

UNIVERSITY OF BERGEN
DEPARTMENT OF INFORMATICS

Learning a Parallelepiped attack against Hawk digital signature scheme

Author: Eirik Djupvik Skjerve

Supervisors: Igor Aleksandrovich Semaev & Martin Feussner



UNIVERSITY OF BERGEN
Faculty of Science and Technology

March, 2025

Abstract

In this work, we do cryptanalysis on the Hawk digital signature scheme using the *Learning a Parallelepiped* method which broke the GGH and basic NTRU digital signature schemes.

Acknowledgements

Acknowledgements here

Eirik D. Skjerve

Contents

1	Introduction	1
1.1	Context and motivation	1
1.2	Objectives	2
1.3	Thesis outline	3
1.4	Detailed tentative roadmap	3
1.4.1	Schedule	4
2	Background	5
2.1	Cryptology	5
2.1.1	Cryptography	6
2.1.2	Cryptanalysis	6
2.2	Digital Signatures	6
2.2.1	Hash-and-Sign	6
2.2.2	GGH	6
2.2.3	NTRU	6
2.3	Algebra	6
2.3.1	Polynomials	6
2.3.2	Polynomial rings	6
2.3.3	Number fields	6
2.4	Linear Algebra and Lattices	6
2.5	Probability Theory	7
2.6	Gradient Search	7
2.6.1	Overview	7
2.6.2	Gradients	8
2.6.3	Gradient descent and optimization	8
3	Hawk and HPP	9
3.1	Hawk	10
3.1.1	Overview	10

3.1.2	Parameters	11
3.1.3	Hawk key pairs and key pair generation	11
3.1.4	Solving the NTRU-equation	12
3.1.5	Discrete Gaussian Distribution	13
3.1.6	Hawk signature generation	14
3.1.7	Hawk signature verification	14
3.1.8	Hawk security	15
3.2	Implementation of Hawk	15
3.3	HPP	16
3.3.1	Setup and idealized version	16
3.3.2	Covariance matrix estimation	17
3.3.3	Hidden parallelepiped to hidden hypercube transformation	18
3.3.4	Moments and Gradient Descent	19
3.4	HPP against the Normal Distribution	22
4	Cryptanalysis of Hawk	24
4.1	Overview of method	24
4.2	Covariance matrix and hypercube transformation	25
4.3	Gradient search overview	26
4.4	Practical method	28
4.5	Results	30
4.6	Conclusion	31
5	Results	32
6	Discussion	33
	Acronyms	34
	Bibliography	35
A	Generated code from Protocol buffers	36

List of Figures

3.1	Hidden parallelepiped problem in dimension 2	17
3.2	Hidden hypercube problem in dimension 2	19
3.3	Hidden parallelepiped problem in dimension 2 for normal distribution . .	23
3.4	Hidden hypercube problem in dimension 2 for normal distribution	23
4.1	Hidden parallelepiped problem in dimension 2 for rounded normal distribution	27
4.2	Hidden hypercube problem in dimension 2 for rounded normal distribution	27

List of Tables

3.1	Parameter sets for Hawk	11
4.1	Closeness measure for Hawk attack	31

Listings

A.1 Source code of something	36
--	----

Chapter 1

Introduction

1.1 Context and motivation

Digital signatures are an integral part of secure communication today. They enable a receiver of a digital message to mathematically verify the sender is who they say they are. The widely used Digital Signature Algorithm (DSA) and the Rivest, Shamir, Adleman (RSA) signature scheme are in peril due to the potential emergence of quantum computers which can break the hard problems DSA and RSA-sign are based upon. Whether practical quantum computers with these powers will emerge any time soon is debatable. However, measures against the looming threat has already begun. In 2016, the National Institute of Standards and Technology (NIST) announced a process for selecting new standard schemes for Key Encapsulation Methods (KEMs) and digital signatures that are resilient against quantum attacks (<https://www.nist.gov/pqcrypto>). Many of the submissions to this process, including KRYSTALS-Dilithium which is to be standardized, are based on lattice problems that are believed to be hard to solve for both classical and quantum computers.

Cryptographic schemes based on lattice problems are not an entirely new phenomenon, however. NTRU-Sign [2], the signature counterpart of the NTRU crypto-system, is a digital signature scheme based on the hardness of the Closest Vector Problem (CVP), a well known lattice problem (source?). The original scheme was broken by Phong. Q. Nguyen & Oded Regev in 2006 [5]; not by solving the CVP, but by retrieving a secret key by observing enough signatures. In other words, each signature leaks some information about the secret key. The title of their paper and the name of the attack is *Learning a Parallelepiped*, and the problem to solve in this attack will henceforth be denoted as the Hidden

Parallelepiped Problem (HPP) as one tries to *learn* a parallelepiped. Countermeasures for this attack was proposed, but ultimately broken again in 2012 due to a more advanced extension of the original attack [1].

Hawk [3] is a digital signature scheme submitted to NIST’s standardization process and is a viable candidate for standardization due to its speed and small signature- and keysizes. It is also a lattice-based signature scheme akin to NTRU-sign, but with some significant changes, and a different underlying hard problem on which its security is based upon. This thesis will investigate if a method based on HPP can be aimed at Hawk to retrieve information about the secret key, and ultimately break the scheme.

1.2 Objectives

The objective of this thesis consists of two main parts:

- **Implementation of Hawk in Rust.** As the first part of this thesis I implement the Hawk digital signature scheme according to [3] in the Rust programming language.¹ Implementing a scheme and its algorithms is a good way to more deeply learn how it works. I chose to do the implementation in Rust for the sake of becoming more adept at this programming language as a personal bonus objective of the thesis. Moreover, having ones own implementation of a scheme makes it easier to experiment on, run simulations with, adjust, and modify it to ones need. It would in any case be challenging to understand and work with dense, long, and complicated source code someone else has written. For the Hawk teams source code in C and a reference implementation in Python see <https://github.com/hawk-sign>.
- **Cryptanalysis and experimentation.** The second part of this thesis is cryptanalysis of Hawk. The goal is to use the *Learning a parallelepiped* attack and do suitable modifications to attack Hawk. This requires both theoretical and practical work, and experiments will, like the Hawk implementation itself, be implemented in Rust.

¹Disclaimer: this implementation is not meant to be comparable with the Hawk teams implementation for real life usage, as it is not highly optimized and not all formal requirements are met.

1.3 Thesis outline

Chapter 2 will introduce important notions and mathematical background used in this thesis. Chapter 3 will introduce Hawk and its implementation, and the *Learning a Paralelepiped* attack. In Chapter 4 the cryptanalysis of Hawk is presented. The final chapter will discuss results and future work.

1.4 Detailed tentative roadmap

1. Introduce idea of a digital signature
2. Introduce lattice facts and lattice problems used in digital signatures
3. Introduce other linear algebra and statistics / probability theory stuff
4. Introduce notion of gradient search and variations
5. Describe Hawk in detail
6. Describe Hawk implementation in detail
7. Describe basic HPP attack using notation from original paper
8. Proof and discussion of HPP against normally distributed samples, still using notation from original paper
9. Describe general application of HPP against Hawk using Hawk notation and conventions (e.g. column vectors instead of row vectors, matrix B instead of V, etc.)
10. Describe measuring of DGD properties, and implementation of this
11. Detailed description of attack in practice, discuss implementation challenges w.r.t. memory, runtime, etc.
12. Results and discussion of these, limitations, considerations, etc.

1.4.1 Schedule

- **Week 9, 28.02:** Concluding that experiments were unsuccessful. Further experiments code runs will be to produce measurements that will be reported in the thesis
Still nice to have 512 GB instance in NREC
- **Week 10, 07.03**
- **Week 11, 14.03**
- **Week 12, 21.03**
- **Week 13, 28.03**
- **Week 14, 04.04**
- **Week 15, 11.04**
- **Week 16, 18.04**
- **Week 17, 25.04**
- **Week 18, 02.05**
- **Week 19, 09.05**
- **Week 20, 16.05**
- **Week 21, 23.05**

Chapter 2

Background

In this chapter, the field of cryptology will be introduced, with an emphasis on digital signatures and cryptanalysis. We also introduce some necessary facts and notions related to linear algebra and lattices, as well as probability theory and distributions. Lastly, we introduce the notion of *Gradient Search* and ADAM-optimizers, which will be a central tool in this thesis.

2.1 Cryptology

For this section, [4] will be used.

2.1.1 Cryptography

2.1.2 Cryptanalysis

2.2 Digital Signatures

2.2.1 Hash-and-Sign

2.2.2 GGH

2.2.3 NTRU

2.3 Algebra

2.3.1 Polynomials

2.3.2 Polynomial rings

2.3.3 Number fields

2.4 Linear Algebra and Lattices

Denote by \mathbf{v} an $n \times 1$ column vector on the form

$$\mathbf{v} = \begin{bmatrix} v_0 \\ v_1 \\ \dots \\ v_{n-1} \end{bmatrix}$$

and by \mathbf{B} an $n \times m$ matrix on the form

$$\mathbf{B} = \begin{bmatrix} b_{0,0} & b_{0,1} & \cdots & b_{0,n-1} \\ b_{1,0} & b_{1,1} & \cdots & b_{1,n-1} \\ \cdots & \cdots & \cdots & \cdots \\ b_{m-1,0} & b_{m-1,1} & \cdots & b_{m-1,n-1} \end{bmatrix}$$

Generally, entries v_i and $b_{i,j}$ are integers unless stated otherwise. Some places the thesis will use row notation instead of column notation for the vectors, so that \mathbf{v} is a $1 \times n$ row vector on the form

$$\mathbf{c} = [v_0, v_1, \dots, v_{n-1}]$$

In these cases this will be pointed out.

We denote by $\langle \cdot, \cdot \rangle$ the dot-product of two vectors of equal dimensions as

$$\langle \mathbf{x}, \mathbf{y} \rangle = \mathbf{x}^t \mathbf{y} = \sum_{i=0}^{n-1} x_i y_i$$

2.5 Probability Theory

2.6 Gradient Search

2.6.1 Overview

Used in this section: [7] Gradient descent is a widely used method in optimization and learning problems.

