

2010

Contributions to the theory and application of cryptographic hash functions

Mohammad Reza Reyhanitabar
University of Wollongong, rezar@uow.edu.au

Follow this and additional works at: <https://ro.uow.edu.au/theses>

University of Wollongong

Copyright Warning

You may print or download ONE copy of this document for the purpose of your own research or study. The University does not authorise you to copy, communicate or otherwise make available electronically to any other person any copyright material contained on this site.

You are reminded of the following: This work is copyright. Apart from any use permitted under the Copyright Act 1968, no part of this work may be reproduced by any process, nor may any other exclusive right be exercised, without the permission of the author. Copyright owners are entitled to take legal action against persons who infringe their copyright. A reproduction of material that is protected by copyright may be a copyright infringement. A court may impose penalties and award damages in relation to offences and infringements relating to copyright material.

Higher penalties may apply, and higher damages may be awarded, for offences and infringements involving the conversion of material into digital or electronic form.

Unless otherwise indicated, the views expressed in this thesis are those of the author and do not necessarily represent the views of the University of Wollongong.

Recommended Citation

Reyhanitabar, Mohammad Reza, Contributions to the theory and application of cryptographic hash functions, Doctor of Philosophy thesis, School of Computer Science and Software Engineering - Faculty of Informatics, University of Wollongong, 2010. <https://ro.uow.edu.au/theses/3139>

Research Online is the open access institutional repository for the University of Wollongong. For further information contact the UOW Library: research-pubs@uow.edu.au

NOTE

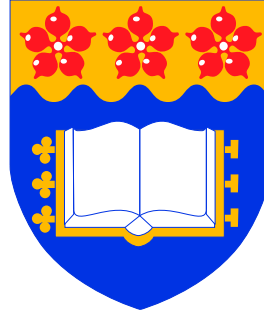
This online version of the thesis may have different page formatting and pagination from the paper copy held in the University of Wollongong Library.

UNIVERSITY OF WOLLONGONG

COPYRIGHT WARNING

You may print or download ONE copy of this document for the purpose of your own research or study. The University does not authorise you to copy, communicate or otherwise make available electronically to any other person any copyright material contained on this site. You are reminded of the following:

Copyright owners are entitled to take legal action against persons who infringe their copyright. A reproduction of material that is protected by copyright may be a copyright infringement. A court may impose penalties and award damages in relation to offences and infringements relating to copyright material. Higher penalties may apply, and higher damages may be awarded, for offences and infringements involving the conversion of material into digital or electronic form.



Contributions to the Theory and Application of Cryptographic Hash Functions

A thesis submitted in fulfilment of the
requirements for the award of the degree

Doctor of Philosophy

from

UNIVERSITY OF WOLLONGONG

by

Mohammad Reza Reyhanitabar

School of Computer Science and Software Engineering

Faculty of Informatics

August 2010

© Copyright 2010

by

Mohammad Reza Reyhanitabar

All Rights Reserved

*Dedicated to
my wife: Somaye*

Certification

I, Mohammad Reza Reyhanitabar, declare that this thesis, submitted in fulfilment of the requirements for the award of Doctor of Philosophy, in the School of Computer Science and Software Engineering, Faculty of Informatics, University of Wollongong, is wholly my own work unless otherwise referenced or acknowledged below. The document has not been submitted for qualifications at any other academic institution.

Mohammad Reza Reyhanitabar
August 18, 2010

Abstract

Cryptographic hash functions have been used to a great extent in many applications; most importantly, as building blocks for digital signature schemes and message authentication codes (MACs), as well as in commitment schemes, password protection, key derivation, and almost every practical cryptographic protocol. Unlike many other cryptographic primitives which are usually intended to fulfill specific security notions, hash functions, as workhorses of cryptography, are often expected to satisfy a wide and application dependent spectrum of security notions, ranging from merely being a one-way function to acting as a truly random function or random oracle (ideal hash).

In this Thesis, we revisit the theory and application of cryptographic hash functions. We provide new contributions to this field, which has been explored for over three decades, yet remains a highly active and interesting area of research. We pursue, in particular, a line of research considering essential theoretical questions in regard to the security features of hash functions, including formal definitions of security notions, the relationships among different security notions, and the possibility of designing property-preserving domain extension transforms for hash functions.

First, we study notions of security for cryptographic hash functions. Our main goal in this part is to consider the two essential theoretical questions in regard to security notions for hash functions; namely, formal definitions of security notions and the relationships among different security notions. Our contribution in this part includes: a clear categorization of security notions, the introduction of a new set of enhanced security notions and, most importantly, a full picture of the relationships among the security notions.

