A note on the genus of the HAWK lattice

Daniël M. H. van Gent
Centrum Wiskunde en Informatica
dmhvg@cwi.nl

January 2025

The cryptographic scheme and NIST candidate HAWK [DPPvW22; ABC$^+$24] makes use of a particular *module lattice* and relies for its security on the assumption that finding module lattice isomorphisms (module LIP) is hard. To support this assumption, we compute the *mass* of the HAWK lattice, which gives a lower bound on the number of isometry classes of module lattices which cannot be distinguished from the HAWK lattice by an easily computed invariant called the *genus*. This number turns out to be so large that an attack based on the genus alone seems infeasible.

We assume the reader is familiar with some basic number theory. We will use definitions and notation from [Kir16], restating some. Fix some integers $m \geq 1$ and $n \geq 2$. Let $E = \mathbb{Q}(\zeta)$ be the number field where ζ is a primitive 2^n-th root of unity and let $K = \mathbb{Q}(\zeta + \zeta^{-1})$ be its maximal totally real subfield. We write $\overline{\cdot}$ for the non-trivial automorphism of E over K, which is given by $\zeta \mapsto \zeta^{-1}$. We equip E with a positive definite Hermitian form $\Phi(x, y) = \overline{x} \cdot y$. The maximal order $\mathcal{O}_E$ of E is an $\mathcal{O}_E$-lattice in E, and we let $H = \mathcal{O}_E^m$ be its m-fold orthogonal sum. This H is the module lattice used by HAWK when $m = 2$ and $n \in \{9, 10, 11\}$, depending on the security parameter.

Definition 1. Let Λ be an $\mathcal{O}_E$-lattice. We write $\Lambda_\mathfrak{p}$ for its localization at a prime ideal $\mathfrak{p}$ of K, and $[\Lambda]$ for its isometry class. The *genus* of Λ is the sequence $g(\Lambda) = ([\Lambda_\mathfrak{p}])_\mathfrak{p}$, where $\mathfrak{p}$ ranges over all primes of K. The *mass* of Λ is

$$\mathrm{Mass}(\Lambda) = \mathrm{Mass}(g(\Lambda)) = \sum_{[\Lambda']} \frac{1}{\#\,\mathrm{Aut}(\Lambda')},$$

where the sum ranges over all isometry classes of lattices with genus $g(\Lambda)$.

Although we are more interested in the in the number of terms in the above sum, the ‘size’ of the genus, a lower bound of $\{\zeta^i \mid i \in \mathbb{Z}\} \subseteq \mathrm{Aut}(\Lambda')$ for every $\mathcal{O}_E$-lattice Λ' shows that the number of isometry classes with genus g is at least $2^n \cdot \mathrm{Mass}(g)$. We can efficiently compute the mass of a genus using Siegel’s mass formula, which we specialize for $\mathcal{O}_E$.

Theorem 2 (cf. Proposition 4.2.7 in [Kir16])**.** *Let Λ be an $\mathcal{O}_E$-lattice of rank m. Then*

$$\mathrm{Mass}(\Lambda) = 2^{1-m2^{n-1}} \cdot \prod_{\mathfrak{p}} \lambda(\Lambda_\mathfrak{p}) \cdot \prod_{i=1}^{m} \begin{cases} \frac{\zeta_E}{\zeta_K}(1-i) & \text{if } i \text{ is odd} \\ \zeta_K(1-i) & \text{if } i \text{ is even} \end{cases},$$

where λ is as in Definition 4.2.6 of [Kir16], $\mathfrak{p}$ ranges over all primes of K, and ζ is the Dedekind zeta function. □

It remains to compute the local factors $\lambda(H_\mathfrak{p})$. However, compared to the zeta functions they barely contribute to the mass.

Write $\mathrm{d}_{B/A}$ for the relative discriminant of a finite separable field extension $A \subseteq B$, and similarly $N_{B/A}$ and $\mathrm{Tr}_{B/A}$ for its relative norm and trace. We first collect some data about the field extension $K \subseteq E$.

