Improved Practical Key Recovery on HAWK

MiniMax

November 2026

Abstract

HAWK is a lattice-based digital signature scheme introduced at ASIACRYPT 2022 that bases its security on the module lattice isomorphism problem over power-of-two cyclotomic rings. Its secret key is a unimodular two-by-two basis over the ring of integers of degree n, while the public key is the associated Hermitian Gram matrix. For the challenge parameter set HAWK-256 at ring degree $n = 256$, the specification claims 64 bits of security against key recovery. Recently, Straznickas and Weis (ePrint 2026/1593) reduced HAWK-n key recovery to shortest vector computation in a public rank-n cocycle lattice associated with the half-period Galois involution, followed by an intertwiner sublattice separation and a tower descent over nested subfields. Their released HAWK-256 pipeline requires progressive lattice sieving up to dimension 118 and consumes approximately 1.28×10^6 CPU-core-seconds across 96 cores (3 h 42 min wall-clock).

In this paper, we present an improved end-to-end key recovery attack against HAWK-256 driven solely from a genuine 450-byte reference public key on a single CPU core in 1,851.8 CPU-core-seconds (30.9 minutes). First, rather than applying modulo-two parity only as a post-hoc filter, we close the parity congruence into a public sublattice $\Lambda' \subset \Lambda_\tau$ of index 2^{n-1}. While Λ' preserves both the ambient rank n and the provable two-block SVP oracle dimension $n/2 + 1$, its covolume sparsification isolates the secret cocycle element as the unique shortest vector up to sign with gap $\lambda_2/\lambda_1 = 2$, eliminates the intertwiner stage, and lowers the expected BKZ block size by $\Delta\beta(n) = \frac{\ln 2}{2}\, n/\ln n + O(n/\ln^2 n)$ (from $92 \to 58$ at HAWK-256, $205 \to 156$ at HAWK-512, and $432 \to 351$ at HAWK-1024). Second, we show that the root Hermite factor required to reach $\lambda_1(\Lambda')$ at $n = 256$ is strictly less than unity, and we overcome severe condition-number squaring in Gram-mode basis reduction via an exact high-precision Cholesky embedding coupled with fast integer lattice reduction. This basis preconditioning lowers the required maximum sieve dimension from 118 to 80, yielding a 690× end-to-end speedup verified by the reference implementation and reducing the heuristic gate security of HAWK-256, HAWK-512, and HAWK-1024 by 9.28, 11.15, and 23.74 bits, respectively.

1 Introduction

Lattice-based cryptography provides versatile foundations for post-quantum digital signatures, most notably through the hash-and-sign paradigm pioneered by GPV [14] and realized over NTRU lattices in FALCON [19]. While FALCON achieves compact signatures and public keys, its signing algorithm relies on floating-point fast Fourier orthogonalization and variable-time Gaussian sampling over cyclotomic fields, which complicates constant-time implementation and side-channel protection.

To address these implementation challenges, Ducas, Postlethwaite, Pulles, and van Woerden introduced HAWK at ASIACRYPT 2022 [9], basing its security on the Module Lattice Isomorphism Problem (Module-LIP) [11, 9]. Instead of hiding a secret basis of a specific NTRU module, HAWK fixes the canonical module lattice $\mathbb{Z}^{2n}$—viewed as the rank-two free module R_n^2 over the power-of-two cyclotomic ring $R_n = \mathbb{Z}[\zeta_{2^\ell}]$ of degree $n = 2^{\ell-1}$—and selects a short unimodular basis $B \in \mathrm{SL}_2(R_n)$ as the secret key. The public key is the Hermitian Gram matrix $Q = B^*B \in M_2(R_n)$, where B^* denotes the conjugate transpose under the complex conjugation

involution of R_n. Because the secret geometry is isomorphic to the trivial orthogonal lattice $\mathbb{Z}^{2n}$, Gaussian sampling during signing reduces to simple integer sampling in the secret frame followed by multiplication by B^{-1}, avoiding floating-point arithmetic altogether.

The HAWK NIST specification [10] defines three parameter sets: HAWK-256 ($n = 256$, $\ell = 9$), which serves as a cryptanalytic challenge instance claiming 64 bits of classical security, and the NIST Round 3 standardization candidates HAWK-512 ($n = 512$, $\ell = 10$, NIST Level I) and HAWK-1024 ($n = 1024$, $\ell = 11$, NIST Level V). Following the τ-cocycle cryptanalysis of Straznickas and Weis [23], the HAWK specification was withdrawn from the NIST post-quantum standardization process on July 29, 2026 [10].

1.1 Prior Cryptanalysis

Direct lattice reduction attacks against HAWK embed the public Gram matrix Q into a rank-$2n$ Euclidean lattice and search for any unit-norm vector of the quadratic form defined by Q, corresponding to a secret basis column. Under standard lattice reduction heuristics, solving this search problem in dimension $2n$ requires prohibitively large block sizes even at $n = 256$. Subsequent algebraic analyses investigated symplectic automorphisms for the one-more-SVP problem [16], subfield-guessing attacks and their super-polynomial complexity [17, 21], and a conditional reduction from rank $2n$ to rank n given a nontrivial automorphism [13].

A major breakthrough was achieved by Straznickas and Weis [23], who made the rank-n descent unconditional by exploiting the Galois tower of power-of-two cyclotomic fields. Let $\tau : \zeta_{2^\ell} \mapsto -\zeta_{2^\ell}$ denote the Galois involution fixing the subfield of degree $n/2$. Rather than recovering B directly, they targeted the multiplicative τ-cocycle element $V_\tau = B^{-1}\tau(B) \in \mathrm{SL}_2(R_n)$. Because $Q = B^*B$ is public, V_τ satisfies two public $\mathbb{Q}$-linear matrix constraints (an adjoint symmetry condition and a Gram intertwining relation, defined formally in Section 3). The integer matrices satisfying both constraints form a public rank-n lattice Λ_τ, termed the τ-cocycle lattice.

Straznickas and Weis proved that the isometry class of Λ_τ under its trace-determinant form is completely independent of the secret key: up to scaling by $\sqrt{n/4}$, it decomposes orthogonally as $\mathbb{Z}^{n/2+1} \oplus \sqrt{2}\,\mathbb{Z}^{n/2-1}$. As a result, Λ_τ possesses $n/2 + 1$ pairs of mutually orthogonal shortest vectors of Euclidean length $\sqrt{n/4}$, only one pair of which is $\pm V_\tau$. Their attack pipeline finds short vectors in Λ_τ via progressive lattice sieving, isolates $\pm V_\tau$ using an auxiliary intertwiner sublattice construction [23, Remark 6.2] or post-hoc parity filtering, and finally descends the cyclotomic tower $\ell \to \ell - 1 \to \cdots \to 3$ to recover an equivalent secret key B_{rec} satisfying $B_{\mathrm{rec}}^* B_{\mathrm{rec}} = Q$. At $n = 256$, their released pipeline drives a progressive multi-core sieve [24] up to maximum sieving dimension 118, taking 3 hours and 42 minutes on a 96-core Intel Sapphire Rapids server ($\approx 1.28 \times 10^6$ allocated CPU-core-seconds, or $\approx 1.11 \times 10^6$ active thread-seconds).

1.2 Our Contributions and Technical Overview

In this work, we demonstrate that end-to-end key recovery against HAWK-256 at its full ring degree $n = 256$ can be executed on a single CPU core in 1,851.8 CPU-core-seconds (30.9 minutes CPU, 31.0 minutes wall-clock)—7.2× faster in wall-clock time on 1/96 of the cores and a factor of 690× lower in allocated core-seconds (601× in active thread-seconds) than the previously published pipeline [23]. Our attack takes only the 450-byte reference public key as input and outputs a 592-byte secret key accepted by the authors' unmodified reference signer and verifier. We establish three results that account for this improvement:

1. **Lattice Dimension Invariance vs. Lattice Quality Optimization in Λ'.** Because the involution τ acts as the identity modulo 2 on R_n, the secret cocycle element always satisfies $V_\tau \equiv I \pmod 2$. Whereas prior work [23] treated this congruence as an $O(n)$ post-hoc filter applied after sieving, we close the congruence coset $2\Lambda_\tau \cup (2\Lambda_\tau + I)$ into a public

sublattice $\Lambda' = 2\Lambda_\tau + \mathbb{Z}w_0 \subset \Lambda_\tau$ of index 2^{n-1} by solving a single public linear system over $\mathbb{F}_2$. Passing from Λ_τ to Λ' does *not* reduce the lattice dimension: Λ' retains full $\mathbb{Z}$-rank n, preserves the provable two-block SVP oracle dimension $n/2+1$, and shares the leading asymptotic GSA block-size ratio $\lim_{n\to\infty} \beta(n)/n = 1/2$. Instead, Λ' substantially improves the *lattice quality*: multiplying the covolume by 2^{n-1} at unchanged target norm $\lambda_1(\Lambda') = \sqrt{n/4}$ halves the Hermite ratio $\lambda_1/\operatorname{vol}^{1/n}$ from $\approx 2^{-1/4} = 0.8409$ to $\approx 2^{-5/4} = 0.4204$ (0.4222 at $n = 256$), isolates $\pm V_\tau$ as the unique shortest vector pair with gap $\lambda_2(\Lambda')/\lambda_1(\Lambda') = 2$, and eliminates the intertwiner stage. Asymptotically, this reduces the GSA block size by $\Delta\beta(n) = \frac{\ln 2}{2}\, n/\ln n + O(n/\ln^2 n)$; concretely, it lowers the expected BKZ block size β from $92 \to 58$ at HAWK-256, $205 \to 156$ at HAWK-512, and $432 \to 351$ at HAWK-1024.

2. **Structural Limit Analysis and Exact Cholesky Preconditioning.** We show that for Λ' at rank $n = 256$, the Hermite ratio $\lambda_1(\Lambda')/\operatorname{vol}(\Lambda')^{1/256} = 0.4222$ implies a required root Hermite factor of $0.996624 < 1$. Because any basis reduction algorithm governed by the Geometric Series Assumption enforces a root Hermite factor at least 1, pure profile flattening can never reach $\lambda_1(\Lambda')$; recovery can succeed only when a block-SVP or sieving oracle detects the tail projection of V_τ. In addition, we show that what forces prior pipelines to sieve up to dimension 118 is not the intrinsic geometry of the lattice, but severe ill-conditioning of its natural integer basis ($\approx 2^{41}$ basis condition number), which is squared when processed in Gram mode. By computing an exact high-precision Cholesky factorization of the Gram matrix, embedding it into an integer basis, reducing it with `flatter` [20], and recovering the exact unimodular transformation via triangular backward substitution, we compress the Gram matrix from 40–41-bit entries to 27-bit entries with a Gram diagonal ratio of 2.2–3.0 and a 4× better post-LLL starting norm.

