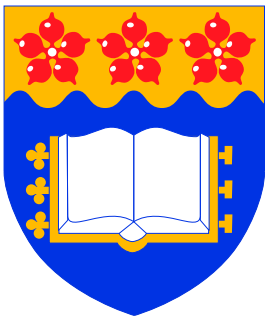
2010

Contributions to the theory and application of cryptographic hash functions

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



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

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

List of Tables

List of Figures

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