Lecture Notes in Computer Science 1440
Edited by G. Goos, J. Hartmanis and J. van Leeuwen

Springer
Berlin
Heidelberg
New York
Barcelona
Hong Kong
London
Milan
Paris
Singapore
Tokyo

Kevin S. McCurley Claus Dieter Ziegler (Eds.)

Advances in Cryptology 1981 – 1997

Electronic Proceedings and Index of the CRYPTO and EUROCRYPT Conferences 1981 – 1997

Springer

Volume Editors

Kevin S. McCurley
IBM Almaden Research Center
650 Harry Road, San Jose, CA 95120, USA
E-mail: mccurley@almaden.ibm.com

Claus Dieter Ziegler
Fachinformationszentrum Karlsruhe, Abteilung Mathematik und Informatik
Franklinstrasse 11, D-10587 Berlin, Germany
E-mail: cdz@zblmath.fiz-karlsruhe.de

Cataloging-in-Publication data applied for

Die Deutsche Bibliothek - CIP-Einheitsaufnahme

Advances in cryptology : 1981 - 1997 ; electronic proceedings and index of the Crypto and Eurocrypt Conferences 1981 - 1997 / Kevin S. McCurley ; Claus Dieter Ziegler (ed.). - Berlin ; Heidelberg ; New York ; Barcelona ; Hong Kong ; London ; Milan ; Paris ; Singapore ; Tokyo : Springer, 1999
(Lecture notes in computer science ; Vol. 1440)
ISBN 3-540-65069-5

CR Subject Classification (1991): E.3, G.2.1, D.4.6, K.6.5, F.2.1-2, C.2, J.1

ISSN 0302-9743
ISBN 3-540-65069-5 Springer-Verlag Berlin Heidelberg New York

Typesetting: Camera-ready by author
SPIN 10638017 06/3142 – 5 4 3 2 1 0 Printed on acid-free paper

Table of Contents

Foreword

About Cryptology

It is now widely perceived that we are experiencing an information revolution whose effects will ultimately be as pervasive and profound as was brought by the industrial revolution of the last century. From the beginning of time, information has been an important asset for humans. In the early days of human existence, the mere knowledge of where to most easily gather food was the difference between life and death. Throughout history, information has provided the means for winning wars, making fortunes, and shaping history. The underlying theme of the information revolution is that we continue to find new ways to use information. These new uses for information serve to highlight our need to protect different aspects of information.

Cryptology may be broadly defined as the scientific study of adversarial information protection. Cryptology has traditionally dealt with the confidentiality of information, but innovation in using information produces new requirements for protection of that information. Some are longstanding and fundamental - how do we guarantee that information is "authentic"? How do we guarantee that information is timely? How can we produce bits that have the same properties as "money"? Each of these questions has been grappled with in the cryptologic research community.

History of the IACR

Cryptography has a long and illustrious history, but relatively little published scientific literature existed prior to the mid 1970s, when public key cryptography was discovered and interest was sparked in the scientific study of information protection. The early 1980's saw a number of conferences on the subject of cryptography, including the first conference held in Santa Barbara in 1981, organized by Alan Gersho of UCSB. This was followed in 1982 by the CRYPTO '82 conference. A report on this conference was published by David Kahn in Cryptologia the following year:

> "At the initiative of David Chaum the organizer of CRYPTO '82, some attendees met the last day to begin organizing what they

> tentatively called an International Association for Cryptologic Research. Its main functions would be (1) to coordinate meetings on cryptology as to time, place and program and in some cases to run them, and (2) to publish a bulletin to give notice of conferences and of cryptologic sessions other conferences. Members of the organizing committee are Chaum; Henry J. Beker of RACAL-Comsec Ltd. in Salisbury, England; Whitfield Diffie of BNR in Palo Alto, California; Robert R. Jueneman of Satellite Business Systems in McLean, Virginia; Ernest F. Brickell of Sandia National Laboratories in Albuquerque, New Mexico; Stephen Kent of Bolt, Beranek & Newman in Cambridge, Massachusetts; and David Kahn of Great Neck, New York, an editor of Cryptologia."

