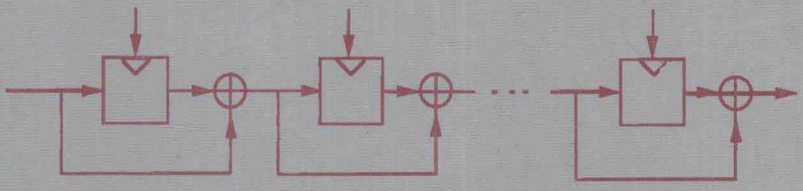
Lecture Notes in Computer Science 756

Josef Pieprzyk Babak Sadeghiyan

Design of Hashing Algorithms



Springer-Verlag

Josef Pieprzyk Babak Sadeghiyan

Design of Hashing Algorithms

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

Series Editors

Gerhard Goos
Universität Karlsruhe
Postfach 69 80
Vincenz-Priessnitz-Straße 1
D-76131 Karlsruhe, Germany

Juris Hartmanis
Cornell University
Department of Computer Science
4130 Upson Hall
Ithaca, NY 14853, USA

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

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

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

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

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
|	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

Lecture Notes in Computer Science

For information about Vols. 1–680
please contact your bookseller or Springer-Verlag

Vol. 681: H. Wansing, The Logic of Information Structures. IX, 163 pages. 1993. (Subseries LNAI).

Vol. 682: B. Bouchon-Meunier, L. Valverde, R. R. Yager (Eds.), IPMU '92 – Advanced Methods in Artificial Intelligence. Proceedings, 1992. IX, 367 pages. 1993.

Vol. 683: G.J. Milne, L. Pierre (Eds.), Correct Hardware Design and Verification Methods. Proceedings, 1993. VIII, 270 Pages. 1993.

Vol. 684: A. Apostolico, M. Crochemore, Z. Galil, U. Manber (Eds.), Combinatorial Pattern Matching. Proceedings, 1993. VIII, 265 pages. 1993.

Vol. 685: C. Rolland, F. Bodart, C. Cauvet (Eds.), Advanced Information Systems Engineering. Proceedings, 1993. XI, 650 pages. 1993.

Vol. 686: J. Mira, J. Cabestany, A. Prieto (Eds.), New Trends in Neural Computation. Proceedings, 1993. XVII, 746 pages. 1993.

Vol. 687: H. H. Barrett, A. F. Gmitro (Eds.), Information Processing in Medical Imaging. Proceedings, 1993. XVI, 567 pages. 1993.

Vol. 688: M. Gauthier (Ed.), Ada-Europe '93. Proceedings, 1993. VIII, 353 pages. 1993.

Vol. 689: J. Komorowski, Z. W. Ras (Eds.), Methodologies for Intelligent Systems. Proceedings, 1993. XI, 653 pages. 1993. (Subseries LNAI).

Vol. 690: C. Kirchner (Ed.), Rewriting Techniques and Applications. Proceedings, 1993. XI, 488 pages. 1993.

Vol. 691: M. Ajmone Marsan (Ed.), Application and Theory of Petri Nets 1993. Proceedings, 1993. IX, 591 pages. 1993.

Vol. 692: D. Abel, B.C. Ooi (Eds.), Advances in Spatial Databases. Proceedings, 1993. XIII, 529 pages. 1993.

Vol. 693: P. E. Lauer (Ed.), Functional Programming, Concurrency, Simulation and Automated Reasoning. Proceedings, 1991/1992. XI, 398 pages. 1993.

Vol. 694: A. Bode, M. Reeve, G. Wolf (Eds.), PARLE '93. Parallel Architectures and Languages Europe. Proceedings, 1993. XVII, 770 pages. 1993.

Vol. 695: E. P. Klement, W. Slany (Eds.), Fuzzy Logic in Artificial Intelligence. Proceedings, 1993. VIII, 192 pages. 1993. (Subseries LNAI).

Vol. 696: M. Worboys, A. F. Grundy (Eds.), Advances in Databases. Proceedings, 1993. X, 276 pages. 1993.

Vol. 697: C. Courcoubetis (Ed.), Computer Aided Verification. Proceedings, 1993. IX, 504 pages. 1993.

Vol. 698: A. Voronkov (Ed.), Logic Programming and Automated Reasoning. Proceedings, 1993. XIII, 386 pages. 1993. (Subseries LNAI).

Vol. 699: G. W. Mineau, B. Moulin, J. F. Sowa (Eds.), Conceptual Graphs for Knowledge Representation. Proceedings, 1993. IX, 451 pages. 1993. (Subseries LNAI).