The general method works by measuring the gradient of the target function $\nabla f(\theta)$ w.r.t. to its parameters θ to get the direction in which $\theta f(\theta)$ changes the most. One then takes a "step" based on this direction (for a descent, one moves against the gradient, for an ascent, with the gradient), influenced by the hyperparameter δ , which determines the magnitude of the step.

Before going more in depth of the methods, we quickly define the gradient of a function.

2.6.2 Gradients

Let $\theta = [\theta_1, \theta_2, \dots, \theta_n]$ The gradient of a multivariate function $f(\theta)$ is defined as the vector of partial derivatives evaluated at θ

$$\nabla f(\theta) = \begin{bmatrix} \frac{\partial f}{\partial \theta_1}(\theta) \\ \frac{\partial f}{\partial \theta_2}(\theta) \\ \dots \\ \frac{\partial f}{\partial \theta_n}(\theta) \end{bmatrix}$$

2.6.3 Gradient descent and optimization

In Algorithm 1 the so-called "vanilla" gradient descent is described.

Algorithm 1 Vanilla gradient descent

Require: differentiable target function f

- 1: initialize θ_0 as a starting point
 - 2: **while** θ_t is not optimal **do**
 - 3: $\theta_t \leftarrow \theta_{t-1} - \delta \cdot \nabla f_{\theta}(\theta_{t-1})$
-

Note that for vanilla gradient descent as described in Algorithm 1, to compute the gradient one needs the entire dataset for each iteration, which sometimes can be too large to fit in memory, or too large to be computationally efficient.

Many optimization techniques are utilized in gradient descent today, which overcome this hurdle.

Chapter 3

Hawk and HPP

3.1 Hawk

In this section we introduce the digital signature scheme Hawk [3], which will later be the target for our cryptanalysis. As mentioned in the introduction, Hawk is a lattice based signature scheme that shares some key points with that of NTRU-sign [2], the target for the original HPP attack. The first part of this chapter/section will give an introduction on how the Hawk scheme works on a high level. After this, the implementation of Hawk will be described, where more detail about specific subroutines and parts of the procedures will be given.

In this section, quite a few parts of Hawk as described in [3] are left out due to the focus of this thesis. For example, Hawk utilizes compression of keys and signatures (which influence the key generation and signature generation procedures), and some of their security considerations regarding a practical implementation is based on side channel attacks, both of which is not a concern in this thesis. Moreover, their security analysis is based on experimental lattice reduction and security proofs of the underlying hard problems (namely the *Lattice Isomorphism Problem* and the *One More Shortest Vector Problem*), which, again, is not the focus of this thesis.

3.1.1 Overview

In Hawk, polynomials are defined over the cyclotomic number field $\mathcal{K}_n = \mathbb{Q}[X]/(X^n + 1)$ which has the corresponding ring of integers $\mathbb{Z}[X]/(X^n + 1)$. Such a polynomial $f \in \mathcal{K}_n$ can also be represented by a (column) vector of its coefficients in \mathbb{Q}^n (in practical setting, coefficients are in \mathbb{Z}^n), denoted $\text{vec}(f)$, where the index of each coefficient corresponds to its power of X in f .¹ Explicitly, if $f = a_0X^0 + a_1X^1 + \dots + a_{n-1}X^{n-1}$

$$\text{vec}(f) = \begin{bmatrix} a_0 \\ a_1 \\ \dots \\ a_{n-1} \end{bmatrix}$$

We define a mapping

$$\text{rot} : \mathcal{K}_n \rightarrow \mathbb{Q}^{n \times n}, \text{rot}(f) = \begin{bmatrix} \text{vec}(f) & \text{vec}(fX) & \text{vec}(fX^2) & \dots & \text{vec}(fX^{n-1}) \end{bmatrix}$$

¹This is a polynomial representation that is frequent in programming implementations when a dedicated algebra library is not used.

which enables one to construct a matrix in $\mathbb{Q}^{n \times n}$ from a single polynomial in \mathcal{K}_n . A vector $\text{vec}(fX^k)$ to any power k will henceforth be referred to as a "shift" of f , since all entries with powers X^{n-t} for $n-t+k < n-1$ are shifted k times, and entries with powers X^{n-s} where $n-s+k \geq n$ will "go around" and be negated as $-X^{n-s+k \bmod n}$.

This should maybe be in the background section...

The hash function used in Hawk is SHAKE256, an extendable output function (XOF) which enables arbitrary output length, unlike hash functions like SHA256 which has a static output size of 256 bits. This property is useful since SHAKE256 can be used in all three degrees of Hawk.

Should probably describe this a bit better

3.1.2 Parameters

Below is the parameters for Hawk degree 256, 512, and 1024. Note that this list only contains the relevant parameters for this thesis, and that many parameters relevant to compression and decompression are omitted.

Define the integer polynomial ring $\mathbb{Z}[X]/(X^n+1)$

Table 3.1: Parameter sets for **Hawk**

Name	HAWK-256	HAWK-512	HAWK-1024
Targeted security	Challenge	NIST-I	NIST-V
Bit security λ	64	128	256
Degree n	256	512	1024
Transcript size limit q_s	2^{32}	2^{64}	2^{64}
Centered binomial η for sampling (f, g)	2	4	8
Signature std. dev. σ_{sign}	1.010	1.278	1.299
Verification std. dev. σ_{verify}	1.042	1.425	1.571

Insert more relevant parameters here

3.1.3 Hawk key pairs and key pair generation

A Hawk private key is represented by the matrix

$$\mathbf{B} = \begin{bmatrix} f & F \\ g & G \end{bmatrix} \in \mathcal{K}_n^{2 \times 2}$$

Here, entries are chosen such that f and g have small coefficients, and the equation $fG - FG = 1 \bmod X^n + 1$ holds, and consequently $\det(\mathbf{B}) = 1$, making \mathbf{B} invertible. The inverse of \mathbf{B} is

$$\mathbf{B}^{-1} = \begin{bmatrix} G & -F \\ -g & f \end{bmatrix} \in \mathcal{K}_n^{2 \times 2}$$

A Hawk public key is defined as

$$\mathbf{Q} = \begin{bmatrix} q_{00} & q_{01} \\ q_{10} & q_{11} \end{bmatrix} = \mathbf{B}^* \mathbf{B} = \begin{bmatrix} f^*f + g^*g & f^*F + g^*G \\ F^*f + G^*g & F^*F + G^*G \end{bmatrix}$$

where f^* denotes the Hermitian adjoint of f , explicitly $f^* = f_0 - f_{n-1}X - \dots - f_1X^{n-1}$, and \mathbf{B}^* is the transpose of \mathbf{B} , \mathbf{B}^T where each entry is taken the Hermitian adjoint of. Explicitly:

$$\mathbf{B}^* = \begin{bmatrix} f^* & g^* \\ F^* & G^* \end{bmatrix}$$

We can also define rot on a matrix as the mapping

$$\text{rot} : \mathcal{K}_n^{2 \times 2} \rightarrow \mathbb{Q}^{2n \times 2n}, \text{rot}\left(\begin{bmatrix} f & F \\ g & G \end{bmatrix}\right) = \begin{bmatrix} \text{rot}(f) & \text{rot}(F) \\ \text{rot}(g) & \text{rot}(G) \end{bmatrix}$$

Note that when working with $\text{rot}(\mathbf{B})$ instead of \mathbf{B} , the Hermitian adjoint \mathbf{B}^* corresponds to the transpose of $\text{rot}(\mathbf{B})$, as $\text{rot}(\mathbf{B}^*) = \text{rot}(\mathbf{B})^T$.

$\text{rot}(\mathbf{B})$ serves as a basis for the private lattice in which a (hash digest of a) message will be signed in the signature generation step. A simplified version of the key generation is described in the following algorithm:

Algorithm 2 Simplified Hawk Key Generation

- 1: Sample $f, g \in \mathbb{Z}[X]/(X^n + 1)$ from $\text{bin}(\eta)$
 - 2: Compute F, G s.t. $fG - Fg = 1 \mod \mathbb{Z}[X]/(X^n + 1)$ holds
 - 3: $\mathbf{B} \leftarrow \begin{bmatrix} f & F \\ g & G \end{bmatrix}$
 - 4: $\mathbf{Q} \leftarrow \mathbf{B}^* \mathbf{B}$
 - 5: **return** private key \mathbf{B} , public key \mathbf{Q}
-

3.1.4 Solving the NTRU-equation

An important point in the key generation process is finding proper polynomials F and G that satisfy the NTRU-equation $fG - Fg = 1 \mod \mathbb{Z}[X]/(X^n + 1)$. Importantly, coefficients of F and G need to be rather small, and the procedure of solving the equation is a time-consuming part of the key generation process. In the original NTRU system (both encryption and signature) resultants are used. Hawk uses the method proposed by Pornin and Prest in [6] which improves upon the existing resultant method in terms of both time- and memory complexity.

Need
some
explanation
of resultants
here

3.1.5 Discrete Gaussian Distribution

Before introducing the Hawk signature generation we describe the procedure to sample from the Discrete Gaussian Distribution, as described in [3].

