only when the basis P, Q are eigenvectors of some small endomorphism composed with identity or Frobenius, the attack works. Thus they calculated the proportion of weak eigenspaces for FESTA in the full basis, which is about $O(\min\{\frac{1}{d^2}, \frac{1}{B}\})$.

Summary

The authors proposed a generalized lollipop attack on M-SIDH and FESTA.

- For M-SIDH, it is broken whenever E_0 has a small endomorphism or is defined over $\mathbb{F}_p$. More general, if E_0 is close to its Frobenius conjugate or itself, then M-SIDH is insecure.
- For FESTA, only when the basis P, Q are eigenvectors of some small endomorphism composed with identity or Frobenius, the attack works. Thus they calculated the proportion of weak eigenspaces for FESTA in the full basis, which is about $O(\min\{\frac{1}{d^2}, \frac{1}{B}\})$.
- The attack on CSIDH using the same strategy fails.

Thanks for listening!

Questions?