

# Lecture Notes in Computer Science

1334

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

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

Yongfei Han Tatsuaki Okamoto  
Sihan Qing (Eds.)

# Information and Communications Security

First International Conference, ICIS '97  
Beijing, China, November 11-14, 1997  
Proceedings



Springer

## Series Editors

Gerhard Goos, Karlsruhe University, Germany

Juris Hartmanis, Cornell University, NY, USA

Jan van Leeuwen, Utrecht University, The Netherlands

## Volume Editors

Yongfei Han, Program Co-Chair

Gemplus Technologies Asia PTE LTD

89, Science Park Drive #04-01/05

The Rutherford, Singapore Science Park, Singapore 118261

E-mail: YongFei.HAN@ccmail.edt.fr

Tatsuaki Okamoto, Program Co-Chair

NTT Labs, Room 609A

1-1 Hikarinooka, Yokosuka-shi, 239 Japan

E-mail: okamoto@sucaba.isl.ntt.co.jp

Sihan Qing, Director

Engineering Research Center for Information Security Technology

Chinese Academy of Sciences

Beijing 100080, P.R. China

E-mail: qsh@sun.ihep.ac.cn

Cataloging-in-Publication data applied for

## **Die Deutsche Bibliothek - CIP-Einheitsaufnahme**

**Information and communications security : first international conference ; proceedings / ICICS '97, Beijing, China, November 11 - 13, 1997. Yongfei Han ... (ed.). - Berlin ; Heidelberg ; New York ; Barcelona ; Budapest ; Hong Kong ; London ; Milan ; Paris ; Santa Clara ; Singapore ; Tokyo : Springer, 1997**

(Lecture notes in computer science ; Vol. 1334)

ISBN 3-540-63696-X

CR Subject Classification (1991): E.3-4, G.2.1, D.4.6, F.2.1-2, C.2, J.1, K.6.5

ISSN 0302-9743

ISBN 3-540-63696-X Springer-Verlag Berlin Heidelberg New York

This work is subject to copyright. All rights are reserved, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, re-use of illustrations, recitation, broadcasting, reproduction on microfilms or in any other way, and storage in data banks. Duplication of this publication or parts thereof is permitted only under the provisions of the German Copyright Law of September 9, 1965, in its current version, and permission for use must always be obtained from Springer-Verlag. Violations are liable for prosecution under the German Copyright Law.

© Springer-Verlag Berlin Heidelberg 1997

Printed in Germany

Typesetting: Camera-ready by author

SPIN 10647862 06/3142 - 5 4 3 2 1 0 Printed on acid-free paper

## Preface

The International Conference on Information and Communications Security (ICICS) represents international research and development in the area of information and communications security. The conference is held every two years (during years when Asiacrypt is not held) in different Asian countries, and it attracts an audience from the academic, commercial, and industrial communities. ICICS '97 is held in the Chinese Academy of Sciences in Beijing, P. R. China, November 11-14 1997.

ICICS '97 was sponsored by the Chinese Academy of Sciences, the National Natural Science Foundation of China, and the China Computer Federation.

The conference was organized by the Engineering Research Center for Information Security Technology in the Chinese Academy of Sciences in co-operation with the International Association for Cryptologic Research (IACR), IEICE, and the Asiacrypt Steering Committee.

There were 87 papers submitted for inclusion, from an international authorship, 37 papers among them have been accepted as regular papers, and 11 as short papers. We would like to thank the authors of all papers submitted, both those whose work is included in these proceedings, and those whose work could not be accommodated. Without their research and writing up there would be no conference.

The number of submitted papers put an additional strain on the program committee members. We are grateful to them all for their work in reviewing the papers in a short time and for freely giving us the benefit of their experience and support in a variety of ways. We also would like to thank all the other reviewers for their reviewing the papers.

We wish to thank all the participants, organizers, and contributors of the ICICS '97 conference.

