A Note on FESTA

Subham Das

Indian Institute of Science Education and Research, Mohali
su8h.das@gmail.com

1 Introduction

In the article [BMP23] the authors claim that the choice of diagonal matrices to scale torsion point images in the countermeasure FESTA is not a singular choice, and that the security of the scheme shall not be jeopardized if the commutative subgroup of diagonal matrices could be replaced by any other commutative subgroup of invertible matrices, such as that of circulant matrices[1]. In the framework of [FFP24], it is interesting to ask if the corresponding level structures reduce to each other. Here we confirm that the circulant case indeed reduces to the diagonal case as proposed in [BMP23] when the scaling matrices are defined over $(\mathbb{Z}/N\mathbb{Z})^\times$ for $N = p^r$ for prime $p > 2$. In the special case when the matrices are defined over finite fields i.e, $N = p$ for some large prime, the reduction to the diagonal case holds for any (non-trivial) commutative subalgebra. However, when $N = 2^k$, we show that a reduction between the two cases is not possible by our method, which is in contrast to the aforementioned claim.

2 Preliminaries

2.1 Matrices

Definition 2.1. *A $n \times n$ circulant matrix C takes the following form:*

$$\begin{pmatrix} c_0 & c_{n-1} & \cdots & c_2 & c_1 \\ c_1 & c_0 & c_{n-1} & & c_2 \\ \vdots & c_1 & c_0 & \ddots & \vdots \\ c_{n-2} & & \ddots & \ddots & c_{n-1} \\ c_{n-1} & c_{n-2} & \cdots & c_1 & c_0 \end{pmatrix}$$

Definition 2.2. *For a ring R and $n \geq 1$, let $\alpha \in R$ be a principal n-th root of unity. The Discrete Fourier transform over a ring R is defined as follows (in*

[1] Implicitly, the choice of scaling matrices sourced from the group must be non-trivial to prevent exploitation by the SIDH attacks.

matrix notation):

$$\begin{pmatrix} f_0 \\ f_1 \\ \vdots \\ f_{n-1} \end{pmatrix} = \begin{pmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & \alpha & \alpha^2 & \cdots & \alpha^{n-1} \\ 1 & \alpha^2 & \alpha^4 & \cdots & \alpha^{2(n-1)} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \alpha^{n-1} & \alpha^{2(n-1)} & \cdots & \alpha^{(n-1)(n-1)} \end{pmatrix} \begin{pmatrix} v_0 \\ v_1 \\ \vdots \\ v_{n-1} \end{pmatrix}$$

2.2 Level structures

We shall use the framework of isogeny problems with level structure as proposed in [FFP24] to phrase the underlying problem in FESTA. The definition of a Γ-SIDH problem is as follows:

Definition 2.3. *Fix coprime integers d, N and $\Gamma \leq GL_2(\mathbb{Z}/N\mathbb{Z})$. Let $E \xrightarrow{\phi} E'$ be an isogeny of degree d and S be a Γ level structure.*
The (d, Γ)-modular isogeny problem (of level N) asks that given $(E, S, E', \phi(S))$ to compute ϕ. When d is clear, this is referred to as the Γ-SIDH problem.

If one replaces Γ by $\left\{ \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} \right\} \leq SL_2$, then we have the underlying Γ-SIDH problem for FESTA, and analogously for other Γ.

3 Reduction

Lemma 3.1. *For a matrix $A \in SL_2(\mathbb{Z}/N\mathbb{Z})$ and $\Gamma \leq SL_2(\mathbb{Z}/N\mathbb{Z})$, a Γ-SIDH problem reduces to $A^{-1}\Gamma A$-SIDH problem, given an oracle to solve discrete log in $\mu_N \subset \mathbb{F}_{q^r}^\times$, the subgroup of nth roots of unity.*

Proof. Let (E, S, E', S') be a Γ-SIDH problem. Choose a representative (P, Q) of S, and compute its Weil pairing $W_1 := e_N(P, Q)$. Define $\bar{S} = A^{-1}\Gamma A \cdot (P, Q)$. The Weil pairing gives us

$$e_N(\phi(\bar{S})) = e_N(\bar{S})^{\deg \phi} = W_1^d$$

Now, choose a representative $(P', Q') := \phi(P, Q)$ of $\phi(S)$ and compute the Weil pairing $W_2 = e_N(P', Q')$. Use the oracle to compute discrete logarithm x of W_1^d to base W_2 and find a matrix $\gamma' \in \Gamma$ such that $\det \gamma' = x$. Define $\bar{S}' := A^{-1}\Gamma A \cdot \gamma' \cdot (P', Q')$; then $\bar{S}' = \phi(\bar{S})$. Hence $(E, \bar{S}, E', \bar{S}')$ is an instance of $A^{-1}\Gamma A$-SIDH problem, having the same solution as the Γ-SIDH problem. □

3.1 For $N = p^k$ with odd p

Lemma 3.2. *If C denotes a circulant matrix defined over[2] $\mathbb{Z}/N\mathbb{Z}$ and F denotes the Discrete Fourier transform matrix defined over $\mathbb{Z}/N\mathbb{Z}$, then for some diagonal matrix D we have that $C = F^{-1}DF$.*

[2] This theorem holds for any ring R such that F is invertible in $\mathcal{M}_{n\times n}(R)$.

