Lattice cryptography: isomorphisms & dual attacks

Pulles, L.N.

Acknowledgments

I would first like to thank my promotors, ***Prof.dr. Léo Ducas*** and ***Prof.dr. Ronald Cramer*** for their supervision during my PhD.

Léo, my first promotor and main advisor, introduced me to lattices with great enthusiasm. His focus on geometric intuition and the right formalism were valuable and inspirational to me. His push in the right direction, or pull from the wrong 'rabbit holes' were helpful in becoming a better researcher.

Ronald, my second promotor and group leader, is gratefully acknowledged for the opportunities that he provided directly and indirectly by bringing together such a wonderful group of people.

I am grateful to Prof.dr. ***Cong Ling***, Prof.dr. ***Phong Nguyen*** and dr. ***Thomas Debris***, members of my Doctorate Committee, for reading my thesis and providing feedback.

Moreover, I would like to thank all my co-authors: ***Wessel***, mijn academische grote broer, voor de fijne carpoolritjes vanuit Leiden en voor het uitstippelen van mijn academische pad; ***Eamonn*** for your humour and passionate story-telling, for enlightening me about LaTeX pedantry and the English language, and for your genuine interest in my well-being; ***Joppe***, ***Olivier***, ***Serge***, ***Yu-Hsuan***, ***Thomas Pornin*** and ***Thomas Prest*** for helping Hawk fly; ***Mehdi*** for the great remote collaboration; ***Damien***, for hosting me twice at CryptoLab in Lyon; ***Daan van G.*** voor het laten zien dat artikelen kort kunnen zijn; ***Marc*** voor alle programmeer tips en tricks; ***Paul*** for doing an internship with me; ***Alexander K.***, ***Elena***, ***Fernando*** and ***Julian*** for joining forces and helping with computations.

Paranymph, academic twin and fellow duckling ***Shane*** was the ideal office mate. It was a joy to jointly chair the activity committee. Your compassion and patience are admirable, and your advice in various

personal matters was valuable. I hope your ears did not go numb from hearing all my random fun facts.

Paranimf en grote speler ***Jelle***, ik dank je voor de vele lange avonden in Kafé België, waarin je zeer gepassioneerd praatte over de meest onnozele onderwerpen. De roadtrips door Tunesië en met ***Yaïr*** door Roemenië, langs holbewoners en beren, respectievelijk, waren origineel en onvergetelijk.

Thanks to all the crypto group members and colleagues at CWI, for making it such a warm and vibrant research environment. I got off to a flying start at CWI by joining the amazing trip to Pampus for CWI's 75 year anniversary in my second week, and joining the activity committee that same day. I am grateful to my fellow hardworking committee members ***Isa***, ***Ruben***, ***Hema***, ***Arjan***, ***Vlad***, ***Sanne***, ***Sebas***, ***Max***, ***Nikhil***, ***Shane***, ***Lynn***, ***Ila***, ***Henrik***, ***Randy***, ***Jelena***, ***Emil***, ***Savvina***, ***Irene***, ***Estéban***, ***Alexander B.***, for organising together so many events, such as workshops on making soap or solving Rubik's cubes, a trip to Texel, movie nights and tournaments. It is great to see the Monday tea tasting sessions being continued up to this day. Thanks to ***Simona*** and ***Maxime*** for smoothly running our group seminar. ***Aron*** and ***Eamonn***, we had some great evenings at het concertgebouw, and many *encores*. ***Sophie***, wat een goed idee om met collega's de Amstel Gold Race (AGR) te fietsen. Daarnaast gaat mijn dank uit naar alle vaste krachten: ***Emil*** (voor het tot leven brengen van de tot dood verklaarde server), ***Dick*** (voor het soepeltjes regelen van contracten, en deelnames aan AGR of BAPC), ***Irene***, ***Minnie***, ***Susanne***, ***Joan-Anne*** en ***Pascal***. I enjoyed playing foosball with ***Arjan***, ***Daan P.***, ***Davi***, ***Dyon***, ***Fran***, ***Isa***, ***Léo C.***, ***Lisa***, ***Llorenç***, ***Lorenzo***, ***Lynn***, ***Marten***, ***Max***, ***Nikhil***, ***Randy***, ***Ruben***, ***Sebas***, ***Sebastiaan***, ***Shane***, ***Simona***, ***Yanlin***, ***Yaroslav***, and more, to lower strain on the brain.

To all my ICPC friends, ***Pim***, ***Reinier***, ***Jorke***, ***Wouter*** and ***Yu-Hsuan***, it was a joy coding with you. Mijn waardering gaat uit naar ***Marcel*** voor de productieve CodeCup weekenden met culinaire meesterwerken, en ik dank ***Kim*** dat ik als begeleiding mee mocht naar de onvergetelijke IOI in Szeged. Bedankt oud-huisgenoten ***Edzard*** en ***Jelte*** voor de fietsrondjes, en ***Bas*** voor de potjes *Age of Empires II*.

Tot slot wil ik mijn vrienden, familie en vriendin bedanken voor al hun steun en toeverlaat tijdens mijn promotietraject. ***Puck***, dank je wel voor alle gekkigheid en vrolijkheid, zelfs als het druk werd, de afgelopen 3 jaar. Hiermee is het proefschrift compleet. Op naar Bordeaux!

Curriculum Vitæ

Ludo Niels Pulles was born in Wageningen (Gelderland) on 13 March 1997, and raised in Gennep (Limburg). He obtained his high school diploma from Stedelijk Gymnasium Nijmegen in 2015.

Subsequently, he went studying at Utrecht University, and obtained bachelor's degrees in computer science, mathematics and physics in 2018, after having written an honours bachelor thesis titled 'A theoretic background on Pollard's Rho algorithm.' After an interlude of studying in Stockholm for half a year, he continued to study mathematics at Universiteit Leiden, and obtained his master's degree in 2021. His master thesis 'Finite separable rings' was supervised by Prof.dr. H.W. Lenstra Jr.

In 2021, Ludo became a PhD candidate in the Cryptology Group at Centrum Wiskunde & Informatica (CWI) in Amsterdam, and was supervised by Prof.dr. Léo Ducas. Here, he was able to apply his knowledge in mathematics and algorithms to topics in cryptology. His main focus was the cryptanalysis of lattice-based schemes, including determining the concrete hardness of attacks on them. He is involved in the design of the signature scheme Hawk, which is part of NIST's standardisation process of additional digital signatures.

After his PhD, Ludo has moved to Bordeaux, where he is working as a postdoctoral researcher at Université de Bordeaux, with dr. Alice Pellet–Mary.