August, 1997

*Yongfei Han  
Tatsuaki Okamoto  
Sihan Qing*

# ICICS Steering Committee and ICICS '97 Program Committee

## 1 STEERING COMMITTEE

Chin-Chen Chang  
James W. Gray, III  
Yongfei Han  
Kwangjo Kim  
Tatsuaki Okamoto  
Sihan Qing  
Vijay Varadharajan

## 2 PROGRAM COMMITTEE

### Co-Chairs

Yongfei Han (GemPlus)  
Tatsuaki Okamoto (NTT, Japan)  
Sihan Qing (ERCIST, China)

### Member

Elisa Bertino (University of Milano, Italy)  
Chin-Chen Chang (NCCU, Taiwan)  
Robert Deng (NUS, Singapore)  
Dieter Gollmann (University of London, UK)  
James W. Gray, III (UST, Hong Kong)  
Erland Jonsson (Chalmers University of Technology, Sweden)  
Kwangjo Kim (ETRI, S. Korea)  
Wenbo Mao (HP, UK)  
Tsutomu Matsumoto (Yokohama National University, Japan)  
Mitsuru Matsui (Mitsubishi, Japan)  
Ueli Maurer (ETH, Switzerland)  
Catherline Meadows (Naval Research Lab. USA)  
Kazuo Ohta (NTT, Japan)  
Eiji Okamoto (JAIST, Japan)  
Jean-Jacques Quisquater (UCL, Belgium)  
Phil Rogaway (UC Davis, USA)  
Ravi Sandhu (George Mason University, USA)  
Yiqun Lisa Yin (RSA, USA)  
Moti Yung (CertCo, USA)  
Vijay Varadharajan (Western Sydney University, Australia)

### General Chair and Organizing Chair

**General Chair:** Sihan Qing  
**Organizing Chair:** Xizhen Ni

# CONTENTS

## Session 1: Theoretical Foundations of Security

*Minimizing the use of random oracles in authenticated encryption schemes* ..... 1

Mihir Bellare and Phillip Rogaway

*Zero-knowledge proofs of decision power: new protocols and optimal round-complexity* ..... 17

Giovanni Di Crescenzo, Kouichi Sakurai and Moti Yung

*Computational learning theoretic cryptanalysis of language theoretic cryptosystems* .... 28

Takeshi Koshihara

*A language for specifying sequences of authorization transformations and its applications* ..... 39

Yun Bai and Vijay Varadharajan

## Session 2: Secret Sharing

*On the decomposition constructions for perfect secret sharing schemes* ..... 50

Hung-Min Sun and Bor-Liang Chen

*Traceable visual cryptography* ..... 61

Ingrid Biehl and Susanne Wetzel

*Remarks on the multiple assignment secret sharing scheme* ..... 72

Hossein Ghodosi, Josef Pieprzyk and Rei Safavi-Naini

*Secret sharing in hierarchical groups* ..... 81

Chris Charnes, Keith Martin, Josef Pieprzyk and Rei Safavi-Naini

## Session 3: Network Security

*Stateless connections* ..... 87

Tuomas Aura and Pekka Nikander

*Design of a security platform for CORBA based application* ..... 98

Rakman Choi, Jungchan Na, Kwonil Lee, Eunmi Kim and Wooyong Han

*Secure document management and distribution in an open network environment* ..... 109

Antonio Lioy, Fabio Maino and Marco Mezzalama

## Session 4: Authentication and Identification

*A<sup>2</sup> - code = Affine resolvable + BIBD* ..... 118

Satoshi Obana and Kaoru Kurosawa

<i>Multisender authentication systems with unconditional security</i> .....	130
K. M. Martin and Rei Safavi-Naini	

<i>Proposal of user identification scheme using mouse</i> .....	144
Kenichi Hayashi, Eiji Okamoto and Masahiro Mambo	

## **Session 5: Boolean Functions and Stream Ciphers**

<i>An effective genetic algorithm for finding highly nonlinear Boolean Functions</i> .....	149
William Millan, Andrew Clark and Ed Dawson	

<i>Duality of Boolean functions and its cryptographic significance</i> .....	159
Xiao-Mo Zhang, Yuliang Zheng and Hideki Imai	

<i>Construction of correlation immune Boolean functions</i> .....	170
Ed Dawson and Chuan-Kun Wu	

<i>An improved key stream generator based on the programmable cellular automata</i> .....	181
Miodrag J. Mihaljević	

## **Session 6: Security Evaluation**

<i>A Trust policy framework</i> .....	192
Audun Jøsang	

<i>Critical analysis of security in voice hiding techniques</i> .....	203
Liwu Chang and Ira S. Moskowitz	

