Attacks on Hash Functions and Applications

PROEFSCHRIFT

ter verkrijging van
de graad van Doctor aan de Universiteit Leiden,
op gezag van Rector Magnificus prof. mr. P.F. van der Heijden,
volgens besluit van het College voor Promoties
te verdedigen op dinsdag 19 juni 2012
klokke 15.00 uur

door

Marc Martinus Jacobus Stevens,

geboren te Hellevoetsluis
in 1981

Samenstelling van de promotiecommissie:

Promotores:

Prof. dr. R. Cramer (CWI & Universiteit Leiden)
Prof. dr. A.K. Lenstra (École Polytechnique Fédérale de Lausanne)

Copromotor:

Dr. B.M.M. de Weger (Technische Universiteit Eindhoven)

Overige leden:

Prof. dr. E. Biham (Technion)
Dr. B. Schoenmakers (Technische Universiteit Eindhoven)
Prof. dr. P. Stevenhagen (Universiteit Leiden)
Prof. dr. X. Wang (Tsinghua University)

The research in this thesis has been carried out at the Centrum Wiskunde & Informatica in the Netherlands and has been funded by the NWO VICI grant of Prof. dr. R. Cramer.

Attacks on Hash Functions and Applications

Attacks on Hash Functions and Applications
Marc Stevens
Printed by Ipskamp Drukkers
AMS 2000 Subj. class. code: 94A60
NUR: 919
ISBN: 978-94-6191-317-3

Universiteit Leiden

Centrum Wiskunde & Informatica

Cover design by Ankita Sonone.

Contents