

Cover Page



Universiteit Leiden



The handle <http://hdl.handle.net/1887/19093> holds various files of this Leiden University dissertation.

Author: Stevens, Marc Martinus Jacobus

Title: Attacks on hash functions and applications

Issue Date: 2012-06-19

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

Copyright © M. Stevens, Amsterdam 2012. All rights reserved.

Cover design by Ankita Sonone.

Contents

I	Introduction	1
1	Hash functions	3
1.1	Authenticity and confidentiality	3
1.2	Rise of a digital world	4
1.3	Security frameworks	5
1.4	Cryptographic hash functions	8
1.5	Differential cryptanalysis	15
2	MD5 collision attack by Wang et al.	17
2.1	Preliminaries	17
2.2	Description of MD5	19
2.3	Collision attack overview	21
2.4	Two message block collision	23
2.5	Differential paths	23
2.6	Sufficient conditions	24
2.7	Collision finding	25
2.8	Tables: differential paths and sufficient conditions	27
II	Contributions	31
3	Our contributions	33
3.1	Overview	33
3.2	Chosen-prefix collision applications	33
3.3	Results on MD5	34
3.4	Results on SHA-1	34
3.5	General results	36
3.6	Recommendations	38
3.7	Directions for further research	39
3.8	Thesis outline	40
4	Chosen-prefix collision abuse scenarios	43
4.1	Survey	43
4.2	Creating a rogue Certification Authority certificate	48
4.3	Nostradamus attack	56
4.4	Colliding executables	58
5	Differential cryptanalysis and paths	61
5.1	Introduction	61
5.2	Definitions and notation	63
5.3	$\mathcal{F}_{\text{md4cf}}$: MD4 based compression functions	65

5.4	Properties of the step functions	69
5.5	Differential paths	74
5.6	Differential path construction	80
6	MD5	89
6.1	Overview	89
6.2	Differential path construction	89
6.3	Collision finding	98
6.4	Identical-prefix collision attack	101
6.5	Chosen-prefix collision attack	102
7	SHA-0 and SHA-1	115
7.1	Overview	116
7.2	Description of SHA-0 and SHA-1	117
7.3	Techniques towards collision attacks	120
7.4	Differential path construction	128
7.5	Differential cryptanalysis	140
7.6	SHA-1 near-collision attack	164
7.7	Chosen-prefix collision attack	183
8	Detecting collision attacks	187
8.1	Extra line of defense	187
8.2	Core principle	188
8.3	Application to MD5	189
8.4	Application to SHA-1	192
	Appendices	192
A	MD5 compression function constants	193
B	MD5 and SHA-1 bitconditions	195
C	MD5 boolean function bitconditions	197
C.1	Bitconditions applied to boolean function F	198
C.2	Bitconditions applied to boolean function G	199
C.3	Bitconditions applied to boolean function H	200
C.4	Bitconditions applied to boolean function I	201
D	MD5 chosen-prefix collision birthday search cost	203
E	Rogue CA Construction	209
F	SHA-1 disturbance vector analysis	219

References and indices	225
References	225
Index	234
Notation	239
List of Algorithms	240
List of Figures	240
List of Tables	240
List of Theorems	241
Nederlandse samenvatting	243
Acknowledgments	245
Curriculum Vitae	247