3. **Sieve Dimension Reduction from 118 to 80 and Security Impact on HAWK-512/1024.** Alongside pre-sieving conditioning ablations ($\delta = 0.75$ LLL at 12.9× speedup over $\delta = 0.99$ and BKZ-20 profile equilibration), feeding our Cholesky-preconditioned basis directly into the General Sieve Kernel (`g6k`) [2] progressive pump-and-jump tour recovers $\pm V_\tau$ on a single core at sieve dimension $d = 80$ rather than $d = 118$ in 1,469.5 s (1,851.8 s end-to-end). Because the sieve database scales as $2^{0.2075d}$ and runtime scales as database$^{1.13}$, dropping the maximum sieve dimension by 38 predicts a 481× reduction in sieve work, matching our measured 690× end-to-end speedup. Across the full HAWK family, our sublattice construction reduces heuristic AGPS20 gate complexity by 9.28 bits on HAWK-256 ($2^{50.83} \to 2^{41.56}$), 11.15 bits on HAWK-512 ($2^{80.79} \to 2^{69.64}$), and 23.74 bits on HAWK-1024 ($2^{146.48} \to 2^{122.73}$).

1.3 Paper Organization

Section 2 establishes our notation for power-of-two cyclotomic fields, Galois involutions, Hermitian forms, and Euclidean lattice reduction invariants. Section 3 reviews the HAWK signature specification and the construction of the τ-cocycle lattice Λ_τ. Section 4 introduces the modulo-two sublattice Λ', proves its index, isometry class, and unique-SVP gap, and explains how it eliminates the intertwiner stage. Section 5 analyzes the structural Hermite limit at $n = 256$ and details our exact Cholesky basis preconditioning and conditioning schedule. Section 6 describes the progressive sieving tour, exact coordinate recovery, and τ-tower descent. Section 7 presents our sieve dimension scaling analysis, experimental measurements, and extrapolations to HAWK-512 and HAWK-1024. Section 8 discusses the scope and limitations of our results.

Table 1: Comparison of end-to-end key recovery attacks against HAWK-256 ($n = 256$, $\ell = 9$).

Metric	**Straznickas–Weis [23]**	**This Work**
Target lattice	Λ_τ (rank 256)	$\Lambda' \subset \Lambda_\tau$ (rank 256)
Sublattice index $[\Lambda_\tau : \Lambda']$	1	2^{255}
Minimal vector pairs at λ_1	129	1 ($\pm V_\tau$)
Spectral gap (λ_2/λ_1)	1	2
Intertwiner stage	Required	Eliminated
Expected BKZ block size β	92	58
Basis preconditioning	Gram-mode LLL/BKZ	Exact Cholesky + `flatter`
Maximum sieve dimension $d_{\max}$	118	80
Sieve database size[a]	$\approx 2.35 \times 10^7$	$\approx 9.93 \times 10^4$
Allocated CPU cores	96	1
Total CPU time[b]	$\approx$ 1,278,720 s	**1,851.8 s**
End-to-end speedup factor[b]	1.0×	**690**×
Reference C verification	Pass	Pass ($B^*_{\mathrm{rec}} B_{\mathrm{rec}} = Q$)

[a] Heuristic database size $(4/3)^{d/2} \approx 2^{0.2075d}$ at maximum sieve dimension d. [b] Baseline: 3 h 42 min wall-clock across 96 Sapphire Rapids cores ($\approx 1.28 \times 10^6$ allocated core-s, or $\approx 1.11 \times 10^6$ active thread-s giving 601×). This work: 30.9 min CPU (31.0 min wall) on 1 core.

2 Preliminaries

We first summarize the algebraic properties of power-of-two cyclotomic fields, their Galois involutions, and the Euclidean lattice reduction invariants used throughout this paper.

2.1 Cyclotomic Fields and Rings of Integers

Let $\ell \geq 2$ be an integer and set $n = 2^{\ell-1}$. We denote by $L = \mathbb{Q}(\zeta_{2^\ell})$ the 2^ℓ-th cyclotomic field generated by a primitive 2^ℓ-th root of unity $\zeta = \zeta_{2^\ell}$ satisfying $\zeta^n + 1 = 0$. The field L is a totally complex Galois extension of $\mathbb{Q}$ of degree $[L : \mathbb{Q}] = n$. Its ring of integers is the monogenic polynomial ring

$$R_n \;=\; \mathcal{O}_L \;=\; \mathbb{Z}[\zeta] \;\cong\; \mathbb{Z}[X]/(X^n + 1).$$

Every element $f \in L$ expands uniquely in the power basis $\{1, \zeta, \ldots, \zeta^{n-1}\}$ as $f = \sum_{j=0}^{n-1} f_j \zeta^j$ with rational coefficients $f_j \in \mathbb{Q}$, and $f \in R_n$ if and only if $f_j \in \mathbb{Z}$ for all $0 \leq j < n$. We identify $f \in L$ with its coefficient vector $(f_0, f_1, \ldots, f_{n-1})^T \in \mathbb{Q}^n$. The absolute field trace $\mathrm{Tr}_{L/\mathbb{Q}} : L \to \mathbb{Q}$ satisfies $\mathrm{Tr}_{L/\mathbb{Q}}(1) = n$ and $\mathrm{Tr}_{L/\mathbb{Q}}(\zeta^j) = 0$ for all $1 \leq j < n$, so that $\mathrm{Tr}_{L/\mathbb{Q}}(f) = n f_0$.

2.2 Galois Automorphisms and Fixed Subfields

The Galois group $\mathrm{Gal}(L/\mathbb{Q}) \cong (\mathbb{Z}/2^\ell\mathbb{Z})^\times \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{\ell-2}\mathbb{Z}$ acts on L by sending $\zeta \mapsto \zeta^k$ for odd integers k. Three commuting involutions play a central role in the cryptanalysis of HAWK:

1. **Complex conjugation c:** defined by $c(\zeta) = \zeta^{-1} = -\zeta^{n-1}$. Its fixed subfield is the maximal totally real subfield $L^+ = \mathbb{Q}(\zeta + \zeta^{-1})$ of degree $n/2$.

2. **The half-period involution τ:** defined by $\tau(\zeta) = \zeta^{1+n} = -\zeta$. In the power basis, τ acts diagonally by negating odd-indexed coordinates:

$$\tau\Big(\sum_{j=0}^{n-1} f_j \zeta^j\Big) \;=\; \sum_{j=0}^{n-1} (-1)^j f_j \zeta^j.$$

   Its fixed subfield is the previous cyclotomic field in the power-of-two tower,

$$K \;=\; L^{\langle\tau\rangle} \;=\; \mathbb{Q}(\zeta^2) \;=\; \mathbb{Q}(\zeta_{2^{\ell-1}}),$$

   which has degree $[K : \mathbb{Q}] = n/2$ and ring of integers $R_{n/2} = \mathbb{Z}[\zeta^2]$.

3. **The composite involution** $\sigma = c\tau = \tau c$**:** defined by $\sigma(\zeta) = -\zeta^{-1} = \zeta^{n-1}$.

The subgroup $\langle c, \tau \rangle \cong (\mathbb{Z}/2\mathbb{Z})^2$ fixes the totally real subfield $F = L^{\langle c,\tau\rangle} = K^+ = \mathbb{Q}(\zeta^2 + \zeta^{-2})$ of degree $[F : \mathbb{Q}] = n/4$. All three involutions preserve the ring of integers R_n and extend entrywise to matrices over L and R_n.

2.3 Matrix Operations and Hermitian Gram Forms

For any 2×2 matrix $Y = \left(\begin{smallmatrix} y_{00} & y_{01} \\ y_{10} & y_{11} \end{smallmatrix}\right) \in M_2(L)$, its classical adjoint (adjugate) is

$$\operatorname{adj}(Y) \;=\; \begin{pmatrix} y_{11} & -y_{01} \\ -y_{10} & y_{00} \end{pmatrix},$$

which is a $\mathbb{Q}$-linear involution on $M_2(L)$ satisfying $Y \operatorname{adj}(Y) = \operatorname{adj}(Y)Y = (\det Y)I_2$. When $Y \in \mathrm{SL}_2(R_n)$, we have $\det Y = 1$ and hence $Y^{-1} = \operatorname{adj}(Y) \in M_2(R_n)$. We write $Y^* = c(Y)^T$ for the Hermitian conjugate transpose of Y. A matrix $Q \in M_2(L)$ is Hermitian if $Q^* = Q$, and totally positive definite if x^*Qx is totally positive in L^+ for every nonzero $x \in L^2$. For any basis matrix $B \in \mathrm{SL}_2(R_n)$, its Hermitian Gram matrix $Q = B^*B$ is Hermitian, unimodular ($\det Q = 1$), and totally positive definite.

2.4 Euclidean Lattices and Reduction Heuristics

A full-rank Euclidean lattice Λ of rank d is a discrete additive subgroup $\Lambda = \mathbb{Z}b_1 \oplus \cdots \oplus \mathbb{Z}b_d$ equipped with a positive definite symmetric bilinear form $\langle \cdot, \cdot \rangle$ and norm $\|v\| = \sqrt{\langle v, v \rangle}$. Given an ordered basis $\mathbf{B} = (b_1, \ldots, b_d)$, its Gram matrix is $G = (\langle b_i, b_j \rangle)_{1 \le i,j \le d} \in M_d(\mathbb{R})$. The volume (covolume) of Λ is $\operatorname{vol}(\Lambda) = \sqrt{\det G}$, which is an invariant independent of the choice of basis; if $\mathbf{B}' = U\mathbf{B}$ for a unimodular transformation $U \in \mathrm{GL}_d(\mathbb{Z})$, then $G' = UGU^T$ and $\det G' = \det G$. For a full-rank sublattice $\Lambda' \subset \Lambda$ of finite index $[\Lambda : \Lambda']$, their volumes and Gram determinants satisfy

$$\operatorname{vol}(\Lambda') \;=\; [\Lambda : \Lambda']\, \operatorname{vol}(\Lambda), \qquad \det \mathrm{Gram}(\Lambda') \;=\; [\Lambda : \Lambda']^2 \det \mathrm{Gram}(\Lambda).$$

The i-th successive minimum $\lambda_i(\Lambda)$ is the smallest radius $r > 0$ such that the closed ball of radius r contains i linearly independent vectors of Λ. The Gaussian Heuristic predicts that the shortest nonzero vector of a random rank-d lattice has norm $\mathrm{GH}(\Lambda) \approx \sqrt{d/(2\pi e)}\, \operatorname{vol}(\Lambda)^{1/d}$. A basis reduction algorithm such as LLL [15] or BKZ [22, 5] with root Hermite factor $\delta_0 \ge 1$ produces a first basis vector b_1 satisfying $\|b_1\| \le \delta_0^{d-1} \operatorname{vol}(\Lambda)^{1/d}$. Under the Geometric Series Assumption (GSA) [5, 1], the Gram–Schmidt orthogonalized vectors b_i^* of a BKZ-β reduced basis satisfy $\|b_i^*\|/\|b_{i-1}^*\| \approx \delta_\beta^{-2}$, where $\delta_\beta = \big((\pi\beta)^{1/\beta}\beta/(2\pi e)\big)^{1/(2(\beta-1))} > 1$ for $\beta \ge 36$. In a unique-SVP (uSVP) instance where $\lambda_1(\Lambda) \ll \mathrm{GH}(\Lambda)$, BKZ-$\beta$ or a progressive sieve of dimension d_{sieve} recovers the unique shortest vector $\pm v_{\min}$ once the orthogonal projection of $v_{\min}$ onto the tail subspace $\operatorname{span}(b_{d-\beta+1}^*, \ldots, b_d^*)$ becomes shorter than the local Gaussian heuristic of that tail block [1].

