Studying FESTA

Mathieu Bouget

March 25, 2025

1 Preliminaries

2 SIDH

The Supersingular Isogeny Diffie-Hellmann is a scheme derived from the usual Diffie-Hellmann exchange where we have a group $G = \langle g \rangle$ and Alice choose a secret integer a and send g^a, Bob choose a secret b and send g^b to Alice, at the end they are both able to compute g^{ab} which is their shared secret. There is a starting curve E_0, Alice chooses an isogeny $\varphi_A : E_0 \to E_A$ and send E_A to Bob who sent in the same time the curve E_B he obtained from the isogeny $\varphi_B : E_0 \to E_B$ he had chosen before. This protocol requires additionnal information because it's not as simple as the case in group where the knowledge of g^b and a make Alice able to construct $g^{ab} = (g^b)^a$. Alice knows φ_A and E_B and would want to create something like $\varphi'_A : E_B \to E_{AB}$

2.1 High-level

Before going into more details about the mathematical tools (2-dimension isogenies) and strategies to break a generic SIDH instance, I introduce a generic condition on the degree of the secret isogeny and the torsion of E_0 that is sufficient to find φ.

Theorem 1 *[1] Let $\varphi : E_0 \to E$ be a secret degree disogeny (where d is known) and assume we are given the images of φ on a basis $\{P, Q\}$ of $E_0[N]$, where N and d are assumed smooth and coprime, and $N^2 > 4d$. Let $\mathbb{F}_q$ be the smallest field over which $E_0[N], E_0[d]$ and φ are defined, then the kernel of φ can be computed in a polynomial number of operations in $\mathbb{F}_q$.*

In fact this attack require only $N^2 > d$ to run but may return an ambiguous result in this case. Intuitively, the larger N the more information is given

about the behaviour of φ and the larger d is the more complex φ is and so is difficult to recover from torsion points. φ.

2.2 Mathematical tools

Giving the images of torsion points was considered safe until a mathematical result based on elliptic curve product and higher-dimensionnal isogenies gave ways to recover the secret isogeny in classical polynomial-time. We recall here a result that make torsion-point attacks possibles.

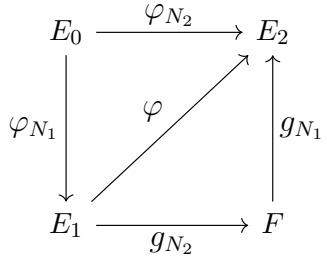
Theorem 2 *Let E_0, E_1 and 2 be three elliptic curves definied over $\overline{\mathbb{F}}_p$ such that there exist two isogenies $\varphi_{N_1} : E_0 \to E_1$ and $\varphi_{N_2} : E_0 \to E_2$ of coprime degrees $\deg(\varphi_{N_1}) = N_1$ and $\deg(\varphi_{N_2}) = N_2$. Then, the subgroup*

$$\{([N_2]\varphi_{N_1} \times [N_1]\varphi_{N_2}) \circ (P, P) \mid P \in E_0[N_1 + N_2]\}$$

is the kernel of a $(N_1 + N_2, N_1 + N_2)$-polarised isogeny Φ having product codomain $E_0 \times F$ and matrix form

$$\begin{pmatrix} \widehat{\varphi}_{N_1} & -\widehat{\varphi}_{N_2} \\ g_{N_2} & \widehat{g}_{N_1} \end{pmatrix}$$

where g_{N_i} are N_i-isogenies such that the following diagram commutes



In [2] and in attacks on SIDH, discussion are about finding an isogeny φ_f in order to use this theorem, once the isogeny has been found we juste need to evaluate a two-dimensions isogeny in order to recover the kernel of the secret isogeny φ_A.

3 FESTA

In 2023, a public key encryption scheme based on the SIDH attack was introduced in [3] and relies on a trapdoor function.

3.1 High-level description

The public parameters are a supersingular elliptic curve E_0 definied over $\mathbb{F}_{p^2}$ and a basis $\mathcal{B}_{E_0[2^b]} = (P_b, Q_b)$ of the 2^b-torsion of E_0.