Denote by $\mathcal{D}_{2\mathbb{Z}+c,\sigma}$ the Discrete Gaussian Distribution with parameter c and σ . Let $\rho_\sigma : \mathbb{Z} \rightarrow \mathbb{R}, \rho_\sigma(x) = \exp(\frac{-x^2}{2\sigma^2})$. The Probability Density Function (PDF) of $\mathcal{D}_{2\mathbb{Z}+c,\sigma}$ is defined as:

$$\Pr[X = x] = \frac{\rho_\sigma(x)}{\sum_{y \in 2\mathbb{Z}+c} \rho_\sigma(y)}$$

For $z \geq 0$ we define the function $P_c(z) = \Pr[|X| \geq z]$ when $X \sim \mathcal{D}_{2\mathbb{Z}+c,\sigma}$. Using this function for $c \in \{0, 1\}$, one computes two Cumulative Distribution Tables (CDT) T_0 and T_1 such that $T_0[k] = P_0(2 + 2k)$ and $T_1[k] = P_1(3 + 2k)$ where $T_c[k]$ denotes the k -th index in the table. In practice, to avoid using floating point numbers, the entries in the table is scaled by 2^{78} such that entries are integers with a high enough precision. For this overview, however, we only consider the unscaled version. Using the tables, we can define a procedure **sample** given by the following algorithm:

Algorithm 3 sample

Require: parameter $c \in \{0, 1\}$

- 1: $q \leftarrow$ uniformly sampled from $[-1, 1] \in \mathbb{Q}$
 - 2: $z \leftarrow 0$
 - 3: **while** $T_c[z] \neq 0$ **do**
 - 4: **if** $|q| \leq T_c[z]$ **then**
 - 5: $z \leftarrow z + 1$
 - 6: **else**
 - 7: $z \leftarrow 2z + c$
 - 8: **if** $q < 0$ **then**
 - 9: $z \leftarrow -z$
 - 10: **return** z
-

This algorithm only samples one point given parameter c . We can extend this to generate vectors of length n where each entry is distributed according to $\mathcal{D}_{2\mathbb{Z}+c,\sigma}$ by the following procedure:

Algorithm 4 Sample vector of length n according to $\mathcal{D}_{2\mathbb{Z}+c,\sigma}$

Require: Binary vector \mathbf{t} with entries uniformly distributed from $\{0, 1\}$

- 1: $\mathbf{x} \leftarrow$ empty vector of length $2n$
 - 2: **for** $i = 0, 1, \dots, 2n - 1$ **do**
 - 3: $\mathbf{x}[i] \leftarrow \text{sample}(\mathbf{t}[i])$
 - return** \mathbf{x}
-

In this manner, one can sample a lattice point \mathbf{x} which is relatively close to a target lattice point \mathbf{t} , which will be used in the signature generation step.

3.1.6 Hawk signature generation

To generate a Hawk signature of a message \mathbf{m} , one computes a hash digest \mathbf{h} of the message, and samples a point \mathbf{x} from $\mathcal{D}_{2\mathbb{Z}^{2n}+\mathbf{t}, \sigma_{\text{sign}}}$ that is close to \mathbf{h} in the private lattice generated by $\text{rot}(\mathbf{B})$. By transforming the point \mathbf{x} back to the lattice \mathbb{Z}^{2n} via \mathbf{B}^{-1} one has a signature that can be verified by anyone that has access to the public key \mathbf{Q} . Below is the (simplified) procedure formulated in Algorithm 5:

Algorithm 5 Simplified Hawk Signature Generation

Require: Message \mathbf{m} , private key \mathbf{B}

```

1:  $M \leftarrow H(\mathbf{m})$  ▷  $H$  is a hash function
2:  $\mathbf{h} \leftarrow H(M \parallel \text{salt})$  ▷  $\text{salt}$  is a randomly generated value and  $\parallel$  denotes concatenation
3:  $\mathbf{t} \leftarrow \mathbf{B}\mathbf{h} \bmod 2$  ▷ Reduction  $\bmod 2$  is done entrywise
4:  $\mathbf{x} \leftarrow \text{sample}(\mathbf{t})$ 
5: if  $\|\mathbf{x}\|^2 \geq 4 \cdot \sigma_{\text{sign}}^2 \cdot 2n$  then
6:   restart
7: else
8:    $\mathbf{w} \leftarrow \mathbf{B}^{-1}\mathbf{x}$ 
9:    $\mathbf{s} \leftarrow \frac{1}{2}(\mathbf{h} - \mathbf{w})$ 
10:  return signature  $\mathbf{s}$ , salt  $\text{salt}$ 
```

3.1.7 Hawk signature verification

To verify a Hawk signature, one simply recomputes the vector \mathbf{h} from \mathbf{m} and salt and in turn the vector \mathbf{w} , and check if the \mathbf{Q} -norm of \mathbf{w} , $\|\mathbf{w}\|_{\mathbf{Q}}^2$ is not too high. A signature with \mathbf{Q} -norm of appropriately short length will be considered valid. A summary of the simplified procedure is given in Algorithm 6:

Algorithm 6 Simplified Hawk Signature Verification

Require: Signature \mathbf{s} , message \mathbf{m} , salt salt , public key \mathbf{Q}

```

1:  $M \leftarrow H(\mathbf{m})$ 
2:  $\mathbf{h} \leftarrow H(M \parallel \text{salt})$ 
3:  $\mathbf{w} \leftarrow \mathbf{h} - 2\mathbf{s}$ 
4: if  $\|\mathbf{w}\|_{\mathbf{Q}}^2 \geq 4 \cdot \sigma_{\text{verify}}^2 \cdot 2n$  then
5:   return false
6: else return true
```

We now briefly show why verification works:

As defined,

$$\begin{aligned}\|\mathbf{w}\|_{\mathbf{Q}} &= \sqrt{\mathbf{w}^* \mathbf{Q} \mathbf{w}} \implies \|\mathbf{w}\|_{\mathbf{Q}}^2 = |\mathbf{w}^* \mathbf{Q} \mathbf{w}| \\ \mathbf{w}^* \mathbf{Q} \mathbf{w} &= \mathbf{w}^* \mathbf{B}^* \mathbf{B} \mathbf{w} = (\mathbf{B} \mathbf{w})^* (\mathbf{B} \mathbf{w}) = \|\mathbf{B} \mathbf{w}\|^2 = \|\mathbf{x}\|^2 \\ \text{since } \mathbf{w} &= \mathbf{B}^{-1} \mathbf{x} \implies \|\mathbf{B} \mathbf{w}\|^2 = \|\mathbf{B} \mathbf{B}^{-1} \mathbf{x}\|^2 = \|\mathbf{x}\|^2\end{aligned}$$

This shows that by knowing \mathbf{Q} , one can measure the length of vectors in the secret lattice generated by \mathbf{B} . To find vectors close to a target vector \mathbf{t} in the private lattice, however, requires knowledge about \mathbf{B} .

3.1.8 Hawk security

3.2 Implementation of Hawk

3.3 HPP

In this section we present the *Learning a Parallelepiped* attack as described in [5]. Note that in this section bold lowercase \mathbf{v} denotes a *row*-vector to follow the same notation as in the original paper.

3.3.1 Setup and idealized version

Let $\mathbf{V} \in \mathcal{GL}(\mathbb{R})$ be a secret $n \times n$ unimodular matrix and $\mathcal{P}(\mathbf{V})$ be a fundamental parallelepiped, defined as the set $\{\mathbf{xV} : \mathbf{x} \in [-1, 1]^n\}$. Let $\mathbf{v} = \mathbf{xV}$. The problem to solve is informally described below and visualized in figure 3.1.

Problem 1 *Given enough vectors $\mathbf{v} = \mathbf{xV}$ (i.e. by observing a large enough subset of $\mathcal{P}(\mathbf{V})$), where both \mathbf{x} and \mathbf{V} is unknown, recover rows of $\pm\mathbf{V}$*

The following three steps are used to solve Problem 1:

1. Estimate the covariance matrix $\mathbf{V}^t\mathbf{V}$
2. Transform samples $\mathbf{v} \in \mathcal{P}(\mathbf{V})$ to $\mathbf{c} \in \mathcal{P}(\mathbf{C})$ where $\mathcal{P}(\mathbf{C})$ is a hypercube, i.e. $\mathbf{CC}^t = \mathbf{I}_n$
3. Do gradient descent to minimize the fourth moment of one-dimensional projections and reveal a row of $\pm\mathbf{C}$ which finally can be transformed into a row of $\pm\mathbf{V}$

In the following, each of these steps will be covered in detail.

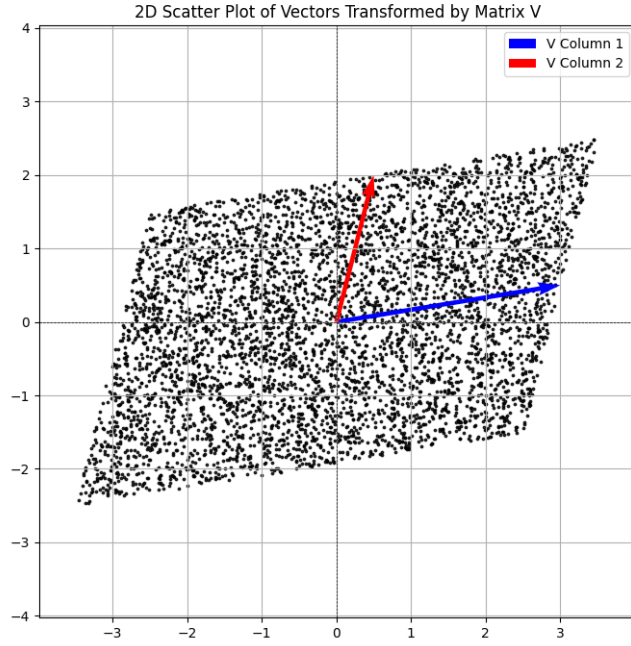


Figure 3.1: Hidden parallelepiped problem in dimension 2

3.3.2 Covariance matrix estimation

Given enough samples on the form $\mathbf{v} = \mathbf{xV}$, we want to estimate the covariance matrix $\mathbf{G} \approx \mathbf{V}^t \mathbf{V}$. This is achieved as $\mathbf{v}^t \mathbf{v} = (\mathbf{xV})^t (\mathbf{xV}) = \mathbf{V}^t \mathbf{x}^t \mathbf{x} \mathbf{V}$. Now, by taking the expectation of the inner term we get $\mathbb{E}[\mathbf{x}^t \mathbf{x}] = \mathbf{I}_n/3$ where \mathbf{I}_n is the $n \times n$ identity matrix because of the following: Since all $x_i \in \mathbf{x}$ are distributed according to the uniform distribution over $[-1, 1]$ and each x_i are independent, we have that $\mathbb{E}[x_i] = 0$ and $\mathbb{E}[x_i x_j] = \mathbb{E}[x_i] \mathbb{E}[x_j] = 0$ when $i \neq j$. For the case when $i = j$, we have

$$\mathbb{E}[x_i x_j] = \mathbb{E}[x^2] = \int_a^b x^2 \frac{1}{b-a} dx = \int_{-1}^1 x^2 \frac{1}{2} dx = \frac{1}{3}$$

Therefore, $\mathbb{E}[\mathbf{x}^t \mathbf{x}]$ is an $n \times n$ matrix with $\frac{1}{3}$ down the diagonal and is 0 otherwise, i.e. $\mathbf{I}_n/3$. Thus, as number of samples grow, $\mathbf{v}^t \mathbf{v} \rightarrow \mathbf{V}^t (\mathbf{I}_n/3) \mathbf{V}$, and therefore $\mathbf{v}^t \mathbf{v} \cdot 3 \rightarrow \mathbf{V}^t \mathbf{V}$. In conclusion: by taking the average of $\mathbf{v}^t \mathbf{v}$ for all collected samples, and multiplying the resulting $n \times n$ matrix with 3, one has a good approximation of the covariance matrix $\mathbf{V}^t \mathbf{V}$.

