Lattice cryptography: from cryptanalysis to New Foundations

Woerden, W.P.J. van

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).

CWI
Centrum Wiskunde & Informatica

Universiteit Leiden

Wessel van Woerden

Lattice Cryptography

from Cryptanalysis to New Foundations

To my family and friends.

Contents