The key generation consists in the choice of a secret isogeny φ_A from E_0 to a curve E_A, as in SIDH some additionnal information is given about φ_A. Since the knowledge of $\varphi_A|_{E[2^b]}$ (ie $(\varphi_A(P_b), \varphi_A(Q_b))$ lets an attacker able to recover φ_A, the information about behaviour of φ_A on the 2^b-torsion is scaled with a matrix $\mathbf{A}$ which belon to the trapdoor with φ_A. Thus, the trapdoor is $(\varphi_A, \mathbf{A})$ and the public key is $\mathtt{pk} = (E_A, R_A, S_A)$ where

$$\begin{pmatrix} R_A \\ S_A \end{pmatrix} = \mathbf{A} \cdot \varphi_A \begin{pmatrix} P_b \\ Q_b \end{pmatrix}$$

$$\begin{array}{ccc} E_0 & \xrightarrow{\varphi_A} & E_A \\ \Big\downarrow{\scriptstyle \varphi_1} & & \Big\downarrow{\scriptstyle \varphi_2} \\ E_1 & & E_2 \end{array}$$

Evaluation The inputs of the evaluation function are two isogeny $\varphi_1 : E_0 \to E_1$ and $\varphi_2 : E_A \to E_2$ plus a scaling matrix $\mathbf{B}$. Using a representation of the isogenies using a generator of their kernel described in a deterministicaly generated basis, the domain of $f_{\mathtt{pk}}$ is

$$\mathbb{Z}/d_1\mathbb{Z} \times \mathbb{Z}/d_2\mathbb{Z} \times \mathcal{M}_b$$

where $\mathcal{M}_b$ is the set of scaling matrices. The output of the function are curves E_1 and E_2 plus additionnal information about φ_1 and φ_2, that is some torsion points scaled with $\mathbf{B}$. The output is $(E_1, R_1, S_1, E_2, R_2, S_2)$ where

$$\begin{pmatrix} R_1 \\ S_1 \end{pmatrix} = \mathbf{B} \cdot \varphi_1 \begin{pmatrix} P_b \\ Q_b \end{pmatrix} \qquad \begin{pmatrix} R_2 \\ S_2 \end{pmatrix} = \mathbf{B} \cdot \varphi_2 \begin{pmatrix} R_A \\ S_A \end{pmatrix} = \mathbf{B} \cdot \varphi_2 \cdot \mathbf{A} \cdot \varphi_A \begin{pmatrix} P_b \\ Q_b \end{pmatrix}$$

Inversion We have

$$\begin{aligned}
(\varphi_2 \circ \varphi_A \circ \widehat{\varphi}_1) \begin{pmatrix} R_1 \\ S_1 \end{pmatrix} &= \varphi_2 \circ \varphi_A \circ \widehat{\varphi}_1 \cdot \mathbf{B}\varphi_1 \begin{pmatrix} P_b \\ Q_b \end{pmatrix} \\
&= \mathbf{B} \cdot \varphi_2 \circ \varphi_A \circ [\widehat{\varphi}_1 \circ \varphi_1] \begin{pmatrix} P_b \\ Q_b \end{pmatrix} \\
&= [d_1]\mathbf{B} \cdot \varphi_2 \circ \varphi_A \begin{pmatrix} P_b \\ Q_b \end{pmatrix} \\
&= [d_1]\mathbf{B}\mathbf{A^{-1}} \cdot \varphi_2 \circ \mathbf{A}\varphi_A \begin{pmatrix} P_b \\ Q_b \end{pmatrix} \\
&= [d_1]\mathbf{B}\mathbf{A^{-1}} \cdot \varphi_2 \begin{pmatrix} R_A \\ S_A \end{pmatrix} \\
&= [d_1]\mathbf{B}\mathbf{A^{-1}} \cdot \mathbf{B} \begin{pmatrix} R_2 \\ S_2 \end{pmatrix} \\
&= [d_1]\mathbf{A^{-1}} \cdot \begin{pmatrix} R_2 \\ S_2 \end{pmatrix}
\end{aligned}$$

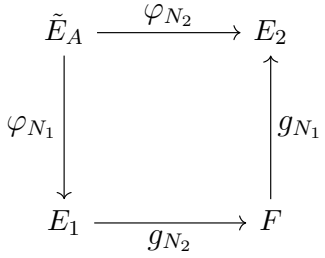
Then we can recover the isogeny $\psi = \varphi_2 \circ \varphi_A \circ \widehat{\varphi}_1$ using the SIDH attack, extraction of isogenies φ_1 and φ_2 follows (and $\mathbf{B}$) using the knowledge of φ_A.

