Universiteit Leiden
The Netherlands

Random walks on Arakelov class groups
Boer, K. de

Citation
Boer, K. de. (2022, September 22). *Random walks on Arakelov class groups*. Retrieved from https://hdl.handle.net/1887/3463719

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/1887/3463719

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

Random Walks on Arakelov Class Groups

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 22 september 2022
klokke 11.15 uur

door

Koen de Boer
geboren te Nijmegen, Nederland,
in 1991

Promotores:

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

Co-promotor:

Dr. B. Wesolowski	(Université de Bordeaux)

Promotiecommissie:

Prof. dr. F.A.J. de Haas	(Universiteit Leiden)
Dr. E. Kirshanova	(Technology Innovation Institute, Abu Dhabi & Immanuel Kant Baltic Federal University, Kaliningrad)
Prof. dr. R.M. van Luijk	(Universiteit Leiden)
Prof. dr. R. Schoof	(Università di Roma “Tor Vergata”)
Prof. dr. D. Stehlé	(École Normale Supérieure de Lyon)

The research was carried out in the Cryptology Group at CWI Amsterdam. The PhD position was funded by the ERC Advanced Grant 740972 (ALGSTRONGCRYPTO) and by the European Union Horizon 2020 Research and Innovation Program Grant 780701 (PROMETHEUS).

Koen de Boer

Random Walks on Arakelov Class Groups

and Their Applications in Cryptography and Algorithmic Number Theory

To my family.

Contents

List of Figures