CRYPTO '83 then became the first conference officially sponsored by IACR. From these early beginnings, IACR has grown to be a scientific organization with over a thousand members worldwide, representing over 65 countries. IACR now sponsors two conferences each year, called CRYPTO and EUROCRYPT. CRYPTO is held each year in August at the University of California in Santa Barbara, USA. EUROCRYPT is held each spring in a different location in Europe. IACR will also begin sponsorship of the Asiacrypt conference in 2000.

Proceedings of CRYPTO and EUROCRYPT

The work published here includes the proceedings of all conferences that have been organized by the International Association for Cryptologic Research since 1983. In addition, material from a few other conferences that spawned IACR is included:

- proceedings of CRYPTO '81. These were first published as a technical report by the University of California, Santa Barbara, and have had only very limited circulation prior to this volume. In addition, it was previously published in SIGACT News in 1983.
- proceedings of the 1982 predecessor to EUROCRYPT. The IACR was in the process of being formed at that time, but there was already an intent among many of the organizers for this to be the first in a series of European conferences on cryptology organized by IACR. The '82 conference was not originally called EUROCRYPT, but is now generally referred to as EUROCRYPT '82.
- proceedings of CRYPTO '82 and '83. These were originally published by Plenum Publishing. As of the time of this writing (mid-1998), the proceedings of CRYPTO '83 are no longer available in print.
- abstracts from EUROCRYPT '86. This volume was only distributed to conference attendees.

EUROCRYPT '86 and CRYPTO '81 had no formal proceedings, and the material included here consists mostly of abstracts. In fact, over time it is possible to detect a noticeable change in the tone of papers in all of these volumes, from early publication of "Extended Abstracts" to more carefully refereed high quality papers.

The proceedings of both CRYPTO and EUROCRYPT have been published by Springer-Verlag since 1984 in the series "Lecture Notes in Computer Science". Prior to 1994, authors submitted abstracts that were distributed to attendees at the conference, and these abstracts were then refined and published as a formal proceedings at a later date. (an exception was made at EUROCRYPT '86). Beginning with CRYPTO '94, proceedings of EUROCRYPT and CRYPTO have been available at the conference.

The Evolution of Cryptology Research

The work published here represents the majority of the important research work that has been published by the open cryptologic research community during the last fifteen years. In spite of the great work that has been done, there are still huge gaps in our knowledge of information protection. I hope that the republication of these proceedings will stimulate further research in the field and I thank Springer-Verlag for supporting the initiative to produce them.

Looking at how the field has evolved over the years, there are some noticeable trends. The ones that are most noticeable to this author are the following:

Complexity-based reasoning on security

The first mention that I am aware of involving reasoning about security based on what an adversary could *compute* appeared in Shannon's seminal paper of 1948. Once Diffie and Hellman published their paper on public key cryptography, we were presented with concrete constructions that led to a huge body of work on complexity-based reasoning on security. In recent years some of the work in complexity-based security has incorporated some of the original ideas of Shannon on information-theoretic security. In spite of the considerable progress that has been made, I would argue that the field is still not closed, because some of the assumptions we are required to make in order to prove reasonable security are still questionable. Moreover, computing is fundamentally about resource management, and in spite of Moore's law, there continue to be increasing demands for processing speed, storage, and communication. The constructions that we have today may have considerable room for improvement, both in their security and their practicality.

Environmental Attacks and Protocols

I use the term "environmental attacks" to include things such as fault analysis, timing attacks, and power analysis. Each of these has been demonstrated to pose a serious hazard in real world applications, and also serves to highlight several defects in our abstract modeling of security. First is the fact that our models of computers fail to take into account all aspects of their physical instantiation. Looking at a computer as a "black box" provides an elegant abstraction, but in practice the box exists in three dimensional space, manipulates energy, and produces ancillary outputs. Future models of computers and security may emerge to describe these phenomena. The second deficiency in our understanding has to do with the fact that true security requires analysis of protocols instead of serial algorithms. If we include parallel and distributed algorithms, then the difference between a protocol and an algorithm is that an algorithm *may* involve multiple parties, but a protocol always does. When reasoning about security, there are always at least two parties: the adversary and the participant. Any analysis that fails to address the capabilities of an adversary to affect the outputs is doomed to failure.

Linear and Differential Cryptanalysis

Linear and Differential cryptanalysis have emerged as the most effective general techniques available for attacking practical ciphers. At the same time, progress has been made in designing ciphers that are resistant to these attacks.