The $\times 8$ Integer Gram Convention. Following the convention in the HAWK cryptanalysis pipeline [23], quadratic forms defined via normalized field traces over F are scaled by 8 so that all Gram matrices have exact integer entries. In this convention, a vector of theoretical Euclidean norm $\sqrt{n/4}$ has integer Gram norm squared $8 \cdot (n/4) = 2n$. At $n = 256$, the target integer squared norm of $\pm V_\tau$ is therefore $2n = 512$, and the integer Gram determinant shifts by $8^n = 2^{3n}$ relative to the unscaled trace form.

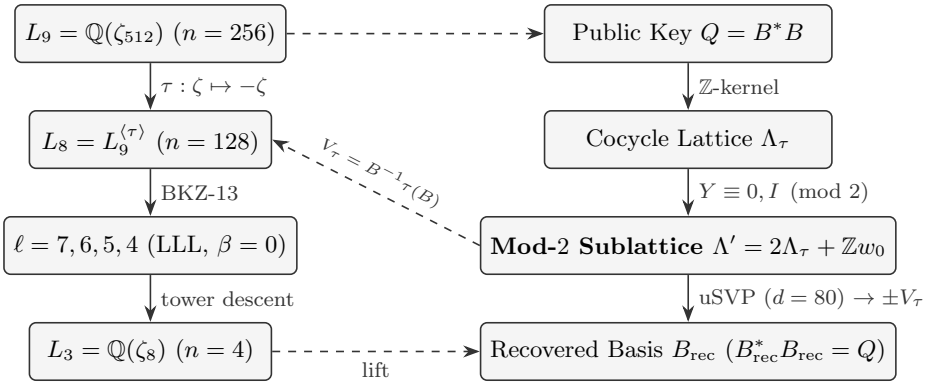

Figure 1: Algebraic structure of HAWK-256 key recovery: the cyclotomic field tower $L_9 \supset L_8 \supset \cdots \supset L_3$ on the left and our cocycle sublattice reduction pipeline $\text{pk} \to \Lambda_\tau \to \Lambda' \to V_\tau \to B_{\text{rec}}$ on the right.

3 Specification of HAWK and the Cocycle Lattice

This section reviews the key generation procedure and Module-LIP security formulation of HAWK [9, 10], followed by the algebraic construction and key-independent geometry of the τ-cocycle lattice Λ_τ introduced by Straznickas and Weis [23].

3.1 HAWK Key Generation and the Module-LIP Problem

In HAWK-n [9, 10], key generation samples a secret unimodular matrix $B = \left(\begin{smallmatrix} f & F \\ g & G \end{smallmatrix}\right) \in \mathrm{SL}_2(R_n)$ whose entries have small coefficients in the power basis of R_n and satisfy $fG - gF = 1$. The secret key encodes B (a compact 592-byte decoded secret key layout at $n = 256$ containing (f, g, F, G) and precomputed signing data), while the public key is a compressed encoding of the Hermitian Gram matrix

$$Q \;=\; B^*B \;=\; \begin{pmatrix} q_{00} & q_{01} \\ q_{10} & q_{11} \end{pmatrix} \in M_2(R_n),$$

where $q_{00}, q_{11} \in R_n \cap L^+$ are self-conjugate and $q_{10} = c(q_{01})$. At $n = 256$, the compressed public key occupies exactly 450 bytes.

Recovering a valid signing key from the public key Q is an instance of the search Module-LIP problem over R_n: given Q, find any secret basis $B_{\text{rec}} \in \mathrm{SL}_2(R_n)$ such that

$$B_{\text{rec}}^* B_{\text{rec}} \;=\; Q. \tag{1}$$

Any two solutions B_{rec} and B of (1) are related by $B_{\text{rec}} = UB$, where $U \in \mathrm{SL}_2(R_n)$ is a unitary matrix satisfying $U^*U = I_2$. By Kronecker's theorem on roots of unity in R_n, any such unitary transformation U is signed-permutation equivalent to I_2 up to powers of ζ [11, 9], meaning that B_{rec} has the exact same Euclidean geometry and signing capability as B. Thus, any equivalent basis B_{rec} satisfying (1) is a fully functional secret key accepted by the reference implementation.

3.2 The τ-Cocycle Lattice Λ_τ

Rather than attacking $Q = B^*B$ in dimension $2n$, Straznickas and Weis [23] observed that applying the half-period involution τ to $Q = B^*B$ yields $\tau(Q) = \tau(B)^*\tau(B)$. Eliminating the unknown secret basis B in favor of the multiplicative τ-cocycle element

$$V_\tau \;=\; B^{-1}\tau(B) \;\in\; \mathrm{SL}_2(R_n) \tag{2}$$

exposes linear algebraic relations that V_τ must obey. First, because τ is an involution and $\det V_\tau = 1$, we have $\tau(V_\tau) = \tau(B)^{-1}B = V_\tau^{-1} = \mathrm{adj}(V_\tau)$. Second, substituting $\tau(B) = BV_\tau$ into $\tau(Q) = \tau(B)^*\tau(B)$ gives

$$\tau(Q) \;=\; (BV_\tau)^*(BV_\tau) \;=\; V_\tau^* B^* B V_\tau \;=\; V_\tau^* Q V_\tau.$$

Multiplying on the left by $(V_\tau^*)^{-1} = (\mathrm{adj}(V_\tau))^T = c(\tau(V_\tau))^T = \sigma(V_\tau)^T$ turns this quadratic relation into a linear intertwining equation in V_τ. Figure 1 illustrates the resulting algebraic hierarchy.

Definition 1 (The τ-Cocycle Lattice Λ_τ [23])**.** For a public Gram matrix $Q \in M_2(R_n)$, the τ-cocycle lattice $\Lambda_\tau \subset M_2(R_n)$ is the $\mathbb{Z}$-module of integral matrices satisfying the two linear constraints

$$\Lambda_\tau \;=\; \Big\{ Y \in M_2(R_n) \;\Big|\; \underbrace{\tau(Y) = \mathrm{adj}(Y)}_{\text{(C1)}},\quad \underbrace{QY = \sigma(Y)^T \tau(Q)}_{\text{(C2)}} \Big\}. \tag{3}$$

Direct public computation of Λ_τ from the public key relies on the fact that both (C1) and (C2) are homogeneous $\mathbb{Q}$-linear equations in the $4n$ integer coordinates of $Y \in M_2(R_n) \cong \mathbb{Z}^{4n}$. Constraint (C1) imposes $\tau(y_{00}) = y_{11}$, $\tau(y_{01}) = -y_{01}$, and $\tau(y_{10}) = -y_{10}$, which immediately halves the ambient dimension from $4n$ to $2n$. Constraint (C2) then imposes n independent linear equations determined by the public entries of Q and $\tau(Q)$, cutting the rank down to n.

Proposition 2 (Rank, Quadratic Form, and Key-Independent Isometry Class of Λ_τ [23])**.** *Let $Q = B^*B$ for any $B \in \mathrm{SL}_2(R_n)$. Then Λ_τ is a saturated public $\mathbb{Z}$-submodule of $M_2(R_n)$ of rank n. Equipped with the bilinear form induced by the trace-determinant quadratic form*

$$q_\tau(Y) \;=\; \mathrm{Tr}_{F/\mathbb{Q}}(\det Y),$$

the Euclidean lattice (Λ_τ, q_τ) has the key-independent isometry class [23, Lemmas 4.3–4.4 and Proposition 4.5]

$$\Lambda_\tau \;\cong\; \sqrt{\frac{n}{4}} \Big(\mathbb{Z}^{\,n/2+1} \;\oplus\; \sqrt{2}\,\mathbb{Z}^{\,n/2-1} \Big). \tag{4}$$

In particular, $\lambda_1(\Lambda_\tau) = \sqrt{n/4}$ is attained by exactly $n/2+1$ pairs of mutually orthogonal shortest vectors, one pair of which is $\pm V_\tau = \pm B^{-1}\tau(B)$.

Proposition 2 reveals both the power and the bottleneck of working directly in Λ_τ. On the one hand, conjugation by B maps Λ_τ isometrically onto the canonical cocycle lattice of the identity Gram matrix $Q = I_2$, which explains why the geometry of Λ_τ is completely independent of the secret key B. In the $\times 8$ integer Gram convention at $n = 256$, Proposition 2 predicts the exact log-determinant

$$\log_2 \det \mathrm{Gram}(\Lambda_\tau) \;=\; n \log_2(2n) + \Big(\frac{n}{2} - 1\Big) \;=\; 256 \times 9 + 127 \;=\; 2431.00, \tag{5}$$

providing a bit-exact certificate that an extracted integer basis spans the full saturated kernel Λ_τ. On the other hand, because Λ_τ contains $\mathbb{Z}^{n/2+1}$ scaled by $\sqrt{n/4}$, there are $n/2 + 1 = 129$ pairs of shortest vectors tied at the exact same minimum norm $\lambda_1(\Lambda_\tau)$, corresponding to 128 spurious norm-one units alongside the single target $\pm V_\tau$. Any shortest vector solver operating on Λ_τ is confronted with a 129-fold degenerate minimum, forcing the pipeline of [23] to collect a large pool of minimal vectors via high-dimension sieving and subsequently separate $\pm V_\tau$ using an auxiliary intertwiner sublattice.

4 The Modulo-Two Sublattice and Unique-SVP Reduction

We now construct the modulo-two cocycle sublattice $\Lambda' \subset \Lambda_\tau$, determine its index and key-independent isometry class, and prove that it isolates the secret cocycle element $\pm V_\tau$ as the unique shortest vector pair while lowering the expected BKZ block size.

4.1 Modulo-Two Parity of the Secret Cocycle Element

To break the $(n/2+1)$-fold shortest-vector degeneracy of Λ_τ before invoking any lattice reduction algorithm, we exploit the action of the half-period involution τ modulo 2. In the ring of integers $R_n = \mathbb{Z}[\zeta]$, we have $\tau(\zeta) = -\zeta = \zeta - 2\zeta \equiv \zeta \pmod{2R_n}$. By $\mathbb{Z}$-linearity, every element $x = \sum_{j=0}^{n-1} x_j \zeta^j \in R_n$ satisfies

$$\tau(x) \;=\; \sum_{j=0}^{n-1} (-1)^j x_j \zeta^j \;\equiv\; \sum_{j=0}^{n-1} x_j \zeta^j \;=\; x \pmod{2R_n}. \tag{6}$$

Applying (6) entrywise to the secret basis $B \in \mathrm{SL}_2(R_n)$ yields $\tau(B) \equiv B \pmod{2M_2(R_n)}$. Because $\det B = 1$, the inverse $B^{-1} = \mathrm{adj}(B)$ also has integral entries in R_n, and multiplying on the left by B^{-1} gives the exact modulo-two identity congruence

$$V_\tau \;=\; B^{-1}\tau(B) \;\equiv\; B^{-1}B \;=\; I_2 \pmod{2M_2(R_n)}. \tag{7}$$

In the pipeline of Straznickas and Weis [23, Appendix D], the congruence (7) is used solely as an $O(n)$ post-hoc parity filter on short vectors that the sieve has already paid to find inside Λ_τ. While post-hoc filtering identifies $\pm V_\tau$ once it appears in the sieve output, it does nothing to simplify the geometry of the lattice during reduction: the sieve must still contend with all $n/2+1$ minimal vector pairs of Λ_τ.