We then investigate the property preservation capabilities of domain extension transforms for hash functions. Almost all cryptographic hash functions are designed based on the following two-step approach: first, a compression function is designed which is only capable of hashing fixed-length messages, then, a domain extension

transform is applied to obtain a full-fledged hash function. The possibility of designing a property-preserving domain extension transform, which is also known as a property-preserving mode of operation, is an important problem to be considered with regard to the construction of secure hash functions. We make the following two contributions. Firstly, we analyse the most powerful multi-property-preserving (MPP) domain extension transforms for hash functions in the literature, and provide a full picture of their MPP capabilities with regard to a large collection of known security notions. Secondly, we investigate the capabilities of several different domain extension transforms in regard to preserving an interesting recently proposed security notion, called enhanced target collision resistance (eTCR).

Finally, as an interesting application of hash functions, we consider manual channel message authentication protocols using hash functions. In the manual channel model for message authentication, also known as the two-channel or SAS-based model, the sender and the receiver are assumed to have access to a low-bandwidth auxiliary channel, ensuring authentication, in addition to a typical insecure channel; however, neither they share any secret information nor there is any trusted public key infrastructure (PKI). We investigate the problem of random oracle instantiation for a three-round interactive message authentication protocol (IMAP). We also provide an efficient non-interactive message authentication protocol (NIMAP) in the manual channel model that is based on an eTCR hash function.

Acknowledgements

I would like to start by thanking my principal supervisor, Professor Willy Susilo, for his support and interest in my thesis. I had the opportunity to take advantage of his extensive knowledge and experience in the field of cryptography; without which, it would not have been possible to complete this thesis. I am also indebted to my co-supervisor, Associate Professor Yi Mu, for his invaluable advice, motivating discussions, and help.

I would also like to thank the other members of the Centre for Computer and Information Security Research (CCISR) and the School of Computer Science and Software Engineering. In particular, I am grateful to Professor Jennifer Seberry, for her advice, constructive comments, and for providing me with a full picture of the historical developments in the field of modern cryptography, based on her own extensive experience in the area.

I would like to thank Professor Reihaneh Safavi-Naini and Professor Philip Ogunbona, who supervised me during the early stages of my candidature, for providing me with their advice.

Since commencing my PhD in 2006, I have been based in the main Lab of CCISR, with my friendly lab-mates who have made it a much easier job for me to settle in a new country and do my PhD. I would like to thank all these friends for their help. I would like to specially thank Angela (Dr. Angela Piper) for her invaluable comments and help to improve the readability of my thesis. I would also like to thank Siamak (Dr. Siamak Fayyaz Shahandashti), Rungrat (Dr. Rungrat Wiangsripanawan), Faisal (Shekh Faisal Abdul-Latip), Allen (Dr. Man Ho Allen Au), Xinyi (Dr. Xinyi Huang), Wei (Wei Wu), Tsz (Tsz Hon Yuen), and Pairat (Pairat Thorncharoensri). I should also mention Dr. Shuhong Wang, with whom I had a joint work in 2007.

I extend my gratitude to my thesis examiners, Professor Josef Pieprzyk, director of the centre for Advanced Computing - Algorithms and Cryptography (ACAC) at

the Macquarie University, and Dr. Udaya Parampalli of the Department of Computer Science and Software Engineering at the University of Melbourne, for their comprehensive and constructive comments on my thesis.

I would also like to thank Associate Professor Mahmoud Salmasizadeh of the Sharif University of Technology (SUT) in Iran. He introduced me to the fascinating field of cryptography and communications security, when I started my Master's course in Telecommunications Engineering in 2000. Upon receiving my M.Sc. degree from Sharif University of Technology in 2003, I had the opportunity to work on several projects on real-world applications of cryptography under his supervision at the Electronic Research Center of SUT. The acquired valuable experience in this field motivated me to pursue my research in cryptography by commencing my PhD studies in 2006.

Last, but certainly not the least, I am most grateful to my wife, Somaye, who has been encouraging and supporting me throughout the course. Despite all the difficulties of living in a whole new country and being away from family, she always helped me and was endlessly patient, providing me with enough time to complete my thesis. I am also indebted to my mother-in-law, Farideh, for her constant support of us both. My final and special thanks go to the souls of my father, Mohammad, my mother, Batoul, and my father-in-law, Hassan.

Thanks to everyone!

Reza

Publications

The following papers have been published and presented based on the contributions of this Thesis.