Lemma 3. *The extensions $E/\mathbb{Q}$ and $K/\mathbb{Q}$ are totally ramified above 2 with primes $\mathfrak{P} = (1-\zeta)$ and say $\mathfrak{p}$ respectively, and are unramified elsewhere. We also have $\mathrm{d}_{E/K} = \mathfrak{p}^2$ and $\mathrm{Tr}_{E/K}(\mathcal{O}_E) \subseteq \mathfrak{p}$.*

Proof. We refer to [Neu99]. Note that $\mathcal{O}_E = \mathbb{Z}[\zeta] = \mathbb{Z}[X]/(f)$ for $f = X^{2^{n-1}} + 1$ by (I.10.2). Hence

$$\mathrm{d}_{E/\mathbb{Q}} = N_{E/\mathbb{Q}}(f'(\zeta)) \cdot \mathbb{Z} = N_{E/\mathbb{Q}}(2^{n-1}\zeta^{2^{n-1}-1}) \cdot \mathbb{Z} = 2^{(n-1)2^{n-1}} \cdot \mathbb{Z}$$

by (III.2.4) and (III.2.9). By (I.10.1), the extension $E/\mathbb{Q}$ is totally ramified above 2 with prime $\mathfrak{P} = (1-\zeta)$, while it is unramified elsewhere by (III.2.12). Consequently, $K/\mathbb{Q}$ is totally ramified above 2 with some prime $\mathfrak{p}$, and $\mathfrak{P}^2 = \mathfrak{p}\mathcal{O}_E$.

Note that $\mathcal{O}_K = \mathcal{O}_E \cap K = \mathbb{Z}[\zeta+\zeta^{-1}]$ and $\mathcal{O}_E = \mathcal{O}_K[\zeta] = \mathcal{O}_K[X]/(g)$ for $g = X^2 - (\zeta+\zeta^{-1})X + 1$. Since $(1-\zeta^2)\mathbb{Z}[\zeta^2]$ is the prime of $\mathbb{Q}(\zeta^2)$ above 2, we have $\mathfrak{P}^2 = (1-\zeta^2)\mathcal{O}_E = (\zeta - \zeta^{-1})\mathcal{O}_E$. Then

$$\mathrm{d}_{E/K} = N_{E/K}(g'(\zeta)) \cdot \mathcal{O}_K = N_{E/K}(\zeta - \zeta^{-1}) \cdot \mathcal{O}_K = N_{E/K}(\mathfrak{P}^2) = \mathfrak{p}^2, \quad \text{and}$$
$$\mathrm{Tr}_{E/K}(\mathcal{O}_E) = \mathrm{Tr}_{E/K}(1 \cdot \mathcal{O}_K + \zeta \cdot \mathcal{O}_K) = 2 \cdot \mathcal{O}_K + (1+\zeta^2)\zeta^{-1} \cdot \mathcal{O}_K \subseteq \mathfrak{P}^2 \cap \mathcal{O}_K = \mathfrak{p},$$

as was to be shown. □

Lemma 4. *Let $\mathfrak{p}$ be a prime of K. Then*

$$\lambda(H_\mathfrak{p}) = \begin{cases} 1 & \text{if } \mathfrak{p} \text{ is odd} \\ 2^{-1} & \text{if } \mathfrak{p} \text{ is even and } m \text{ is odd} \\ 2^m - 1 & \text{if } \mathfrak{p} \text{ is even and } m \text{ is even} \end{cases}.$$

Proof. Note that $H_\mathfrak{p}$ is unimodular, i.e. $\mathfrak{p}^0$-modular. If $\mathfrak{p}$ is odd, we are done by Lemma 4.2.9 in [Kir16]: We are in the case where $E_\mathfrak{p}/K_\mathfrak{p}$ is either split or inert by Lemma 3, $\dim_K(E) = 2$ and $m = m_0$. Now assume $\mathfrak{p}$ is the unique prime above 2. If m is odd, we are done by Theorem 4.5.2 in [Kir16], so assume m is even. We compute the parameters to Theorem 4.5.5 in [Kir16]. We have $q = \#(\mathcal{O}_K/\mathfrak{p}) = 2$ and $e = \mathrm{ord}_\mathfrak{p}(\mathrm{d}_{E/K}) = 2$ by Lemma 3. We have $\mathfrak{n}(H_\mathfrak{p}) = \mathcal{O}_{K,\mathfrak{p}}$ and $\mathfrak{n}(\mathfrak{P}H_\mathfrak{p}) = \mathfrak{p}\mathcal{O}_{K,\mathfrak{p}}$, so $\ell_0 = 0$ and $\ell_1 = 1$. Since the hyperbolic lattices have norm $\mathrm{Tr}_{E/K}(\mathfrak{P}^i) \subseteq \mathrm{Tr}_{E/K}(\mathcal{O}_K) \subseteq \mathfrak{p}$ by Lemma 3, we conclude that we are not in case 1 of the theorem. Hence $\lambda(H_\mathfrak{p}) = q^{m(e/2-1)}(q^m - 1) = 2^m - 1$. □