New Applications

Cryptology is no longer restricted to the study of only encryption and confidentiality. As new uses of information emerge, they bring with them new requirements for information. As a result, we have seen discussion of cryptographic constructions for electronic cash, timestamping, program checking, intellectual property protection, etc. Each of these applications raises whole new areas for investigation.

It is ironic that the publication of this CDROM itself raises interesting and serious issues in the protection of information, since the information age is changing the very foundation of what it means to "publish". Some have argued that electronic publishing raises serious concerns about the mechanism for archiving scientific work for the ages. Others have argued that the role of traditional publishers is threatened by the information age. Some publishers are concerned that their ability to make a living is threatened by electronic distribution of information, since bits are easily copied and the meaning of traditional copyrights are evolving. Nevertheless, Springer-Verlag has taken the lead in developing technologies that offer new capabilities for the use of information.

Some Statistics

I close this section with some statistics and trivia about the body of literature. This collection contains 1285 individual papers, by a total of 854 authors. In what follows, we use a shorthand notation for references. For example, a reference of the form c90-323 refers to a paper in CRYPTO '90 starting on page 323, and e91-14 refers to a paper in EUROCRYPT '91 starting on page 14.

Most Authors on a Single Paper

The following papers have the most co-authors.

10 authors c83-171, Davio, M., Desmedt, Y., Fosseprez, M., Govaerts, R., Hulsbosch, J., Neutjens, P., Piret, P., Quisquater, J. J., Vandewalle, J. and Wouters, P., Analytical characteristics of the DES

7 authors c88-37, Ben-Or, M., Goldreich, O., Goldwasser, S., Hastad, J., Kilian, J., Micali, S. and Rogaway, P., Everything provable is provable in zero-knowledge

7 authors c91-44, Bird, R., Gopal, I., Herzberg, A., Janson, P., Kutten, S., Molva, R. and Yung, M., Systematic design of two-party authentication protocols

7 authors e92-194, Desmedt, Y., Landrock, P., Lenstra, A. K., McCurley, K. S., Odlyzko, A. M., Rueppel, R. A. and Smid, M. E., The Eurocrypt '92 Controversial Issue: Trapdoor Primes and Moduli

6 authors e89-267, Vandewalle, J., Chaum, D., Fumy, W., Jansen, C. J. A., Landrock, P. and Roelofsen, G., A European call for cryptographic algorithms: RIPE; Race Integrity Primitives Evaluation

6 authors e91-547, Preneel, B., Chaum, D., Fumy, W., Jansen, C. J. A., Landrock, P. and Roelofsen, G., Race Integrity Primitives Evaluation

6 authors c92-471, Blundo, C., De Santis, A., Herzberg, A., Kutten, S., Vaccaro, U. and Yung, M., Perfectly-secure key distribution for dynamic conferences

5 authors c96-329, Hughes, R. J., Luther, G. G., Morgan, G. L., Peterson, C. G. and Simmons, C., Quantum Cryptography over Underground Optical Fibers

5 authors c81-154, Diffie, W., Klein, M., Dertouzos, M. L., Gleason, A. and Smith, D., Panel Discussion: National Security and Commercial Security: Division of Responsibility

5 authors c84-144, Davio, M., Desmedt, Y., Goubert, J., Hoornaert, F. and Quisquater, J. J., Efficient hardware and software implementations for the DES

5 authors e85-43, Vandewalle, J., Govaerts, R., De Becker, W., Decroos, M. and Speybrouck, G., Implementation study of public key cryptography protection in an existing electronic mail and document handling system.