Rewrite this computation: not quite correct notation for integration

3.3.3 Hidden parallelepiped to hidden hypercube transformation

Given a good approximation $\mathbf{G} \approx \mathbf{V}^t \mathbf{V}$, the next step is to calculate a linear transformation \mathbf{L} such that the following is true:

1. $\mathbf{C} = \mathbf{V}\mathbf{L}$ is orthonormal, i.e. the rows are pairwise orthogonal and the norm of each row is 1. In other words, $\mathbf{C}\mathbf{C}^t = \mathbf{I}$. Consequently, $\mathcal{P}(\mathbf{C})$ becomes a hypercube.
2. If \mathbf{v} is uniformly distributed over $\mathcal{P}(\mathbf{V})$ then $\mathbf{c} = \mathbf{v}\mathbf{L}$ is uniformly distributed over $\mathcal{P}(\mathbf{C})$.

This is achieved by taking the Cholesky decomposition of $\mathbf{G}^{-1} = \mathbf{L}\mathbf{L}^t$ where \mathbf{L} is a lower-triangular matrix. To compute Cholesky decomposition of \mathbf{G}^{-1} , we must first show that \mathbf{G} is symmetric positive definite.

1. \mathbf{G} is symmetric $\iff \mathbf{G}^t = \mathbf{G}$ which is clear as $\mathbf{G}^t = (\mathbf{V}^t \mathbf{V})^t = \mathbf{V}^t (\mathbf{V}^t)^t = \mathbf{V}^t \mathbf{V} = \mathbf{G}$.
2. \mathbf{G} is positive definite if for any non-zero column vector $\mathbf{x} \in \mathbb{R}^n$, $\mathbf{x}^t \mathbf{G} \mathbf{x} > 0$. We have that $\mathbf{x}^t \mathbf{G} \mathbf{x} = \mathbf{x}^t \mathbf{V}^t \mathbf{V} \mathbf{x} = (\mathbf{V} \mathbf{x})^t (\mathbf{V} \mathbf{x})$. Denote by $\mathbf{y} = \mathbf{V} \mathbf{x}$. Since $\mathbf{x} \neq \mathbf{0}$ and \mathbf{V} is invertible (and therefore non-zero) it is clear that $\mathbf{y} \neq \mathbf{0}$ and $\mathbf{y}^t \mathbf{y} = \|\mathbf{y}\|^2 > 0$.

Since \mathbf{G} is symmetric positive definite we can do decomposition to get \mathbf{L} . Then:

1. if $\mathbf{C} = \mathbf{V}\mathbf{L}$, then $\mathbf{C}\mathbf{C}^t = \mathbf{V}\mathbf{L}\mathbf{L}^t\mathbf{V}^t = \mathbf{V}\mathbf{G}^{-1}\mathbf{V}^t = \mathbf{V}(\mathbf{V}^t \mathbf{V})^{-1}\mathbf{V}^t = \mathbf{V}\mathbf{V}^{-1}\mathbf{V}^{-t}\mathbf{V}^t = \mathbf{I}$
2. since entries in \mathbf{x} are uniformly distributed, $\mathbf{c} = \mathbf{C}\mathbf{x}$ is uniformly distributed over $\mathcal{P}(\mathbf{C})$

By multiplying our samples \mathbf{v} by \mathbf{L} on the right, we transform them from the hidden parallelepiped to the hidden hypercube. Therefore, the problem to solve now can be called the "Hidden Hypercube Problem". If one finds the rows of $\pm \mathbf{C}$, one can simply multiply the result on the right by \mathbf{L}^{-1} to obtain the solution for \mathbf{V} .

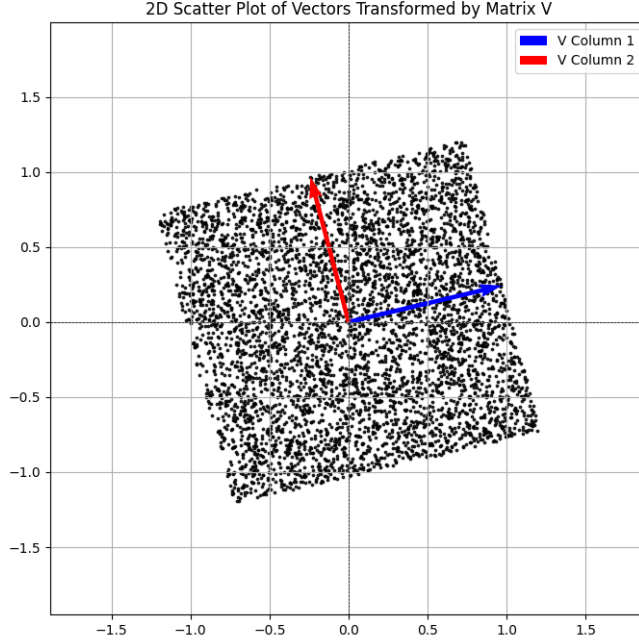


Figure 3.2: Hidden hypercube problem in dimension 2

3.3.4 Moments and Gradient Descent

The last major step in the attack is to measure and minimize the fourth moment of one-dimensional projections to disclose rows of $\pm \mathbf{C}$. Let $mom_{k,\mathbf{C}}(\mathbf{w})$ be defined as the k -th moment of $\mathcal{P}(\mathbf{C})$ projected onto \mathbf{w} , i.e. $\mathbb{E}[\langle \mathbf{c}, \mathbf{w} \rangle^k]$ where $\mathbf{c} = \mathbf{x}\mathbf{C}$ for \mathbf{x} uniformly distributed and $\mathbf{w} \in \mathbb{R}^n$. Looking at the term $\langle \mathbf{c}, \mathbf{w} \rangle$, we have $\langle \mathbf{x}\mathbf{C}, \mathbf{w} \rangle = \langle \sum_{i=1}^n x_i c_i, \mathbf{w} \rangle$ where c_i is the i -th row of \mathbf{C} . Since x_i is a scalar, we can move it out of the dot-product brackets. $\sum_{i=1}^n x_i \langle c_i, \mathbf{w} \rangle$. Evaluating this inside the $\mathbb{E}[\]$ we have $\mathbb{E}[\sum_{i=1}^n x_i \langle c_i, \mathbf{w} \rangle^k]$. We look at the two cases when $k = 2$ and $k = 4$.

- **k = 2** : $\mathbb{E}[(\sum_{i=1}^n x_i \langle c_i, \mathbf{w} \rangle)^2] = \mathbb{E}[\sum_i^n \sum_j^n x_i x_j \langle c_i, \mathbf{w} \rangle \langle c_j, \mathbf{w} \rangle]$. As seen before in section 3.3.2, $\mathbb{E}[x_i x_j] = \frac{1}{3}$ when $i = j$ and 0 otherwise. Thus, we have the final expression $mom_{2,\mathbf{C}}(\mathbf{w}) = \frac{1}{3} \sum_i^n \langle c_i, \mathbf{w} \rangle^2$ which can also be written as $= \frac{1}{3} \mathbf{w}\mathbf{C}^t \mathbf{C}\mathbf{w}$
- **k = 4** :

$$\mathbb{E}[(\sum_{i=1}^n x_i \langle c_i, \mathbf{w} \rangle)^4] = \mathbb{E}[\sum_i^n \sum_j^n \sum_k^n \sum_l^n x_i x_j x_k x_l \langle c_i, \mathbf{w} \rangle \langle c_j, \mathbf{w} \rangle \langle c_k, \mathbf{w} \rangle \langle c_l, \mathbf{w} \rangle]$$

There are three cases for the indices i, j, k and l :

1. **All equal:** If $i = j = k = l$, we simply have $\sum_i^n \mathbb{E}[x^4] \langle c_i, \mathbf{w} \rangle^4 = \frac{1}{5} \sum_i \langle c_i, \mathbf{w} \rangle^4$ due to the fact that $\mathbb{E}[x^4] = \int_{-1}^1 x^4 \frac{1}{2} dx = \frac{1}{5}$
2. **None equal:** If $i \neq j \neq k \neq l$ the expression is zero due to $\mathbb{E}[x_i] = 0$ and all x_i, x_j, x_k, x_l are independent.
3. **Pairwise equal:** If either
 - $i = j \neq k = l$
 - $i = k \neq j = l$
 - $i = l \neq j = k$

then we have $\sum_{i \neq j} \mathbb{E}[x_i^2 x_j^2] \langle c_i, \mathbf{w} \rangle^2 \langle c_j, \mathbf{w} \rangle^2 = \frac{1}{9} \sum_{i \neq j} \langle c_i, \mathbf{w} \rangle^2 \langle c_j, \mathbf{w} \rangle^2$. By putting the above together we get

$$\frac{1}{5} \sum_{i=1}^n \langle c_i, \mathbf{w} \rangle^4 + 3 \left(\frac{1}{9} \sum_{i \neq j} \langle c_i, \mathbf{w} \rangle^2 \langle c_j, \mathbf{w} \rangle^2 \right)$$

and the final expression becomes

$$mom_{4,\mathbf{C}}(\mathbf{w}) = \frac{1}{5} \sum_{i=1}^n \langle c_i, \mathbf{w} \rangle^4 + \frac{1}{3} \sum_{i \neq j} \langle c_i, \mathbf{w} \rangle^2 \langle c_j, \mathbf{w} \rangle^2$$

Now, since \mathbf{C} is orthonormal, and by restricting \mathbf{w} to the unit sphere in \mathbb{R}^n , we can simplify the expressions further. The second moment becomes $mom_{2,\mathbf{C}}(\mathbf{w}) = \frac{1}{3} \mathbf{w} \mathbf{C}^t \mathbf{C} \mathbf{w}^t = \frac{1}{3} \mathbf{w} \mathbf{I} \mathbf{w}^t = \frac{1}{3} \mathbf{w} \mathbf{w}^t = \frac{1}{3} \|\mathbf{w}\|^2 = \frac{1}{3}$.