4.2 Closing the Congruence Coset into Λ'

Our first key modification is to incorporate the parity constraint (7) directly into the lattice definition before preconditioning or sieving, in the spirit of modular hint integration via sublattice sparsification [6]. The set of elements $Y \in \Lambda_\tau$ satisfying $Y \equiv I_2 \pmod 2$ is an affine coset of $2\Lambda_\tau$, not a subgroup. However, taking the union of the zero coset $2\Lambda_\tau$ and the identity coset $2\Lambda_\tau + I_2$ closes this affine constraint into a full-rank sublattice of Λ_τ (note that our symbol Λ' denotes this index-2^{n-1} modulo-two sublattice, distinct from the rescaled lattice denoted Λ' in [23, Corollary 4.6]).

Definition 3 (The Modulo-Two Sublattice Λ')**.** Let $\Lambda_\tau \subset M_2(R_n)$ be the τ-cocycle lattice of Q, and let $w_0 \in \Lambda_\tau$ be any element satisfying $w_0 \equiv I_2 \pmod{2M_2(R_n)}$. The modulo-two cocycle sublattice $\Lambda' \subset \Lambda_\tau$ is defined by

$$\Lambda' \;=\; 2\Lambda_\tau + \mathbb{Z}\, w_0 \;=\; \big\{\, Y \in \Lambda_\tau \;\big|\; Y \equiv 0 \text{ or } Y \equiv I_2 \pmod{2M_2(R_n)} \,\big\}. \tag{8}$$

Constructing an explicit $\mathbb{Z}$-basis of Λ' from any $\mathbb{Z}$-basis $\{b_1, \ldots, b_n\}$ of Λ_τ requires only elementary linear algebra over $\mathbb{F}_2$. Reducing the basis elements $b_1, \ldots, b_n$ modulo 2 yields a linear system $\sum_{i=1}^n c_i (b_i \bmod 2) = I_2 \bmod 2$ in $c \in \mathbb{F}_2^n$. Because $V_\tau \in \Lambda_\tau$ satisfies $V_\tau \equiv I_2 \pmod 2$, this $\mathbb{F}_2$-system is guaranteed to be consistent. Selecting any solution $c \in \mathbb{F}_2^n$ with $c_{i_0} = 1$, lifting $c_i \in \{0,1\} \subset \mathbb{Z}$ to form $w_0 = \sum_{i=1}^n c_i b_i \in \Lambda_\tau$, and replacing the single generator b_{i_0} by w_0 while doubling all remaining generators $2b_i$ $(i \neq i_0)$ produces a $\mathbb{Z}$-basis of Λ'.

4.3 Index, Isometry Class, and Unique-SVP Gap of Λ'

We now prove that passing from Λ_τ to Λ' isolates $\pm V_\tau$ as the unique shortest vector pair with a factor-of-two Euclidean norm gap.

Theorem 4 (Isometry Class, Unique Minimum, and Index of Λ')**.** *Let $Q = B^*B$ for $B \in \mathrm{SL}_2(R_n)$ with $n = 2^{\ell-1} \geq 4$. Then the modulo-two sublattice $\Lambda' \subset \Lambda_\tau$ satisfies the following properties:*

(i) The sublattice index is $[\Lambda_\tau : \Lambda'] = 2^{n-1}$, so that $\det \mathrm{Gram}(\Lambda') = 2^{2(n-1)} \det \mathrm{Gram}(\Lambda_\tau)$.

(ii) Equipped with the quadratic form q_τ, the Euclidean lattice (Λ', q_τ) has the key-independent isometry class

$$\Lambda' \;\cong\; \sqrt{\frac{n}{4}}\Big(\mathbb{Z} \;\oplus\; 2\mathbb{Z}^{\,n/2} \;\oplus\; 2\sqrt{2}\,\mathbb{Z}^{\,n/2-1}\Big). \tag{9}$$

(iii) The first successive minimum $\lambda_1(\Lambda') = \sqrt{n/4}$ is attained uniquely *at $\pm V_\tau = \pm B^{-1}\tau(B)$, and the second successive minimum satisfies $\lambda_2(\Lambda') = 2\sqrt{n/4}$, giving an exact Euclidean gap*

$$\frac{\lambda_2(\Lambda')}{\lambda_1(\Lambda')} \;=\; 2. \tag{10}$$

Proof. Twisted conjugation by the unimodular secret basis $B \in \mathrm{SL}_2(R_n)$ defines a $\mathbb{Z}$-linear bijection $\Phi_B : Y \mapsto BY\tau(B)^{-1}$ from $\Lambda_\tau(Q)$ onto the canonical cocycle lattice $\Lambda_\tau(I_2)$ associated with the identity Gram matrix $Q = I_2$ [23, Proposition 4.5]. Since $\det(\Phi_B(Y)) = \det Y$, Φ_B is an isometry with respect to q_τ. Because $\tau(B) \equiv B \pmod 2$, reducing modulo 2 gives $\Phi_B(Y) \equiv BYB^{-1} \pmod 2$, so $\Phi_B(Y) \equiv 0$ or $I_2 \pmod 2$ if and only if $Y \equiv 0$ or $I_2 \pmod 2$ (where $\{Y \in \Lambda_\tau : Y \equiv 0 \pmod 2\} = 2\Lambda_\tau$ by saturation of Λ_τ in $M_2(R_n)$). Thus Φ_B maps $\Lambda'(Q)$ isometrically onto $\Lambda'(I_2)$, and maps $V_\tau = B^{-1}\tau(B)$ to $BV_\tau\tau(B)^{-1} = I_2$.

In $\Lambda_\tau(I_2)$, the orthogonal decomposition $\Lambda_\tau(I_2) \cong \sqrt{n/4}\,(\mathbb{Z}^{n/2+1} \oplus \sqrt{2}\,\mathbb{Z}^{n/2-1})$ of Proposition 2 has an explicit orthogonal $\mathbb{Z}$-basis $\{e_0, e_1, \ldots, e_{n/2}, f_1, \ldots, f_{n/2-1}\}$, where $e_0 = I_2$ has norm $\sqrt{n/4}$, the vectors $e_1, \ldots, e_{n/2}$ are mutually orthogonal off-diagonal/monomial units of norm $\sqrt{n/4}$, and $f_1, \ldots, f_{n/2-1}$ have norm $\sqrt{n/2}$. Here $e_0 = I_2$ is the sole basis element congruent to I_2 modulo 2: every other basis generator e_j $(1 \le j \le n/2)$ and f_k $(1 \le k \le n/2-1)$ has support disjoint from the identity diagonal modulo 2, and no nontrivial $\mathbb{F}_2$-linear combination of $\{e_1, \ldots, e_{n/2}, f_1, \ldots, f_{n/2-1}\}$ is congruent to 0 or I_2 modulo 2.

A vector $Y = \alpha_0 e_0 + \sum_{j=1}^{n/2} \alpha_j e_j + \sum_{k=1}^{n/2-1} \beta_k f_k \in \Lambda_\tau(I_2)$ with integer coordinates $\alpha_j, \beta_k \in \mathbb{Z}$ therefore satisfies $Y \equiv 0$ or $I_2 \pmod 2$ if and only if $\alpha_j \equiv 0 \pmod 2$ for all $1 \le j \le n/2$ and $\beta_k \equiv 0 \pmod 2$ for all $1 \le k \le n/2-1$, while $\alpha_0 \in \mathbb{Z}$ is arbitrary (α_0 even gives $Y \equiv 0 \pmod 2$, and α_0 odd gives $Y \equiv I_2 \pmod 2$). Therefore,

$$\Lambda'(I_2) \;=\; \mathbb{Z}e_0 \;\oplus\; \bigoplus_{j=1}^{n/2} \mathbb{Z}(2e_j) \;\oplus\; \bigoplus_{k=1}^{n/2-1} \mathbb{Z}(2f_k),$$

which establishes the index $[\Lambda_\tau : \Lambda'] = 2^{n/2+(n/2-1)} = 2^{n-1}$ in (i) and the orthogonal decomposition (9) in (ii). Finally, since $\|e_0\| = \sqrt{n/4}$, $\|2e_j\| = 2\sqrt{n/4}$, and $\|2f_k\| = 2\sqrt{2}\sqrt{n/4}$, the unique shortest nonzero vectors of $\Lambda'(I_2)$ are $\pm e_0$ of norm $\lambda_1(\Lambda') = \sqrt{n/4}$, corresponding under Φ_B^{-1} to $\pm V_\tau$, while the next shortest linearly independent vectors are $\pm 2e_j$ of norm $\lambda_2(\Lambda') = 2\sqrt{n/4}$. This proves (iii). □

4.4 Determinant Certificate and Intertwiner Elimination

Figure 2 illustrates the geometric transformation proved in Theorem 4. At $n = 256$, Theorem 4(i) and (5) yield a second bit-exact algebraic certificate for our implementation: in the $\times 8$ integer Gram convention, the Gram matrix of Λ' satisfies

$$\log_2 \det \mathrm{Gram}(\Lambda') \;=\; \log_2 \det \mathrm{Gram}(\Lambda_\tau) + 2(n-1) \;=\; 2431.00 + 2 \times 255 \;=\; 2941.00. \tag{11}$$

Any bug in the $\mathbb{F}_2$ solve or sublattice construction would alter this integer determinant; verifying $\log_2 \det \mathrm{Gram}(\Lambda') = 2941.00$ certifies that $[\Lambda_\tau : \Lambda'] = 2^{255}$ holds exactly.

Equally important, Theorem 4(iii) removes the intertwiner separation stage of Straznickas and Weis [23, Remark 6.2]. Because $\pm V_\tau$ is the unique shortest vector of Λ' with a factor-of-two gap to all linearly independent vectors, any basis reduction or sieving tour that reaches the minimum of Λ' outputs $\pm V_\tau$ directly as its first basis vector.

