



Universiteit  
Leiden  
The Netherlands

## Lattice cryptography: from cryptanalysis to New Foundations

Woerden, W.P.J. van

### Citation

Woerden, W. P. J. van. (2023, February 23). *Lattice cryptography: from cryptanalysis to New Foundations*. Retrieved from <https://hdl.handle.net/1887/3564770>

Version: Publisher's Version

License: [Licence agreement concerning inclusion of doctoral thesis in the Institutional Repository of the University of Leiden](#)

Downloaded from: <https://hdl.handle.net/1887/3564770>

**Note:** To cite this publication please use the final published version (if applicable).

**Lattice Cryptography,  
from Cryptanalysis to New Foundations**

Proefschrift

ter verkrijging van  
de graad van doctor aan de Universiteit Leiden,  
op gezag van rector magnificus prof.dr.ir. H. Bijl,  
volgens besluit van het college voor promoties  
te verdedigen op donderdag 23 februari 2022  
klokke 13.45 uur

door

**Wessel Pieter Jacobus van Woerden**

geboren te Rijnwoude, Nederland,

in 1995

**Promotores:**

Prof.dr. L. Ducas (CWI Amsterdam & Universiteit Leiden)

Prof.dr. R.J.F. Cramer (CWI Amsterdam & Universiteit Leiden)

**Promotiecommissie:**

Prof.dr. H.J. Hupkes

Dr. T.C. Streng

Prof.dr. C. Bachoc (Université de Bordeaux)

Dr. N. Stephens-Davidowitz (Cornell University)

Prof.dr. P.Q. Nguyen (Inria Paris &  
École Normale Supérieure, Paris)

The research was carried out in the Cryptology Group at CWI Amsterdam.  
The PhD position was funded by the ERC Advanced Grant 740972  
(ALGSTRONGCRYPTO).



Wessel van Woerden

**Lattice Cryptography**  
**from Cryptanalysis to New Foundations**

To my family and friends.

# Contents

|  |           |
|--|-----------|
| <b>Contents</b>                              | <b>v</b>  |
| <b>I Introduction and Preliminaries</b>      | <b>1</b>  |
| <b>1 Introduction</b>                        | <b>3</b>  |
| <b>2 Preliminaries</b>                       | <b>21</b> |
| 2.1 Notation . . . . .                       | 21        |
| 2.2 Lattices and their properties . . . . .  | 22        |
| 2.3 Lattice problems . . . . .               | 28        |
| 2.4 Projecting . . . . .                     | 30        |
| 2.5 Volumes & distributions . . . . .        | 40        |
| 2.6 Heuristics . . . . .                     | 45        |
| 2.7 Cryptography . . . . .                   | 49        |
| <b>II Short and Close Lattice Vectors</b>    | <b>59</b> |
| <b>3 Theory of Lattice Sieving</b>           | <b>61</b> |
| 3.1 Introduction . . . . .                   | 61        |
| 3.2 Heuristic lattice sieving . . . . .      | 63        |
| 3.3 Bucketing and sieving variants . . . . . | 70        |
| 3.4 Advanced lattice sieving . . . . .       | 76        |
| 3.5 The General Sieve Kernel . . . . .       | 79        |

|          |  |            |
|----------|--|------------|
| <b>4</b> | <b>Advanced Lattice Sieving on GPUs, with Tensor Cores</b> | <b>85</b>  |
| 4.1      | Introduction . . . . .                                     | 85         |
| 4.2      | GPU architecture and sieve design . . . . .                | 90         |
| 4.3      | Bucketing . . . . .  | 97         |
| 4.4      | Reducing . . . . .   | 105        |
| 4.5      | A dual hash for BDD . . . . .                              | 113        |
| 4.6      | New records . . . . .                                      | 126        |
| <b>5</b> | <b>The Closest Vector Problem with Preprocessing</b>       | <b>133</b> |
| 5.1      | Introduction . . . . .                                     | 133        |
| 5.2      | The randomized iterative slicer . . . . .                  | 139        |
| 5.3      | The random walk model . . . . .                            | 142        |
| 5.4      | Numerical approximations . . . . .                         | 146        |
| 5.5      | An exact solution . . . . .                                | 150        |
|          | <b>III Basis Reduction</b>                                 | <b>157</b> |
| <b>6</b> | <b>Background on Basis Reduction</b>                       | <b>159</b> |
| 6.1      | Introduction . . . . .                                     | 159        |
| 6.2      | HKZ reduction . . . . .                                    | 162        |
| 6.3      | The LLL algorithm . . . . .                                | 163        |
| 6.4      | BKZ reduction . . . . .                                    | 170        |
| 6.5      | Behaviour of reduction algorithms . . . . .                | 173        |
| <b>7</b> | <b>Overstretched NTRU</b>                                  | <b>179</b> |
| 7.1      | Introduction . . . . .                                     | 179        |
| 7.2      | The NTRU lattice and estimates . . . . .                   | 186        |
| 7.3      | A new dense sublattice discovery estimate . . . . .        | 194        |
| 7.4      | A concrete average-case analysis . . . . .                 | 201        |
| 7.5      | Experimental validation . . . . .                          | 210        |
| <b>8</b> | <b>Basis Reduction for Binary Codes</b>                    | <b>217</b> |
| 8.1      | Introduction . . . . .                                     | 217        |
| 8.2      | Binary linear codes . . . . .                              | 221        |
| 8.3      | Orthopodality and the epipodal matrix . . . . .            | 224        |
| 8.4      | Size-reduction and its fundamental domain . . . . .        | 228        |
| 8.5      | LLL for binary codes . . . . .                             | 238        |

---

|           |  |            |
|-----------|--|------------|
| 8.6       | Perspectives . . . . .   | 246        |
| <b>IV</b> | <b>The Lattice Isomorphism Problem, Remarkable Lattices and Cryptography</b> | <b>251</b> |
| <b>9</b>  | <b>The Lattice Isomorphism Problem</b>                                       | <b>253</b> |
| 9.1       | Introduction . . . . .   | 253        |
| 9.2       | LIP & quadratic forms . . . . .  | 255        |
| 9.3       | Invariants . . . . .   | 260        |
| 9.4       | Characteristic sets . . . . .  | 264        |
| 9.5       | Solving LIP . . . . .  | 268        |
| 9.6       | A canonical function . . . . .   | 272        |
| 9.7       | Applications to perfect form enumeration . . . . .                           | 276        |
| <b>10</b> | <b>Remarkable Lattices &amp; Cryptography</b>                                | <b>283</b> |
| 10.1      | Introduction . . . . .   | 283        |
| 10.2      | LIP and self-reducibility . . . . .  | 290        |
| 10.3      | Zero Knowledge Proof of Knowledge . . . . .                                  | 299        |
| 10.4      | Key Encapsulation Mechanism . . . . .  | 303        |
| 10.5      | Signature scheme . . . . .   | 307        |
| 10.6      | Cryptanalysis . . . . .  | 311        |
| 10.7      | Instantiating from remarkable lattices . . . . .                             | 316        |
| 10.8      | HAWK: fast, compact and simple . . . . .                                     | 319        |
|           | <b>Bibliography</b>  | <b>323</b> |
|           | <b>Samenvatting</b>  | <b>347</b> |
|           | <b>Summary</b>   | <b>349</b> |
|           | <b>Acknowledgments</b>   | <b>351</b> |
|           | <b>Curriculum Vitae</b>  | <b>353</b> |
|           | <b>List of Publications</b>  | <b>355</b> |