5 authors c85-3, Estes, D., Adleman, L. M., Kompella, K., McCurley, K. S. and Miller, G. L., Breaking the Ong-Schnorr-Shamir signature scheme for quadratic number fields
5 authors c86-277, Orton, G. A., Roy, M. P., Scott, P. A., Peppard, L. E. and Tavares, S. E., VLSI implementation of public-key encryption algorithms
5 authors c88-297, Abadi, M., Allender, E., Broder, A., Feigenbaum, J. and Hemachandra, L. A., On generating solved instances of computational problems
5 authors e89-294, Chaum, D., den Boer, B., van Heyst, E., Mjoelsnes, S. F. and Steenbeek, A., Efficient offline electronic checks (extended abstract)
5 authors e90-161, Preneel, B., Van Leekwijck, W., Van Linden, L., Govaerts, R. and Vandewalle, J., Propagation characteristics of Boolean functions
5 authors e90-253, Bennett, C. H., Bessette, F., Brassard, G., Salvail, L. and Smolin, J., Experimental quantum cryptography
5 authors e90-465, Guillou, L. C., Quisquater, J. J., Walker, M., Landrock, P. and Shaer, C., Precautions taken against various potential attacks in ISO/IEC DIS 9796
5 authors e92-356, Biehl, I., Buchmann, J. A., Meyer, B., Thiel, C. and Thiel, C., Tools for proving zero knowledge
5 authors c92-215, Dwork, C., Feige, U., Kilian, J., Naor, M. and Safra, M., Low communication 2-prover zero-knowledge proofs for NP
5 authors e93-126, Kurosawa, K., Okada, K., Sakano, K., Ogata, W. and Tsujii, S., Nonperfect secret sharing schemes and matroids
5 authors e94-433, Charnes, C., O'Connor, L., Pieprzyk, J., Safavi-Naini, R. and Zheng, Y., Comments on Soviet encryption algorithm
5 authors c94-150, Blundo, C., De Santis, A., Di Crescenzo, G., Gaggia, A. Giorgio and Vaccaro, U., Multi-secret sharing schemes

Most Papers by a Single Author

The following authors have the most papers published in the series:

Chaum, D. (38) c81-138, c82-199, c83-153, c83-387, c84-432, c84-481, e85-241, c85-18, c85-192, c86-49, c86-118, c86-195, c86-200, e87-127, e87-227, c87-87, c87-156, c87-462, e88-177, c88-319, e89-267, e89-288, e89-294, c89-212, c89-591, e90-458, c90-189, c90-206, e91-96, e91-257, e91-547, e91-554, c91-470, e92-390, c92-1, c92-89, e93-344, e94-86

Desmedt, Y. (34) c83-171, e84-62, e84-142, c84-144, c84-147, c84-359, c85-42, c85-516, c85-537, e86-17, c86-111, c86-459, c87-21, c87-120, e88-23, e88-183, c88-375, e89-75, e89-122, c89-6, c89-307, e90-1, e90-11, c90-169, c90-177, e91-81, e91-205, c91-457, e92-25, e92-194, c92-549, e94-275, e95-147, e96-107

Yung, M. (30) c84-439, c85-128, c87-40, c87-135, e89-3, e89-192, e89-196, e90-412, c90-94, c90-177, c90-366, e91-205, c91-44, c92-196, c92-442, c92-471, e93-267, e94-67, c95-222, c95-287, c95-339, e96-72, c96-89, c96-186, e97-62, e97-280, e97-450, c97-31, c97-264, c97-440

Beth, T. (11) e82-1, e84-88, c86-302, e87-25, e88-77, e89-533, e90-189, c90-169, e91-316, e93-65, c94-318

Program Committee Service

Serving on a program committee is a time consuming task, and often results in little recognition from the community. The following people have served on at least five program committees:

– Odlyzko, Andrew (10)
– Rivest, Ronald (9)
– Schnorr, Claus (7)
– Massey, James L. (7)
– Beth, Thomas (7)
– Berson, Thomas (7)
– Rueppel, Rainer (6)
– Desmedt, Yvo (6)
– Davies, Donald W. (6)
– Damgård, Ivan (6)
– Brickell, Ernest (6)
– Simmons, Gustavus J. (5)
– Quisquater, Jean-Jacques (5)
– Okamoto, Tatsuaki (5)
– Maurer, Ueli (5)
– Ingemarsson, Ingemar (5)
– Feigenbaum, Joan (5)
– Diffie, Whitfield (5)
– Denning, Dorothy (5)
– Chaum, David (5)
– Beker, Henry (5)

A complete list of program committees is included in this volume.

Kevin S. McCurley
IBM Almaden Research Center
September 1998

Preface

One of the challenges of embracing the information age is to enhance and carry forward the enormous amount of information that is archived in paper format. In this collection we have collected together the 14692 pages of information from the 32 volumes of conference proceedings of CRYPTO and EUROCRYPT. In addition, we have derived textual information that can be used to index and search this archive.