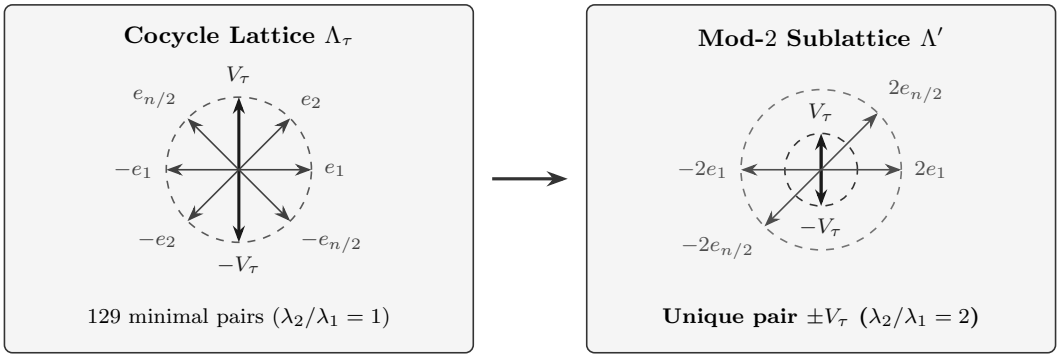

Figure 2: Geometric effect of closing the modulo-two parity constraint into $\Lambda' \subset \Lambda_\tau$, transforming $\Lambda_\tau \cong \sqrt{n/4}\left(\mathbb{Z}^{n/2+1} \oplus \sqrt{2}\,\mathbb{Z}^{n/2-1}\right)$ into $\Lambda' \cong \sqrt{n/4}\left(\mathbb{Z} \oplus 2\mathbb{Z}^{n/2} \oplus 2\sqrt{2}\,\mathbb{Z}^{n/2-1}\right)$: the $n/2 = 128$ spurious shortest vector pairs $e_1, \ldots, e_{n/2}$ fail $Y \equiv I_2 \pmod 2$ and are doubled to norm $2\lambda_1$, isolating $\pm V_\tau$ as the unique shortest vector pair with gap $\lambda_2(\Lambda')/\lambda_1(\Lambda') = 2$.

4.5 Lattice Dimension Invariance vs. Quality Optimization

To situate Λ' relative to the complexity bounds of Straznickas and Weis [23], it is essential to separate lattice *dimension* from lattice *quality*:

1. **Invariance of Ambient Rank n and Provable SVP Dimension $n/2+1$:** Because $\Lambda' = 2\Lambda_\tau + \mathbb{Z}w_0$ has finite index $[\Lambda_\tau : \Lambda'] = 2^{n-1}$ inside Λ_τ, its ambient $\mathbb{Z}$-rank remains n, and the provable two-block SVP oracle dimension $n/2+1$ of [8, 23] is unchanged. Moreover, although Λ_τ is a free rank-4 module over $\mathcal{O}_F = \mathbb{Z}[\zeta^2+\zeta^{-2}]$ ($[F:\mathbb{Q}] = n/4$), its F-discriminant $2 + \zeta^2 + \zeta^{-2} = (\zeta + \zeta^{-1})^2$ is a non-square in F, which obstructs exterior-square module reductions from lowering the $\mathbb{Z}$-rank below n. Under the Geometric Series Assumption (GSA) unique-SVP projection condition [1] $\sqrt{\beta/n}\,\lambda_1 \approx \delta_\beta^{2\beta-n}\,\mathrm{vol}(\Lambda)^{1/n}$ with $\ln \delta_\beta = \frac{\ln(\beta/(2\pi e))}{2\beta}(1 + o(1))$, the asymptotic BKZ block sizes of Λ_τ and Λ' satisfy

$$\beta(\Lambda_\tau) \;=\; \frac{n}{2} - \frac{3\ln 2}{8}\frac{n}{\ln n} + O\!\left(\frac{n}{\ln^2 n}\right), \qquad \beta(\Lambda') \;=\; \frac{n}{2} - \frac{7\ln 2}{8}\frac{n}{\ln n} + O\!\left(\frac{n}{\ln^2 n}\right), \quad (12)$$

   sharing the same leading asymptotic ratio $\lim_{n\to\infty} \beta(n)/n = 1/2$.

2. **Lattice Quality Optimization and Expected BKZ Block-Size Reduction:** While the dimension is unchanged, multiplying the covolume by 2^{n-1} at unchanged target norm $\lambda_1(\Lambda') = \sqrt{n/4}$ cuts the Hermite ratio $\lambda_1/\mathrm{vol}^{1/n}$ in half from $2^{-(n-2)/(4n)} \to 2^{-1/4} \approx 0.8409$ on Λ_τ to $2^{-(5n-6)/(4n)} \to 2^{-5/4} \approx 0.4204$ on Λ' (0.4222 at $n = 256$). By (12), this yields a diverging second-order block-size reduction

$$\Delta\beta(n) \;=\; \beta(\Lambda_\tau) - \beta(\Lambda') \;=\; \frac{\ln 2}{2}\,\frac{n}{\ln n} + O\!\left(\frac{n}{\ln^2 n}\right) \xrightarrow{n\to\infty} +\infty,$$

   which lowers the expected BKZ block size β (obtained by solving $\sqrt{\beta/n}\,\lambda_1 = \delta_\beta^{2\beta-n}\,\mathrm{vol}(\Lambda)^{1/n}$ and rounding to the nearest integer) by 34, 49, and 81 across HAWK-256, HAWK-512, and HAWK-1024 (Section 7.3).

5 Structural Limits and Exact Cholesky Preconditioning

Having isolated $\pm V_\tau$ in Λ', we now analyze the structural root Hermite factor threshold at $n = 256$ and detail our exact Cholesky preconditioning pipeline, which eliminates Gram-mode condition-number squaring prior to lattice sieving.

5.1 The Structural Hermite Limit at $n = 256$

Before describing our basis preconditioning, we note a direct consequence of Theorem 4 at $n = 256$ that explains why no pure basis-flattening algorithm (such as LLL, `flatter`, or small-block BKZ governed by a root Hermite factor bound) can ever reach $\lambda_1(\Lambda')$ without triggering the unique-SVP projection mechanism.

Proposition 5 (Structural Root Hermite Factor Limit at $n = 256$)**.** *For the modulo-two sublattice Λ' at rank $n = 256$, the Hermite ratio between the first minimum and the normalized covolume is*

$$\frac{\lambda_1(\Lambda')}{\mathrm{vol}(\Lambda')^{1/n}} \;=\; 2^{-(5n-6)/(4n)} \;=\; 2^{-637/512} \;\approx\; 0.4222,$$

and the root Hermite factor δ_0 required for a GSA-governed basis profile $\|b_1\| = \delta_0^{n-1}\,\mathrm{vol}(\Lambda')^{1/n}$ to reach $\lambda_1(\Lambda')$ is

$$\delta_{0,\mathrm{req}} \;=\; \Big(\frac{\lambda_1(\Lambda')}{\mathrm{vol}(\Lambda')^{1/n}}\Big)^{1/(n-1)} \;=\; (0.4222)^{1/255} \;\approx\; 0.996624 \;<\; 1. \tag{13}$$

Proof. In the $\times 8$ integer Gram convention at $n = 256$, the shortest vector $\pm V_\tau$ has squared norm $\lambda_1^2 = 2n = 512 = 2^9$, so $\lambda_1 = \sqrt{512} \approx 22.6274$. By (11), the integer Gram determinant is $\det \mathrm{Gram}(\Lambda') = 2^{2941}$, so the normalized squared covolume is $(\det \mathrm{Gram}(\Lambda'))^{1/256} = 2^{2941/256} \approx 2872.90$, giving a squared ratio $\lambda_1^2/(\det \mathrm{Gram}(\Lambda'))^{1/256} = 2^{9-2941/256} = 2^{-637/256} \approx 0.17822$ and a linear ratio $\lambda_1/\,\mathrm{vol}(\Lambda')^{1/256} = 2^{-637/512}$ (or 0.4222 in Euclidean norm). Since any basis reduction profile parameterized by a root Hermite factor δ_0 enforces $\|b_1\| \approx \delta_0^{n-1}\,\mathrm{vol}(\Lambda')^{1/n}$ with $\delta_0 \geq 1$, reaching $\|b_1\| = \lambda_1(\Lambda')$ through profile flattening alone would require $\delta_0 = (0.4222)^{1/255} \approx 0.996624 < 1$, which is impossible. □

Proposition 5 establishes that at $n = 256$, $\lambda_1(\Lambda')$ lies strictly below $\mathrm{vol}(\Lambda')^{1/n}$. Pure profile-compression tools such as `flatter` [20] therefore saturate once the basis profile approaches $\mathrm{vol}(\Lambda')^{1/n}$ (empirically saturating at 7,939.76× the target squared norm 512, even at root Hermite factor 1.01). The attack can succeed only via the standard unique-SVP projection mechanism [1]: progressive BKZ or sieving must reduce the basis sufficiently that the orthogonal projection $\pi_{n-d+1}(V_\tau)$ onto the last d Gram–Schmidt vectors becomes recognizable to an SVP oracle. This structural threshold is why BKZ alone suffices for $n \leq 128$, whereas $n = 256$ requires a progressive sieve.

5.2 Saturated Integer Kernel Extraction

Given the 450-byte public key, we decode $Q \in M_2(R_{256})$ and assemble the homogeneous linear constraint matrix representing (C1) and (C2) of (3). After eliminating $2n = 512$ coordinates via the diagonal symmetry of (C1), constraint (C2) yields a 1024×512 integer matrix with 15-bit entries, from which we select 256 linearly independent rows (0.3 CPU-core-seconds).

Following [23], we extract an exact $\mathbb{Z}$-basis of the saturated integer kernel Λ_τ by first computing the Hermite normal form (HNF) with unimodular transformation in Sage. While HNF completes in 17.1 s and returns an exact basis of Λ_τ, the resulting unimodular transformation suffers severe coefficient swell, producing basis entries of up to 5,483–6,351 bits. Running standard `fplll`/Sage LLL directly on this HNF basis fails to terminate within 14 minutes, as standard LLL bit-complexity $O(d^5\beta_{\mathrm{bits}}^2)$ grows by roughly $(256/32)^5 \times (6351/1700)^2 \approx 3.4 \times 10^5$ relative to an $n = 32$ (1,700-bit HNF) baseline. Replacing standard LLL with Ryan and Heninger's `flatter` [20] (at its default root Hermite factor 1.0219) reduces the HNF kernel to a 12–13-bit basis of Λ_τ in 125.9 s of CPU time. The entire kernel extraction stage completes in 143.0 CPU-core-seconds and is certified exact by verifying $\log_2 \det \mathrm{Gram}(\Lambda_\tau) = 2431.00$.

5.3 Condition-Number Squaring in Gram-Mode GSO

After forming $\Lambda' = 2\Lambda_\tau + \mathbb{Z}w_0$ and its 256×256 integer Gram matrix $G_p = \mathrm{Gram}(\Lambda')$ (1.9 CPU-core-seconds), we must reduce Λ'. Because Λ' is naturally equipped with the trace-determinant Gram matrix G_p rather than an explicit Euclidean coordinate embedding in $\mathbb{Z}^{256}$, the standard approach in [23] operates `fpylll` in *Gram mode*, feeding G_p directly to LLL and BKZ.