By rewriting and expanding the fourth moment:

$$\begin{aligned} mom_{4,\mathbf{C}}(\mathbf{w}) &= \frac{1}{5} \sum_{i=1}^n \langle c_i, \mathbf{w} \rangle^4 + \frac{1}{3} \sum_{i \neq j} \langle c_i, \mathbf{w} \rangle^2 \langle c_j, \mathbf{w} \rangle^2 \\ mom_{4,\mathbf{C}}(\mathbf{w}) &= \frac{1}{5} \sum_{i=1}^n \langle c_i, \mathbf{w} \rangle^4 + \frac{1}{3} \sum_{i=1}^n \sum_{j=1}^n \langle c_i, \mathbf{w} \rangle^2 \langle c_j, \mathbf{w} \rangle^2 - \frac{1}{3} \sum_{i=1}^n \langle c_i, \mathbf{w} \rangle^2 \langle c_i, \mathbf{w} \rangle^2 \\ mom_{4,\mathbf{C}}(\mathbf{w}) &= \frac{1}{5} \sum_{i=1}^n \langle c_i, \mathbf{w} \rangle^4 + \frac{1}{3} \sum_{i=1}^n \sum_{j=1}^n \langle c_i, \mathbf{w} \rangle^2 \langle c_j, \mathbf{w} \rangle^2 - \frac{1}{3} \sum_{i=1}^n \langle c_i, \mathbf{w} \rangle^4 \\ mom_{4,\mathbf{C}}(\mathbf{w}) &= \frac{1}{3} \|\mathbf{w}\|^4 - \frac{2}{15} \sum_{i=1}^n \langle c_i, \mathbf{w} \rangle^4 = \frac{1}{3} - \frac{2}{15} \sum_{i=1}^n \langle c_i, \mathbf{w} \rangle^4 \end{aligned}$$

We also need to compute the gradient of the fourth moment, $\nabla mom_{4,\mathbf{C}}(\mathbf{w})$.

- The gradient of the first term, $\frac{1}{3}\|\mathbf{w}\|^4$, is computed as follows:
We rewrite $\|\mathbf{w}\|^4$ as $(\mathbf{w}\mathbf{w}^t)^2$. Using the chain rule we have that
 $\nabla((\mathbf{w}\mathbf{w}^t)^2) = 2(\mathbf{w}\mathbf{w}^t) \cdot \frac{\partial}{\partial \mathbf{w}_j}(\mathbf{w}\mathbf{w}^t) = 2(\mathbf{w}\mathbf{w}^t) \cdot 2\mathbf{w}$.
The gradient of the first term is then $\frac{1}{3} \cdot 2(\mathbf{w}\mathbf{w}^t) \cdot 2\mathbf{w} = \frac{4}{3}\|\mathbf{w}\|^2\mathbf{w}$.
- For the second term, $\frac{2}{15}\sum_{i=1}^n \langle c_i, \mathbf{w} \rangle^4$ we have the following:

$$\nabla \sum_{i=1}^n \langle c_i, \mathbf{w} \rangle^4 = \sum_{i=1}^n \nabla (\langle c_i, \mathbf{w} \rangle^4)$$

Looking at just the inner term, $\nabla(\langle c_i, \mathbf{w} \rangle^4) = 4\langle c_i, \mathbf{w} \rangle^3 \cdot \frac{\partial}{\partial w_j}(\langle c_i, \mathbf{w} \rangle) = 4\langle c_i, \mathbf{w} \rangle^3 \cdot c_i$

The gradient of the second term is therefore $\frac{8}{15} \sum_{i=1}^n \langle c_i, \mathbf{w} \rangle^3 c_i$

Putting together the terms we get

$$\nabla mom_{4,\mathbf{C}}(\mathbf{w}) = \frac{4}{3}\|\mathbf{w}\|^2\mathbf{w} - \frac{8}{15} \sum_{i=1}^n \langle c_i, \mathbf{w} \rangle^3 c_i$$

The key observation is that by minimizing $mom_{4,\mathbf{C}}(\mathbf{w})$ one has to maximize the term $-\frac{2}{15} \sum_{i=1}^n \langle c_i, \mathbf{w} \rangle^4$. Since c_i and \mathbf{w} are both on the unit circle, and all c_i are orthogonal to each other, the term is maximized whenever $\mathbf{w} = c_i$ since $\langle c_i, \pm c_i \rangle = \langle \mathbf{w}, \pm \mathbf{w} \rangle = 1$. Using this observation, we can run a gradient descent to minimize $mom_{4,\mathbf{C}}(\mathbf{w})$ and find rows of $\pm \mathbf{C}$. A simple gradient descent is described in the following algorithm:

Algorithm 7 Gradient descent

Require: Parameter δ , samples \mathbf{c}

- 1: Choose random vector \mathbf{w} on the unit sphere
 - 2: Compute an approximation $\mathbf{g} \leftarrow \nabla mom_{4,\mathbf{C}}(\mathbf{w})$
 - 3: Set $\mathbf{w}_{new} \leftarrow \mathbf{w} - \delta \mathbf{g}$
 - 4: Normalize \mathbf{w}_{new} as $\frac{\mathbf{w}_{new}}{\|\mathbf{w}_{new}\|}$
 - 5: Approximate $mom_{4,\mathbf{C}}(\mathbf{w})$ and $mom_{4,\mathbf{C}}(\mathbf{w}_{new})$
 - 6: **if** $mom_{4,\mathbf{C}}(\mathbf{w}) \geq mom_{4,\mathbf{C}}(\mathbf{w}_{new})$ **then**
 - 7: Return \mathbf{w}
 - 8: **else**
 - 9: Set $\mathbf{w} \leftarrow \mathbf{w}_{new}$ and go to step 2
-

This procedure is repeated until all rows of $\pm \mathbf{C}$ is found. Each row is transformed by \mathbf{L}^{-1} to get the row in $\pm \mathbf{V}$.

3.4 HPP against the Normal Distribution

Assume now that the signatures on the form $\mathbf{v} = \mathbf{xV}$ where $x_i \sim \mathcal{N}(0, \sigma^2)$. After converting $\mathcal{P}(\mathbf{V})$ to $\mathcal{P}(\mathbf{C})$, the fourth moment of $\mathcal{P}(\mathbf{C})$ is constant over \mathbf{w} on the unit circle. To show this, we simply do the same calculations as in the previous section, with the difference that x follows a normal distribution. Considering

$$mom_{4,\mathbf{C}}(\mathbf{w}) = \mathbb{E}\left[\left(\sum_{i=1}^n x_i \langle c_i, \mathbf{w} \rangle\right)^4\right] = \mathbb{E}\left[\sum_i^n \sum_j^n \sum_k^n \sum_l^n x_i x_j x_k x_l \langle c_i, \mathbf{w} \rangle \langle c_j, \mathbf{w} \rangle \langle c_k, \mathbf{w} \rangle \langle c_l, \mathbf{w} \rangle\right]$$

for the three different cases:

- **All equal:** If $i = j = k = l$, we simply have $\sum_i^n \mathbb{E}[x_i^4] \langle c_i, \mathbf{w} \rangle^4 = 3\sigma^4 \sum_i \langle c_i, \mathbf{w} \rangle^4$ due to the well known fact that $\mathbb{E}[x^4] = 3\sigma^4$ for x distributed according to $\mathcal{N}(0, \sigma^2)$.
- **None equal:** Since $\mathbb{E}[x] = 0$ as in the case of the uniform distribution, this results in zero.
- **Pairwise equal:** If either

- $i = j \neq k = l$
- $i = k \neq j = l$
- $i = l \neq j = k$

we have $\sum_{i \neq j} \mathbb{E}[x_i^2 x_j^2] \langle c_i, \mathbf{w} \rangle^2 \langle c_j, \mathbf{w} \rangle^2 = \sigma^4 \sum_{i \neq j} \langle c_i, \mathbf{w} \rangle^2 \langle c_j, \mathbf{w} \rangle^2$ since $\mathbb{E}[x^2] = \sigma^2$.