- Mohammad Reza Reyhanitabar, Willy Susilo, and Yi Mu, “Enhanced Security Notions for Dedicated-Key Hash Functions: Definitions and Relationships,” *Proceedings of the 17th International Workshop on Fast Software Encryption – FSE 2010*. In Seokhie Hong and Tetsu Iwata (Eds.): LNCS, vol. 6147, pp. 192–211, Springer (2010).
- Mohammad Reza Reyhanitabar, Willy Susilo, and Yi Mu, “Enhanced Target Collision Resistant Hash Functions Revisited,” *Proceedings of the 16th International Workshop on Fast Software Encryption – FSE 2009*. In Orr Dunkelman (Ed.): LNCS, vol. 5665, pp. 327-344, Springer (2009).
- Mohammad Reza Reyhanitabar, Willy Susilo, and Yi Mu, “Analysis of Property-Preservation Capabilities of the ROX and ESh Hash Domain Extenders,” *Proceedings of the 14th Australasian Conference on Information Security and Privacy – ACISP 2009*. In Colin Boyd and Juan González Nieto (Eds.): LNCS, vol. 5594, pp. 153-170, Springer (2009).
- Mohammad Reza Reyhanitabar, Shuhong Wang, and Reihaneh Safavi-Nainin, “Non-interactive Manual Channel Message Authentication Based on eTCR Hash Functions,” *Proceedings of the 12th Australasian Conference on Information Security and Privacy – ACISP 2007*. In Josef Pieprzyk, Hossein Ghodosi, and Ed Dawson (Eds.): LNCS, vol. 4586, pp. 385-399, Springer (2007).

The following article has been prepared by combining and extending some of the results from the two conference papers published in the FSE 2009 and FSE 2010 proceedings.

- Mohammad Reza Reyhanitabar, Willy Susilo, and Yi Mu, “An Investigation of Enhanced Target Collision Resistance Property for Hash Functions: Implications, Separations, and Domain Extension,” Available from Cryptology ePrint Archive, Report 2009/506, at: <http://eprint.iacr.org/2009/506> (Submitted to a Journal.)

I have also contributed to the following paper, but it is not directly based on the content of this Thesis.

- Shekh Faisal Abdul-Latip, Mohammad Reza Reyhanitabar, Willy Susilo, and Jennifer Seberry, “On the Security of NOEKEON against Side Channel Cube Attacks,” *Proceedings of the 6th Information Security Practice and Experience Conference – ISPEC 2010*. In Jin Kwak, Robert Deng, and Yoojae Won (Eds.): LNCS, vol. 6047, pp. 45-55, Springer (2010).

Contents

Abstract	v
Acknowledgements	vii
Publications	ix
List of Abbreviations	xvii
1 Introduction	1
1.1 A Historical Review	1
1.2 Motivations and Goals	7
1.3 Organization of this Thesis	11
2 Background	13
2.1 Notations and Conventions used in the Thesis	13
2.2 Computational Problems	14
2.3 Models of Computation	16
2.3.1 Uniform Models	17
2.3.2 Non-uniform Models	19
2.4 Computational Security	22
2.4.1 Asymptotic Security	25
2.4.2 Concrete Security	28
2.5 Information-Theoretic Security	30
2.5.1 Universal Classes of Hash Functions	31
3 Security Notions: Definitions and Relationships	33
3.1 Introduction	33
3.1.1 Our Contributions	35

3.1.2	Organization of this Chapter	36
3.2	Definitions of Security Notions	36
3.2.1	Notions of Security in the Dedicated-key Setting	38
3.2.2	Notions of Security in the Keyless Setting	51
3.2.3	Ideal Hash	58
3.3	Notions of Implication and Separation	60
3.3.1	Complexity-Theoretic Viewpoint	60
3.3.2	Relationships in the Hash Function Settings	62
3.4	Relationships among Security Notions in the Dedicated-key Setting	64
3.4.1	Previously Known Relationships	65
3.4.2	Enhanced Target Collision Resistance <i>vs.</i> Collision Resistance	65
3.4.3	A Full Picture of Relationships	73
3.4.4	Security-Preserving Implications	76
3.4.5	Provisional Implications	77
3.4.6	Conventional Separations	82
4	Property Preservation Analysis of Domain Extension Transforms	97
4.1	Introduction	98
4.1.1	Our Contribution	99
4.1.2	Organization of this Chapter	101
4.2	Preliminaries	101
4.2.1	Target Security Properties	101
4.2.2	Hash Domain Extension	103
4.2.3	Orthogonality of Property Preservation	106
4.3	Our Target Domain Extension Transforms	107
4.3.1	Padding Schemes	107
4.3.2	Modes of Iteration	108
4.3.3	Full-fledged Constructions	109
4.4	Analysis of the Random-Oracle XOR Transform	112
4.4.1	Indifferentiability	112
4.4.2	MAC Preservation	115
4.4.3	PRF Preservation	117
4.5	Analysis of the Enveloped Shoup Transform	119
4.6	eTCR-Preservation Analysis of Transforms	123
4.6.1	Merkle-Damgård Variants	123

