Lattice cryptography: from cryptanalysis to New Foundations

Woerden, W.P.J. van

Acknowledgments

I would like to thank my advisors, Prof.dr. Léo Ducas and Prof.dr. Ronald Cramer for their supervision.

Léo, my promotor and main advisor, has always shown an unwavering support and enthusiasm for my research and has happily shared his knowledge and insights with me. He always has a unique, often geometric, and intuitive view on lattices and related topics, and I am grateful that he has taught me these ways. After my Bachelor, Master and now PhD thesis under his advice, I can only conclude that we made a great team.

Ronald, my second promotor and group leader, is gratefully acknowledged for his wisdom and great stories. I am grateful for the opportunities he gave me, both directly, but also indirectly, by bringing together such a great group of people.

I am also very grateful to the members of the Doctorate Committee for reading my thesis and for providing feedback.

Additionally, I would like to thank my colleagues from the Cryptology Group at CWI, and other colleagues at CWI, Leiden University, and abroad, for providing me with a friendly, motivating and always curious environment.

To my family and friends, thank you all for your unwavering love, interest and support, for all the light and deep conversations and lessons that shaped me, for allowing me to unwind my mind, and for making me feel at home regardless of the location.

Special thanks go to the many friends and colleagues that helped with proofreading parts of this thesis, and my sisters Marjolein and Sanne for their help with the cover design.

Curriculum Vitae

Wessel van Woerden was born in Koudekerk aan den Rijn, Rijnwoude, the Netherlands, on March 8, 1995. He also grew up there, and obtained his high school diploma from Groene Hart Lyceum in Alphen aan den Rijn in 2013. That year he also graduated from the Pre-University College of Universiteit Leiden. After this he continued his studies at Universiteit Leiden. In 2016, he obtained his bachelor degrees *summa cum laude* in both Mathematics and Computer Science. In 2018 he obtained his master's degree *summa cum laude* in Mathematics. His interest in lattices started with his bachelor thesis "The closest vector problem in cyclotomic lattices" and continued with his master thesis "Perfect quadratic forms: an upper bound and challenges in enumeration", both written under the supervision of Prof.dr. Léo Ducas.

In 2018, Wessel obtained a PhD position at the Universiteit Leiden under supervision of Prof.dr. Léo Ducas and Prof.dr. Ronald Cramer, to do research in the Cryptology Group at Centrum Wiskunde & Informatica (CWI) in Amsterdam. Here he combined his interest in lattices and algorithms with the topic of cryptology. His main focus was on cryptanalysis of lattice-based schemes, ranging from asymptotic to concrete hardness estimates in theory, and record computations in practice. These cryptanalytic results, and a remaining interest in lattice packings and isomorphisms from his master thesis, also motivated constructive work, eventually leading in a joint effort to the signature scheme HAWK.

In 2022, he started as a post-doc in the Number Theory group at Institut de Mathématiques de Bordeaux.

List of Publications

This thesis is based on the following published papers.

[DLW20] **The randomized slicer for CVPP: sharper, faster, smaller, batchier**
Léo Ducas, Thijs Laarhoven, and Wessel van Woerden,
PKC, 23rd Annual International Conference, 2020.

[SHVW20] **A canonical form for positive definite matrices**
Mathieu Dutour Sikirić, Anna Haensch, John Voight, and Wessel van Woerden,
ANTS XIV, 2020.

[DSW21] **Advanced Lattice Sieving on GPUs, with Tensor Cores**
Léo Ducas, Marc Stevens, and Wessel van Woerden,
Eurocrypt, 40th Annual International Conference, 2021.

[DW21] **NTRU Fatigue: How Stretched is Overstretched?**
Léo Ducas and Wessel van Woerden,
Asiacrypt, 27th Annual International Conference, 2021.

[DW22] **On the Lattice Isomorphism Problem, Quadratic Forms, Remarkable Lattices, and Cryptography**
Léo Ducas and Wessel van Woerden,
Eurocrypt, 41st Annual International Conference, 2022.

[DDW22] **An Algorithmic Reduction Theory for Binary Codes: LLL and more**
Thomas Debris-Alazard, Leo Ducas, and Wessel van Woerden,
IEEE Transactions on Information Theory, 2022.

The following published paper is briefly summarised in this thesis.

[DPPvW22] **Hawk: Module LIP makes Lattice Signatures Fast, Compact and Simple**
Léo Ducas, Eamonn W. Postlethwaite, Ludo N. Pulles, and Wessel van Woerden,
Asiacrypt, 28th Annual International Conference, 2022.

The author has additionally published the following papers, which are not included in the thesis.

[DW18] **The closest vector problem in tensored root lattices of type A and in their duals**
Léo Ducas and Wessel van Woerden,
Designs, Codes and Cryptography, 2018.

[Woe20] **An upper bound on the number of perfect quadratic forms**
Wessel van Woerden,
Advances in Mathematics, 2020.