However, the natural basis of Λ' exhibits a basis condition number of approximately 2^{41} (2^{36} GSO spread) with 40–41-bit Gram entries. In `fpylll`'s Gram mode, Gram–Schmidt orthogonalization (GSO) operates directly on inner products $G_p = BB^T$, which *squares the condition number* relative to basis-mode GSO on B [18, 12]. As a result, Gram-mode LLL in hardware double and long-double precision aborts immediately inside Babai's nearest-plane routine. Switching to arbitrary-precision floating-point arithmetic (MPFR) allows a single Gram-mode LLL pass to finish, but it consumes 299–333 s and leaves the shortest basis vector at 2.828×10^5 times the target squared norm 512.

5.4 Exact Cholesky Embedding and Unimodular Recovery

Whereas [23] applies a scaled Cholesky embedding only after an initial Gram-mode BKZ warm-up, we move high-precision Cholesky embedding and `flatter` ahead of initial LLL to avoid Gram-mode condition-number squaring altogether:

1. **High-Precision Cholesky Factorization.** We compute the lower-triangular Cholesky factor $L \in M_{256}(\mathbb{R})$ satisfying $G_p = LL^T$ using high-precision (1,600-bit) floating-point arithmetic, round the scaled factor to an integer basis matrix $B_{\mathrm{chol}} = \lfloor 2^s L \rceil \in M_{256}(\mathbb{Z})$ ($s = 61$ for exact unimodular preconditioning, followed by $s = 21$ on G_1 for the `g6k` embedding; 3.7 CPU-core-seconds).

2. **Fast Basis-Mode Reduction via `flatter`.** Because B_{chol} is an explicit integer basis matrix whose condition number is the square root of that of G_p, we reduce B_{chol} in basis mode using `flatter` (55.6 CPU-core-seconds), obtaining a reduced integer matrix $B_{\mathrm{red}} = UB_{\mathrm{chol}}$.

3. **Exact Unimodular Transform Recovery.** Rather than relying on floating-point Gram updates, we recover the exact integer unimodular transformation matrix $U = B_{\mathrm{red}} B_{\mathrm{chol}}^{-1} \in \mathrm{GL}_{256}(\mathbb{Z})$ by exact triangular backward substitution against the lower-triangular factor B_{chol}, and apply U to the exact integer Gram matrix:

$$G_1 \;=\; UG_pU^T. \tag{14}$$

In 59.3 CPU-core-seconds total, this preconditioning transforms G_p (which had 40–41-bit entries and $\sim 2^{41}$ basis condition number) into an exact integer Gram matrix G_1 with 27-bit entries and a Gram diagonal ratio of 2.2–3.0. Subsequent LLL on the preconditioned lattice starts at 71,197×–76,752× the target norm instead of 282,800× (a 4× improvement in starting quality before any BKZ or sieving begins).

5.5 Relaxed LLL and BKZ Conditioning Warm-Up

Three further empirically driven ablations on the preconditioned basis inform our pre-sieving design:

- **Relaxing LLL from $\delta = 0.99$ to $\delta = 0.75$.** Running `fplll`'s [12] default $\delta = 0.99$ LLL on this instance costs 1,126.8 CPU-core-seconds. Relaxing the classical Lovász parameter [15] to $\delta = 0.75$ reduces the LLL time to 87.5 CPU-core-seconds (12.9× speedup) with zero penalty to downstream convergence because a subsequent BKZ-20 conditioning pass or `flatter` compression repairs the basis profile.

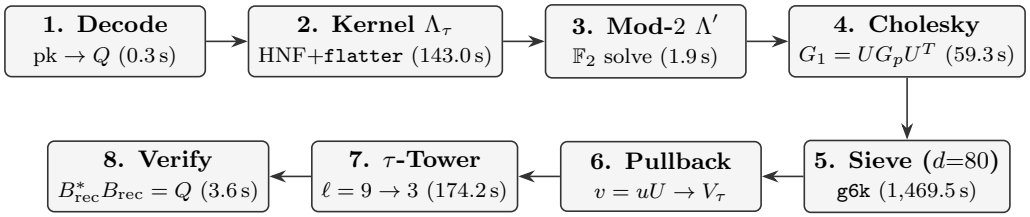

Figure 3: End-to-end 8-stage HAWK-256 single-core key recovery pipeline with measured CPU-core-seconds for each stage (total 1,851.8 s, or 30.9 minutes).

- **BKZ-20 Conditioning Warm-Up.** A naive schedule that runs four tours at each block size $\beta = 3, 4, 5, \ldots$ without a low-β warm-up fails to converge. In our control experiment on the same key without warm-up, running BKZ across $\beta \in \{3, 4, 5, 6, 7, 8\}$ consumed 130 s in total while the automatic abort condition triggered three times (at $\beta \in \{4, 6, 8\}$) and the first vector stalled at 1.2×10^5 times the target norm. The reason is structural: BKZ-β requires approximately $d/(\beta - 1)$ tours to equilibrate its GSA profile across dimension $d = 256$ [5], which is ≈ 13 tours at $\beta = 20$ versus only ≈ 4 tours at $\beta = 58$. Supplying a dedicated BKZ-20 conditioning warm-up equilibrates the global basis slope before ramping the block size.
- **Replacing Enumeration BKZ with `g6k`.** In `fpylll` 0.6.4 [12], standard enumeration-based BKZ in fixed-precision floating-point (`d`, `ld`, `dpe`) aborts in Babai's nearest-plane loop across Gram and Cholesky-basis presentations at $\beta \geq 5$, whereas driving reduction directly through the General Sieve Kernel (`g6k`) [2] on the `flatter`-preconditioned Cholesky basis bypasses `fplll`'s enumeration loop and progresses smoothly to the lattice minimum.

6 Progressive Sieving and Tower Descent

With the preconditioned Gram matrix $G_1 = UG_pU^T$ in hand, this section describes the progressive sieving tour in `g6k`, the exact coordinate pullback to Λ', and the subsequent τ-tower descent to recover an equivalent secret key.

6.1 Progressive Pump-and-Jump Sieve Ladder

Figure 3 summarizes the complete eight-stage recovery chain. Once the preconditioned Gram matrix $G_1 = UG_pU^T$ is embedded at scale $s = 21$ and initialized with internal LLL (2.4 s), we invoke the General Sieve Kernel (`g6k`) [2] on a single thread using its progressive pump-and-jump BKZ tour across five sieve dimensions:

$$d_{\text{sieve}} \in \{40,\ 50,\ 60,\ 70,\ 80\}. \tag{15}$$

Because $B_{\text{chol}} = \lfloor 2^s L \rceil$ scales Euclidean lengths by 2^s with $s = 21$, the unique shortest vector $\pm V_\tau$ of integer Gram norm squared $2n = 512$ corresponds to an embedded lattice vector of squared Euclidean norm

$$\|b_{\text{target}}\|^2 \approx 2^{2s} \cdot 2n = 2^{42} \cdot 512 = 2^{51}.$$

During the progressive sieve ladder (15), the tours at $d_{\text{sieve}} \in \{40, 50, 60, 70, 80\}$ take 85.6 s, 142.9 s, 215.2 s, 331.8 s, and 691.6 s of CPU time (88.9 s, 143.6 s, 216.3 s, 333.2 s, and 694.1 s wall-clock), reaching a cumulative single-core SVP runtime of 1,469.5 CPU-core-seconds (1,478.5 s wall-clock time) while driving the squared norm ratio $\|b_1\|^2/\|b_{\text{target}}\|^2$ down along the sequence 72,768 → 57,524 → 36,216 → 19,417 → 8,979 → 0.999625. At $d_{\text{sieve}} = 80$, the pump projects $\pm V_\tau$ into the active sieve window and lifts it to row 0 of the basis, achieving an embedded squared norm of 0.999625×2^{51} (the deviation of 3.75×10^{-4} coming solely from the $s = 21$ integer rounding of B_{chol}).

6.2 Exact Preconditioned Coordinate Recovery

After the sieve places the shortest vector $b_{\min}$ at row 0 of the reduced embedded basis, we must recover the exact integer coordinate vector $v \in \mathbb{Z}^{256}$ of $\pm V_\tau$ with respect to our original $\mathbb{Z}$-basis of Λ'. As in [23], because the $s = 21$ Cholesky factor $B_s = \lfloor 2^{21} \operatorname{chol}(G_1) \rceil$ is lower triangular, exact triangular backward substitution of $b_{\min}$ against B_s returns an integer coordinate vector $u \in \mathbb{Z}^{256}$.

Because the sieve operated on B_s (the Cholesky embedding of $G_1 = UG_pU^T$), the coordinate vector u is expressed in the *preconditioned* basis of Λ', whose Gram matrix is $G_1 = UG_pU^T$ from (14), rather than in the unpreconditioned basis of Λ', whose Gram matrix is $G_p = \operatorname{Gram}(\Lambda')$. Evaluating u in G_1 and mapping back to the original Λ' basis via the saved unimodular transformation $U \in \mathrm{GL}_{256}(\mathbb{Z})$ yields:

$$v \;=\; u\,U \;\in\; \mathbb{Z}^{256} \quad\Longrightarrow\quad v\,G_p\,v^T \;=\; u\,(UG_pU^T)\,u^T \;=\; u\,G_1\,u^T \;=\; 2n \;=\; 512. \tag{16}$$

Our verification routine confirms (16) alongside four exact algebraic certificates in under 2 CPU-seconds: (i) $\log_2 \det \operatorname{Gram}(\Lambda') = 2941.00 = 2431 + 2 \times 255$, certifying $[\Lambda_\tau : \Lambda'] = 2^{255}$; (ii) row 0 of the reduced embedded basis attains squared norm 0.999625×2^{51}; (iii) $uG_1u^T = 512$ in the preconditioned Gram form and $vG_pv^T = 512$ in the original Λ' Gram form, matching $2n = 512$; and (iv) mapping $v \in \mathbb{Z}^{256}$ through the $\mathbb{Z}$-basis of Λ' yields the exact matrix $V_\tau = B^{-1}\tau(B) \in \mathrm{SL}_2(R_{256})$, satisfying $V_\tau \equiv I_2 \pmod 2$ and $V_\tau\tau(V_\tau) = I_2$.

6.3 The τ-Tower Descent at $n = 256$

Once $V_\tau = B^{-1}\tau(B)$ is recovered at level $\ell = 9$ ($n = 256$), the remaining task is to solve Hilbert-90 / cocycle splitting down the cyclotomic tower $L_9 \supset L_8 \supset \cdots \supset L_3$ to reconstruct an equivalent secret basis $B_{\mathrm{rec}} \in \mathrm{SL}_2(R_{256})$ satisfying $B^*_{\mathrm{rec}}B_{\mathrm{rec}} = Q$. For this stage, we invoke the τ-tower descent algorithm of Straznickas and Weis [23] (building on [13]) without modification.