Proof. Any circulant matrix can be decomposed into a polynomial in terms of the permutation matrix P as $C = \sum_{i=0}^{n} c_i P^i$ where c_i are entries of the circulant matrix. Since the permutation matrix is defined over R, the eigenvectors of P are $(\alpha^k, \alpha^{2k}, \ldots, \alpha^{(n-1)k})$ for $0 \leq k \leq n-1$ where α is a principal n-th root of unity. Then the permutation matrix (and subsequently linear combination of it's powers) can be diagonalized by conjugating with a matrix which has the eigenvectors as columns. This matrix is precisely the Discrete Fourier Transform matrix as defined above. Hence the circulant matrix can be written as $C = F^{-1}DF$ where D is the diagonal matrix obtained from the linear combination of diagonal matrices. □

Using the above two lemmas, one can conclude the following theorem:

Theorem 3.3. *For* $\mathfrak{D} = \left\{ \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} \right\}$ *and* $\mathfrak{C} = \left\{ \begin{pmatrix} a & b \\ b & a \end{pmatrix} \right\}$ *such that both are subgroups of* $SL_2(\mathbb{Z}/N\mathbb{Z})$*, where* $N = p^k$ *for* $p > 2$ *and* $k > 0$*. Then the* $\mathfrak{C}$*-SIDH problem reduces to* $\mathfrak{D}$*-SIDH problem.*

3.2 For $N = 2^k$

Theorem 3.4. *For a invertible matrix of the form* $\begin{pmatrix} a & b \\ b & a \end{pmatrix}$*, there does not exist a diagonalization over the ring* $\mathbb{Z}/N\mathbb{Z}$ *where* $N = 2^k$*, for* $k > 0$*.*

Proof. Let $A : \begin{pmatrix} a & b \\ b & a \end{pmatrix} \in SL_2(\mathbb{Z}/N\mathbb{Z})$ such that it is invertible, which implies $\det A = (a^2 - b^2)$ is a unit. Since the odd numbers in $(\mathbb{Z}/N\mathbb{Z})$ are the units, it is not possible if both a and b are odd (or even), hence one must be odd and the other must be a even for the matrix A to be invertible. Without loss of generality, assume that a is a even and b is a odd.

The characteristic polynomial of A is $p(t) = (t-a)^2 - b^2$. If we solve the equation for the eigenvalues, $(t-a)^2 = b^2 \mod N$ entails that $(t-a)$ is a odd since b is a odd. Since a is a even and $(t-a)$ is a odd, it implies that the eigenvalues must be a odd. Let λ be an eigenvalue of A and $v := \begin{pmatrix} x \\ y \end{pmatrix}$ be the corresponding eigenvector. From the equation $Av = \lambda v$ we obtain the equations $ax + by = \lambda x \mod N$ and $ay + bx = \lambda y \mod N$. Adding both of them, we obtain $(a + b - \lambda)(x + y) = 0 \mod N$.

Suppose x, y are not both odd (or even) at the same time, i.e, $(x + y)$ and $(x - y)$ are odd. This implies that $(a + b - \lambda) = 0 \mod N \implies a + b = \lambda \mod N$. Then substituting λ in the equation $ax + by = \lambda x \mod N$ we have $b(y - x) = 0 \mod N$. Since both are odd by assumption, it is a clear contradiction. Hence x, y must be both odd (or even). We have the modular matrix[3] (v_1, v_2) obtained from the corresponding eigenvectors v_i whence $v_i = \begin{pmatrix} x_i \\ y_i \end{pmatrix}$ with x_i, y_i being both odd (or even). However for all possible combinations of v_i (i.e, when v_i is comprised

[3] The matrix P such that $A = PDP^{-1}$ where D is a diagonal matrix.

of units or non-units), the modular matrix turns out to be singular. This entails that a diagonalization is not possible for A over the ring $(\mathbb{Z}/N\mathbb{Z})$. $\square$

Hence our strategy of the previous section fails and we cannot say anything conclusively regarding the reduction of the circulant case to the original diagonal case. This is indeed contrasting to the claim of [BMP23], since this reduction does not hold when $N = 2^k$, a parameter choice made in FESTA.

3.3 Finite Fields

For a finite field $k = \mathbb{Z}/p\mathbb{Z}$ for $p > 2$, it is a well known result that the 2-dimensional commutative matrix subalgebras of $\mathcal{M}_{n\times n}(k)$ could be classified up to isomorphism as follows:

$$\mathfrak{D} = \left\{ \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} \right\} \quad \mathfrak{C} = \left\{ \begin{pmatrix} a & b \\ b & a \end{pmatrix} \right\} \quad \mathfrak{T} = \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \right\}$$

In [FFP24] the authors have already showed the reductions between $\mathfrak{T}$ and $\mathfrak{D}$. In Theorem 3.3 above, we have shown that $\mathfrak{C}$ reduces to $\mathfrak{D}$. Thus one can conclude that for $N = p$, the choice for any commutative subalgebra in FESTA still reduces to the original formulation of FESTA.

Acknowledgements. I would like to thank Prof. Péter Kutas for posing the question and verifying the results.

References

BMP23. Andrea Basso, Luciano Maino, and Giacomo Pope. FESTA: Fast encryption from supersingular torsion attacks. Cryptology ePrint Archive, Paper 2023/660, 2023.

FFP24. Luca De Feo, Tako Boris Fouotsa, and Lorenz Panny. Isogeny problems with level structure. Cryptology ePrint Archive, Paper 2024/459, 2024.