Vol. 700: A. Lingas, R. Karlsson, S. Carlsson (Eds.), Automata, Languages and Programming. Proceedings, 1993. XII, 697 pages. 1993.

Vol. 701: P. Atzeni (Ed.), LOGIDATA+: Deductive Databases with Complex Objects. VIII, 273 pages. 1993.

Vol. 702: E. Börger, G. Jäger, H. Kleine Büning, S. Martini, M. M. Richter (Eds.), Computer Science Logic. Proceedings, 1992. VIII, 439 pages. 1993.

Vol. 703: M. de Berg, Ray Shooting, Depth Orders and Hidden Surface Removal. X, 201 pages. 1993.

Vol. 704: F. N. Paulisch, The Design of an Extendible Graph Editor. XV, 184 pages. 1993.

Vol. 705: H. Grünbacher, R. W. Hartenstein (Eds.), Field-Programmable Gate Arrays. Proceedings, 1992. VIII, 218 pages. 1993.

Vol. 706: H. D. Rombach, V. R. Basili, R. W. Selby (Eds.), Experimental Software Engineering Issues. Proceedings, 1992. XVIII, 261 pages. 1993.

Vol. 707: O. M. Nierstrasz (Ed.), ECOOP '93 – Object-Oriented Programming. Proceedings, 1993. XI, 531 pages. 1993.

Vol. 708: C. Laugier (Ed.), Geometric Reasoning for Perception and Action. Proceedings, 1991. VIII, 281 pages. 1993.

Vol. 709: F. Dehne, J.-R. Sack, N. Santoro, S. Whitesides (Eds.), Algorithms and Data Structures. Proceedings, 1993. XII, 634 pages. 1993.

Vol. 710: Z. Ésik (Ed.), Fundamentals of Computation Theory. Proceedings, 1993. IX, 471 pages. 1993.

Vol. 711: A. M. Borzyszkowski, S. Sokołowski (Eds.), Mathematical Foundations of Computer Science 1993. Proceedings, 1993. XIII, 782 pages. 1993.

Vol. 712: P. V. Rangan (Ed.), Network and Operating System Support for Digital Audio and Video. Proceedings, 1992. X, 416 pages. 1993.

Vol. 713: G. Gottlob, A. Leitsch, D. Mundici (Eds.), Computational Logic and Proof Theory. Proceedings, 1993. XI, 348 pages. 1993.

Vol. 714: M. Bruynooghe, J. Penjam (Eds.), Programming Language Implementation and Logic Programming. Proceedings, 1993. XI, 421 pages. 1993.

Vol. 715: E. Best (Ed.), CONCUR'93. Proceedings, 1993. IX, 541 pages. 1993.

Vol. 716: A. U. Frank, I. Campari (Eds.), Spatial Information Theory. Proceedings, 1993. XI, 478 pages. 1993.

Vol. 717: I. Sommerville, M. Paul (Eds.), Software Engineering – ESEC '93. Proceedings, 1993. XII, 516 pages. 1993.

Vol. 718: J. Seberry, Y. Zheng (Eds.), Advances in Cryptology – AUSCRYPT '92. Proceedings, 1992. XIII, 543 pages. 1993.

Vol. 719: D. Chetverikov, W.G. Kropatsch (Eds.), Computer Analysis of Images and Patterns. Proceedings, 1993. XVI, 857 pages. 1993.

Vol. 720: V.Mařík, J. Lažanský, R.R. Wagner (Eds.), Database and Expert Systems Applications. Proceedings, 1993. XV, 768 pages. 1993.

Vol. 721: J. Fitch (Ed.), Design and Implementation of Symbolic Computation Systems. Proceedings, 1992. VIII, 215 pages. 1993.

Vol. 722: A. Miola (Ed.), Design and Implementation of Symbolic Computation Systems. Proceedings, 1993. XII, 384 pages. 1993.

Vol. 723: N. Aussenac, G. Boy, B. Gaines, M. Linster, J.-G. Ganascia, Y. Kodratoff (Eds.), Knowledge Acquisition for Knowledge-Based Systems. Proceedings, 1993. XIII, 446 pages. 1993. (Subseries LNAI).

Vol. 724: P. Cousot, M. Falaschi, G. Filè, A. Rauzy (Eds.), Static Analysis. Proceedings, 1993. IX, 283 pages. 1993.

Vol. 725: A. Schiper (Ed.), Distributed Algorithms. Proceedings, 1993. VIII, 325 pages. 1993.

