Lecture Notes in Computer Science 756
Edited by G. Goos and J. Hartmanis

Advisory Board: W. Brauer D. Gries J. Stoer

Josef Pieprzyk Babak Sadeghiyan

Design of Hashing Algorithms

Springer-Verlag
Berlin Heidelberg New York
London Paris Tokyo
Hong Kong Barcelona
Budapest

Authors

Josef Pieprzyk
Department of Computer Science, Centre for Computer Security Research
University of Wollongong
Wollongong, N.S.W. 2500, Australia

Babak Sadeghiyan
Computer Engineering Department, Amir-Kabir University of Technology
Tehran, Iran

CR Subject Classification (1991): E.3-4, G.2.1, F.2.2, D.4.6, C.2.0

ISBN 3-540-57500-6 Springer-Verlag Berlin Heidelberg New York
ISBN 0-387-57500-6 Springer-Verlag New York Berlin Heidelberg

Typesetting: Camera-ready by author
Printing and binding: Druckhaus Beltz, Hemsbach/Bergstr.
45/3140-543210 - Printed on acid-free paper

Preface

Historically, computer security is related to both cryptography and access control in operating systems. Cryptography, although mostly applied in the military and diplomacy, was used to protect communication channels and storage facilities (especially the backups). In the seventies there was a breakthrough in cryptography - the invention of public-key cryptography. It started in 1976 when Diffie and Hellman formulated their public-key distribution system and formally defined public-key cryptosystems. Two years later two practical implementations of public-key cryptosystems were published. One was designed by Rivest, Shamir, and Adleman (called the RSA system); the authors based the system on the two "difficult" numerical problems: discrete logarithm and factorization. The other invented by Merkle and Hellman was based on the knapsack problem, which is even "harder" than these used in the RSA system. Since that time cryptography, traditionally seen as the theory of encryption algorithms, has extended its scope enormously. Now it comprises many new areas, namely authentication, digital signature, hashing, secret sharing, design and verification of cryptographic protocols, zero knowledge protocols, quantum cryptography, etc.

This work presents recent developments in secure hashing algorithm design. The main part of the work was written when the authors were with the Department of Computer Science, University of New South Wales, Australian Defence Force Academy, and Babak Sadeghiyan was a PhD student working with Josef Pieprzyk as his supervisor.

Hashing is a process of creating a short digest (i.e. 64 bits) for a message of arbitrary length, for example 20 Mbytes. Hashing algorithms were first used for searching records in databases. These algorithms are designed to create a uniform distribution of collisions (two messages collide if their digests

are the same). In cryptographic applications, hashing algorithms should be "collision-free", i.e. finding two different messages hashed to the same digest should be computationally intractable. Hashing algorithms are central for digital signature applications and are used for authentication without secrecy.

There have been many proposals for secure hash algorithms, and some of them have been in use for a while. However, many of them have proved insecure. One of the major reasons for this is the progress in technology. The failed effort of many researchers suggests that we should work on some guidelines or principles for the design of hash functions. This work presents some principles for the design of secure hash algorithms. Hash algorithms are classified based on whether they apply a block cipher as the underlying one-way function or not.

For a block-cipher-based hash scheme, if the underlying block cipher is secure against chosen plaintext/ciphertext attack, the hash scheme is secure against meet-in-the-middle attack. We develop structures, based on DES-like permutations and assuming the existence of pseudorandom function generators, which can be adopted both for the structure of block-cipher-based hash schemes and for the underlying block ciphers to be used in such schemes.

Non-block-cipher-based hash functions include a spectrum of many different proposals based on one-way functions from different branches of mathematics. So, in the book, generalized schemes for the construction of hash functions are developed, assuming the existence of a one-way permutation. The generalized constructions are improvements upon the Zheng, Matsumoto and Imai's hashing scheme, based on the duality between pseudorandom bit generators and hash functions, but they incorporate strong one-way permutations. It is shown that we can build such strong permutations with a three-layer construction, in a theoretical approach. Two schemes for the construction of families of strong one-way permutations are also proposed.

Acknowledgement

We were very fortunate to receive help from many people throughout the time of this project. Firstly, we would like to express our deep gratitude to Professor Jennifer Seberry for her critical comments, helpful suggestions and encouragement. Also we would like to thank Professor Tsutomu Matsumoto and Dr Rei Safavi-Naini for their thoughtful criticism, suggestions and corrections. We also received helpful comments about the work from Dr Lawrence Brown, Professor Andrzej Gościnski, Dr Thomas Hardjono, Dr Xian-Mo Zhang and Dr Yuliang Zheng. We thank all our friends from the Department of Computer Science, University College, University of NSW, for their friendliness and everyday support. In particular our thanks go to Dr George Gerrity, Mr Per Hoff, Mr Jeff Howard, Dr Jadwiga Indulska, Mr Martin Jaatun, Mr Ken Miles, Mr Andy Quaine and Mr Wen Ung. Finally we would like to thank Mrs Nilay Genctruck for proof-reading the final manuscript.

This project was partially supported by the Australian Research Council grant number A49131885.

September 1993

Josef Pieprzyk

Babak Sadeghiyan

Contents

List of Symbols

C	Ciphertext
M	Message or a plaintext
K	Key
Σ	Alphabet
$\sum$	Summation
$\subset$	Subset
$\rightarrow$	Mapping
$\circ$	Composition of functions
$\in$	Set membership
$\equiv$	Congruence
$!$	Factorial
$\mid$	Such that (set notation)
$\oplus$	Exclusive-or (of Booleans)
$\vee$	Or (of Booleans)
$\wedge$	And (of Booleans)
$\|\|$	Concatenation
$O(f)$	Big-Oh of the function f
$\cup$	Union
$\lceil x \rceil$	Smallest integer greater than x
$\lfloor x \rfloor$	Greatest integer smaller than x
N	The set of natural numbers
Z_n	The set of integers modulo n
$\mid x \mid$	Absolute value of the number x
$\#S$	Number of elements in the set S
$\log_n$	Logarithm to the base n