Table 5. We compute the mass of H for $m = 2$ and multiple values of n.

n	$(\zeta_E/\zeta_K)(0)$	$\zeta_K(-1)$	$\mathrm{Mass}(H)$
7	$1.36969375610352 \cdot 2^{43}$	$1.16760364270761 \cdot 2^{149}$	$1.19944456426526 \cdot 2^{67}$
8	$1.13294712862486 \cdot 2^{119}$	$1.43912186258186 \cdot 2^{395}$	$1.22283673646503 \cdot 2^{261}$
9	$1.02161863077143 \cdot 2^{301}$	$1.09587067352026 \cdot 2^{984}$	$1.67934284547651 \cdot 2^{775}$
10	$1.52878054160373 \cdot 2^{729}$	$1.27373529240083 \cdot 2^{2353}$	$1.46044629763225 \cdot 2^{2061}$
11	$1.74088377909975 \cdot 2^{1714}$	$1.72075720829338 \cdot 2^{5475}$	$1.12336436688259 \cdot 2^{5145}$

We used the following PARI/GP [PARI] code.

```
fE=x^(2^(n-1))+1;
fK=minpoly(Mod(x+1/x,fE));
zE=lfun(fE,x+O(x^2))/lfun(fK,x+O(x^2))
zK=lfun(fK,-1)
mass=2^(1-2^n)*3*zE*zK
```

We take $m = 2$. Note that the rank of H as $\mathbb{Z}$-lattice is $m2^{n-1} = 2^n$. For $8 \leq n \leq 11$, the mass of H is larger than 2^{2^n}. It shows that the genus has insufficient distinguishing power to efficiently solve the Decisional Lattice Isomorphism Problem (DLIP): If H' is a random lattice in the genus of H, the probability that it is isomorphic to H is negligible. Moreover, for $n \in \{10, 11\}$, the mass is also larger than $(2^{2^n})^2$, leaving no room for a genus-based quantum search or birthday attack either.

The following corollary to the mass formula shows that a LIP to DLIP reduction, as for example in [Szy03], based on the genus alone would be infeasible, since all $\mathcal{O}_E$-lattice in E^2 have large mass.

Corollary 6. *If $\Lambda \subseteq E^2$ is an $\mathcal{O}_E$-lattice of rank* 2*, then* $\mathrm{Mass}(\Lambda) \geq \frac{1}{3}\mathrm{Mass}(\mathcal{O}_E^2)$.

Proof. By Proposition 4.2.10 in [Kir16] and Lemma 3 we have $\prod_{\mathfrak{p}} \lambda(\Lambda_{\mathfrak{p}}) \geq 1$. The result then follows from Theorem 2 and Lemma 4. □

References

[PARI] *PARI/GP version 2.15.4*. available from http://pari.math.u-bordeaux.fr/. The PARI Group. Univ. Bordeaux, 2023.

[ABC+24] G. Alagic, M. Bros, P. Ciadoux, D. Cooper, Q. Dang, T. Dang, J. Kelsey, J. Lichtinger, YK. Liu, C. Miller, D. Moody, R. Peralta, R. Perlner, A. Robinson, H. Silberg, D. Smith-Tone, and N. Waller. *Status Report on the First Round of the Additional Digital Signature Schemes for the NIST Post-Quantum Cryptography Standardization Process*. NIST IR 8528, 2024. DOI: https://doi.org/10.6028/NIST.IR.8528.

[DPPvW22] Léo Ducas, Eamonn W. Postlethwaite, Ludo N. Pulles, and Wessel van Woerden. Hawk: module LIP makes lattice signatures fast, compact and simple. In Springer-Verlag, 2022.

[Kir16] Markus Kirschmer. *Definite quadratic and hermitian forms with small class number (Habilitation)*. RWTH Aachen University, 2016.

[Neu99] Jürgen Neukirch. *Algebraic Number Theory*. Springer Berlin, 1999.

[Szy03] Michael Szydlo. Hypercubic lattice reduction and analysis of ggh and ntru signatures. In Eli Biham, editor, *Advances in Cryptology — EUROCRYPT 2003*, pages 433–448. Springer Berlin Heidelberg, 2003.