Putting together expressions we get

$$mom_{4,\mathbf{C}}(\mathbf{w}) = 3\sigma^4 \sum_i \langle c_i, \mathbf{w} \rangle^4 + 3(\sigma^4 \sum_{i \neq j} \langle c_i, \mathbf{w} \rangle^2 \langle c_j, \mathbf{w} \rangle^2)$$

$$mom_{4,\mathbf{C}}(\mathbf{w}) = 3\sigma^4 \sum_i \langle c_i, \mathbf{w} \rangle^4 + 3\sigma^4 \sum_i \sum_j \langle c_i, \mathbf{w} \rangle^2 \langle c_j, \mathbf{w} \rangle^2 - 3\sigma^4 \sum_i \langle c_i, \mathbf{w} \rangle^4$$

$$mom_{4,\mathbf{C}}(\mathbf{w}) = 3\sigma^4 \sum_i \sum_j \langle c_i, \mathbf{w} \rangle^2 \langle c_j, \mathbf{w} \rangle^2$$

$$mom_{4,\mathbf{C}}(\mathbf{w}) = 3\sigma^4 (\|\mathbf{w}\|^2)^2 = 3\sigma^4$$

Since $mom_{4,\mathbf{C}}(\mathbf{w})$ is constant for \mathbf{w} on the unit sphere regardless of σ^2 , the term no longer depends on the secret matrix \mathbf{C} and the attack will not work.

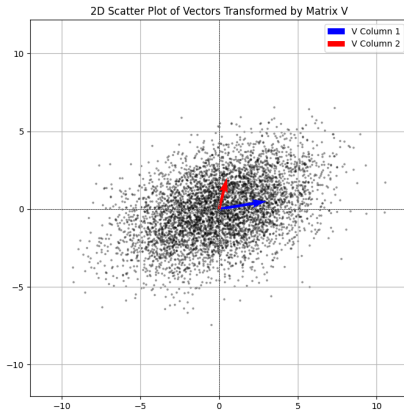


Figure 3.3: Hidden parallelepiped problem in dimension 2 for normal distribution

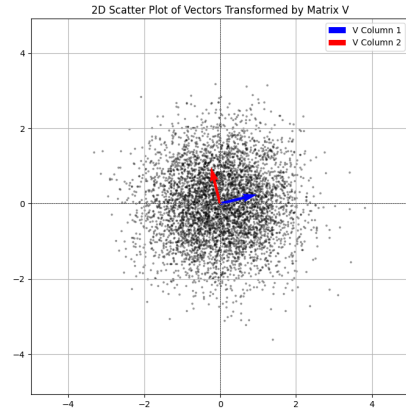


Figure 3.4: Hidden hypercube problem in dimension 2 for normal distribution

Chapter 4

Cryptanalysis of Hawk

4.1 Overview of method

Consider the Discrete Gaussian Distribution as described in [3] and section 3.1.5. We use our implementation of Hawk to sample many points from the practical distribution based on tables. Let $\widehat{\mathcal{D}}$ denote the practical discrete Gaussian distribution from sampled points. Let $\hat{\mu}, \hat{\sigma}^2$ be the expectation and variance of $\widehat{\mathcal{D}}$. Assume we sample t points from $\widehat{\mathcal{D}}$ as $X = \{x_1, x_2, \dots, x_t\}$. We estimate $\hat{\mu}$ and $\hat{\sigma}^2$ simply as $\hat{\mu} = \frac{1}{t} \sum_{i=1}^t x_i$ and $\hat{\sigma}^2 = \frac{1}{t} \sum_{i=1}^t (x_i - \hat{\mu})^2$. For simplicity, we can also assume $\hat{\mu} = 0$ as claimed in [3]. To simplify later computations we also normalize our samples by computing $Z = \{z_1, z_2, \dots, z_t\} = \{\frac{x_1}{\hat{\sigma}}, \frac{x_2}{\hat{\sigma}}, \dots, \frac{x_t}{\hat{\sigma}}\}$ such that $\mathbb{V}[z_i] = 1$. Denote now by $\mu_4 = \mathbb{E}[z_i^4] = \frac{1}{t} \sum_{i=1}^n z_i^4$.

Assume observed signatures on the form $\mathbf{c} = \mathbf{C}\mathbf{z}$ where \mathbf{C} is orthonormal (columns are unit vectors and pairwise orthogonal). Note that in this section we denote by \mathbf{u} a vector on the unit sphere \mathbb{R}^{2n} instead of \mathbf{w} as in the previous section, to avoid confusion with the Hawk notation for $\mathbf{w} = \mathbf{B}^{-1}\mathbf{x}$. Also note that henceforth we will consider $\mathbf{w} = \mathbf{B}^{-1}\mathbf{x}$ as a signature instead of $\mathbf{s} = \frac{1}{2}(\mathbf{h} - \mathbf{w})$ since \mathbf{w} is easily recoverable given \mathbf{s} and message \mathbf{m} . Lastly, we consider \mathbf{B} as $\text{rot}(\mathbf{B})$ in this section.

By rewriting the terms from the original HPP paper [5] for this new, normalized, distribution $\widehat{\mathcal{D}}$, we have that

$$\text{mom}_{4,\mathbf{C}}(\mathbf{u}) = 3\|\mathbf{u}\|^4 + (\mu_4 - 3) \sum_{i=1}^n \langle c_i, \mathbf{u} \rangle^4$$

and

$$\nabla mom_{4,\mathbf{C}}(\mathbf{u}) = 12\|\mathbf{u}\|^2\mathbf{u} + 4(\mu_4 - 3)\sum_{i=1}^n \langle c_i, \mathbf{u} \rangle^3 c_i$$

where \mathbf{u} is a vector on the unit sphere of \mathbb{R}^{2n} , i.e. $\|\mathbf{u}\| = 1$. This means that if the difference $(\mu_4 - 3)$ is significant enough, one might be able to employ the same minimization technique as in the original attack to reveal a column of \mathbf{C} because $\langle c_i, \mathbf{u} \rangle^4 = 1$ if $\mathbf{u} = \pm c_i$ since $\langle c_i, c_i \rangle^4 = 1$. Note that if $(\mu_4 - 3) < 0$ we have the same case as in the original attack, where minimization of the entire term entails maximization of $\sum_{i=1}^n \langle c_i, \mathbf{u} \rangle^4$, which gives us a row of $\pm \mathbf{C}$. If $(\mu_4 - 3) > 0$, we need to maximize the entire term $3\|\mathbf{u}\|^4 + \sum_{i=1}^n \langle c_i, \mathbf{u} \rangle^4$, which is achieved by doing a gradient *ascent* instead of a gradient *descent*.

4.2 Covariance matrix and hypercube transformation

In the original HPP attack one has to estimate the matrix $\mathbf{G} \approx \mathbf{V}^t \mathbf{V}$. For Hawk, the signatures are on the form $\mathbf{w} = \mathbf{B}^{-1} \mathbf{x}$. Then we would need to compute $\mathbf{G} = \mathbf{B}^{-1} \mathbf{B}^{-T}$ (the HPP paper uses row vectors while Hawk use columns vectors). However, the public key $\mathbf{Q} = \mathbf{B}^T \mathbf{B}$, enables us to skip this step. Recall that in the original attack one has to take Cholesky decomposition (or an equivalent decomposition) of the inverse of the covariance matrix such that $\mathbf{G}^{-1} = \mathbf{L} \mathbf{L}^T$. For $\mathbf{G} = \mathbf{B}^{-1} \mathbf{B}^{-T}$, the inverse, $\mathbf{G}^{-1} = \mathbf{B}^T \mathbf{B} = \mathbf{Q}$. Therefore, we can simply take the Cholesky decomposition of \mathbf{Q} to get \mathbf{L} such that $\mathbf{Q} = \mathbf{L} \mathbf{L}^T$. By multiplying our samples \mathbf{w} by \mathbf{L}^T on the left, we have transformed our samples to the hidden hypercube as in the original attack.

By taking $\mathbf{C} = \mathbf{L}^T \mathbf{B}^{-1}$, we have that

$$\mathbf{C}^T \mathbf{C} = (\mathbf{L}^T \mathbf{B}^{-1})^T (\mathbf{L}^T \mathbf{B}^{-1}) = \mathbf{B}^{-T} \mathbf{L} \mathbf{L}^T \mathbf{B}^{-1} = \mathbf{B}^{-T} \mathbf{Q} \mathbf{B}^{-1} = \mathbf{B}^{-T} \mathbf{B}^T \mathbf{B} \mathbf{B}^{-1} = \mathbf{I}_n$$

and

$$\mathbf{C} \mathbf{C}^T = (\mathbf{L}^T \mathbf{B}^{-1}) (\mathbf{L}^T \mathbf{B}^{-1})^T = \mathbf{L}^T \mathbf{B}^{-1} \mathbf{B}^{-T} \mathbf{L} = \mathbf{L}^T \mathbf{Q}^{-1} \mathbf{L} = \mathbf{L}^T (\mathbf{L} \mathbf{L}^T)^{-1} \mathbf{L} = \mathbf{L}^T \mathbf{L}^{-T} \mathbf{L}^{-1} \mathbf{L} = \mathbf{I}_n$$

Thus \mathbf{C} is an orthonormal matrix. Since \mathbf{w} is distributed according to $\widehat{\mathcal{D}}$ over $\mathcal{P}(\mathbf{B}^{-1})$, by taking $\mathbf{c} = \mathbf{L}^T \mathbf{w}$ we have $\mathbf{c} = \mathbf{L}^T \mathbf{B}^{-1} \mathbf{x} = \mathbf{C} \mathbf{x}$, \mathbf{c} is distributed according to $\widehat{\mathcal{D}}$ over $\mathcal{P}(\mathbf{C})$.

We summarize this step of the attack against Hawk in the following algorithm

Algorithm 8 Hawk Hypercube Transformation

Require: Samples $\mathbf{w} = \mathbf{B}^{-1}\mathbf{x}$ and public key \mathbf{Q}

- 1: Compute \mathbf{L} s.t. $\mathbf{Q} = \mathbf{L}\mathbf{L}^T$ ▷ by Cholesky decomposition
 - 2: Compute $\mathbf{c} = \mathbf{L}^T\mathbf{w}$
 - 3: **return** \mathbf{c} and \mathbf{L}^{-T}
-

4.3 Gradient search overview

Now, given samples $\mathbf{c} \in \mathcal{P}(\mathbf{C})$, we run a gradient search to minimize or maximize the fourth moment of one-dimensional projections onto \mathbf{u} , as in the original attack. In addition to multiplying the samples by \mathbf{L}^T , we also divide them by the scalar σ , to normalize the samples so each sample in the vector \mathbf{c} has variance 1. This also aligns with our theoretical analysis of $mom_{4,\mathbf{C}}(\mathbf{u})$. Even though the distribution $\hat{\mathcal{D}}$ is discrete, the shape of the samples $\mathbf{c} \in \mathcal{P}(\mathbf{C})$ will still have a somewhat spherical shape, as illustrated in figures 4.1 and 4.2. The hope is that the areas in the directions of the columns of $\pm\mathbf{C}$ will deviate just enough from a perfect spherical shape to give us a clear global minima/maxima in the gradient landscape.

