Compressed Σ-protocol theory

Attema, T.

Compressed Σ-Protocol Theory

Thomas Attema

This research has been supported by the Netherlands Organisation for Applied Scientific Research (TNO) and carried out at the Cryptology Group of Centrum Wiskunde & Informatica (CWI).

ISBN: 978-94-6469-236-5
Printed by: ProefschriftMaken || www.proefschriftmaken.nl
Cover design by: Univorm

Compressed Σ-Protocol Theory

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 1 juni 2023
klokke 13:45 uur

door

Thomas Attema
geboren te Amersfoort, Nederland
in 1990

Promotores:

Prof.dr. R. Cramer	(CWI Amsterdam & Leiden University)
Prof.dr. S.O. Fehr	(CWI Amsterdam & Leiden University)

Promotiecommissie:

Prof.dr. H.J. Hupkes	
Prof.dr. F.M. Spieksma	
Prof.dr. J. Groth	(DFINITY, Switzerland)
Prof.dr. A. Lysyanskaya	(Brown University, United States)
Prof.dr. J.B. Nielsen	(Aarhus University, Denmark)

Contents