## **Session 7: Signatures**

<i>Two efficient RSA multisignature schemes</i> .....	217
Sangjoon Park, Sangwoo Park, Kwangjo Kim and Dongho Won	

<i>Proxy signatures, Revisited</i> .....	223
Seungjoo Kim, Sangjoon Park and Dongho Won	

## **Session 8: Block Ciphers**

<i>Related-key cryptanalysis of 3-WAY, Biham-DES, CAST, DES-X NewDES, RC2, and TEA</i> .....	233
John Kelsey, Bruce Schneier and David Wagner	

<i>A multiplication-addition structure against differential attack</i> .....	247
Feng Zhu and Bao-An Guo	

<i>On strict estimation method of provable security against differential</i> .....	258
Yasuyoshi Kaneko, Shiho Moriai and Kazuo Ohta	

<i>Improved fast software implementation of block ciphers</i> .....	269
Takeshi Shimoyama, Seiichi Amada and Shiho Moriai	

<i>Security comments on the Hwang-Chen algebraic-code cryptosystem</i> .....	274
Mohssen M. Alabbadi	

## **Session 9: Public Key Systems I**

<i>Efficient elliptic curve exponentiation</i> .....	282
Atsuko Miyaji, Takatoshi Ono and Henri Cohen	

<i>Efficient construction of secure hyperelliptic discrete logarithm problems</i> .....	292
Jinhui Chao, Nori Matsuda and Shigeo Tsujii	

## **Session 10: Cryptanalysis of Public Key Systems**

<i>A new and optimal chosen-message attack on RSA-type cryptosystems</i> .....	302
Daniel Bleichenbach, Marc Joye and Jean-Jacques Quisquater	

<i>On weak RSA-keys produced from Pretty Good Privacy</i> .....	314
Yasuyuki Sakai, Kouichi Sakurai and Iirokazu Ishizuka	

## **Session 11: Subliminal Channels**

<i>Self-synchronized message randomization methods for subliminal channels</i> .....	325
Kazukuni Kobara and Hideki Imai	

<i>Hiding the Hidden: A software system for concealing ciphertext as innocuous text</i> .....	335
Mark Chapman and George Davida	

## **Session 12: Public Key Systems II**

<i>Digital signature and public key cryptosystem in a prime order subgroup of <math>Z_n^*</math></i> .....	346
Colin Boyd	

<i>Trapdoor one-way permutations and multivariate polynomials</i> .....	356
Jacques Patarin and Louis Goubin	

<i>Asymmetric cryptography with S-Boxes</i> .....	369
Jacques Patarin and Louis Goubin	

<i>On the powerline system</i> .....	381
Paul Camion and Hervé Chabanne	



### Session 13: Key Recovery/ Fair Cryptosystem

<i>Making unfair a "fair" blind signature scheme .....</i>	386
Jacques Traoré	
<i>Enforcing traceability in software .....</i>	398
Colin Boyd	
<i>Publicly verifiable partial key escrow .....</i>	409
Wenbo Mao	

### Session 14: Intellectual Property Protection

<i>A secure code for recipient watermarking against conspiracy attacks by all users .....</i>	414
Hajime Watanabe and Tadao Kasami	

### Session 15: Protocols

<i>Protocols for issuing public-key certificates over the Internet .....</i>	424
James W. Gray, III and Kin Fai Epsilon IP	
<i>Distributed cryptographic function application protocols .....</i>	435
André Postma, Thijs Krol and Egbert Molenkamp	
<i>Fault tolerant anonymous channel .....</i>	440
Wakaha Ogata, Kaoru Kurosawa, Kazue Sako and Kazunori Takatani	
<i>An implementable scheme for secure delegation of computing and data .....</i>	445
Josep Domingo - Ferrer and Ricardo X. Sanchez del Castillo	

### Session 16: Electronic Commerce

<i>Electronic commerce with secure intelligent trade agent .....</i>	452
Jaco van der Merwe and S. H. von Solms	
<i>Efficient scalable fair cash with off-line extortion prevention .....</i>	463
Holger Peterson and Guillaume Poupard	
<i>An anonymous and undeniable payment scheme .....</i>	478
Liqun Chen and Chris J. Mitchell	
<i>Author Index .....</i>	483