Vol. 726: T. Lengauer (Ed.), Algorithms – ESA '93. Proceedings, 1993. IX, 419 pages. 1993

Vol. 727: M. Filgueiras, L. Damas (Eds.), Progress in Artificial Intelligence. Proceedings, 1993. X, 362 pages. 1993. (Subseries LNAI).

Vol. 728: P. Torasso (Ed.), Advances in Artificial Intelligence. Proceedings, 1993. XI, 336 pages. 1993. (Subseries LNAI).

Vol. 729: L. Donatiello, R. Nelson (Eds.), Performance Evaluation of Computer and Communication Systems. Proceedings, 1993. VIII, 675 pages. 1993.

Vol. 730: D. B. Lomet (Ed.), Foundations of Data Organization and Algorithms. Proceedings, 1993. XII, 412 pages. 1993.

Vol. 731: A. Schill (Ed.), DCE – The OSF Distributed Computing Environment. Proceedings, 1993. VIII, 285 pages. 1993.

Vol. 732: A. Bode, M. Dal Cin (Eds.), Parallel Computer Architectures. IX, 311 pages. 1993.

Vol. 733: Th. Grechenig, M. Tscheligi (Eds.), Human Computer Interaction. Proceedings, 1993. XIV, 450 pages. 1993.

Vol. 734: J. Volkert (Ed.), Parallel Computation. Proceedings, 1993. VIII, 248 pages. 1993.

Vol. 735: D. Bjørner, M. Broy, I. V. Pottosin (Eds.), Formal Methods in Programming and Their Applications. Proceedings, 1993. IX, 434 pages. 1993.

Vol. 736: R. L. Grossman, A. Nerode, A. P. Ravn, H. Rischel (Eds.), Hybrid Systems. VIII, 474 pages. 1993.

Vol. 737: J. Calmet, J. A. Campbell (Eds.), Artificial Intelligence and Symbolic Mathematical Computing. Proceedings, 1992. VIII, 305 pages. 1993.

Vol. 738: M. Weber, M. Simons, Ch. Lafontaine, The Generic Development Language Deva. XI, 246 pages. 1993.

Vol. 739: H. Imai, R. L. Rivest, T. Matsumoto (Eds.), Advances in Cryptology – ASIACRYPT '91. X, 499 pages. 1993.

Vol. 740: E. F. Brickell (Ed.), Advances in Cryptology – CRYPTO '92. Proceedings, 1992. X, 593 pages. 1993.

Vol. 741: B. Preneel, R. Govaerts, J. Vandewalle (Eds.), Computer Security and Industrial Cryptography. Proceedings, 1991. VIII, 275 pages. 1993.

Vol. 742: S. Nishio, A. Yonezawa (Eds.), Object Technologies for Advanced Software. Proceedings, 1993. X, 543 pages. 1993.

Vol. 743: S. Doshita, K. Furukawa, K. P. Jantke, T. Nishida (Eds.), Algorithmic Learning Theory. Proceedings, 1992. X, 260 pages. 1993. (Subseries LNAI)

Vol. 744: K. P. Jantke, T. Yokomori, S. Kobayashi, E. Tomita (Eds.), Algorithmic Learning Theory. Proceedings, 1993. XI, 423 pages. 1993. (Subseries LNAI)

Vol. 745: V. Roberto (Ed.), Intelligent Perceptual Systems. VIII, 378 pages. 1993. (Subseries LNAI)

Vol. 746: A. S. Tanguiane, Artificial Perception and Music Recognition. XV, 210 pages. 1993. (Subseries LNAI).

Vol. 747: M. Clarke, R. Kruse, S. Moral (Eds.), Symbolic and Quantitative Approaches to Reasoning and Uncertainty. Proceedings, 1993. X, 390 pages. 1993.

Vol. 748: R. H. Halstead Jr., T. Ito (Eds.), Parallel Symbolic Computing: Languages, Systems, and Applications. Proceedings, 1992. X, 419 pages. 1993.

Vol. 749: P. A. Fritzson (Ed.), Automated and Algorithmic Debugging. Proceedings, 1993. VIII, 369 pages. 1993.

Vol. 750: J. L. Díaz-Herrera (Ed.), Software Engineering Education. Proceedings, 1994. XII, 601 pages. 1994.

Vol. 751: B. Jähne, Spatio-Temporal Image Processing. XII, 208 pages. 1993.