Running the tower descent on our recovered V_τ at $n = 256$ completes in 174.2 CPU-core-seconds and records the exact BKZ block-size trace across tower levels $\ell \in \{9, 8, 7, 6, 5, 4, 3\}$:

$$\big\{\, 9 : \textsc{Preset},\quad 8 : 13,\quad 7 : 0,\quad 6 : 0,\quad 5 : 0,\quad 4 : 0,\quad 3 : \textsc{Base} \,\big\}.$$

Here $\ell = 9$ takes our preset cocycle V_τ, the first subfield level $\ell = 8$ ($n = 128$) requires only BKZ block size $\beta = 13$, every intermediate level $\ell \in \{7, 6, 5, 4\}$ ($n \in \{64, 32, 16, 8\}$) is solved by pure LLL ($\beta = 0$), and $\ell = 3$ ($n = 4$) is the base level. The descent outputs $B_{\mathrm{rec}} \in \mathrm{SL}_2(R_{256})$ satisfying $B^*_{\mathrm{rec}}B_{\mathrm{rec}} = Q$ bit-for-bit. For HAWK-512 ($\ell = 10$, $n = 512$), where the tower's first sub-level is an $\ell = 9$ ($n = 256$) cocycle solve [23], our 27.9-minute Λ' cocycle solve (30.9 minutes including $\ell = 9 \to 3$ descent) directly replaces the default Gram-mode BKZ at $\ell = 9$.

7 Sieve Dimension Scaling and Experimental Verification

We now report the stage-by-stage timing breakdown of our single-core HAWK-256 key recovery, analyze the runtime scaling from sieve dimension $d = 118$ down to $d = 80$, and evaluate the concrete security impact on HAWK-256, HAWK-512, and HAWK-1024.

7.1 Stage-by-Stage Timing Breakdown

All computational costs are reported in CPU-core-seconds, measured via operating-system resource accounting summed across the parent process and all child processes so that every stage is fully included.

To ensure transparent accounting of parallelism, we note that the decisive SVP stage (Stage 5) ran **strictly single-threaded**, accumulating 1,469.5 s of CPU time against 1,478.5 s of wall-clock time (0.994 cores). Across the entire chain, pre-SVP setup and preconditioning account

Table 2: Stage-by-stage single-core CPU-core-second breakdown for end-to-end HAWK-256 key recovery ($n = 256$, $\ell = 9$), compared against Straznickas and Weis [23].

Stage	Operation	Time (s)	Share
Public-key decode	Decode Q and build 1024×512 constraint matrix	0.3 s	$< 0.1\%$
Cocycle kernel	Extract saturated $\mathbb{Z}$-basis of Λ_τ (HNF 17.1 s + `flatter` 125.9 s)	143.0 s	7.7%
Sublattice setup	Solve $\mathbb{F}_2$ parity system and form $G_p = \mathrm{Gram}(\Lambda')$	1.9 s	0.1%
Cholesky preconditioning	Compute $G_p = LL^T$, reduce B_{chol} via `flatter`, recover U, G_1	59.3 s	3.2%
Pre-SVP subtotal	**All setup and preconditioning stages (Stages 1–4)**	**204.5 s**	**11.0%**
Progressive sieve	**Single-thread `g6k` tour ($d \in \{40, 50, 60, 70, 80\}$)**	**1,469.5 s**	**79.4%**
Tower descent	Coordinate pullback $v = uU$ and τ-tower ($\ell = 9 \to 3$)	174.2 s	9.4%
Reference check	Encode 592-byte key and run C reference sign/verify	3.6 s	0.2%
Total time	**Complete end-to-end HAWK-256 key recovery**	**1,851.8 s**	**100.0%**
Prior baseline [23]	3 h 42 min across 96 cores	1,278,720 s	—
Speedup factor	**Ratio against baseline [23]**	**690×**	—

Table 3: Sieve database and runtime scaling from $d = 118$ [23] to $d = 80$ (this work).

Metric	$d = 118$ ([23])	$d = 80$ (This Work)	Ratio
Database size[a]	$2^{24.49} \approx 2.35 \times 10^7$	$2^{16.60} \approx 9.93 \times 10^4$	236×
Predicted sieve time[b]	$2^{27.67}$	$2^{18.76}$	481×
Measured total time	**1,278,720 s**	**1,851.8 s**	**690×**

[a] Heuristic database size $2^{0.2075\,d}$. [b] Empirical scaling law $\propto$ (database)$^{1.13} \approx 2^{0.2345\,d}$ (in relative units).

for 204.5 s (11.0%), progressive sieving accounts for 1,469.5 s (79.4%), and coordinate pullback, τ-tower descent, and reference verification account for 177.8 s (9.6%), totaling 1,851.8 CPU-core-seconds (30.9 minutes CPU, 1,861.8 s or 31.0 minutes end-to-end wall-clock). Table 2 provides the complete stage-by-stage breakdown.

7.2 Sieve Dimension Reduction from $d = 118$ to $d = 80$

The 690× speedup over [23] reduces to a single structural quantity: *the maximum sieving dimension $d_{\max}$ required for the reduction to expose $\pm V_\tau$*. In [23], the progressive BGJ-style sieve [24] is driven to a final sieving dimension of 118 along the slide schedule $(60, 70, 80, 95, 108, 118)$. In our pipeline, the progressive sieve reaches the minimum of Λ' at $d_{\max} = 80$.

Standard heuristic and empirical scaling laws explain why reducing $d_{\max}$ from 118 to 80 yields a factor of $\approx$ 500–690 in runtime. A lattice sieve in dimension d maintains a database of size $N_{\mathrm{db}}(d) \approx (4/3)^{d/2} \approx 2^{0.2075\,d}$ [4, 2]. Practical CPU sieving runtime scales approximately as $T_{\mathrm{sieve}}(d) \propto N_{\mathrm{db}}(d)^{1.13} \approx 2^{0.2345\,d}$ (in standalone single-pump probes on Λ', `g6k` builds databases of 65,394 vectors in 10.6 s CPU at $d = 70$ and 275,569 vectors in 124.0 s CPU at $d = 80$, while full progressive tours take 331.8 s and 691.6 s CPU at $d = 70$ and $d = 80$). Table 3 compares the predicted scaling ratios between $d = 118$ and $d = 80$ against our end-to-end measurement.

As Table 3 demonstrates, the empirical throughput law predicts a 481× reduction in sieve work, closely matching our measured 690× end-to-end speedup (with the remaining gap reflecting elimination of the 16-minute intertwiner stage, 96-core parallelization overhead, and `g6k`'s early-exit progressive tour versus `svp_tool`). Two mechanisms account for the drop $118 \to 80$:

1. **Unique-SVP isolation and block-size reduction in Λ' (Section 4):** Doubling the $n/2$ spurious minimal pairs of Λ_τ increases the covolume $\mathrm{vol}(\Lambda') = 2^{n-1}\,\mathrm{vol}(\Lambda_\tau)$ while keeping $\|V_\tau\| = \sqrt{n/4}$ unchanged, which lowers the required BKZ block size from $\beta = 92$ to $\beta = 58$ (9.28 bits in the AGPS20 gate model) and eliminates the intertwiner stage.

Table 4: Expected BKZ block size β, effective sieve dimension β_{eff}, and heuristic AGPS20 gate complexity on Λ_τ [23, Appendix C] versus our modulo-two sublattice Λ' across HAWK-256, HAWK-512, and HAWK-1024.

Variant	n	Claimed	$\beta(\Lambda_\tau)$	$\beta(\Lambda')$	$\beta_{\text{eff}}(\Lambda')$	Gates (Λ_τ [23])	Gates (Λ', Ours)	ΔSec
HAWK-256	256	64 bits	92	**58**	**40**	$2^{50.83}$	$\mathbf{2^{41.56}}$[a]	**−9.28 bits**
HAWK-512	512	128 bits	205	**156**	**136**	$2^{80.79}$	$\mathbf{2^{69.64}}$	**−11.15 bits**
HAWK-1024	1024	256 bits	432	**351**	**312**	$2^{146.48}$	$\mathbf{2^{122.73}}$	**−23.74 bits**

[a] Evaluated from the AGPS20 classical list-decoding cost model (`jschanck/eprint-2019-1161`, commit `1ec49e5`); since the precomputed CSV starts at $d = 64$, $C_{\text{gate}}(40) = 33.56$ ($2^{41.56}$ total) is evaluated directly from the exact AGPS20 spherical-wedge list-decoding circuit at $d = 40$ ($n_{\text{code}} = 4095$), agreeing within 0.11 bits with two-point affine continuation from $d = 64, 72$ ($2^{41.44}$, −9.39 bits; $\leq 2^{48.49}$ if clamped at $d = 64$).

2. **Eliminating Gram-mode skew via exact Cholesky preconditioning (Section 5):** The same cocycle isometry class is solved by plain LLL ($\beta = 2$) at $n = 64$ and small-block BKZ ($\beta \leq 13$) at $n = 128$, yet stalls at $\beta = 40$ at $n = 256$ under naive Gram-mode reduction because the natural Gram matrix has $\sim 2^{41}$ basis condition number and Gram-mode GSO squares its condition number. Replacing Gram mode with our exact Cholesky embedding and `flatter` preconditioning improves the post-LLL squared norm by 4× and allows the progressive pump-and-jump ladder to detect V_τ at $d = 80$.

7.3 Security Impact on HAWK-256, HAWK-512, and HAWK-1024

To assess the concrete impact of Λ' across all three HAWK parameter sets (HAWK-256 at $n = 256$ claiming 64 bits, HAWK-512 at $n = 512$ claiming 128 bits for NIST Level I, and HAWK-1024 at $n = 1024$ claiming 256 bits for NIST Level V), we follow the HAWK specification [10, §5.3] and Straznickas–Weis [23, Appendix C]: from the expected BKZ block size β, we compute $\mathrm{d4f}(\beta) = \mathrm{round}\big(\beta \ln(4/3)/\ln(\beta/(2\pi e))\big)$ [7], the effective sieve dimension $\beta_{\text{eff}} = 8\lfloor(\beta - \mathrm{d4f}(\beta))/8\rfloor$ (note that β_{eff} is invariant even if β is replaced by $\lceil\beta^*\rceil$ under $\delta_\beta^{2\beta-n-1}$), and the classical list-decoding gate complexity $\log_2 n + C_{\text{gate}}(\beta_{\text{eff}})$ in the AGPS20 gate model [3, 23] (alongside the provable $(n/2+1)$-dimensional SVP bounds of 2^{52}, 2^{86}, and 2^{158} gates per oracle call, or 2^{72}, 2^{108}, and 2^{182} total gates including the $O(n^2 \log n)$ reduction calls [8, 23]).

Table 4 summarizes the resulting block-size and gate-complexity reductions across all three parameter sets:

- **HAWK-256 ($n = 256$, claimed 64 bits):** Passing from Λ_τ to Λ' lowers the GSA-intersect BKZ block size by 34 (from $\beta = 92$ to $\beta = 58$, or from 82.58 to 60.19 under the HAWK BKZ simulator [9]) and lowers the effective sieve dimension from 72 to 40. This reduces the AGPS20 gate cost by **9.28 bits** (from $2^{50.83}$ to $\mathbf{2^{41.56}}$ gates; $2^{41.44}$ under $d = 64, 72$ affine continuation), while our single-core execution completes end-to-end in **1,851.8 s** ($\approx 2^{10.9}$ core-seconds) at sieve dimension $d = 80$.

