Lecture Notes in Computer Science 1561

Edited by G. Goos, J. Hartmanis and J. van Leeuwen

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

Ivan Damgård (Ed.)

# Lectures on Data Security

## Modern Cryptology in Theory and Practice

Springer

Series Editors

Gerhard Goos, Karlsruhe University, Germany
Juris Hartmanis, Cornell University, NY, USA
Jan van Leeuwen, Utrecht University, The Netherlands

Volume Editor

Ivan Bjerre Damgård
BRICS, University of Aarhus
Ny Munkegade, Building 540
DK-8000 Aarhus C, Denmark
E-mail: ivan@daimi.aau.dk

Cataloging-in-Publication data applied for

Die Deutsche Bibliothek - CIP-Einheitsaufnahme

**Lectures on data security** : modern cryptology in theory and practice / Ivan Damgård (ed.). - Berlin ; Heidelberg ; New York ; Barcelona ; Hong Kong ; London ; Milan ; Paris ; Singapore ; Tokyo : Springer, 1999
(Lecture notes in computer science ; 1561)
ISBN 3-540-65757-6

Cover illustration taken from the contribution by Stefan Wolf, pages 217 ff

CR Subject Classification (1998): E.3, G.2.1, D.4.6, K.6.5, F.2.1-2, C.2, J.1

ISSN 0302-9743
ISBN 3-540-65757-6 Springer-Verlag Berlin Heidelberg New York



Typesetting: Camera-ready by author
SPIN 10702913 06/3142 — 5 4 3 2 1 0 Printed on acid-free paper

# Preface

In July 1998, a summer school in cryptology and data security was organized at the computer science department of Aarhus University, Denmark. This took place as a part of a series of summer schools organized by the European Educational Forum, an organization consisting of the research centers TUCS (Finland), IPA (Holland) and BRICS (Denmark, Aarhus). The local organizing committee consisted of Jan Camenisch, Janne Christensen, Ivan Damgaård (chair), Karen Møller, and Louis Salvail. The summer school was supported by the European Union.

Modern cryptology is an extremely fast growing field and is of fundamental importance in very diverse areas, from theoretical complexity theory to practical electronic commerce on the Internet. We therefore set out to organize a school that would enable young researchers and students to obtain an overview of some main areas, covering both theoretical and practical topics. It is fair to say that the school was a success, both in terms of attendance (136 participants from over 20 countries) and in terms of contents. It is a pleasure to thank all of the speakers for their cooperation and the high quality of their presentations.

A total of 13 speakers gave talks: Mihir Bellare, University of California, San Diego; Gilles Brassard, University of Montreal; David Chaum, DigiCash; Ronald Cramer, ETH Zürich; Ivan Damgård, BRICS; Burt Kaliski, RSA Inc.; Lars Knudsen, Bergen University; Peter Landrock, Cryptomathic; Kevin McCurley, IBM Research, Almaden; Torben Pedersen, Cryptomathic; Bart Preneel, Leuven University; Louis Salvail, BRICS; Stefan Wolf, ETH Zürich.

It was natural to take the opportunity kindly offered by Springer-Verlag to publish a set of papers reflecting the contents of the school. Although not all speakers were able to contribute, due to lack of time and resources, this volume does cover all the main areas that were presented. The intention of all papers found here is to serve an educational purpose: elementary introductions are given to a number of subjects, some examples are given of the problems encountered, as well as solutions, open problems, and references for further reading. Thus, in general we have tried to give an up-to-date overview of the subjects we cover, with an emphasis on insight, rather than on full-detail technical presentations. Several results, however, are in fact presented with full proofs. The papers have not been refereed as for a journal.

I would like to thank all of the authors for their contributions and the hard work and time they have invested.

Ivan Damgård