We evaluate the functions $mom_{4,\mathbf{C}}(\mathbf{u})$ as $\mathbb{E}[\langle \mathbf{c}, \mathbf{u} \rangle^4]$ and $\nabla mom_{4,\mathbf{C}}(\mathbf{u})$ as $\mathbb{E}[\nabla \langle \mathbf{c}, \mathbf{u} \rangle^4] = 4\mathbb{E}[\langle \mathbf{c}, \mathbf{u} \rangle^3 \mathbf{c}]$. These can be evaluated by precomputed samples $\{\mathbf{c}_1, \mathbf{c}_2, \dots, \mathbf{c}_t\}$, or by continuously generating one and one signature sample since we have access to the signature generation algorithm.

Algorithm 9 Gradient descent on $\mathcal{P}(\mathbf{C})$

Require: Samples on the form $\mathbf{c} = \mathbf{C}\mathbf{x}$, descent parameter δ

- 1: $\mathbf{u} \leftarrow$ random vector on unit sphere in \mathbb{R}^{2n}
 - 2: **loop**
 - 3: $\mathbf{g} \leftarrow \nabla mom_{4,\mathbf{C}}(\mathbf{w})$
 - 4: $\mathbf{u}_{new} = \mathbf{u} - \delta \mathbf{g}$
 - 5: normalize \mathbf{u}_{new} as $\frac{\mathbf{u}_{new}}{\|\mathbf{u}_{new}\|}$
 - 6: **if** $mom_{4,\mathbf{C}}(\mathbf{u}_{new}) \geq mom_{4,\mathbf{C}}(\mathbf{u})$ **then**
 - 7: **return** \mathbf{u}
 - 8: **else**
 - 9: $\mathbf{u} \leftarrow \mathbf{u}_{new}$
 - 10: go to step 3
-

This might be redundant, as the method will be described in chapter on HPP

For a gradient *ascent* one can flip the sign and inequality sign on lines 4 and 6, respectively.

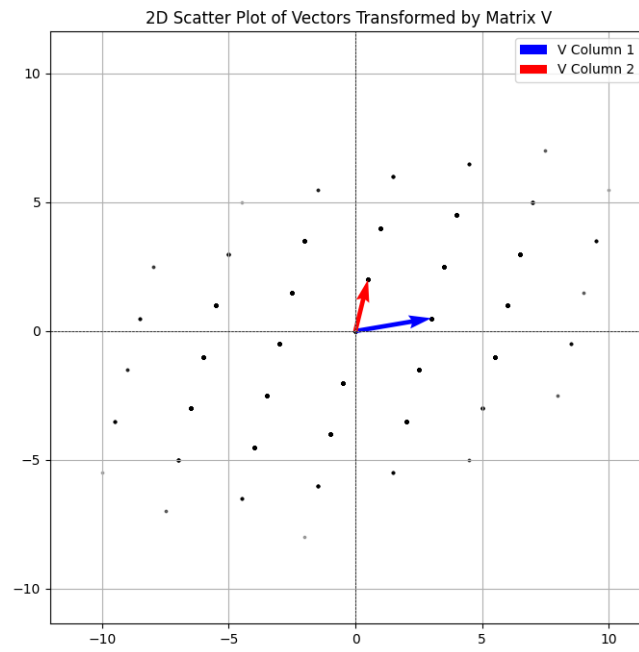


Figure 4.1: Hidden parallelepiped problem in dimension 2 for rounded normal distribution

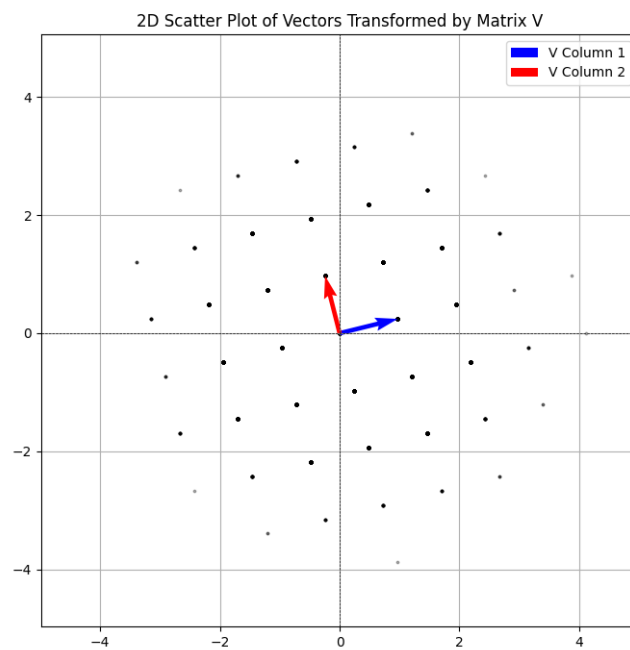


Figure 4.2: Hidden hypercube problem in dimension 2 for rounded normal distribution

4.4 Practical method

Below is a basic description of the approach.

Algorithm 10 Proposed basic version of attack

- 1: Collect signatures $\mathbf{w} = \mathbf{B}^{-1}\mathbf{x}$
 - 2: Using public key \mathbf{Q} , find \mathbf{L} s.t. $\mathbf{Q} = \mathbf{L}\mathbf{L}^T$
 - 3: Transform samples s.t. $\mathbf{c} = \mathbf{L}^T\mathbf{w}$
 - 4: Find columns of $\pm\mathbf{C}$ by doing gradient search over $\mathcal{P}(\mathbf{C})$
 - 5: Multiply columns of $\pm\mathbf{C}$ by \mathbf{L}^{-T} on the left and round the result to get columns in $\pm\mathbf{B}^{-1}$
-

After having transformed the samples $\mathbf{w} \in \mathcal{P}(\mathbf{B}^{-1})$ to $\mathbf{c} \in \mathcal{P}(\mathbf{C})$ we want to recover columns of $\pm\mathbf{C}$ and transform them back to columns of $\pm\mathbf{B}^{-1}$ by multiplying by \mathbf{L}^{-T} on the left. Due to the special structure of Hawk private keys, finding one column of \mathbf{B} automatically gives n columns. Unfortunately, since revealing a single column of \mathbf{B}^{-1} reveals a "shift" of either the two polynomials G and g or F and f , this is not enough to disclose the entire matrix. If samples were on the form $\mathbf{w} = \mathbf{B}\mathbf{x}$, a single column would reveal f and g (or F and G), and one could simply reconstruct F and G (or f and g) by solving the NTRU-equation as in the key generation step of Hawk. Nevertheless, if one finds two columns of \mathbf{B}^{-1} , it is easy to check if they are shifts of each other. If they are not, one has found shifts of all four polynomials in the secret key, and by trying all combinations of shifts, of which there are $4n^2$ (accounting for negative and positive sign), one can easily verify if a candidate \mathbf{B}' is valid by checking if \mathbf{B}' is unimodular and if $\mathbf{B}'^T\mathbf{B}' = \mathbf{Q}$. If so, one is able to forge signatures, and the attack is done.

After each gradient ascent and/or descent returns a possible solution \mathbf{z}' , we multiply it to the left as $\mathbf{b}' = \mathbf{L}^{-T}\mathbf{z}'$ where \mathbf{b}' is a possible column of $\pm\mathbf{B}^{-1}$ as \mathbf{z}' is a possible column of $\pm\mathbf{C} = \mathbf{L}^T \cdot (\pm\mathbf{B}^{-1})$. Since in experiments we have access to the correct secret key, we simply check directly if $\mathbf{b}' \in \pm\mathbf{B}^{-1}$. In a real word attack however, one would, as described above, have to compute candidate \mathbf{B}' and check if $\mathbf{B}'^T\mathbf{B}' = \mathbf{Q}$.

Having access to the correct \mathbf{B}^{-1} we can do measures on how close a proposed solution \mathbf{b}' is to one of the columns of \mathbf{B}^{-1} . We can for example take the difference in length of $|\mathbf{b}'|$ and each vector in $|\mathbf{B}^{-1}|$, i.e. $\text{diff}_{\min} = \min\{||\mathbf{b}'| - |\mathbf{b}_i|| : \mathbf{b}_i \in \pm\mathbf{B}^{-1}\}$. A low value for this (this depends on the Hawk parameter n) would indicate a good guess, whereas a higher value indicates greater difference between the vectors, and thus a bad guess. One can also take the average of the difference of the entries in the vectors, i.e.

$\text{diff}_{\min} = \min\{\frac{1}{2n}|\mathbf{b}' - \mathbf{b}_i| : \mathbf{b}_i \in \pm \mathbf{B}^{-1}\}$. Alternatively, one can count entrywise how many entries out of $2n$ that matches between \mathbf{b}' and \mathbf{b}_i .

A concern about this approach of attacking Hawk is the gradient search, as described in Algorithm 2 and 3. In the original HPP attack, they used a standard gradient descent with a constant stepsize/descent parameter δ . This worked fine for attack on GGH and NTRU when the global minima (of which there are $2n$) of the gradient landscape was very obvious. In the gradient landscape of Hawk however, there is much more noise, and the global minima is not as clear, as it depends on the discrepancy $(\mu_4 - 3)$, which is quite small. Generally, a constant stepsize δ entails a tradeoff between slow convergence and the risk of "overshooting" the correct global extremum. We therefore employ the method of ADAM-optimizer, as described in chapter 2. Below is a description of the gradient search using ADAM-optimizer in our setting.