- **HAWK-512 ($n = 512$, claimed 128 bits, NIST Level I):** The required BKZ block size drops by 49 (from $\beta = 205$ to $\beta = 156$, or from 197.68 to 158.18 under the BKZ simulator), lowering β_{eff} from 176 to 136 (matching the BKZ simulator) and reducing the AGPS20 gate complexity by **11.15 bits** from $2^{80.79}$ to $\mathbf{2^{69.64}}$ (58.4 bits below the 128-bit NIST Level I claim; $2^{67.35}$ at $d = 128$ if $\lfloor\beta - \mathrm{d4f}(\beta)\rfloor = 135$ is floored prior to rounding down to a multiple of 8). Carrying forward the empirical ratio $d/\beta(\Lambda') = 80/58 \approx 1.379$ and throughput law $T(d) \propto 2^{0.2345\,d}$ from $n = 256$ projects a sieve dimension of $d \approx 215$ (213 at $80/59 \times 157$) and ≈ 3.4–5.0×10^{12} CPU-core-seconds ($\approx 2^{41.6}$–$2^{42.2}$ core-s).

- **HAWK-1024 ($n = 1024$, claimed 256 bits, NIST Level V):** The required BKZ block size drops by 81 (from $\beta = 432$ to $\beta = 351$, or from 429.16 to 358.29 under the BKZ simulator),

lowering β_{eff} from 392 to 312 and reducing the AGPS20 gate complexity by **23.74 bits** from $2^{146.48}$ to $\mathbf{2^{122.73}}$ ($2^{125.11}$ under the BKZ simulator, pushing HAWK-1024 below the 2^{128} NIST Level I threshold and more than 133 bits below the 256-bit NIST Level V claim), with a projected sieve dimension of $d \approx 480$–484 (≈ 2.6–4.9×10^{31} core-s $\approx 2^{104.3}$–$2^{105.3}$).

7.4 Reference Verification and Key Equivalence

To verify end-to-end correctness beyond mathematical identities, we encode the recovered basis $B_{\text{rec}} \in \mathrm{SL}_2(R_{256})$ into the exact 592-byte decoded secret-key layout expected by the official HAWK NIST submission reference C implementation [9, 10] and pass it directly to the unmodified reference signing and verification routines alongside the 450-byte original public key. Both the signing routine (using B_{rec}) and the verification routine (using the original 450-byte public key Q) succeed on the first attempt.

The recovered 592-byte secret key (MD5 digest `13189d8cd2143a3b90f1652699516126`) differs byte-for-byte from the original secret key generated alongside the challenge (MD5 digest `cf5859cccdec228ef12cb3f877860ba3`) while satisfying $B^*_{\text{rec}} B_{\text{rec}} = Q$ identically. As explained in Section 3, recovering a distinct unitary-equivalent secret key that signs validly under the original reference public key (MD5 digest `2ee40754e31b8f29a137824d2a7e79d6`) confirms that the recovery uses zero secret information at any stage.

8 Scope and Limitations

To keep our claims rigorous and reproducible, we explicitly state the scope and boundaries of this work:

1. **Algebraic Attribution vs. End-to-End Engineering:** The τ-cocycle lattice Λ_τ and the τ-tower descent algorithm are due to Straznickas and Weis [23], whose tower descent procedure we use unmodified. What is new in this work is closing the modulo-two congruence into the unique-SVP sublattice Λ' ahead of reduction, deriving the second-order asymptotic blocksize shift $\Delta\beta(n) = \frac{\ln 2}{2}\, n/\ln n$ and concrete β reductions across HAWK-256/512/1024, identifying the structural root Hermite factor barrier $\delta_{0,\text{req}} = 0.996624 < 1$, eliminating Gram-mode condition-number squaring via pre-LLL exact Cholesky preconditioning, `flatter`, and exact unimodular Gram pullback $G_1 = UG_pU^T$ ($v = uU$), and demonstrating that the complete chain executes on a single core at $n = 256$ in 1,851.8 CPU-core-seconds (690× faster than previously published).

2. **Single Reference Key Instance:** Our experimental measurements at $n = 256$ are conducted on a genuine reference public key (alongside controlled ablation runs for HNF/LLL, Gram-mode MPFR, and BKZ warm-up), comparing against the published Λ_τ baseline. Because Theorem 4 guarantees that the isometry class of Λ' is strictly independent of the secret key, the target norm, determinant, and gap $\lambda_2/\lambda_1 = 2$ are identical for every HAWK-256 key, though minor run-to-run variance in sieve tour timing is expected across seeds.

3. **Reproducibility Suite:** Our verification suite supports both fast verification from the saved reduced basis (validating the sublattice certificates, GSA/AGPS20 security estimates, coordinate recovery, and C reference signing in seconds) and full end-to-end re-execution from the 450-byte public key alone.

Use of AI. The cryptanalytic results and artifacts were initially developed through an autonomous agent system powered by a MiniMax internal model. We validated the key technical claims and refined the presentation of the manuscript.

References

[1] M. R. Albrecht and L. Ducas. Lattice attacks on NTRU and LWE: A history of refinements. In J. W. Bos and M. Stam, editors, *Computational Cryptography: Algorithmic Aspects of Cryptology*, volume 469 of *London Mathematical Society Lecture Note Series*, pages 15–40. Cambridge University Press, 2021. IACR ePrint 2021/799.

[2] M. R. Albrecht, L. Ducas, G. Herold, E. Kirshanova, E. W. Postlethwaite, and M. Stevens. The General Sieve Kernel and new records in lattice reduction. In *Advances in Cryptology – EUROCRYPT 2019*, volume 11477 of *LNCS*, pages 717–746. Springer, 2019.

[3] M. R. Albrecht, V. Gheorghiu, E. W. Postlethwaite, and J. M. Schanck. Estimating quantum speedups for lattice sieves. In *Advances in Cryptology – ASIACRYPT 2020*, volume 12492 of *LNCS*, pages 583–613. Springer, 2020. IACR ePrint 2019/1161.

[4] A. Becker, L. Ducas, N. Gama, and T. Laarhoven. New directions in nearest neighbor searching with applications to lattice sieving. In *ACM-SIAM Symposium on Discrete Algorithms (SODA 2016)*, pages 10–24. SIAM, 2016.

[5] Y. Chen and P. Q. Nguyen. BKZ 2.0: Better lattice security estimates. In *Advances in Cryptology – ASIACRYPT 2011*, volume 7073 of *LNCS*, pages 1–20. Springer, 2011.

[6] D. Dachman-Soled, L. Ducas, H. Gong, and M. Rossi. LWE with side information: Attacks and concrete security estimation. In *Advances in Cryptology – CRYPTO 2020*, volume 12171 of *LNCS*, pages 329–358. Springer, 2020.

[7] L. Ducas. Shortest vector from lattice sieving: A few dimensions for free. In *Advances in Cryptology – EUROCRYPT 2018*, volume 10820 of *LNCS*, pages 125–145. Springer, 2018.

[8] L. Ducas. Provable lattice reduction of $\mathbb{Z}^n$ with blocksize $n/2$. *Designs, Codes and Cryptography*, 92(4):909–916, 2024. IACR ePrint 2023/447.

[9] L. Ducas, E. W. Postlethwaite, L. N. Pulles, and W. van Woerden. Hawk: Module LIP makes lattice signatures fast, compact and simple. In *Advances in Cryptology – ASIACRYPT 2022*, volume 13794 of *LNCS*, pages 65–94. Springer, 2022. IACR ePrint 2022/1155.

[10] J. W. Bos, O. Bronchain, L. Ducas, S. Fehr, Y.-H. Huang, T. Pornin, E. W. Postlethwaite, T. Prest, L. N. Pulles, and W. van Woerden. HAWK specification document, version 1.1. NIST Post-Quantum Cryptography Standardization Additional Digital Signature Schemes Submission, February 2025 (advanced to Round 3 May 2026; withdrawn July 29, 2026). Available at `https://hawk-sign.info`.

[11] L. Ducas and W. van Woerden. On the lattice isomorphism problem, quadratic forms, remarkable lattices, and cryptography. In *Advances in Cryptology – EUROCRYPT 2022*, volume 13277 of *LNCS*, pages 643–673. Springer, 2022. IACR ePrint 2021/1332.

[12] The FPLLL development team. `fplll`, a lattice reduction library, Version 5.4.5 (2023), and `fpylll`, a Python interface to `fplll`, Version 0.6.4 (2025). Available at `https://github.com/fplll/fplll` and `https://github.com/fplll/fpylll`.

[13] D. M. H. van Gent and L. N. Pulles. HAWK: Having automorphisms weakens key. *IACR Communications in Cryptology*, 2(2), Article 20, 2025. IACR ePrint 2025/928.

[14] C. Gentry, C. Peikert, and V. Vaikuntanathan. Trapdoors for hard lattices and new cryptographic constructions. In *ACM Symposium on Theory of Computing (STOC 2008)*, pages 197–206. ACM, 2008.

[15] A. K. Lenstra, H. W. Lenstra, Jr., and L. Lovász. Factoring polynomials with rational coefficients. *Mathematische Annalen*, 261(4):515–534, 1982.

[16] H. Luo, K. Jiang, Y. Pan, and A. Wang. Cryptanalysis of rank-2 module-LIP with symplectic automorphisms. In *Advances in Cryptology – ASIACRYPT 2024*, volume 15487 of *LNCS*, pages 359–385. Springer, 2024. IACR ePrint 2024/1173.

[17] B. Nelson, J. Limbrey, C. Ling, and A. Mendelsohn. Cryptanalysis of HAWK: A guessing game. Cryptology ePrint Archive, Paper 2026/1318, 2026.

[18] P. Q. Nguyen and D. Stehlé. An LLL algorithm with quadratic complexity. *SIAM Journal on Computing*, 39(3):874–903, 2009.

[19] P.-A. Fouque, J. Hoffstein, P. Kirchner, V. Lyubashevsky, T. Pornin, T. Prest, T. Ricosset, G. Seiler, W. Whyte, and Z. Zhang. FALCON: Fast-Fourier lattice-based compact signatures over NTRU. NIST Post-Quantum Cryptography Standardization Round 3 Submission, 2020.

[20] K. Ryan and N. Heninger. Fast practical lattice reduction through iterated compression. In *Advances in Cryptology – CRYPTO 2023*, volume 14083 of *LNCS*, pages 3–36. Springer, 2023.

[21] M.-J. O. Saarinen. HAWK "Guessing Game" is not polynomial-time. Cryptology ePrint Archive, Paper 2026/1377, 2026.

[22] C.-P. Schnorr. A hierarchy of polynomial time lattice basis reduction algorithms. *Theoretical Computer Science*, 53(2–3):201–224, 1987.

[23] Z. Straznickas and S. A. Weis. HAWK-n key recovery reduces to SVP in dimension $n/2+1$. Cryptology ePrint Archive, Paper 2026/1593, 2026.

[24] Z. Zhao, J. Ding, and B.-Y. Yang. Sieving with streaming memory access. *IACR Transactions on Cryptographic Hardware and Embedded Systems (TCHES)*, 2025(2):362–384, 2025. IACR ePrint 2024/739.