4.6.2	Randomized Hashing Variant	126
4.6.3	Shoup, Enveloped Shoup, and XOR Linear Hash	128
4.6.4	Linear Hash and its Nested Variant	130
4.7	Can We Preserve All Properties?	136
4.7.1	On Using Auxiliary Random Oracles	136
4.7.2	Open Problems	136
5	Manual Channel Message Authentication using Hash Functions	139
5.1	Introduction	139
5.1.1	Our Contributions	140
5.1.2	Related Works	141
5.1.3	Organization of this Chapter	141
5.2	Manual Channel Authentication Model	142
5.2.1	Communication Model	142
5.2.2	Security Model	143
5.3	Vaudenay’s IMAP Using a Hash Function	145
5.3.1	Definitions of the Security Properties for H	146
5.3.2	Security Analysis	149
5.3.3	Reductions	152
5.4	NIMAPs Using a Hash Function	157
5.5	A NIMAP using eTCR Hash Functions	158
5.5.1	eTCR Security of Randomized Hashing	158
5.5.2	Protocol Description and Security Reduction	159
6	Conclusion	163
	Bibliography	167
A	Proofs Left from Chapter 5	183
A.1	Proof of Lemma 5.4	183
A.2	Proof of Lemma 5.5	187
A.3	Proof of Lemma 5.6	189
A.4	Proof of Theorem 5.1	190

List of Tables

3.1	Some Special-Purpose Properties for an FIL Keyless Hash Function . . .	56
-----	--	----

List of Figures

3.1	Definitions of the Seven Security Notions for Hash Functions	40
3.2	Definitions of enhanced properties for a dedicated-key hash function.	47
3.3	Relationships among the Seven Security Notions for Hash Functions .	65
3.4	Randomized Hashing Construction	72
3.5	A Full Picture of Relationships among the Security Notions	74
3.6	Summary of Our New Relationships among the Security Notions . . .	75
3.7	Construction of Counterexample Hash Functions for Separations . . .	84
4.1	MPP Capabilities of the ESh and ROX Transforms	100
4.2	Overview of Constructions and their Property-Preserving Capabilities	101
4.3	Definitions of the Target Security Properties	102
4.4	Iteration Schemes	110
4.5	Description of a Distinguishing Adversary against the ROX Transform	118
5.1	A Generic NIMAP in the Manual Channel Model	143
5.2	A Generic n -round IMAP in the Manual Channel Model	144
5.3	Three-round Hash Function Based IMAP	147
5.4	Definitions of Security Properties for the Hash Function H	148
5.5	All Possible Interaction Paths for a One-Shot Adversary	151
5.6	Transforming a Class I–Type B Forger	155
5.7	Transforming a Class I–Type C Forger	156
5.8	A Manual Channel NIMAP Based on an eTCR Hash Family	159
A.1	Transforming a Class II–Type B Forger	185
A.2	Transforming a Class II–Type C Forger	186
A.3	Transforming a Class III Forger	188
A.4	Construction of a Forger Following Path-Type 1 from a P_2 Adversary	192
A.5	Construction of a Forger Following Path-Type 1 from a P_3 Adversary	193

A.6	Construction of a Forger Following Path-Type 1 from a P_4 Adversary	194
A.7	Construction of a Forger Following Path-Type 2 from a P_5 Adversary	195

List of Abbreviations

AIL	Arbitrary Input Length
aPre	always Preimage Resistance
aSec	always Second-Preimage Resistance
Coll (CR)	Collision Resistance
CRS	Common Reference String
CTFP	Chosen Target Fixed Prefix
DL	Discrete Logarithm
ESh	Enveloped Shoup
ePre	everywhere Preimage Resistance
eSec	everywhere Second-Preimage Resistance
eTCR	enhanced Target Collision Resistance
FIL	Fixed Input Length
IMAP	Interactive Message Authentication Protocol
LH	Linear Hash
MAC	Message Authentication Code
MD	Merkle-Damgård
MPP	Multi-Property Preserving
NIMAP	Non-interactive Message Authentication Protocol
OW	One Way
PKI	Public Key Infrastructure
PP-MAC	Privacy Preserving MAC
PPT	Probabilistic Polynomial Time
PRF	Pseudo-random Function
PRO	Pseudo-random Oracle

Pre (PR)	Preimage Resistance
pMD	plain Merkle-Damgård
pre-MD	prefix-free Merkle-Damgård
RAM	Random Access Machine
RH	Randomized Hashing
RO	Random Oracle
ROX	Random Oracle Xor
SAS	Short Authentication String
Sec (SPR)	Second-Preimage Resistance
Sh	Shoup
sMD	strengthened Merkle-Damgård
s-P	strengthened-P (strengthened variant of a property P)
TCR	Target Collision Resistance
TM	Turing Machine
UOWHF	Universal One-Way Hash Function
VIL	Variable Input Length
XLH	Xor Linear Hash