3.2 Low-level description

A pure SIDH on ψ would be too expensive to be used in a decryption algorithm so there is a specific construction of φ_A during the setup phase in order to make the attack more efficient. More precisely, there will not be any research phase of a suitable isogeny to construct the 2-dimension isogeny as it is the case in the general SIDH attack. During the setup, two isogenies are actually generated such that their degrees fill the equality $m_1^2 d_{A,1} d_1 + m_2^2 d_{A,2} d_2 = 2^b$ for some $m_1, m_2, b \in \mathbb{Z}$ and from these we compute φ_A.

$$\varphi_A = \varphi_{A,2} \circ \varphi_{A,1}$$

Note that no information about $\varphi_{A,1}$, $\varphi_{A,2}$ (such at $\varphi_{A,1}(P_b)$) is public so it doesn't change the security of the protocol. To recover φ_1 and φ_2 we can use the Theorem 2 with $\varphi_{N_1} = [m_1] \circ \varphi_1 \circ \widehat{\varphi}_{A,1}$ and $\varphi_{N_2} = [m_2] \circ \varphi_2 \circ \varphi_{A,2}$.



We have $N_1 + N_2 = m_1^2 d_1 d_{A,1} + m_2^2 d_2 d_{A,2} = 2^b$ so $\tilde{E}_A[N_1 + N_2]$ is the 2^b-torsion of $\tilde{E}_A$. We have, with $P'_b = \varphi_{A,1}(P_b)$ and $Q'_b = \varphi_{A,1}(Q_b)$.

$$\begin{aligned}
[N_2]\varphi_{N_1}(P'_b) &= [N_2][m_1] \circ \varphi_1 \circ \tilde{\varphi}_{A,1}(P'_b) \\
&= [N_2][m_1] \circ \varphi_1 \circ \tilde{\varphi}_{A,1} \circ \varphi_{A,1}(P_b) \\
&= [N_2][m_1][d_{A,1}] \circ \varphi_1(P_b) \\
&= [m_2^2 d_{A,2} d_2][m_1][d_{A,1}] \circ \varphi_1(P_b) \\
&= [m_2 m_1 d_{A,1}][m_2 d_{A,2} d_2] \circ \varphi_1(P_b) \\
N_1\varphi_{N_2}(P'_b) &= [N_1][m_2] \circ \varphi_2 \circ \varphi_{A,2}(P'_b) \\
&= [N_1][m_2] \circ \varphi_2 \circ \varphi_{A,2} \circ \varphi_{A,1}(P_b) \\
&= [N_1][m_2] \circ \varphi_2 \circ \varphi_A(P_b) \\
&= [N_1][m_2] \circ \varphi_2 \circ \varphi_A(P_b) \\
&= [m_1^2 d_{A,1} d_1][m_2] \circ \varphi_2 \circ \varphi_A(P_b) \\
&= [m_2 m_1 d_{A,1}][m_1 d_1] \circ \varphi_2 \circ \varphi_A(P_b)
\end{aligned}$$

The know the $\varphi_2 \circ \varphi_A(P_b)$ and $\varphi_1(P_b)$ using $\mathbf{A}^{-1}$ up to the matrix $\mathbf{B}$ but it's sufficient to have the whole kernel of ϕ the 2-isogeny which has matrix form :

$$\begin{pmatrix} \varphi_{N_1} & \widehat{\varphi}_{N_2} \\ \_ & \_ \end{pmatrix}$$

4 Attacks

The security of FESTA is based on the hardness of isogeny interpolation when the images of the torsion are scaled with some matrix. Breaking this problem would breaks the entire protocol, however there is a stronger assumption that is made in FESTA which is that there are two interpolation with the same scaling matrix.