Compressing this much information onto a single CDROM required significant effort, but it was felt that this would enhance the usability of the collection with current technology. As a rough estimate we might assume that one printed volume of cryptology proceedings contains in the average about 460 pages. If we assume that a volume of 460 pages is 3.5 centimeters thick, one has to store 1.12 meters of paper proceedings. Suppose one page of a proceedings volume contains in the average 380 words or, including punctuation, 2500 characters (e.g. one page of volume 963 of LNCS contains 482 words or 3200 characters in the average whereas volume 196 contains only 253 words or 1710 characters per page). In this case we have to store 5.582.960 words or 36.730.000 characters or in computer terms about 40 megabytes if we store it as ASCII text.

Unfortunately, producing such text is nearly impossible, and we have chosen to provide information in the form of PDF files containing images. This is dictated by the content of the volumes, which are predominantly text, but are also mathematical in nature, containing many formulas and mathematical expressions. Over the years the fonts and typefaces changed from typewriter styles to DVI files, and particularly the quality of some early printed source documents is rather poor (especially the proceedings of CRYPTO 81 and EUROCRYPT 86). These factors contribute to a very high error rate for optical character recognition (OCR). Since mathematical content is of no value if the accuracy is compromised, we chose to deliver an electronic product that is as faithful as possible to the original material.

Given that a CDROM has a capacity of approximately 650 MB, this implies that the size of one proceedings page should not be much larger than about 40 KB, in order to leave room for a Keyword Index, an Author Index, the Table of Contents and a search engine for efficient and convenient retrieval of the documents.

By experimentation we learned that 400 dpi is a resolution where the OCR software could be trained to produce reasonable results. One page, scanned with a resolution of 400 dpi, has an average size of 140 KB when stored as 4636x3232 resolution TIF file. The TIF files served as the basis for the OCR process, because we need the text versions to produce indices. Once the TIF images were produced, we used an automatic process to crop white space from the borders, and transformed into PDF files using some of the software in the IBM database of US Patents. We experimented a great deal with different settings to balance the space requirement against the quality of the result. The final process took several days of processing on a personal computer.

Creating a search engine for OCR scanned text is a challenge in itself, from both an algorithmic and software point of view. We experimented with various approaches to this, and Kevin McCurley finally decided to write a Java applet for incorporation into the CDROM. This has several advantages:

- it is integrated into the browsing process of HTML and PDF documents,
- it offers portability across many different platforms, which is particularly important for a scientific audience accustomed to Unix workstations.

Unfortunately Java is still rather slow, consumes substantial memory, and has not yet reached full maturity as a programming language. As a result, we expect that some users may have trouble using the Applet, but perhaps this situation will improve with time.

From an algorithmic point of view, the problem of searching OCR data for keywords is the dual problem of spell checking - in the case of spell checking you assume the dictionary is correct, and compare a possibly incorrect word against the dictionary. In the case of searching OCR data, you assume the errors are in the dictionary (unless these can be removed by reference to a dictionary appropriate to the context), and look for occurences of the (presumably correct) search words in your approximate data. A great deal of work has been done in this field in the last few years, but we decided to adopt a simple approach for the applet. The method used by the applet is simply to check each string that is an edit distance of at most one from the target string, and see whether it appears in the text. For this purpose we use a hash table to locate all references to a given string. Note that if this method would not scale well to allow an edit distance of two, since the complexity of the algorithm is exponential in the maximal edit distance d.

In addition, we encountered further questions concerning quality control:

- How can corrupted or irregularly cropped pages be detected sytematically without having to go through all 14692 images by hand?
- How can completeness be ensured?
- How can be ensured that no contribution and no author were missed for the automatically produced Table of Contents and the Author Index?

We are satisfied that our process properly addressed the third point, but the first two remain a concern. When working with the CDROM you will certainly find errors, rough patches, and deficiencies. We invite you to tell us about them and send us suggestions for improvements. Any further information that we can provide to enhance the usability of this CD will be placed at the IACR web site (`http://www.iacr.org/cd/`).

The process of creating this work has been a collaboration between several people. We would like to particularly thank Andy Clark, Alfred Hofmann, Thomas Berson, Whitfield Diffie, Joan Feigenbaum, Bart Preneel, Tom Griffin, Jason Zien, Sridhar Rajagopalan, and our student workers. Although a curious series of accidents during this project delayed the publication, we are quite satisfied that the result will be of use to the research community.

Claus Dieter Ziegler
Kevin S. McCurley
September 1998