Algorithm 11 gradient descent ADAM

Require: signatures $\mathbf{c} = \mathbf{C}\mathbf{x}$

Require: Stepsize δ , decay rates β_1, β_2

```

1:  $\mathbf{u} \leftarrow$  random vector on the unit sphere of  $\mathbb{R}^{2n}$ 
2:  $\mathbf{m}_0 \leftarrow \mathbf{0}$  ▷ Vector of 0's
3:  $\mathbf{v}_0 \leftarrow \mathbf{0}$  ▷ Vector of 0's
4:  $t \leftarrow 0$  ▷ Timestep
5: loop
6:    $t \leftarrow t + 1$ 
7:    $\mathbf{g}_t \leftarrow \nabla \text{mom}_{4,\mathbf{C}}(\mathbf{u})$ 
8:    $\mathbf{m}_t \leftarrow \beta_1 \cdot \mathbf{m}_{t-1} + (1 - \beta_1) \cdot \mathbf{g}_t$ 
9:    $\mathbf{v}_t \leftarrow \beta_2 \cdot \mathbf{v}_{t-1} + (1 - \beta_2) \cdot \mathbf{g}_t^2$ 
10:   $\hat{\mathbf{m}}_t \leftarrow \mathbf{m}_t / (1 - \beta_1^t)$ 
11:   $\hat{\mathbf{v}}_t \leftarrow \mathbf{v}_t / (1 - \beta_2^t)$ 
12:   $\mathbf{u}_{new} \leftarrow \mathbf{u} - \delta \cdot \hat{\mathbf{m}}_t / (\sqrt{\hat{\mathbf{v}}_t} + \epsilon)$  ▷ Flip the  $-$  sign for gradient ascent
13:  normalize  $\mathbf{u}_{new}$  as  $\frac{\mathbf{u}_{new}}{\|\mathbf{u}_{new}\|}$ 
14:  if  $\text{mom}_{4,\mathbf{C}}(\mathbf{u}_{new}) \geq \text{mom}_{4,\mathbf{C}}(\mathbf{u})$  then ▷ Flip the  $\geq$  sign for gradient ascent
15:    return  $\mathbf{u}$ 
16:  else
17:     $\mathbf{u} \leftarrow \mathbf{u}_{new}$ 
18:    go to step 6

```

The ϵ in step 12 of the algorithm is inserted to not divide by 0. Proposed value for $\epsilon = 10^{-8}$, and proposed good values for δ, β_1 and β_2 are 0.001, 0.9 and 0.999 respectively. In this method, the stepsize then depends on δ, \mathbf{m}_t and \mathbf{v}_t . Explanation of variables:

- \mathbf{m}_t estimates an average of previous gradients, as to make movement in one iteration partially depend on the direction of previous iterations.

- \mathbf{v}_t estimates the variance of the previous gradients. Larger variance will reduce the stepsize to not overshoot possible extremum, while lower variance will increase the stepsize to speed up convergence.
- $\hat{\mathbf{m}}_t$ and $\hat{\mathbf{v}}_t$ is bias-correction, so that the first iterations are not biased towards 0.

Below is a more detailed version of the entire attack/experiment.

Algorithm 12 Proposed version of attack with measuring

Require: Hawk parameter n , number of samples t , Hawk key pair \mathbf{B}, \mathbf{Q}

- 1: Collect t signatures $\mathbf{w} = \mathbf{B}^{-1}\mathbf{x}$ ▷ Optional - can also generate signatures continuously
 - 2: Using public key \mathbf{Q} , compute \mathbf{L} s.t. $\mathbf{Q} = \mathbf{L}\mathbf{L}^t$
 - 3: Transform samples s.t. $\mathbf{c} = \mathbf{L}^t\mathbf{w}$
 - 4: **loop**
 - 5: Candidate $\mathbf{z}' \leftarrow$ gradient search ADAM ▷ Do both ascent and descent
 - 6: Candidate $\mathbf{b}' \leftarrow \lfloor \mathbf{L}^{-T}\mathbf{z}' \rfloor$ ▷ Entrywise rounding to nearest integer
 - 7: Check if $\mathbf{b}' \in \mathbf{B}^{-1}$
 - 8: Measure $\text{diff}_{\min}(\mathbf{b}', \mathbf{B}^{-1})$
-

This should be in the theoretical background

The loop from line 4 can be run several times to get a new random starting point \mathbf{u} for the gradient search. Line 6 rounds the candidate *after* multiplying with \mathbf{L}^{-T} to avoid rounding errors. Line 8 can also give which column of \mathbf{B}^{-1} \mathbf{b}' is closest to, so one can compare the vectors side by side.

4.5 Results

The method has unfortunately not proven to work, as no correct key has been found in any of the runs. It seems that regardless of number of signatures (above a certain point, e.g. one million), the method cannot give candidate solutions with better comparison than random guessing. Random guessing in this case is assuming one knows what type of distribution the columns of a secret key is. One knows the distribution that f, g follows, but F and G depends on f and g .

For reference, I ran a test using the closeness measure $\text{diff}_{\min} = \min\{|||\mathbf{b}'| - |\mathbf{b}_i||| : \mathbf{b}_i \in \pm\mathbf{B}^{-1}\}$ by fixing one private key (\mathbf{B}^{-1}), and generating random keys \mathbf{B}'^{-1} (which will serve as random guesses), to check if the attack on average gives better results than random guessing. Table 1 shows the result of comparing a key with 100 random keys,

and the result of 100 random starting points for the gradient search (both ascent and descent).

One thing to note is that Hawk does not specify parameters (such as width σ of $\hat{\mathcal{D}}$) for lower values of n than 256. Therefore, when sampling signatures for $n = 32, 64$ and 128, I use the same tables, i.e. same σ for $\hat{\mathcal{D}}$, as in Hawk 256.

Table 4.1: Closeness measure for Hawk attack

Type	diff _{min}	diff _{max}	Avg diff _{min}	Avg diff _{max}
Key comparison degree 32	6.25	15.81	7.74	11.22
Attack on Hawk 32 (1m samples)	7.14	16.24	8.50	12.87
Key comparison degree 64	10.77	26.51	13.96	22.18
Attack on Hawk 64 (1m samples)	13.49	26.00	16.25	22.59
Key comparison degree 128	25.33	47.26	30.00	41.60
Attack on Hawk 128(1m samples)	24.27	46.91	29.61	46.91
Key comparison degree 256	56.33	82.34	61.02	75.02
Attack on Hawk 256 (1m samples)	something	something		
Attack on Hawk 256 (10m samples)	57.72	77.54	62.37	77.54

Lastly, I include values from sampling points from $\hat{\mathcal{D}}$ for Hawk 256. 100 million vectors \mathbf{x} were sampled, resulting in $2 \cdot 256 \cdot 100$ million independently sampled points from $\hat{\mathcal{D}}$. First, I compute σ^2 and σ , then compute μ_4 of normalized samples on the form $z = \frac{x}{\sigma}$. We then get that

- $\sigma^2 = 4.080429335$
- $\sigma = 2.020007261$
- Normalized $\mu_4 = \mathbb{E}(z^4) = 3.000007624$
- $(\mu_4 - 3) = 0.000007624$

4.6 Conclusion

In conclusion, I think the reason the method has not worked is because of the small value of $(\mu_4 - 3)$, but importantly also because of the noisy nature of the distribution $\hat{\mathcal{D}}$. The noise introduces too many "false" local minima/maxima in the gradient landscape such that it is difficult to find the correct *global* minima/maxima. I do not claim that it is impossible, but my experiments show that it seems infeasible for this particular approach.

Chapter 5

Results

Chapter 6

Discussion

Acronyms

CVP Closest Vector Problem.

DSA Digital Signature Algorithm.

HPP Hidden Parallelepiped Problem.

KEMs Key Encapsulation Methods.

NIST National Institute of Standards and Technology.

RSA Rivest, Shamir, Adleman.

Bibliography

- [1] Léo Ducas and Phong Q. Nguyen. Learning a zonotope and more: cryptanalysis of ntrusign countermeasures. In *Proceedings of the 18th International Conference on The Theory and Application of Cryptology and Information Security, ASIACRYPT'12*, page 433–450, Berlin, Heidelberg, 2012. Springer-Verlag. ISBN 9783642349607. doi: 10.1007/978-3-642-34961-4_27.
URL: https://doi.org/10.1007/978-3-642-34961-4_27.
- [2] Jill Pipher Joseph H. Silverman-William Whyte Jeffrey Hoffstein, Nick Howgrave-Graham. Ntrusign: Digital signatures using the ntru lattice. Technical report, NTRU Cryptosystems, 2003.
- [3] Léo Ducas Serge Fehr Yu-Hsuan Huang Thomas Pornin Eamonn W. Postlethwaite Thomas Prest Ludo N. Pulles Joppe W. Bos, Olivier Bronchain and Wessel van Woerden. Hawk. Technical report, NXP Semiconductors, Centrum Wiskunde & Informatica, Mathematical Institute at Leiden University, NCC Group, PQShield, Institut de Mathématiques de Bordeaux, September 2024.
URL: <https://hawk-sign.info/>.
- [4] Jonathan Katz and Yehuda Lindell. *Introduction to modern cryptography*. CRC Press, Boca Raton, FL, 3 edition, 2020.
- [5] Phong Q. Nguyen and Oded Regev. Learning a parallelepiped: Cryptanalysis of ggh and ntru signatures, 2009.
- [6] Thomas Pornin and Thomas Prest. More efficient algorithms for the NTRU key generation using the field norm. Cryptology ePrint Archive, Paper 2019/015, 2019.
URL: <https://eprint.iacr.org/2019/015>.
- [7] Sebastian Ruder. An overview of gradient descent optimization algorithms, 2017.
URL: <https://arxiv.org/abs/1609.04747>.

Appendix A

Generated code from Protocol buffers

Listing A.1: Source code of something

```
1 System.out.println("Hello Mars");
```