4.1 Computational isogeny with scaled-torsion problem

Even if FESTA relies on a stronges assumption that this problem, there is a major intrest in sutdying current strategies used to break a CIST instance. I briefly introduce the one provided in [4].

We want to recover a secret isogeny $\varphi : E_0 \to E$ of known degree d. We are given the points $S, T \in E[N]$ such that

$$\begin{pmatrix} S \\ T \end{pmatrix} = \mathbf{A} \cdot \varphi \begin{pmatrix} P \\ Q \end{pmatrix}$$

where (P, Q) is a basis of $E_0[N]$ the N-torsion of E_0 and $\mathbf{A}$ a secret matrix.

A direct "SIDH" attack on φ isn't possible here because of the scaling matrix $\mathbf{A}$. So an idea is to attack another isogeny that doesn't contain $\mathbf{A}$ but still discloses information about φ.

For instance, if ω is an endomorphism of E_0, then recovering isogeny $\psi = \varphi \circ \omega \circ \widehat{\varphi}$ could give clues on φ. Intuitively, the presence of φ and $\widehat{\varphi}$ corresponds to an application of $\mathbf{A}$ and then $\mathbf{A}^{-1}$ so it should cancel the scaling as long as ω "commute" with this matrix. More formally, we require that the endomorphism ω acting on $E_0[B]$ as a matrix $\mathbf{M}$ in the basis (P, Q) that commutes with $\mathbf{A}$.

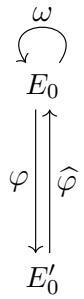
$$\omega \begin{pmatrix} P \\ Q \end{pmatrix} = \mathbf{M} \begin{pmatrix} P \\ Q \end{pmatrix}$$

This way we have, denoting w the degree of ω :

$$\begin{aligned} \varphi \circ \omega \circ \widehat{\varphi} \begin{pmatrix} S \\ T \end{pmatrix} &= \varphi \circ \omega \circ [d]\mathbf{A} \begin{pmatrix} P \\ Q \end{pmatrix} \\ &= [d]\mathbf{A} \circ \varphi \circ \omega \begin{pmatrix} P \\ Q \end{pmatrix} \\ &= [d]\mathbf{AM} \circ \varphi \begin{pmatrix} P \\ Q \end{pmatrix} \\ &= [d]\mathbf{AMA^{-1}} \begin{pmatrix} S \\ T \end{pmatrix} \\ &= [d]\mathbf{M} \begin{pmatrix} S \\ T \end{pmatrix} \end{aligned}$$

This equality implies that it is possible to get the images of $\varphi \circ \omega \circ \widehat{\varphi}$ on the basis (P, Q) of the N-torsion from the only knowledge of the matrix $\mathbf{M}$ and the points (S, T). Then, if the degree of this isogeny is small enough (in fact

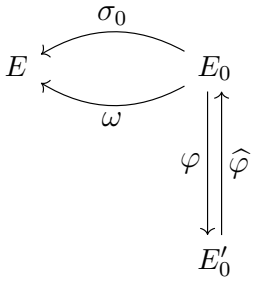
$N^2 > wd^2$), it is possible to recover it completly using SIDH attack. However, recovering this isogeny does not always give meaningfull information about φ. Let's take the trivial example of $\omega = \mathrm{Id}_{E_0}$, the isogeny $\varphi \circ \omega \circ \widehat{\varphi}$ is in this case $[d]$ which doesn't contain any additionnal information on φ.