Vol. 752: T. W. Finin, C. K. Nicholas, Y. Yesha (Eds.), Information and Knowledge Management. Proceedings, 1992. VII, 142 pages. 1993.

Vol. 753: L. J. Bass, J. Gornostaev, C. Unger (Eds.), Human-Computer Interaction. Proceedings, 1993. X, 388 pages. 1993.

Vol. 754: H. D. Pfeiffer, T. E. Nagle (Eds.), Conceptual Structures: Theory and Implementation. Proceedings, 1992. IX, 327 pages. 1993. (Subseries LNAI).

Vol. 755: B. Möller, H. Partsch, S. Schuman (Eds.), Formal Program Development. Proceedings. VII, 371 pages. 1993.

Vol. 756: J. Pieprzyk, B. Sadeghiyan, Design of Hashing Algorithms. XV, 194 pages. 1993.

Vol. 758: M. Teillaud, Towards Dynamic Randomized Algorithms in Computational Geometry. IX, 157 pages. 1993.

Vol. 760: S. Ceri, K. Tanaka, S. Tsur (Eds.), Deductive and Object-Oriented Databases. Proceedings, 1993. XII, 488 pages. 1993.

Vol. 761: R. Shyamasundar (Ed.), Foundations of Software Technology and Theoretical Computer Science. Proceedings, 1993. XIV, 456 pages. 1993.

Contents

Chapter 1

Introduction

1.1 Background and Aims

1.1.1 Introductory Comments

The development of telecommunication and computer technologies have brought us into an era in which inexpensive contact between people or computers on opposite sides of the world is commonplace. The existing services such as electronic mail, electronic funds transfer, and home banking have already changed our way of life. Electronic mail systems significantly reduce our reliance on paper as the major medium for exchange of information, by providing rapid and economic ways for the distribution of data. It is clear that, with the widespread implementation and use of such services, senders and receivers of sensitive or valuable information will require secure means for validating and authenticating the electronic messages they exchange. The least that may be expected of these services is that they should offer the same security level as that of the conventional mechanisms. In the mail service, conventional paper mail has its own envelope, which protects the secrecy of its contents, it is also signed which assures the recipient of its origin. Similar properties should have the electronic mail service.

On the other hand, the increased use of satellite, microwave, cellular mobile and other forms of radio communication allow the illicit interception of communications. Moreover, the widespread use of computers provides

the interceptors with computer data, which can easily be edited to sort the valuable information. Figure 1.1 schematically shows such a scenario.

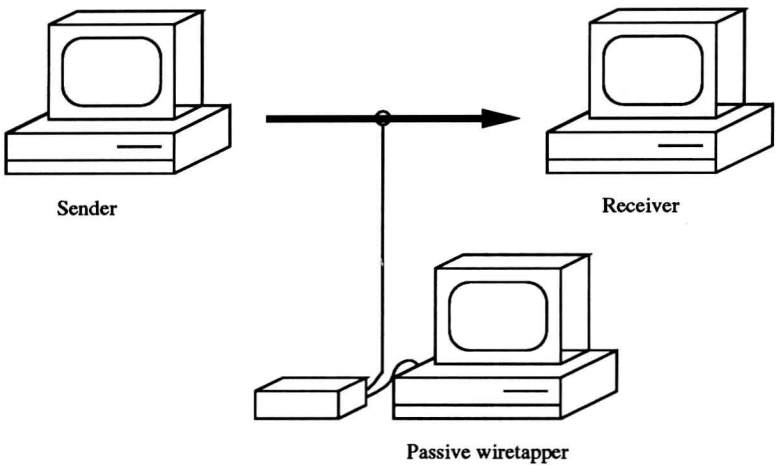


Figure 1.1: Passive Eavesdropping over Communication Networks

While eavesdropping on radio communications is a passive act, an active wiretapper can inject fraudulent messages in other types of communication links such as telephone networks. Figure 1.2 illustrates a possible active wiretapping scenario.

1.1.2 Discussion of Public-key and Private-key Cryptography

Cryptography is the study of mathematical systems for solving two kinds of security problems: privacy and authentication [Diffie and Hellman, 1976]. A privacy system prevents the extraction of information by unauthorized parties from messages transmitted over a public channel, thus assuring the sender of the message it will be read only by the intended recipient. An authentication system prevents the unauthorized injection of messages into a public channel, assuring the receiver of a message of its legitimacy. The authentication problem can be divided into *message authentication*, where the problem is assuring the receiver that the text has not changed since it left the sender, and *user authentication*, where the problem is verifying that