We need to controll the degree of ω in order to apply the SIDH attack. There is an improvement of this technique that reduces the degree in some cases. We now set ω to be an isogeny from E_0 to some other curve E and take another isogeny $\sigma_0 : E_0 \to E$. We controll the endomorphism $\omega' = \widehat{\sigma}_0 \circ \omega$ by the matrix $\mathbf{M}$:

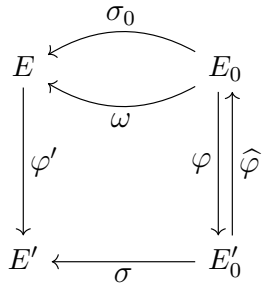
$$(\widehat{\sigma}_0 \circ \omega) \begin{pmatrix} P \\ Q \end{pmatrix} = \mathbf{M} \begin{pmatrix} P \\ Q \end{pmatrix}$$

The diagram is now



The required inequality for using SIDH attack on ψ is $N^2 > swd^2$ where s is the degree of σ_0. For the moment it corresponds to the previous one since $w' = ws$, but the point is that the knowledge of the pushforward of σ_0 through φ eliminates s. Let assume we know σ the pushforward of σ_0 through φ, that is the isogeny that has kernel $\varphi(\mathrm{Ker}\sigma_0)$ going from E'_0 to another curve E' and that effectively computable in some situation. To delete the s of the conditon we need to eliminate σ_0 in $\psi = \varphi \circ \widehat{\sigma}_0 \circ \omega \circ \widehat{\varphi}$ so we let $\psi = \varphi' \circ \omega \circ \widehat{\varphi}$ with φ' the pushforward of φ through σ (we don't

need to actually compute it, as φ we have knowledge on it up to the scaling matrix $\mathbf{A}$). We have the following diagram :



The degree of ψ is clearly wd^2 since φ and φ' have the same degree d. Moreover we have $\varphi' \circ \sigma_0 = \sigma \circ \varphi$ and so $[s]\varphi' = \sigma \circ \varphi \circ \widehat{\omega}_0$. Here is the proof that we can find an SIDH instance on ψ, the found equality is the Lemma 3 of [4].

$$\begin{aligned}
[s]\psi \begin{pmatrix} S \\ T \end{pmatrix} &= [s]\varphi' \circ \omega \circ \widehat{\varphi} \begin{pmatrix} S \\ T \end{pmatrix} \\
&= [s]\varphi' \circ \omega \circ \widehat{\varphi}\mathbf{A}\varphi \begin{pmatrix} P \\ Q \end{pmatrix} \\
&= [sd]\mathbf{A}\varphi' \circ \omega \circ \begin{pmatrix} P \\ Q \end{pmatrix} \\
&= [d]\mathbf{A}\sigma \circ \varphi \circ \widehat{\sigma}_0 \circ \omega \begin{pmatrix} P \\ Q \end{pmatrix} \\
&= [d]\mathbf{A}\mathbf{M}\sigma \circ \varphi \begin{pmatrix} P \\ Q \end{pmatrix} \\
&= [d]\mathbf{A}\mathbf{M}\mathbf{A}^{-\mathbf{1}}\sigma \begin{pmatrix} S \\ T \end{pmatrix} \\
&= [d]\mathbf{M}\sigma \begin{pmatrix} S \\ T \end{pmatrix}
\end{aligned}$$

References

[1] Damien Robert. Breaking sidh in polynomial time. In Carmit Hazay and Martijn Stam, editors, *Advances in Cryptology – EUROCRYPT 2023*, pages 472–503, Cham, 2023. Springer Nature Switzerland.

[2] Luciano Maino, Chloe Martindale, Lorenz Panny, Giacomo Pope, and Benjamin Wesolowski. A direct key recovery attack on sidh. In Car-

mit Hazay and Martijn Stam, editors, *Advances in Cryptology – EUROCRYPT 2023*, pages 448–471, Cham, 2023. Springer Nature Switzerland.

[3] Andrea Basso, Luciano Maino, and Giacomo Pope. Festa: Fast encryption from supersingular torsion attacks. In Jian Guo and Ron Steinfeld, editors, *Advances in Cryptology – ASIACRYPT 2023*, pages 98–126, Singapore, 2023. Springer Nature Singapore.

[4] Wouter Castryck and Frederik Vercauteren. A polynomial time attack on instances of m-sidh and festa. In Jian Guo and Ron Steinfeld, editors, *Advances in Cryptology – ASIACRYPT 2023*, pages 127–156, Singapore, 2023. Springer Nature Singapore.